Siber Güvenlik ve Savunma
Cyber Security and Defence

5. Uluslararası Bilgi Güvenliği ve Kriptoloji Konferansı

5th International Conference on Information Security & Cryptology

17-18 Mayıs
May 2012

ODTÜ Kültür ve Kongre Merkezi
METU Culture and Congress Center
Ankara-TURKEY

Bildiriler Kitabı
Proceedings

www.**iscturkey**.org

Düzenleyenler / Conveners

T.C. ULAŞTIRMA DENİZCİLİK VE HABERLEŞME BAKANLIĞI

BİLGİ GÜVENLİĞİ DERNEĞİ

Destekleyenler / In Collaboration with

BTK BİLGİ TEKNOLOJİLERİ VE İLETİŞİM KURUMU

ODTÜ

editörler / editors
Prof. Dr. Mustafa ALKAN
Prof. Dr. Şeref SAĞIROĞLU
Prof. Dr. Ersan AKYILDIZ

BİLGİ GÜVENLİĞİ VE KRİPTOLOJİ KONFERANSI

ISC Turkey

Bildiriler Kitabı
Proceedings

www.**iscturkey**.org

ISBN 978-9944-0189-2-0

Bildiriler Kitabı İsteme Adresi

Bilgi Güvenliği Derneği
E-mail: www.bilgiguvenligi.org.tr

Bu kitapta yer alan bildiri tam metinleri konferansın konu başlıklarına uygun olarak yazarlar tarafından hazırlanmıştır. Bildiriler yazarların kendi fikirlerini yansıtır ve herhangi bir değişiklik yapılmadan aynı şekilde basılmıştır. Bu kitaptaki yazarların görüşlerinden Bilgi Güvenliği Derneği, ISC Turkey Bilimsel Program Komitesi veya ISC Turkey Konferans Ofisi sorumlu değildir.

The papers in this book compromise the proceedings of the meeting mentioned on the cover title page. They reflect the author's opinions and, in the interests of timely dissemination, are puplished as presented and without change. Their inclusion in this puplication does not necessarily constitute endorsement by information Security Association the scientific programme committe and ISC Turkey Conference Office.

Bu kitabın her hangi bir kısmı veya tamamı Bilgi Güvenliği Derneği'nin önceden yazılı ve onaylı izni alınmadan her hangi bir formda veya elektronik, mekanik, fotokopi kayıt veya diğer bir yöntemle tekrar çoğaltılamaz, herhangi bir alanda saklanamaz, transfer edilemez. Tüm hakları Bilgi Güvenliği Derneği'ne aittir. Bütün hakları saklıdır.

No part of this book may be printed, reproduced or distributed in any elevtronic, mechanical or other means (including photocoping, recording or information storage and retrieval) without permission in writing from Information Security Association of Turkey excep in the case of brief quotations embodied in critical articles and reviews, and also except for reading and browsing via the World Wide Web.
All rihgts are reserved.

Düzenleyenler / Conveners

Destekleyenler / In Collaboration with



Siber Güvenlik ve Savunma

Cyber Security and Defence

5. Uluslararası

Bilgi Güvenliği ve Kriptoloji

Konferansı

5th International Conference on Information Security & Cryptology

17-18 Mayıs May2012

ODTÜ Kültür ve Kongre Merkezi

METU Culture and Congress Center

Ankara-TURKEY

Bildiriler Kitabı

www.iscturkey.org Proceedings



Bildiriler Kitabı
Proceedings

www.**iscturkey**.org

ÖNSÖZ / PREFACE

Uluslararası Bilgi Güvenliği ve Kriptoloji Konferansı (ISCTURKEY'12), Bilgi Güvenliği Derneği, Gazi Üniversitesi, Orta Doğu Teknik Üniversitesi ve Bilgi Teknolojileri ve İletişim Kurumu işbirliği ile Ulaştırma, Denizcilik ve Haberleşme Bakanlığı himayelerinde düzenlenmektedir. Bu sene beşincisi yapılan bu etkinlik 17-18 Mayıs 2012 tarihleri arasında Ankara'da ODTÜ Kongre ve Kültür Merkezinde yapılmıştır.

Uluslararası Bilgi Güvenliği ve Kriptoloji Konferansı düzenlendiği ilk yıldan beri Türkiye'nin bu alanlardaki bilimsel ve sektörel çalışmaların paylaşıldığı, üniversite-kamu-endüstri işbirliğinin geliştirildiği, kamunun bilgilendirildiği, eğitildiği, ulusal ve uluslararası tüm bilim insanları, araştırmacılar ve sektörel uygulayıcılar arasında bilgi alışverişinin sağlandığı, ülkemizdeki bu alandaki en önemli etkinliktir. Her ülke için önemli olan bilgi güvenliği ve kriptoloji kavramlarının, toplumun bireyleri tarafından özümsenmesine yardımcı olmak, ülkemizde bu alanda bilimsel bilgi birikiminin arttırılmasına katkılar sağlamak, kurumlar ve sektör arasındaki işbirliğini arttırmak ve en önemlisi bunu uluslararası boyutta yaparak katılımcıların kazanım ve katkıları arttırmak ve sunulan tüm materyalleri ücretsiz paylaşmak bu konferansın temel hedefleri arasındadır.

Uluslararası Bilgi Güvenliği ve Kriptoloji Konferansı'nın hedefleri doğrultusunda, bu seneki ana tema "Siber Güvenlik ve Savunma" olarak belirlenmiştir. Bilgi ve teknoloji çağı olarak adlandırılan günümüzde, kamu ve özel sektör kurum ve kuruluşlarının bilgi varlıkları her geçen gün daha fazla elektronik ortamlarda yer almaya başlamıştır. Bu verilerin korunması ise her yarım saniyede yeni bir casus yazılımın geliştirildiği ve hemen hemen her saatte yeni bir siber saldırının bulunduğu günümüzde her zamankinden daha önemli hale gelmiştir. Bu bağlamda, ülkelerin askeri, ekonomik, teknolojik ve kritik altyapılarına karşı son zamanlarda büyük artış gösteren siber saldırılara karşı koyabilecek ve/veya engel olabilecek çözüm önerileri diğer konularla beraber özellikle konferans çerçevesinde konunun uzmanları tarafından değerlendirilmiştir.

Konferansın bildiriler kitabında yayınlanması için akademisyenler ve uygulayıcılar tarafından eşbaşkanlara iletilen bildiriler, alanında uzman en az iki hakem tarafından değerlendirilmiştir. Hakem değerlendirilmesi sonucunda uygun bulunan bildiriler sözlü veya poster sunumu için seçilerek bildiriler kitabında basılmıştır. Toplam 87 bildiri başvurusundan 47 adedi oral (sözlü) sunum ve 11 adedi ise poster sunumu için kabul edilmiştir. Sözlü sunum için seçilen bildiriler konferansta altı ayrı salonda, Poster sunumları ise katılımcıların görebileceği bir salonda poster olarak yazarlar tarafından sunulmuştur. Kabul edilen bildiriler ve posterler, siber güvenlik ve savunma stratejileri, steganografi, kriptografi, kriptoanaliz, protokol güvenliği, bilgi güvenliğini sağlama yöntemleri, saldırı tespit yöntemleri, IPv6 güvenliği, RFID, kablosuz ağlar, saldırı tespit sistemleri, bulut bilişim, kayıtlı elektronik posta, kuantum ve kaotik şifreleme ile akıllı kartlarda kullanılan kriptografik protokoller ve bunların uygulamalarına yönelik çalışmaları kapsamaktadır.

Konferans süresince ana tema "Siber Güvenlik ve Savunma" konusu çerçevesinde sözlü sunumların yanında davetli konuşmalara ve çalıştaylara da yer verilmiştir. Rodica Tirtea (European Network and Information Security Agency) tarafından "Ulusal Bilgi Güvenliği ve Gizliliği" ve Nasir Memon (Polytechnic Institute of New York University ve Center for Interdisciplinary Studies in Security and Privacy) tarafından "Biyometrik Yöntemler ile Bilgi Güvenliği" ve Data Devastation şirketinden Joshua MARPET "Gaming the Digital Forensic System" başlıklarında konuşmalar yapmışlardır.

Oturum başkanlığını Prof. Dr. Şeref SAĞIROĞLU'nun yaptığı "Siber Güvenlik" paneli, yine oturum başkanlığını Sn. Prof. Dr. Fatoş Tünay Yarman VURAL'ın yaptığı "Adli Bilişimde Sayısal Sahtecilik", Sn. Doç. Dr. Sıddıka Berna Örs YALÇIN'ın yaptığı "Kriptografik Donanımlar ve Yan Kanal Analizleri", Bilgi Güvenliği Derneği YK Üyesi Sn. Ali YAZICI yaptığı "Siber Savunma" konularında çalıştaylar düzenlenmiştir. Ayrıca, "Ulusal Bilgi Güvenliğinde Log Yönetimi", "KEP Özelinde Kritik Altyapı Güvenliği ve Entegre Yönetim Sistemleri", "VOIP Güvenliği", "Sanallaştırma Veri Güvenliği", "SIP Güvenliği", "Siber Güvenlik Tehditlerine Karşı Farkındalık Geliştirme Eğitimi", "Ağlarda Yeni Güvenlik Tehditleri", "Cep Telefonlarında Veri Güvenliği" gibi konularda eğitimler verilmiştir.

Bu konferansta elde edilen tüm çıktılar (sunumlar, bildiriler kitabı, eğitim materyalleri, videolar) toparlanarak her konferans sonunda olduğu gibi ücretsiz olarak kamuoyu ile paylaşılmaktadır. Ayrıca, konferansın özeti ve çıkarılan derslerde Konferans Sonuç Bildirgesi olarak yayımlanmaktadır.

Bu konferansın gerçekleştirilmesinde emeği geçen başta Düzenleme Kurulu üyelerimiz olmak üzere, Danışma Kurulu üyelerine, davetli konuşmacılara, bildirilerini konferansta sunan yazarlara, görüşlerini panellerde ve oturumlarda paylaşan oturum başkanlarına, panelistlere, konuşmacılara, eğitmenlere, bildirileri değerlendiren hakemlerimize, sektör temsilcilerimize, kurullarda görev alan akademisyenler ile bilgi güvenliği uzmanlarına ve en önemlisi bu etkinliği maddi olarak destekleyen sponsorlarımıza teşekkür ederiz.

Son olarak bu etkinliğimizi destekleyen Onur Kurulu üyelerimize, TBMM Bilişim ve İnternet Araştırma Komisyonu Başkanı Prof. Dr. Necdet ÜNÜVAR ile bu etkinliğimizi ilk günden beri destekleyen ve himayelerine alan Ulaştırma, Denizcilik ve Haberleşme Bakanımız Sn. Binali YILDIRIM'a şükranlarımızı sunarız.

Saygılarımızla.

Prof. Dr. Mustafa ALKAN
Konferans Düzenleme Kurulu Eş Başkanı
Bilgi Güvenliği Derneği Başkanı

Prof. Dr. Şeref SAĞIROĞLU
Konferans Düzenleme Kurulu Eş Başkanı
Gazi Üniversitesi Mühendislik Fakültesi
Bilgisayar Mühendisliği Bölümü

Prof. Dr. Ersan AKYILDIZ
Konferans Düzenleme Kurulu Eş Başkanı
ODTÜ Fen Edebiyat Fakültesi Dekanı

Siber Güvenlik ve Savunma
Cyber Security and Defence

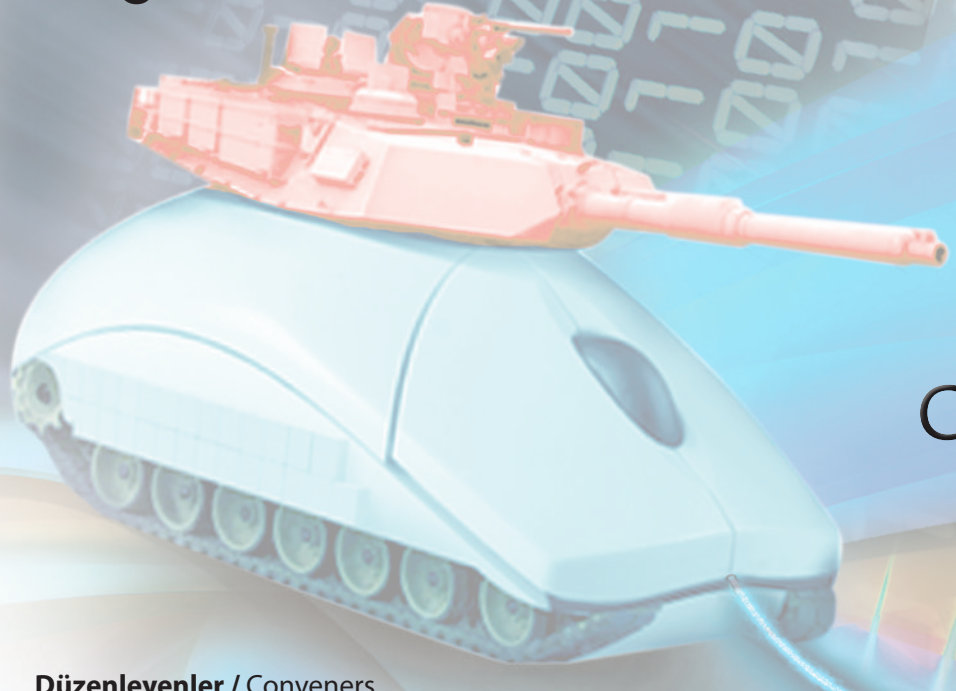
BİLGİ GÜVENLİĞİ VE KRİPTOLOJİ KONFERANSI
ISC Turkey

5. Uluslararası Bilgi Güvenliği ve Kriptoloji Konferansı

5th International Conference on Information Security & Cryptology

17-18 Mayıs May 2012

ODTÜ Kültür ve Kongre Merkezi
METU Culture and Congress Center
Ankara-TURKEY



Kurullar
Committees

Düzenleyenler / Conveners

T.C. ULAŞTIRMA DENİZCİLİK VE HABERLEŞME BAKANLIĞI

BİLGİ GÜVENLİĞİ DERNEĞİ

Destekleyenler / In Collaboration with

BTK BİLGİ TEKNOLOJİLERİ VE İLETİŞİM KURUMU

ODTÜ

ONUR KURULU

Dr. Tayfun ACARER	BTK Başkanı
Prof. Dr. Rıza AYHAN	Gazi Üniversitesi Rektörü
Prof. Dr. Ahmet ACAR	ODTÜ Rektörü

DÜZENLEME KURULU

Mustafa ALKAN,	Bilgi Güvenliği Derneği, Konferans Eş Başkanı
Şeref SAĞIROĞLU,	Gazi Üniversitesi, Konferans Eş Başkanı
Ersan AKYILDIZ,	Orta Doğu Teknik Üniversitesi, Konferans Eş Başkanı
Uraz YAVANOĞLU,	Gazi Üniversitesi
Alper ÖZBİLEN,	Gazi Üniversitesi
Eyüp Burak CEYHAN,	Gazi Üniversitesi
Cabir BİLİRGEN,	Ulaştırma Bakanlığı
Özgür ERALP,	Türkiye Barolar Birliği
Mustafa ÜNVER,	Bilgi Güvenliği Derneği
Demet KABASAKAL,	Bilgi Güvenliği Derneği
Tolga TÜFEKÇİ,	Bilgi Güvenliği Derneği
Cüneyt KAVİ,	Bilgi Güvenliği Derneği
Hakan YILDIRIM,	Bilgi Güvenliği Derneği
Mustafa MACAR,	Bilgi Güvenliği Derneği
Sedat AKLEYLEK,	Ondokuz Mayıs Üniversitesi
Oğuz YAYLA,	Orta Doğu Teknik Üniversitesi
Yıldız BARLAS,	Bilgi Güvenliği Derneği
Mehmet Ali İNCEEFE,	Bilgi Güvenliği Derneği
Ahmet Hamdi ATALAY,	NETAŞ
Ali YAZICI,	ASELSAN
Hakan TEKEDERE,	Gazi Üniversitesi

BİLİM KURULU

Eşref ADALI,	İstanbul Teknik Üniversitesi
Özgür AKAN,	Orta Doğu Teknik Üniversitesi
Mine AKKAN,	9 Eylül Üniversitesi
Sedat AKLEYLEK,	Ondokuz Mayıs Üniversitesi
Ersan AKYILDIZ,	Orta Doğu Teknik Üniversitesi
Aydın ALATAN,	Orta Doğu Teknik Üniversitesi
Mustafa ALKAN,	Gazi Üniversitesi
Ali Ziya ALKAR,	Hacettepe Üniversitesi
Taner ALTUNOK,	Çankaya Üniversitesi
Emin ANARIM,	Boğaziçi Üniversitesi
Veysel ASLANTAŞ,	Erciyes Üniversitesi
Murat AŞKAR,	Orta Doğu Teknik Üniversitesi
Volkan ATALAY,	Orta Doğu Teknik Üniversitesi
Hayrettin BAHŞİ,	TÜBİTAK UEKAE
Selçuk BAKTIR,	TÜBİTAK UEKAE
Ömer Faruk BAY,	Gazi Üniversitesi
Nazife BAYKAL,	Orta Doğu Teknik Üniversitesi
Cüneyt BAZLAMAÇCI,	Orta Doğu Teknik Üniversitesi
Ayşe BAŞAR BENER,	Boğaziçi Üniversitesi
Türksel Kaya BENSGHİR,	TODAİE
Leyla KESER BERBER,	Bilgi Üniversitesi
Erkan BEŞDOK,	Erciyes Üniversitesi
Zeki BİLGİN,	EGM
Kemal BIÇAKCI,	TOBB Ekonomi ve Teknoloji Üniversitesi
Serdar BOZTAŞ,	RMIT Üniversitesi
Ercan BULUŞ,	Namık Kemal Üniversitesi
Murat CENK,	University of Waterloo
John A. CLARK,	University of York
Mehmet Ufuk ÇAĞLAYAN,	Boğaziçi Üniversitesi
Emrah ÇAKÇAK,	Orta Doğu Teknik Üniversitesi
Cebrail ÇİFTLİKLİ,	Erciyes Üniversitesi

İlhami ÇOLAK,	Gazi Üniversitesi
Gökhan DALKILIÇ,	Dokuz Eylül Üniversitesi
Melissa DANFORD,	California State University
Hüseyin DEMİRCİ,	TÜBİTAK
Kıvanç DİNÇER,	TÜBİTAK
Emir DİRİK,	Uludağ Üniversitesi
Asuman DOĞAÇ,	ODTÜ
Ali DOĞANAKSOY,	Orta Doğu Teknik Üniversitesi
Erdoğan DOĞDU,	TOBB Ekonomi ve Teknoloji Üniv.
Ali Bülent EKİN,	Ankara Üniversitesi
Atilla ELÇİ,	Süleyman Demirel Üniversitesi
Ersin ELBAŞI,	TÜBİTAK
Serdar Süer ERDEM,	GYTE
Şaban EREN,	Maltepe Üniversitesi
Pooya FARSHIM,	Orta Doğu Teknik Üniversitesi
Debasis GIRI,	Haldia Institute of Technology
Yurdahan GÜLER,	ODTÜ
İsmail GÜLOĞLU,	Doğuş Üniversitesi
Haluk GÜMÜŞKAYA,	Gediz Üniversitesi
Murat HACIÖMEROĞLU,	Gazi Üniversitesi
Hüseyin HIŞIL,	Yaşar Üniversitesi
Yusuf İPEKOĞLU,	Orta Doğu Teknik Üniversitesi
Ahmet KAPLAN,	TÜBİTAK ULAKBİM
Derviş KARABOĞA,	Erciyes Üniversitesi
Orhun KARA,	TÜBİTAK-UEKAE
Enis KARAARSLAN,	Muğla Üniversitesi
Hacer KARACAN,	Gazi Üniversitesi
Selçuk KAVUT,	GYTE
Alisher KHOLMATOV,	Sabancı Üniversitesi
Engin KIRDA,	ISECLAB
Barış Bülent KIRLAR,	Süleyman Demirel Üniversitesi
Mehmet KİRAZ,	TÜBİTAK-UEKAE

Ahmet KOLTUKSUZ,	Yaşar Üniversitesi
Alptekin KÜPCÜ,	Koç Üniversitesi
Jin Wook LEE,	Samsung Advanced Instıtute of Technology
Albert LEVI,	Sabancı Üniversitesi
Subhamoy MAITRA,	Indian Statistical Institute
Akın MARSAP,	Aydın Üniversitesi
Tekin MEMİŞ,	Kadir Has Üniversitesi
Kıvanç MIHÇAK,	Boğaziçi Üniversitesi
Katerina MITROKOTSA,	Delft University of Technology
Jongsub MOON,	Korea University
Vasif NABİYEV,	Karadeniz Teknik Üniversitesi
Jorge NAKAHARA,	Universite' Libre de Bruxelles (ULB), Belgium
Eiji OKAMOTO,	University of Tsukuba
Mesut ORTA,	Adalet Bakanlığı
Hakan ÖKTEM,	Orta Doğu Teknik Üniversitesi
Bülent ÖRENCİK,	TÜBİTAK MAM
Sıddıka Berna ÖRS,	İstanbul Teknik Üniversitesi
Gökhan ÖZBİLGİN,	Sermaye Piyasası Kurulu
Ferruh ÖZBUDAK,	Orta Doğu Teknik Üniversitesi
Suat ÖZDEMİR,	Gazi Üniversitesi
Ali ÖZDOĞAN,	Polis Akademisi
Atilla ÖZGİT,	Orta Doğu Teknik Üniversitesi
Necla ÖZKAYA,	Erciyes Üniversitesi
Hüseyin POLAT,	Anadolu Üniversitesi
Shahram RAHIMI,	Southern Illinois Üniversitesi
Bimal ROY,	Indian Statistical Institute
Guangzhi QU,	Oakland Üniversitesi
Şeref SAĞIROĞLU,	Gazi Üniversitesi
Tolga SAKALLI,	Trakya Üniversitesi
Gökay SALDAMLI,	Boğaziçi Üniversitesi
A.Nurdan SARAN,	Çankaya Üniversitesi
Erkay SAVAŞ,	Sabancı Üniversitesi

Nur SAYGI,	Bilgi Teknolojileri ve İletişim Kurumu
Zülfükar SAYGI,	TOBB ETÜ
Yücel SAYGIN,	Sabancı Üniversitesi
Berry SCHOENMAKERS,	Eindhoven University of Technology
Ali Aydın SELÇUK,	Bilkent Üniversitesi
Hüsrev Taha SENCAR,	TOBB ETÜ
Cevat SENER,	Orta Doğu Teknik Üniversitesi
Hayri SEVER,	Hacettepe Üniversitesi
İbrahim SOĞUKPINAR,	Gebze Yüksek Teknoloji Enstitüsü
Coşkun SÖNMEZ,	Yıldız Teknik Üniversitesi
Berk SUNAR,	Worcester Polytechnic Institute
Serap ŞAHİN,	İYTE
Mehmet TEKEREK,	KSU Üniversitesi
Tuba TEMİZEL,	Orta Doğu Teknik Üniversitesi
Tuğkan TUĞLULAR,	İzmir Yüksek Teknoloji Enstitüsü
Tolga TÜFEKÇİ,	TURKTRUST
Umut ULUDAĞ,	TÜBİTAK UEKAE
İlkay ULUSOY,	Orta Doğu Teknik Üniversitesi
Osmanbey UZUNKOL,	Carl von Ossietzky Universitat Oldenburg
Muhammet ÜNAL,	Gazi Üniversitesi
Fatoş Yarman VURAL,	Orta Doğu Teknik Üniversitesi
Qinghan XIAO,	Defence Research and Development Canada
Berna ORS YALÇIN,	İstanbul Teknik Üniversitesi
Tolga YALÇIN,	RUHR Universitat Bochum
Tuğrul YANIK,	Fatih Üniversitesi
Berrin YANIKOĞLU,	Sabancı Üniversitesi
Atilla YARDIMCI,	TOBB
Oğuz YAYLA,	Orta Doğu Teknik Üniversitesi
Ali YAZICI,	Atılım Üniversitesi
Hamdi Murat YILDIRIM,	Bilkent Üniversitesi
Melek D. YÜCEL,	Orta Doğu Teknik Üniversitesi
Jianying ZHOU,	ASTAR Institute for Infocomm Research

Danışma Kurulu

Ali YAZICI, ASELSAN

Ahmet Hamdi ATALAY, NETAŞ

Ahmet KAPLAN, TÜBİTAK ULAKBİM

İhsan DURDU, Ulaştırma, Denizcilik ve Haberleşme Bakanlığı

Hayri SEVER, Hacettepe Üniversitesi

Zuhuri YAMAN, TTNET

Volkan ÖZTÜRK, RTÜK

Gürol CANBEK, HAVELSAN

Tolga KILIÇ, AVEA

Armağan ZALOĞLU, McAfee

Tolga TÜFEKÇİ, TÜRKTRUST

Aysun TUNCER, Bilgi Güvenliği Derneği

Leyla Keser BERBER, Bilgi Güvenliği Derneği

Gökhan ÖZBİLGİN, Bilgi Güvenliği Derneği

Ali OK, TÜRKSAT

Ahmet KAPLAN, TÜBİTAK, ULAKBİM

Ferhat YEŞİLLİ, BİH GROUP

Volkan KAPLAN, Gümrük ve Dış Ticaret

Orhan TURAN, Noterler Birliği

Tuncay ÇAKMAK, Gümrük ve Dış Ticaret

Adem TEKEREK, Gazi Üniversitesi

Fatih Ayhan HAKTANIR, ORATEK

Bilal ONAL, Bilgi Güvenliği Derneği

Selim ULKU, Bilgi Güvenliği Derneği

Hakan YILDIRIM, TBMM

Siber Güvenlik ve Savunma
Cyber Security and Defence

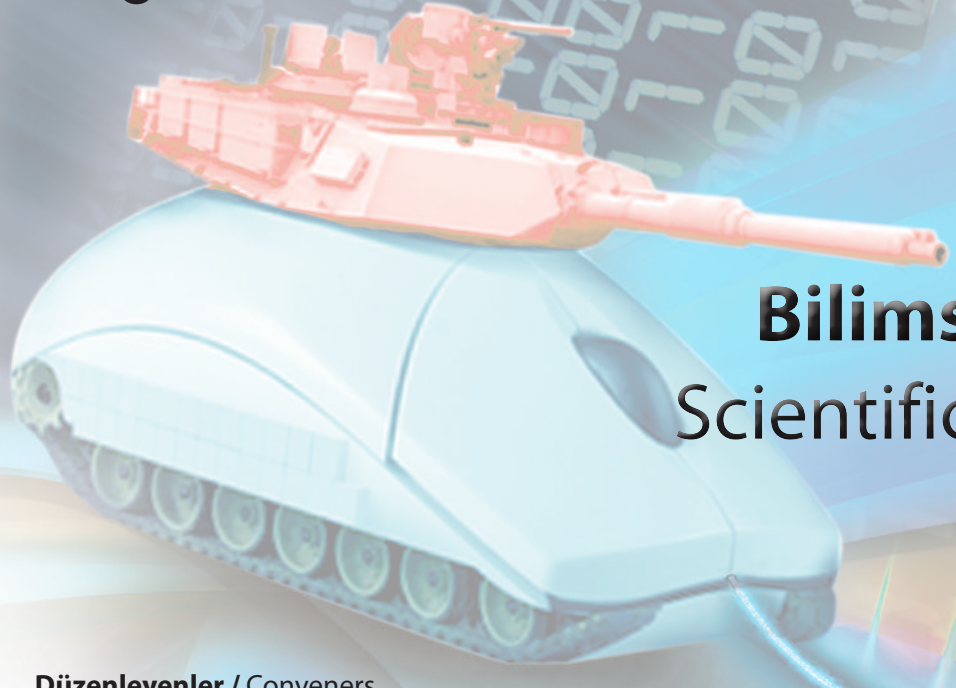
BİLGİ GÜVENLİĞİ VE KRİPTOLOJİ KONFERANSI
ISC Turkey

5. Uluslararası Bilgi Güvenliği ve Kriptoloji Konferansı

5th International Conference on Information Security & Cryptology

17-18 Mayıs
May 2012

ODTÜ Kültür ve Kongre Merkezi
METU Culture and Congress Center
Ankara-TURKEY



Bilimsel Program
Scientific Programme

Düzenleyenler / Conveners

T.C. ULAŞTIRMA DENİZCİLİK VE HABERLEŞME BAKANLIĞI

BİLGİ GÜVENLİĞİ DERNEĞİ

Destekleyenler / In Collaboration with

BTK BİLGİ TEKNOLOJİLERİ VE İLETİŞİM KURUMU

ODTÜ

ISCTURKEY 2012 PROGRAM

1. gün first day 17 MAYIS MAY 2012 PERŞEMBE THURSDAY

09:00 -10:00 — **KAYIT** REGISTRATION

09:45 -10:00 — **ÇAY-KAHVE ARASI** TEA/COFFEE BREAK

10:00 -10:45 — **AÇILIŞ VE PROTOKOL KONUŞMALARI** OPENING CEREMONY — ANA SALON/MAIN HALL - KEMAL KURDAŞ

Sn. Prof. Dr. Mustafa ALKAN
ISCTurkey Konferans Eşbaşkanı/Bilgi Güvenliği Derneği Başkanı *ISCTurkey Conference Chairman/Head of Information Security Association*

Sn. Dr. Tayfun ACARER
Bilgi Teknolojileri ve İletişim Kurumu Başkanı *President of Information Technologies and Communications*

Sn. Prof. Dr. Ahmet ACAR
ODTÜ Rektörü *Rector of METU*

Sn. Prof. Dr. Rıza AYHAN
Gazi Üniversitesi Rektörü *Rector of Gazi University*

Sn.Prof. Dr. Nejdet ÜNÜVAR
Türkiye Büyük Millet Meclisi (TBMM) Bilişim ve İnternet Komisyonu Başkanı *NGAT (National Grand Assembly of Turkey)*

Sn. Binali YILDIRIM
Denizcilik, Ulaştırma ve Haberleşme Bakanı *Minister of Transport, Maritime and Communications*

10:45 -11:00 — **ÇAY-KAHVE ARASI** TEA/COFFEE BREAK

11:00 -12:00 — **DAVETLİ KONUŞMACI** KEYNOTE SPEAKER — Oturum Başkanı Chairman **Prof. Dr. Ersan AKYILDIZ** METU, **Dr. Rodica TIRTEA** European Network and Information Security Agency - ENISA **Title:** European Perspective on National Information Security and Privacy

12:00 -13:00 — **ÖĞLE ARASI** LUNCH BREAK

13:00 -14:45 — **PANEL 1**

SİBER GÜVENLİK CYBER SECURITY
Oturum Başkanı Chairman
Prof. Dr. Şeref SAĞIROĞLU
Gazi University

Konuşmacılar Speakers

Prof. Dr. Nazife BAYKAL ODTÜ Enformatik Enstitüsü Müdürü / *Director of METU Informatics Institute*
Prof. Dr. Türksel BENGSHİR KAYA TODAEİ e-Devlet Merkezi Müdürü / *Director of e-Government Center*
Ömer TEKELİ EGM Bilişim Suçları Dairesi Başkanı / *Head of EGM Cyber Crime Department*
Bilge KARABACAK TÜBİTAK BİLGEM UEKAE Bilişim Sistemleri Güvenliği Bölümü Yöneticisi / *Director of Information System Security Department*
Ali YAZICI ASELSAN Kripto ve Bilgi Güvenliği Müdürü / *Director of Crypto and Information Security Department*
Temsilci, *Savunma Sanayi Müsteşarlığı*
Temsilci, *Ulaştırma, Denizcilik ve Haberleşme Bakanlığı*
Temsilci, *BTK*

14:45 -15:00 — **ÇAY-KAHVE ARASI** TEA/COFFEE BREAK

15:00 -15:45 — **DAVETLİ KONUŞMACI** KEYNOTE SPEAKER — Oturum Başkanı Chair **Prof.Dr. Fatoş Tünay Yarman VURAL** METU, **Prof. Dr. Nasır MEMON** Director of the Information Systems and Internet Security (ISIS) Laboratory **Title:** Biometric Rich Gestures: A Touching Farewell To Passwords?

15:45 -16:30 — **DAVETLİ KONUŞMACI** KEYNOTE SPEAKER — **Joshua MARPET** Data Devastation **Title:** Gaming the Digital Forensics System

16:30 -18:00 — **ÇALIŞTAY 1** WORKSHOP 1

BİLGİ GÜVENLİĞİ STK TOPLANTISI MEETING of INFORMATION SECURITY CSOs

Başkan Chairman
Prof. Dr. Mustafa ALKAN
BGD Başkanı
ISA President of Turkey

SALON HALL A

OTURUM SESSION 1: **AĞ GÜVENLİĞİ** NETWORK SECURITY
Oturum Başkanı Session Chairman:
Prof.Dr. Ali YAZICI, Atılım University

36 Ipv6 Ağlarda Solucan Dağılım Saldırıları ve Önlemler Uraz YAVANOĞLU* (Gazi Üniversitesi), Suat ÖZDEMIR (Gazi Üniversitesi), Şeref SAĞIROĞLU (Gazi Üniversitesi)

34 An Application Of Decision Trees In Intrusion Detection Atilla ÖZGÜR* (ISKUR), Hamit ERDEM (Başkent Üniversitesi)

52 A Two-Layer Fuzzy Genetic Algorithm for Designing Intrusion Detection System Ghazaleh JAVADZADEH* (Sharif University of Technolog),Reza AZMİ

39 Radius Regularization using Learning Automata for Spherical Intelligent Anomaly Detectors Neda AFZALI* (Alzahra University), Reza AZMI, Boshra PISHGOO

SALON HALL B

OTURUM SESSION 2: **SİBER GÜVENLİK** CYBER SECURITY
Oturum Başkanı Session Chairman:
Yrd.Doç.Dr./Assist.Prof.Dr. Murat KOYUNCU, Atılım University

43 Topic-Based Probabilistic Approach to Criminal Network for Suspect Investigation Arzu KAKIŞIM*, (Gebze Yüksek Teknoloji Enstitüsü) İbrahim SOGUKPINAR (Gebze Yüksek Teknoloji Enstitüsü)

67 Bilişim Suçlarında Delillendirme Çağlar ULKUDERNER* (Profelis Bilişim)

69 Siber Güvenlik Makro Analiz Modeli Önerisi ve Türkiye'nin Analizi Hakan ŞENTÜRK* (KHO Savunma Bilimleri Enstitüsü), Celal Zaim ÇİL (Çankaya Üniversitesi),Şeref SAĞIROĞLU (Gazi Üniversitesi)

76 Operating System Evaluation Using Choquet Integral in Terms of Cyber Threats Kerim GÖZTEPE* (War Colleges Command, Army War College), Ahmet EJDER (War Colleges Command)

87 Siber Güvenlik Persfektifinden Makineler Arası İletişim Uygulamalarının İncelenmesi Alper ÖZBİLEN (BTK-TİB), İlhami ÇOLAK (Gazi Üniversitesi), Şeref SAĞIROĞLU (Gazi Üniversitesi)

SALON HALL C

ÇALIŞTAY WORKSHOP 2: **YAN KANAL ANALİZİ ve GÖMÜLÜ SİSTEMLER**
SIDE ANALYSIS and EMBEDED SYSTEMS
Başkan Chair: **Doç. Dr. Sıddıka Berna Örs Yalçın**

Konuşmacılar Speakers

Elif Bilge Kavun
Lightweight Cryptography - What do we really mean by "Lightweight"?
Ahmet Arış
High Speed RSA Implementation
Dr. Amir Moradi
Implementation Attacks against Real-World Targets
David Oswald
Hands-on Side Channel Attacks against Smart Cards and Other Tokens
Dr. Tolga Yalçın
Use of Hardware as a Mathematical Cryptanalysis Tool

SALON HALL D

OTURUM SESSION 3: **BİLGİ GÜVENLİĞİ** INFORMATION SECURITY
Oturum Başkanı Session Chairman:
Y. Doç. Dr./ Asst. Prof. Dr. **Sedat AKLEYLEK Samsun 19 Mayıs Üni.**

48 Güvenli Q Sürü Bellek Yazılım Yongası Üreten Dilbilim Örneği Fevzi ÜNLÜ* (Ege ve Yaşar University)

49 Cycle Counting For Information Security in I@I Swarm Internet Generating Q Swarm Memory Fevzi ÜNLÜ* (Ege ve Yaşar University)

62 Metin ve Grafiksel Öğeleri Birleştiren Yeni bir Parola Tabanlı Kimlik Doğrulama Yöntemi Murat AKPULAT (Gümüşhane Üniversitesi), Kemal BICAKCI* (TOBB/ETÜ), Ugur CİL (TOBB/ETU)

75 Covert Channels Detection using Process Mining Amir Jalaly BIDGOLY* (University of Isfahan), Behrouz Tork LADANI (University Of Isfahan), Ahmad Baraani DASTJERDI (University of Isfahan)

83 Information and Computer Security Awareness of Elementary and High School Students: Sample of Kahramanmaraş City Mehmet TEKEREK* (KSU)

SALON HALL E

OTURUM SESSION 4: **KABLOSUZ AĞLARDA GÜVENLİK** SECURITY IN WIRELESS NETWORKS
Oturum Başkanı Session Chairman:
Doç. Dr. /Assoc. Prof. Dr. **Ali Aydın SELÇUK** Bilkent Üni.

5 On Applications of Privacy-Preserving Collaborative Filtering Schemes Alper BİLGE, Cihan KALELİ, İbrahim YAKUT, Hüseyin POLAT* (Anadolu Üniversitesi)

17 Kablosuz Algılayıcı Ağlarda Güvenli Ortam Erişim Protokolleri Feyza Yıldırım OKAY* (Gazi Üniversitesi), Suat OZDEMIR (Gazi Üniversitesi)

19 Anonymous RFID Authentication Protocol Without a Trusted Party Muhammed Ali BİNGÖL* (TUBITAK BILGEM UEKAE), Mehmet Sabir KİRAZ (TUBITAK BILGEM), Suleyman KARDAS (TUBITAK BILGEM UEKAE), Fatih BİRİNCİ(TUBITAK BILGEM)

72 Recommender System Based on Group Trust Somayeh NAGHSBANDI* (Isfahan University), Behrouz Tork LADANI (University of Isfahan)

SALON HALL F

16:30-18:00 **FİRMA SUNUMLARI**

16:30-18:00 **Ağlarda Yeni Güvenlik Tehtidleri, Akın TOSUNLAR,** VİGASİS

17:00-17:15 **Adli Bilişim ve Sayısal Sahtecilik (Elektronik Belgede Tarih Değiştirme) Özgür YURDUSEV,** VİGASİS

17:15-18:00 **Desktop Sanallaştırma ile Veri Güvenliği Sağlama, Levent TOPRAK** HUAWEI

13:00 -18:00

FUAYE / FOYER

POSTER ALANI
POSTER OTURUMU
POSTER SESSION
13:00-18:00
FUAYE FOYER

1 Ipv6 Security Vulnerabilities
Harith DAWOOD* (Cihan University)

15 Digital Watermarking Enhancement for Satellite Images Using a DCT Algorithm
Mustafa ABUGHARSA* (Misurata University), Mohamed SULLABI (Misurata University), Alhusain TAHER (Misurata University)

44 Enhancing SIEM Correlation Rules Through Baselining Ertuğrul AKBAŞ* (ANET)

33 Encrypted Individual Multiple Choice Questions Mehtap Kose ULUKOK* (Cyprus International University), Zehra Borataş ŞENSOY (Cyprus International University)

63 Şifrelemenin Modellenmesi ve Modern Kriptosistemin Tasarımı Erkan BAYAR* (Marmara Üni.), Hakan KAPTAN (Marmara Üni.)

71 Casus Yazılımların Bilgisayar Sistemlerine Bulaşma Belirtileri ve Çözüm Önerileri
Resul DAŞ* (Fırat Üniversitesi), Şahin KARA (Sakarya Üniversitesi)

18 Sazan Avlama (Phishing): Kullanılan Teknikler ve Bunlardan Korunma Yöntemleri
Ali ŞENOL* (Gazi Üniversitesi), Hacer KARACAN (Gazi Üniversitesi)

23 Server Based Encryption (SERBASEN)Protocol on Air Gap Network Ahmet AYŞAN* (Turkish Air Force Academy), Güray YILMAZ

37 Utilizing a Graphical User Interface for Image Encryption based on Chaotic Algorithm Hidayet OĞRAŞ* (Batman University), Mustafa TÜRK (Fırat University) Thanh Viet PHAM

41 Security Directions in Cloud Computing Environments
Zeynab Abbasi KHALİFELU (Islamic Azad University), Farhad Soleimanian GHAREHCHOPOGH* (Hacettepe University)

82 Akıllı Şebekelerde Siber Güvenlik ve Mahremiyet
Elif Üstündağ SOYKAN* (TÜBİTAK), Seda Demirağ ERSÖZ

ISCTURKEY 2012 PROGRAM
2. gün second day 18 MAYIS MAY 2012 CUMA FRIDAY

10:00 -12:00

SALON MAIN HALL: KEMAL KURDAŞ

10:00 -10:10 **ABOUT ISCISC'12** — Dr. Mohammad Taghi Alavi, Honorary chair of ISCISC'12 (9th International Conference on Information Security and Cryptology IRAN

10:10 -11:00 **EĞİTİM** — Ulusal Bilgi Güvenliğinde Log Yönetiminin Önemi Akın SAĞBİLGE, CRYPTECH

11:10 -12:00 **FİRMA SUNUMU** — Ağ Güvenliği ve Güvenlik Çözümleri HUAWEI

SALON HALL A

OTURUM SESSION 5:
KRİPTOGRAFİK PROTOKOLLER FOUNDATIONS OF CRYPTOGRAPHY **Oturum Başkanı**
Session Chairman: **Y. Doç. Dr./Asst. Prof. Dr. Zülfikar SAYGI, METU**

20 Elektronik Seçim: Norveç'in İnternet Üzerinden Oylama Sistemi ve Kriptografik Altyapısı,
Uğur BOYACİ* (TÜBİTAK BİLGEM), Fatih BİRİNCİ (TUBITAK BILGEM), Mehmet Sabir KİRAZ (TÜBİTAK BİLGEM)

66 Compressed Data Public Key Cryptosystems with DLP Over Extension Fields, Muhammad ASHRSF* (METU), Baris KIRLAR (Suleyman Demirel University)

42 Optimal Control Formulation of Query Model for Authentication Systems, Ali SEZER* (METU), Ferruh OZBUDAK (METU), Ustun YILDIRIM (METU)

73 On The Use Of Continued Fractions For Mutual Authentication, Amadou KANE* (Université Laval)

77 Formalization of Blind Signature Using the Inductive Method, Najmeh Sadat MIRAMIRKHANI* (Sharif University of Technolog) Rasool JALILI (Sharif University of Thechmilogy)

SALON HALL B

OTURUM SESSION 6:
KRİPTOANALİZ CRYPTANALYSIS
Oturum Başkanı Session Chairman:
Doç.Dr./Assoc. Prof. Dr. Ali DOĞANAKSOY, METU

21 Notes on Bent Functions in Polynomial Forms,
Nese OZTOP* (METU) Onur KOCAK (METU) Zulfukar SAYGI (TOBB ETU) Onur KURT (METU)

28 Security Margin of 5-Round DEAL, Orhun KARA* (TÜBİTAK BİLGEM UEKAE)

47 How Biased Are Linear Biases?,
Orhun KARA* (TÜBİTAK BİLGEM UEKAE) Adnan BAYSAL (TÜBİTAK BİLGEM UEKAE)

SALON HALL E

BİLGİ GÜVENLİĞİ INFORMATION SECURITY
Oturum Başkanı Session Chairman: **Yrd.Doç.Dr./Assist.Prof.Dr. Sinan KALKAN,** METU
10:00-10:30 **Siber Tehditlere karşı Bilgi Güvenliği Bilinci Oluşturma ve Eğitim Yöntemleri, Murat AYTUN,** HRIKA Genel Müdürü
10:30-11:00 **VoIP Güvenlik Uyumluluğu: VoIP'i Ağ Güvenlik Planlamasına Dâhil Etmek, Melih TAŞ,** NETAŞ
11:00-11:30 **SIP Saldırı Teknikleri ve Savunma Yöntemleri, Eren AKÇA, Gülten DOĞANÇ,** NETAŞ

SALON HALL C

SİBER GÜVENLİK ve SAVUNMA KOORDİNASYON KURULU TOPLANTISI
CYBER SECURITY and DEFENCE COORDINATION BOARD MEETING
Eş Başkanlar Chairs **Prof. Dr. Ersan AKYILDIZ, Prof.Dr. Şeref SAĞIROĞLU**

Not: Bu toplantı herkese açık değildir.
Sadece davetli kurul üyeleri katılabilecektir.
Note: Only the Board Members Can Attend This Meeting.

SALON HALL D

OTURUM SESSION 7:
KULLANIŞLI GÜVENLİK ve STEGANOGRAFİ USABLE SECURITY and STEGANOGRAPHY
Oturum Başkanı Session Chairman:
Prof. Dr. Ziya AKTAŞ, Başkent University

68 Frei-Chen Maskeleri Tabanlı Yeni Bir Sır Paylaşım Tekniği, Veysel ASLANTAS (Erciyes Üniversitesi), Ebubekir KAYA* (Nevşehir Üniversitesi)

27 Gizli Görüntü Paylaşımında Kullanılan Eşik Şemalarının Performans Değerlendirilmesi,
Guzin ULUTAS* (Karadeniz Teknik Üniversitesi), Mustafa ULUTAS (Karadeniz Teknik Üniversitesi), Vasif NABIYEV (Karadeniz Teknik Üniversitesi)

46 An Imperceptible Watermarking Scheme based on Double Density Dual-Tree Discrete Wavelet Transform in combination with Singular Value Decomposition,
Mary AGOYI* (Cyprus International University), Devrim SERAL (Cyprus International University)

SALON HALL F

UYGULAMALI SUNUMLAR

10:00-11:00 **Fiziksel Güvenlik Çözümleri ile Kamu Güvenliği Sağlama, Fatih ERİKÇİ, HUAWEI**
11:00-12:00 **Phone2DOS – SIP Üzerinden Yeni Bir Saldırı Yöntemi ve Öneriler, Barış DİNLER, VİGASİS**

12:00 -13:00 **ÖĞLE YEMEĞİ** LUNCH BREAK

13:00 -15:00 **EĞİTİM** — KEP Özelinde Kritik Altyapı Güvenliği ve Entegre Yönetim Sistemleri, **Aysun TUNCER,** BGD Üyesi / ARMONES — SALON MAIN HALL: **KEMAL KURDAŞ**

15:00 -15:20 **ÇAY-KAHVE ARASI** TEA/COFFEE BREAK

SALON HALL C

ÇALIŞTAY WORKSHOP

ELEKTRONİK NOTER ve SİBER GÜVENLİK UYGULAMALARI E-NOTARY and CYBER SECURITY APPLICATIONS

Başkan Chairman
Yıldız BARLAS, BGD Yönetim Kurulu Üyesi

Konuşmacılar Speakers

Prof. Dr. Şebnem AKİPEK, Ankara Üniversitesi Hukuk Fakültesi
Doç. Dr. Leyla KESER BERBER, Bilgi Üniversitesi
Cengiz TANRIKULU, Adalet Bakanlığı
Orhan TURAN, Ankara 56. Noteri
Pınar ÜNALÇIN, Durağan Noteri

SALON HALL E

BİLGİ GÜVENLİĞİ SEKTÖR TOPLANTISI MEETING of SECTOR REPRESENTATIVES
Başkan Chairman:
Prof. Dr. Mustafa ALKAN, BGD

SALON HALL F

BGD GENÇ ÜNİVERSİTE TEMSİLCİLERİ TOPLANTISI MEETING of ISA YOUTH UNIVERSITY REPRESENTATIVES
Başkan Chairman:
Ezgi CANKURTARAN

SALON HALL A

OTURUM SESSION 8: **KRİPTOGRAFİNİN TEMELLERİ** FOUNDATIONS OF CRYPTOGRAPHY **Oturum Başkanı**
Session Chairman: **Doç. Dr./Assoc. Prof. Dr. Melek Diker YÜCEL, METU**

25 Hermite Polynomial Representation for Finite Fields Of Characteristic Three
Canan ÖZEL* (METU) Sedat AKLEYLEK (19 Mayis University), Ferruh OZBUDAK (METU)

50 Alternate Models of Elliptic Curves: A Survey Baris KIRLAR* (Suleyman Demirel University), Muhammad ASHRSF (METU)

61 Optimal Frekans Atlamalı Diziler Seda KAHRAMAN* (TOBB ETÜ), Zulfukar SAYGI (TOBB ETÜ)

70 Cyclotomic Sayılar ve Sidel'nikov Dizileri Kamil OTAL* (TOBB ETU), Zulfukar SAYGI (TOBB ETÜ), Çetin ÜRTİŞ (TOBB ETÜ)

SALON HALL B

OTURUM SESSION 9: **KRİPTOANALİZ** FOUNDATIONS OF CRYPTOGRAPHY **Oturum Başkanı** Session Chairman: **Ferruh ÖZBUDAK, METU**

79 A Scalable Platform for Cryptanalysis of Computationally Intensive Algorithms
Hakan SOLMAZ* (Aselsan), Hasan ERDOĞAN (Aselsan), Rıza AYKAÇ (Aselsan)

81 A Proposed Attacking Method on Rabin's Cryptosystem
Sattar B SADKHAN * (University of Babylon)

24 Dinamik S-box Tabanlı Blok Şifrelerin Diferansiyel Kriptanalizi
Fatih ÖZKAYNAK* (Fırat University), Ahmet ÖZER (Fırat Üniversitesi), Sırma YAVUZ (Yıldız Teknik Üniversitesi)

26 Success Probability of The First Attack on Full Round GOST
Orhun KARA* (TÜBİTAK BİLGEM UEKAE), Ferhat KARAKOÇ (TÜBİTAK BİLGEM UEKAE)

SALON HALL D

OTURUM SESSION 10: **BİLGİ GÜVENLİĞİ** INFORMATION SECURITY **Oturum Başkanı** Session Chairman: **Dr.Orhun KARA** TÜBİTAK-BİLGEM

35 CAPTCHA Metinler için YSA Tabanlı Örüntü Tanıma Yaklaşımı
Uraz YAVANOGLU* (Gazi Üniversitesi) Begum MUTLU (Gazi Üniversitesi) Esra SAHİN (Gazi Üniversitesi)

56 Radyo Link ve Uydu Ağları Üzerinde Gelecek Nesil Dar Bant Terminal ile Yapılan Güvenli Haberleşme Test Sonuçları ve Değerlendirilmesi
Orkun DİLLİ* (Hv.Tek.Okl.K.Iığı) Nursel AKÇAM (Gazi Üniversitesi) Murat KOYUNCU (Atılım Üniversitesi)

86 Kayıtlı Elektronik Posta Sistemi ve E-Posta Güvenliği
Mustafa ALKAN* (Gazi Üniversitesi), Mustafa ÜNVER (BTK), Hakan TEKEDERE (Gazi Üniversitesi)

ÇALIŞTAY WORKSHOP 3

Ana Salon Main Hall **KEMAL KURDAŞ**

SİBER SAVUNMA CYBER DEFENSE

Başkan Chairman
Ali YAZICI
BGD YK Üyesi
ASELSAN Kripto ve Bilgi Güvenliği Müdürü

Konuşmacılar Speakers

Ali IŞIKLI, ASELSAN
Bülent SOYDAL, HAVELSAN
Bülent BÜYÜKKAHRAMAN, NETAŞ
Dr. Atilla ÖZGİT, ODTÜ
Aysun TUNCER, BGD YK Üyesi
Dr. Sedat AKLEYLEK, Ondokuz Mayıs Üniversitesi
Ahmet KAPLAN, BGD Üyesi/ULAKBİM
Hakan YILDIRIM, BGD Üyesi/TBMM
Volkan ÖZTÜRK, BGD Üyesi/RTÜK,
Volkan KAPLAN, BGD Üyesi / Gümrük Müsteşarlığı Bilgi İşlem Dairesi Başkanı
S.Barış DİNLER, VIGASİS
Dr. Kerim GÖZTEPE, Harp Akademileri Komutanlığı
Dr. Gökhan ÖZBİLGİN, SPK
Burak ÇİFTER, BGD İstanbul Temsilci Yrd.
M. Ali İNCEEFE, BGD YK Üyesi

SALON HALL A

ÇALIŞTAY WORKSHOP

ADLİ BİLİŞİM VE SAYISAL SAHTECİLİK DIGITAL FORENSICS and FRAUD

Başkan Chairman:
Prof. Dr. F. Tünay Yarman VURAL, ODTÜ

Konuşmacılar Speakers

Emrehan HALICI, Milletvekili, ***Adli Bilişim için Kurumsal Gelişim***
Prof. Dr. Ufuk ÇAĞLAYAN, Boğaziçi Üniversitesi, ***Elektronik Delil Ne Demektir ve Klasik Delilden Farkı Nedir?***
Osman Nihat ŞEN, TİB Internet Daire Başkanı, **Hukukçuların ve Adli Bilişim Uzmanlarının Eğitimi**
Mehmet ORAL, İstanbul Barosu Avukatı, **Türk Adalet Sisteminde Elektronik Delil Kullanımı ve Karşılaşılan Sorunlar**
Prof. Dr. Vahit BIÇAK, Polis Akademisi, **Türkiye'de ve Dünyadaki Elektronik Delil Yasalarının Karşılaştırılması**

SALON HALL B

OTURUM SESSION 11: **KRİPTOGRAFİK DONANIMLAR ve KUANTUM KRİPTOGRAFİ** CRYPTOGRAPHIC HARDWARE and QUANTUM CRYPTOGRAPHY **Oturum Başkanı** Session Chairman: Dr. Tolga YALÇIN

30 Kuantum Anahtar Dağıtımında (KAD) Gizli Anahtar Uzlaştırma: CASCADE Protokolü ve LDPC Kodları Mustafa TOYRAN* (TÜBİTAK), Burcu KORKMAZ (Ege Üniversitesi), Thomas PEDERSEN (TÜBİTAK), A. S. Atilla HASEKİOĞLU (TÜBİTAK), Pars MUTAF (Ege Üniversitesi), M. Ali CAN (TÜBİTAK)

45 A True Random Number Generator and Test Platform Built in FPGA
Salih YILDIRIM* (ASELSAN), Cuneyt BAZLAMACCI

59 Quantum Random Number Generators Mustafa TOYRAN (TÜBİTAK), Thomas PEDERSEN* (TÜBİTAK), A. S. Atilla Hasekioğlu (TÜBİTAK), M. Ali CAN (TÜBİTAK), Fikret HACIZADE (TÜBİTAK)

SALON HALL F

OTURUM SESSION 12:
BİLGİ GÜVENLİĞİNDE YENİ YAKLAŞIMLAR NEW APPROACHES TOWARDS INFORMATION SECURITY
Başkan Chairman: **Dr.Mehmet Sabir KİRAZ, TÜBİTAK-BİLGEM**

SALON HALL D

GÜVENLİK UZMANLAR KURULU TOPLANTISI BOARD MEETING of SECURTIY EXPERTS
Başkanı Chairman **Alper ÖZBİLEN, BGD**
Başkan Yardımcısı Vice Chairman **Ersen ELMAOĞULLARI, SYMANTEC**
Başkan Yardımcısı Vice Chairman **Uraz YAVANOĞLU, Gazi Üniversitesi**

22 On the Random Oracle Model and the Game Hopping Technique Turgut HANOYMAK* (METU), Murat AK (Bilkent University)	**65 Burke Shaw Kaotik Sisteminin Güvenli Haberleşme İçin Elektronik Devre Gerçeklemesi ve Senkronizasyon Uygulaması** İsmail Koyuncu* (Düzce Üniversitesi), Yılmaz UYAROĞLU (Sakarya Üniversitesi), İhsan PEHLİVAN (Sakarya Üniversitesi)
31 Oyun Teorisi Kullanılarak Bulut Bilişimde Ölçeklendirebilir Güvenlik Değerlendirmesi Evrim FURUNCU* (Gebze Institute of Technology), İbrahim SOGUKPINAR (Gebze Institute of Technology)	**10 DSAB – An Efficient Approach for Security in MANET** Rahul Saha* (Lovely Professional University), Gulshan SHARMA (Lovely Professional University), Mritunjay RAI (Lovely Professional University)

KONFERANS ve ÇALIŞTAY BAŞKANLARI DEĞERLENDİRME TOPLANTISI CONFERENCE and WORKSHOP EVALUATION MEETING

KAPANIŞ CLOSING CEREMONY

Siber Güvenlik ve Savunma
Cyber Security and Defence

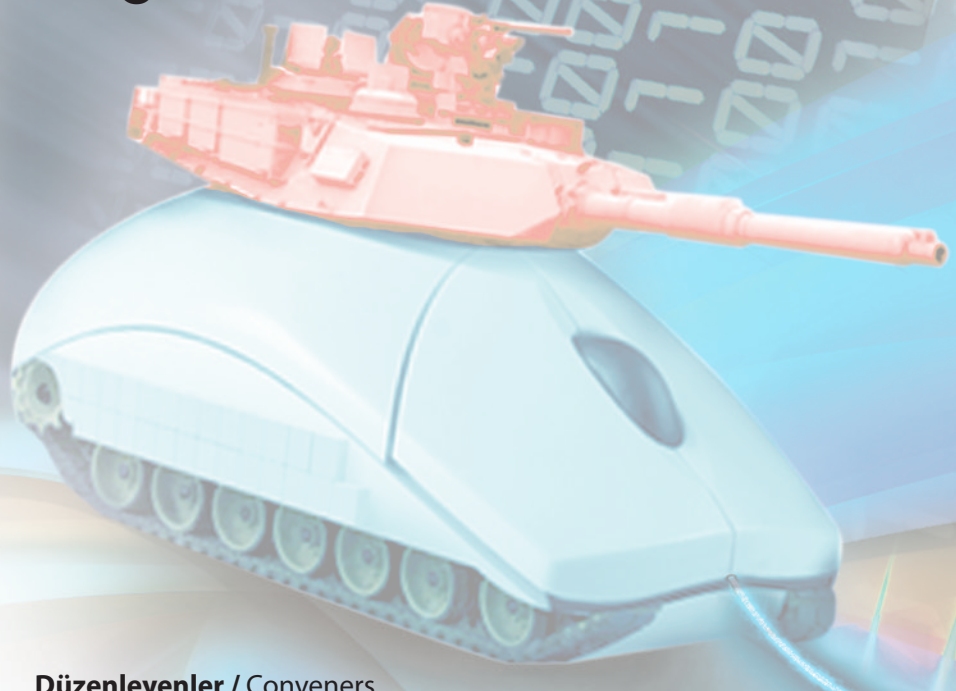
BİLGİ GÜVENLİĞİ VE KRİPTOLOJİ KONFERANSI
ISC Turkey

5. Uluslararası Bilgi Güvenliği ve Kriptoloji Konferansı

5th International Conference on Information Security & Cryptology

17-18 Mayıs
May 2012

ODTÜ Kültür ve Kongre Merkezi
METU Culture and Congress Center
Ankara-TURKEY



İçindekiler
Contents

Düzenleyenler / Conveners

T.C. ULAŞTIRMA DENİZCİLİK VE HABERLEŞME BAKANLIĞI

BİLGİ GÜVENLİĞİ DERNEĞİ

Destekleyenler / In Collaboration with

İÇİNDEKİLER / CONTENTS

ÖNSÖZ / PREFACE I

KURULLAR / COMMITTEES III

BİLİMSEL PROGRAM / SCIENTIFIC PROGRAMME XI

SÖZLÜ BİLDİRİLER / ORAL PRESENTATION

IPv6 Ağlarda Solucan Dağılım Saldırıları ve Önlemler **3**
Uraz YAVANOĞLU, Suat ÖZDEMİR, Şeref SAĞIROĞLU *Gazi Üniversitesi*

An Application of Decision Trees in Intrusion Detection **11**
Atilla ÖZGÜR *ISKUR*, Hamit ERDEM *Başkent University*

A Two-Layer Fuzzy Genetic Algorithm for Designing Intrusion Detection System **17**
Ghazaleh JAVADZADEH *Sharif University of Technolog*, Reza AZMİ

Radius Regularizations Using Learning Automata for Spherical Intelligent Anomaly Detectes **23**
Neda Afzali Seresht Reza Azmi, Boshra Pishgoo

Topic-Based Probabilistic Approach to Criminal Network for Suspect Investigation **28**
Arzu KAKIŞIM, İbrahim SOĞUKPINAR *Gebze Yüksek Teknoloji Enstitüsü*

Bilişim Suçlarında Delillendirme **34**
Çağlar ÜLKÜDERNER *Profelis Bilişim*

Siber Güvenlik Makro Analiz Modeli Önerisi ve Türkiye'nin Analizi **38**
Hakan ŞENTÜRK *KHO Savunma Bilimleri Enstitüsü*, Celal Z. ÇİL *Çankaya Üniversitesi*, Şeref SAĞIROĞLU *Gazi Üniversitesi*

Operating System Evaluation Using Choquet Integral in Terms of Cyber Threats **50**
Kerim GÖZTEPE, Ahmet EJDER *War Colleges Command*

Siber Güvenlik Perspektifinden Makineler Arası İletişim Uygulamalarının İncelenmesi **55**
Alper ÖZBİLEN, İlhami ÇOLAK, Şeref SAĞIROĞLU

Güvenli Q Sürü Bellek Yazılım Yongası Üreten Dilbilim Örneği **61**
Prof. Dr. Fevzi ÜNLÜ *Ege Üniversitesi & Yaşar Üniversitesi*

Cycle Counting For Information Security in I@I Swarm Internet Generating Q Swarm Memory **69**
Prof. Dr. Fevzi ÜNLÜ *Ege University & Yasar University, Izmir*

Metin ve Grafiksel Öğeleri Birleştiren Yeni bir Parola Tabanlı Kimlik Doğrulama Yöntemi **75**
Murat AKPULAT *Gümüşhane Üniversitesi*, Kemal BIÇAKCI *TOBB/ETÜ*, Uğur ÇİL *TOBB/ETU*

Covert Channels Detection using Process Mining **81**
Amir Jalaly BIDGOLY, Behrouz Tork LADANI, Ahmad Baraani DASTJERDI
University of Isfahan

İlköğretim ve Lise Öğrencilerinin Bilgi ve Bilgisayar Güvenliği Farkındalığı: Kahramanmaraş Örneği **87**
Mehmet TEKEREK, *Kahramanmaraş Sütçü İmam Üniversitesi*

On Applications of Privacy-Preserving Collaborative Filtering Schemes **93**
Alper BİLGE, Cihan KALELİ, Ibrahim YAKUT, Hüseyin POLAT *Anadolu University*

Kablosuz Algılayıcı Ağlarda Güvenli Ortam Erişim Protokolleri **100**
Feyza YILDIRIM OKAY, Suat ÖZDEMİR *Gazi Üniversitesi*

Anonymous RFID Authentication Protocol Without a Trusted Party **106**
Mehmet Sabır KİRAZ, Muhammed Ali BİNGOL, Süleyman KARDAŞ, Fatih BİRİNCİ *TUBITAK BILGEM*

Recommender System Based on Group Trust **112**
Somayeh NAGHSHBANDI, Behrouz Tork LADANI *University of Isfahan*

Elektronik Seçim: Norveç'in İnternet Üzerinden Oylama Sistemi ve Kriptografik Alt Yapısı **118**
Uğur BOYACI, Fatih BİRİNCİ, Mehmet Sabir KİRAZ, *TÜBİTAK BİLGEM*

Compressed Data Public Key Cryptosystems with DLP Over Extension Fields **132**
Muhammad ASHRAF *METU*, Barış B. KIRLAR *Süleyman Demirel University*

Optimal Control Formulation of Query Model for Authentication Systems **138**
Ferruh ÖZBUDAK, Ali D. SEZER, Üstün YILDIRIM *METU*

On the use of continued fractions for mutual authentication **141**
Amadou Moctar KANE *Universite LAVAL*

Formalization of Blind Signature using the Inductive Method **148**

Najmeh S. MIRAMIRKHANI, Rasool JALILI *Sharif University*

Hermite Polynomial Representation for Finite Fields of Characteristic Three **155**
Sedat AKLEYLEK *19 Mayıs University*, Ferruh ÖZBUDAK, Canan ÖZEL *METU*

Alternate Models of Elliptic Curves: A Survey **160**
Muhammad ASHRAF *METU*, Barış B. KIRLAR *Süleyman Demirel University*

Optimal Frekans Atlamalı Diziler **169**
Seda KAHRAMAN, Zülfükar SAYGI *TOBB ETÜ*

Cyclotomic Numbers and Sidel'nikov Sequences **175**
Kamil OTAL, Zülfükar SAYGI, Çetin ÜRTİŞ *TOBB ETÜ*

Notes on Bent Functions in Polynomial Forms **179**
Onur KOÇAK, Onur KURT, Neşe ÖZTOP, Zülfikar SAYGI *METU*

Security Margin of 5-Round DEAL **183**
Orhun KARA *TUBITAK BILGEM UEKAE*

How Biased Are Linear Biases **187**
Adnan BAYSAL, Orhun KARA *TUBITAK BILGEM UEKAE*

A Scalable Platform for Cryptanalysis of Computationally Intensive Algorithms **195**
Mustafa Hakan SOLMAZ, Hasan ERDOĞAN, Rıza AYKAÇ *ASELSAN*

A Proposed Attacking Method on Rabin's Cryptosystem **201**
Dr. Sattar B. SADKHAN *University of Babylon*

Frei-Chen Maskeleri Tabanlı Yeni Bir Sır Paylaşım Tekniği **206**
Veysel ASLANTAŞ *Erciyes Üniversitesi*, Ebubekir KAYA *Nevşehir Üniversitesi*

Gizli Görüntü Paylaşımında Kullanılan Eşik Şemalarının Performans Değerlendirilmesi **211**
Güzin ULUTAŞ, Mustafa ULUTAŞ, Vasif V. NABİYEV *Karadeniz Teknik Üniversitesi*

An Imperceptible Watermarking Scheme based on Double Density Dual-Tree Discrete Wavelet Transform in combination with Singular Value Decomposition **218**
Mary AGOYİ, Devrim SERAL *Cyprus International University*

Rasgele Seçilen S-kutularını Temel Alan Blok Şifrelerin Diferansiyel Kriptanalizi **224**
Fatih ÖZKAYNAK, Ahmet Bedri ÖZER *Fırat Üniversitesi*, Sırma YAVUZ *Yıldız Teknik Üniversitesi*

Success Probability of The First Attack on Full **230**
Orhun KARA, Ferhat KARAKOÇ *TUBITAK BILGEM UEKAE*

CAPTCHA Metinler için YSA Tabanlı Örüntü Tanıma Yaklaşımı **235**
Uraz YAVANOĞLU, Begüm MUTLU, Esra ŞAHİN *Gazi Üniversitesi*

Radyo Link ve Uydu Ağları Üzerinde Gelecek Nesil Dar Bant Terminal ile Yapılan Güvenli Haberleşme Test Sonuçları ve Değerlendirilmesi **245**
Orkun DİLLİ *Hv. Tek. Okl. K.lığı*, Nursel AKÇAM *Gazi Üniversitesi*, Murat KOYUNCU *Atılım Üniversitesi*

Kayıtlı Elektronik Posta Sistemi ve E-Posta Güvenliği **251**
Mustafa ALKAN *Gazi Üniversitesi*, Mustafa ÜNVER *BTK*, Hakan TEKEDERE *Gazi Üniversitesi*

Kuantum Anahtar Dağıtımında (KAD) Gizli Anahtar Uzlaştırma: CASCADE Protokolü ve LDPC Kodları **256**
Mustafa TOYRAN, Thomas B. PEDERSEN, A. S. Atilla HASEKİOĞLU,M. Ali CAN *TÜBİTAK*
Burcu A. KORKMAZ Pars MUTAF *Ege Üniversitesi*

A True Random Number Generator and Test Platform Built in FGPA **262**
Salih YILDIRIM *ASELSAN,* Cüneyt BAZLAMACCİ

Quantum Random Number Generators **268**
Muhammet Ali CAN, Fikret HACIZADE, Atilla HASEKİOĞLU,
Thomas PEDERSEN, Mustafa TOYRAN *TÜBİTAK*

On the Random Oracle Model and the Game Hopping Technique **273**
Murat AK, Turgut HANOYMAK, *Turkish Air Force Academy*

Burke Shaw Kaotik Sisteminin Güvenli Haberleşme İçin Elektronik Devre Gerçeklemesi ve Senkronizasyon Uygulaması **279**
İsmail KOYUNCU, Yılmaz UYAROĞLU, İhsan PEHLİVAN

Oyun Teorisi Kullanılarak Bulut Bilişimde Ölçeklendirebilir Güvenlik Değerlendirmesi **285**
Evrim FURUNCU, İbrahim SOĞUKPINAR

DSAB – An Efficient Approach for Security in MANET **291**
Gulshan KUMAR, Rahul SAHA, Mritunjay Kumar RAİ ***Lovely Professional University***

POSTER BİLDİRİLER / POSTER PRESENTATION

IPv6 Security Vulnerabilities **294**
Harith A. DAWOOD *Cihan University*

Digital Watermarking Enhancement for Satellite Images Using a DCT Algorithm **298**
Mustafa B. ABUGHARSA, Mohamed A. SULLABİ, Alhusain M. TAHER *Misurata University*

Sazan Avlama (Phishing): Kullanılan Teknikler ve Bunlardan Korunma Yöntemleri **302**
Ali ŞENOL, Hacer KARACAN *Gazi Üniversitesi*

Server Based Encryption (SERBASEN) Protocol on Air Gap Network **308**
Ahmet İlhan AYŞAN, Güray YILMAZ *Turkish Air Force Academy*

Encrypted Individual Multiple Choice Questions **313**
M. K. ULUKÖK, Z. B. ŞENSOY *Cyprus International University*

Utilizing a Graphical User Interface for Image Encryption based on Chaotic Algorithm EncryptionEnry **316**
Hidayet OGRAS *Batman University*, Mustafa TURK Fırat University,

T. V. PHAM Neda Afzali SERESHT, Reza AZMİ, Boshra PISHGOO

Security Directions in Cloud Computing Environments **321**
Zeinab Abbasi KHALIFEHLOU *Islamic Azad University*,
Farhad Soleimanian GHAREHCHOPOGH *Hacettepe University*

Enhancing SIEM Correlation Rules Through Baselinin **325**
Ertuğrul AKBAŞ *ANET*

Şifrelemenin Modellenmesi ve Modern Kriptosistemin Tasarımı **331**
Erkan BAYAR, Hakan KAPTAN, *Marmara Üniversitesi*

Casus Yazılımların Bilgisayar Sistemlerine Bulaşma Belirtileri ve Çözüm Önerileri **337**
Resul DAŞ *Fırat Üniversitesi,* Şahin KARA *Sakarya Üniversitesi*,
M.Zekeriya GÜNDÜZ *Fırat Üniversitesi*, *Sakarya Üniversitesi*,
Kaynarca Seyfettin Selim Meslek Yüksek Okulu, SAKA

Akıllı Şebekelerde Siber Güvenlik ve Mahremiyet **343**
Elif Üstündağ SOYKAN, Seda Demirağ ERSÖZ *TÜBİTAK*

YAZAR İNDEKSİ / AUTHOR INDEX **349**

Siber Güvenlik ve Savunma
Cyber Security and Defence

BİLGİ GÜVENLİĞİ VE KRİPTOLOJİ KONFERANSI
ISC Turkey

5. Uluslararası Bilgi Güvenliği ve Kriptoloji Konferansı

5th International Conference on Information Security & Cryptology

17-18 Mayıs
May 2012

ODTÜ Kültür ve Kongre Merkezi
METU Culture and Congress Center
Ankara-TURKEY



Sözlü Bildiriler
Oral Presentations

Düzenleyenler / Conveners

T.C. ULAŞTIRMA DENİZCİLİK VE HABERLEŞME BAKANLIĞI

BİLGİ GÜVENLİĞİ DERNEĞİ

Destekleyenler / In Collaboration with

IPv6 Ağlarda Solucan Dağılım Saldırıları ve Önlemler

Uraz Yavanoğlu, Suat Özdemir ve Şeref Sağıroğlu
uraz@gazi.edu.tr, suatozdemir@gazi.edu.tr, ss@gazi.edu.tr

***Özet*—IPv4'ün yetersiz adres alanı ve güvenlik gereksinimleri sonucunda IPv6'ya geçiş kaçınılmaz hale gelmiştir. Genel olarak, IPv6'nın performans, servis kalitesi ve güvenlik performansında artış sağlaması beklenmektedir. Her ne kadar IPv4'e oranla daha güvenli olduğu düşünülse de IPv6'nın da içerdiği bazı güvenlik açıkları bulunmaktadır. Bu çalışmada IPv6'ya geçiş sırasında ve geçiş tamamlandığında IPv6'da kullanan ağlarda görülebilecek en önemli güvenlik sorunlarından biri olan solucan yayılımı incelenmiş, IPv4'de meydana gelen açıklıklarla karşılaştırılmış ve karşılaşılabilecek tehdit karşısında alınabilecek önlemler sunulmuştur.**

***Index Terms*— IPv6, tehdit, solucan, güvenlik açığı, yayılma**

***Abstract*—The transition to IPv6 has become inevitable due to insufficient IPv4 address space. In general, IPv6 is expected to provide increased security, performance and service quality over IPv4. Although it is claimed that IPv6 provides more security than IPv4, it brings some security vulnerabilities. This study investigates worm attacks, or worm propagation and summarizes the worm propagation techniques and their countermeasures.**

***Index Terms*— IPv6, exploit, worm, security vulnerability, propagation**

I. GİRİŞ

IPv4'ün yerini almak için geliştirilen IPv6'nın kullanılmaya başlamasıyla birçok güvenlik problemi de ortaya çıkmıştır [1]. Aslında IPv6, IPv4'e göre IPSec protokolünü içinde barındırması sebebiyle daha güvenli bir protokol olarak ortaya çıkmasına rağmen uygulamadaki zorluklar veya IPv6 kullanan ağların fazla denenmemiş olması nedeniyle ortaya çıkabilecek olası güvenlik açıkları ve problemleri araştırmaya açık güncel konulardır [2].

Öncelikle IPv6'da IPSec desteği zorunlu olmasına rağmen kullanımı zorunlu değildir. IPSec'in kullanılmaması ağın hem eski IP-bağıntılı ataklara hem de IPv6'ya özgü yapılara yönelik ataklara maruz kalmasına sebep olmaktadır. Ayrıca, IPv6'nın bazı yararlı özellikleri tam olarak anlaşılamayan kendi güvenlik uygulamalarına sahiptir ve bu konudaki belirsizlikler IPv6'ya geçiş aşamasında çekinceler yaratmaktadır. Bu belirsizlikleri gidermek maksadıyla bazı uzmanlar DNS SEC hizmetinin de gerekli olduğunu savunmaktadır [3].

Bunlara ek olarak, IPv6'ya geçişte ve sonrasında IPv4 ve IPv6 tabanlı ağların birlikte kullanılacak olması ağlara yönelik atakların çeşitliliğinin artmasına ve dolayısıyla ağ güvenliğinin sağlanmasının zorlaşmasına sebep olacaktır. IPv6'ya geçilmesinin bir fark yaratmadığı, uygulama-katmanı atakları, hileli (rogue) cihazlar, paket taşması (flooding) gibi bazı IPv4 problemlerinin yarattığı sorunlar da elbette devam edecektir. Son olarak, kötü niyetli kişi ve/veya kurumların IPv6-tabanlı ağları hedef almaları sonucunda, birçok yeni ve öngörülemeyen güvenlik sorununun ortaya çıkma olasılığı bulunmaktadır.

108G100 kodlu TÜBİTAK KAMAG Ulusal IPv6 Protokol Altyapısı Tasarımı ve Geçişi Projesi [4] kapsamında gerçekleştirilen bu çalışmada IPv6'ya geçiş sırasında ve geçiş tamamlandığında IPv6 da görülebilecek en önemli güvenlik sorunlarından biri olan solucan dağılımı ve bu atağa karşı geliştirilmiş olası çözümler incelenmiştir. Ulusal IPv6 Protokol Altyapısı Tasarımı ve Geçişi Projesi ile Türkiye'nin IPv6 geçiş aşamasındaki yol haritasının belirlenmesi hedeflenmiştir. Proje kapsamında Türkiye'nin ulusal çapta IPv6'ya geçişinin ve IPv6 üzerindeki uygulamaların hayata geçirilişinin sorunsuz ve güvenli bir şekilde gerçekleşebilmesi için gereken temel bilincin, farkındalığın ve bilgi birikiminin oluşturulması ve IPv6 kullanımının yaygınlaştırılması, farklı geçiş yöntemleri için gereken maliyet ve özelliklerin belirlenmesi, bu kriterleri barındıran bir "IPv6 Bilgi Üretim ve Yönetim Sistemi" oluşturulması projenin amaçlarından sadece birisidir [5]. Bununla birlikte IPv6'ya geçişte kullanılabilecek test yatağı, geçişte kullanılabilecek karar destek sistemi [6], balküpü tasarımı ve video konferans sistemi [7] ise diğer beklenen çıktılardır.

Literatürde IPv6'da solucan dağılımına yönelik çalışmalar bulunmaktadır [8-17]. Bu çalışmalar halen kullanılan geniş çaplı bir IPv6 ağı bulunmaması sebebiyle yerel ortamlar üzerinde ya da GTNetS gibi paket seviyesinde benzetim araçları kullanılarak yapılmaktadır [8]. Chen ve Ji tarafından yapılan çalışmada, belirli bir ortamdan toplanan veriler ile öğrenebilme yeteneğine sahip solucanlar araştırılmıştır. Bu tarz solucanlar bulaşma oranına göre etkiledikleri ağ üzerinde daha hızlı yayılma eğilimi gösterebilmektedir. Bu tip solucanların önlenmesinde kullanılabilecek metotlar çalışma içerisinde tartışılmıştır [9]. Zoe ve arkadaşları tarafından

yapılan bir çalışmada, Temmuz 2001'de ağ ortamlarını etkileyen "Code Red" solucanının yayılma stratejisini ele alarak 2 aşamalı bir model geliştirmişlerdir. Bu model sayesinde ileride oluşabilecek solucan sorunlarının yayılma hızı konuları incelenerek alınması gereken önlemlerin öngörülebileceği ifade edilmektedir [10]. Moore ve arkadaşları tarafından yapılan bir başka çalışmada ise Code Red isimli Internet solucanının izini sürmek amacıyla kullanılan bir yöntem önerilmiştir. Bu sayede Code Red solucanının nasıl bulaştığı hangi aşamalarda zararlara neden olduğu ve ülkelerin bütçesine olan zararları belirlenmiştir [11]. Staniford ve arkadaşları tarafından yapılan bir çalışmada 30 saniye gibi kısa bir süre içerisinde bir milyon bilgisayarın etkilenmesine neden olabilecek flaş solucanların literatürde yer alan Slammer gibi mevcut solucanlara UDP ve TCP başlıkları ile uyarlanması incelenmiştir. Bu incelemeler çerçevesinde flaş solucan yayılımının önlenmesi için çözüm önerileri de sunulmuştur [12]. Wong ve arkadaşları tarafından yapılan bir çalışmada yerleşke ortamındaki Internet kayıtları incelenerek DDoS ataklarına araç olarak kullanılan büyük sayıda e-posta gönderme solucanları incelenmiştir. Bu çalışmada solucanları engelleyecek metodolojinin ancak bu kötücül yazılımları otomatik olarak tanımlayan ve durdurmaya çalışan stratejilerden geçtiği ifade edilmektedir [13]. Antonatos ve arkadaşları tarafından yapılan başka bir çalışmada ise solucanların engellenmesi için rastgele adres uzayı adında bir algoritma önerilmiştir. Solucanlar siber uzayı tarayarak çok vakit harcadıkları için aktif makine IP'lerinin olduğu saldırı listeleri kullanmaktadırlar. Bu çalışmada saldırı listelerine karşı ağa bağlı her makinenin belli aralıklarla IP adresini değiştirmesi önerilmiştir [14].

IPv6 protokolünün geliştirilme amacı Internet'in iki büyük sorunu olan çok hızlı yayılan solucanlar ve yetersiz IP adresi sorunlarına çözüm bulmak olarak özetlenebilir. IPv6 adres uzayının büyüklüğünün solucan yayılımına engel olacağı öngörülmüşse de yapılan çalışmalar sorunun bu kadar basit çözülemeyeceğini göstermektedir [4]. Kamra ve arkadaşları tarafından yapılan bir çalışmada rastgele tarama yapan IPv4 solucanlarına göre DNS sorgularını tarayarak çalışan internet solucanlarının geliştirilebileceği gösterilmiştir [15]. Yangui ve Jiachun tarafından yapılan bir çalışmada ise IPv6 ağında yayılmaya çalışan DNS solucanlarının tespitine yönelik bir algoritma önerilmiştir [16].

Solucanlar incelendiğinde, İnternet Solucanları, P2P Solucanları, E-Posta Solucanları, Anlık Mesajlaşma solucanlarına ayrılarak sistemleri tehdit ettiği görülmektedir [17].

Bildirinin geri kalan kısmı aşağıdaki şekilde düzenlenmiştir. 2. Bölümde IPv6 altyapısı, 3. Bölümde ağlarda solucan dağılımı, 4. Bölümde solucan yayılma modelleri, 5. Bölümde solucan yayılma stratejileri, 6. Bölümde solucan yayılımından korunma metotları ve son olarak 7. Bölümde sonuç ve değerlendirmeler verilmiştir.

II. IPV6 ALTYAPISI VE SOLUCAN DAĞILIMI

IPv6 protokolünün geliştirilme amacı Internet'in iki büyük sorunu olan çok hızlı yayılan solucanlar ve yetersiz IP adresi sorunlarına çözüm bulmak olarak özetlenebilir. IPv6 adres uzayının büyüklüğünün solucan yayılımına engel olacağı öngörülmekte ise de ancak yapılan çalışmalar sorunun bu kadar basit çözülemeyeceğini göstermiştir.

Solucan dağılımlarını daha iyi anlatmak için önemli başlıklar altında konu değerlendirilmiştir.

A. IPv6 Adres Mimarisi [18]

IPv6 adres mimarisindeki adres biçimleri bağlantı-yerel adresleri, tekil yerel adresler, global adresler ve multicast adreslerdir. Unicast adreslerin tüm formları genel olarak iki kısma ayrılmıştır: ağ bölümü ve host bölümü. Ağ bölümü belirli bir LAN, host bölümü de o LAN üzerindeki belirli bir node'u ifade etmektedir. Bu şekilde adres genel olarak iki 64-bit'lik kısma ayrılmıştır.

B. Yerel Bilgi Kaynakları [19]

Bu kaynaklar 6 başlıkta toplanmış ve aşağıda kısaca açıklanmıştır.

Yönlendirme Tabloları ve Protokoller: Genel olarak host yönlendirme tabloları sadece diğer yerel hostların girişlerini ve LAN dışındaki tüm trafik için varsayılan bir yönlendirme girişi içerir. Birçok organizasyon içeride OSPF yada RIP gibi yönlendirme protokolleri kullanır. Çok azı RIP protokolünün IPv6 ağlarına uyarlanmış olan sürümü RIPng protokolünden haberdardır. Bu gibi bir ortamda, bir solucan direk olarak host yönlendirme tabloları ile ilgilenecektir (örneğin: UNIX netstat komutunu kullanarak) ya da pasif dinleyici olarak yönlendirme protokolüne katılacaktır. Solucan dağılımlarına yönelik bazı hususlar aşağıda kısaca özetlenmiştir.

Arayüz belirteçleri: Komşu keşif tabloları bazı yerel olarak kullanılan ağ kartlarını kullanmaya yarayabilir. Her durumda 40 farklı kart tipi, 227 host bulunacaktır. Her bir üretici belirteci için 2^{24} adres bulunacaktır.

Multicast Ping: Multicast solucanlar tarafından hedef keşif noktası olarak kullanılmasına rağmen, IPv6 tasarımında temel bir kısımdır. RFC'ye göre FF0E:0:0:0:0:0:0:101 adresleri "Internetteki tüm NTP sunucuları" nı ifade etmektedir. Bu adrese yapılan bir NTP sorgusu birçok hedefi ortaya çıkarabilir. Bir paket Internette dolaşırken FF05:0:0:0:0:0:0:2 bir sitedeki tüm yönlendiricileri bulur ve FF02:0:0:0:0:0:0:1 yerel bağlantıdaki tüm hostlara gönderme işlemini gerçekleştirebilir.

Host Yapılandırması ve Günlük Dosyaları: Bilgisayarlar genel olarak yerel dosya sunucuları, web vekil sunucuları, yerel DNS sunucuları /etc/hosts file in UNIX, SSH known_hosts dosyaları gibi diğer bilgisayarların adresleriyle yapılandırılmışlardır. Bir solucan yapılandırma dosyalarını, MS Windows işletim sistemine sahip makinelerdeki kayıtları inceleyerek saldırı hedeflerini belirleyebilir.

DNS Bölge Transferi: Tipik DNS sunucular hostlardan bölge geçişlerini engelleyecek şekilde yapılandırılmıştır. Bununla birlikte bazı organizasyonlar içerde bölge geçişlerini sağlayan bir kayda sahip olabilir. Buradan bir solucan bir domain içerisindeki tüm hostların listesini ele geçirebilir.

Pasif Dinleme: Tüm yerel ağlar anahtarlanmış olmasına rağmen, kablosuz ağlar trafiği gözleyerek yerel ağda yeni hedefler keşfetmeyi sağlamaktadır. Buradan ağlarda dış trafikten gelen rastgele adresler yerel trafiğe bağlantı için kullanılabilir.

C. Geniş-Alan Bilgi Kaynakları [19]

Yönlendirme Protokolleri: Bu protokoller kullanılan adres prefixleri hakkında bilgi sağlar. Bu bilgi hem yerel olarak, hem de Internet üzerinden kullanılabilir.

Yerel olarak, saldırı programı yerel yönlendirme trafiğini dinler. Bunun için "tüm yönlendiriciler" multicast grubuna katılmak gereklidir. Uzaktan ise yönlendirme bilgisini içeren genel arşivler bu iş için kullanılabilir.

Sunucu günlükleri: Bağlantı listesindekileri tutan günlük dosyaları geniş-alana yayılmak için iyi bir yöntemdir.

Sunucu adresleri: Tek başına prefix hatırlamak için zordur. Yöneticiler kolayca akılda kalan low-order bit'leri seçerler. Bu durum solucanlar tarafından kullanılmaktadır.

Arama motorları ve DNS: Eğer solucan web sunucuları hedef olarak seçtiyse, web arama motorları potansiyel hedeflere ulaşmak için iyi bir kaynaktır. Aynı zamanda DNS te tek başına uygun host isimlerini bulmak için bir arama motoru gibi kullanılabilmektedir.

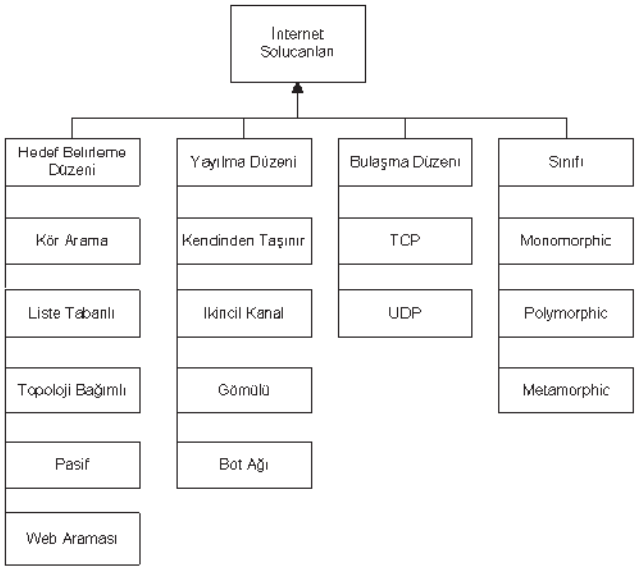
D. Yayılma Stratejileri

Kullanılan Internet kaynağına göre solucan yayılma stratejileri iki fazda gerçekleşebilir. İlk önce, arama motorlarını, sunucu günlüklerini, yönlendirme tablolarındaki bilgileri vs. Kullanarak IPv6 prefixleri bulunur. Bu kaynaklar belirli bir hedefi gösterebilmektedir. Organizasyon ağına bir defa girildiğinde, yerel bilgi kaynaklarını kullanarak bulaşılacak diğer node'ların bilgileri alınabilir. Bu iki fazlı yaklaşım genel dağılım için genişletilebilir. Popüler bir web sunucusuna bulaşmış bir solucan çok çabuk bir şekilde diğer ağlara kolaylıkla bulaşabilir [19].

Solucan yayılma ve hedef belirleme yöntemleri Li ve arkadaşlarının yaptığı ve Şekil 1'de verilmiştir [20].

III. SOLUCAN YAYILMA MODELİ

Ağı rastgele-tarayan solucanlara karşı IPv6 protokolü çok yüksek bir güvenlik sağlamaktadır. IPv6 dünyasında, ağ parametreleri ve solucanın yayılma hızı arasındaki ilişkiyi gösteren analitik modeller üretilmiştir. Kamra ve arkadaşları tarafından bir çalışmada gerçek ölçümlerden seçilen parametrelere ve mevcut internet'e dayanan simülasyon sonuçları, zeki bir solucanın IPv6 dünyasında basit stratejileri kullanarak sürpriz bir hızla yayıldığını gösterilmiştir. Solucanın performansının, ağdaki dizin ve isimlendirme servislerinin ne kadar güvenli olduğuna bağlı olduğu görülmüştür [21].



Şekil 1. İnternet Solucanı hedef belirleme ve yayılma stratejileri [20].

A. Rastgele Tarama [21]

IPv4 İnternet alanında yayılan tipik bir rastgele tarayan solucan (CodeRed sürümleri ve Slammer solucan gibi) rastgele IP adresleri üretir ve bu IP adreslerine sahip hostları enfekte etmeye çalışır.

B. DNS Solucanı [21]

DNS solucanı rastgele taramaya dayanmaz. DNS solucanı, IPv6 adres alanındaki aktif IP'leri bulmak için DNS sorgularını kullanır. İki kısımdan oluşur. Arka-ucunda Internette olabilecek aktüel host isimleri üreten bir adres üreteci vardır. Ön-ucunda ise saldırılıp enfekte edilebilecek uygun IP adreslerini bulmak için DNS çözünürlüğü kullanılır.

String Üretimi: DNS Solucanının arka-ucu Internetteki aktüel hostların muhtemel isimleri olabilecek string'leri üreten bir string üretecine sahiptir. İnternet host isimleri noktalar ile ayrılmış genel bir yapıya sahiptir (örn, www.yahoo.com). Genelde "www" ile başlar ve ".com" ile biterler ve arada da sözlükte bulunabilecek bir kelime bulunur. Bu nedenle, zeki bir DNS solucanı, sözlük saldırısı ile olası Internet host isimlerini üretebilir. Bunun yanında sözlük-tabanlı string üreteci ile solucan web arama makinelerini kullanarak geçerli host isimlerini ve belirli sunucu isimlerini bulabilir [21]

DNS Solucanı [21]:

(1). String üretecini kullanarak yeni bir olası host ismi üret.
(2). Bir DNS sorgusu başlatarak olası host ismini çözümle.

a. Eğer geçerli bir IP adresi dönerse bu isimle aktif bir Internet hostu olduğuna karar ver ve saldırıp enfekte et.
b. Değilse birinci adıma dön.

olmak üzere 2 adımdan oluşmaktadır.

Efektif Tarama Oranı: DNS solucanı yaptığı her tarama için bir DNS sorgusu çalıştırır. Sorgu başarılı olursa sonuç IP adresi enfekte edilir. İşlem için geçen toplam süre DNS gecikmelerinin ve enfekte süresinin toplamıdır. Diğer taraftan eğer DNS sorgusu başarısız olursa, solucan hemen yeni bir string üretmeye başlayacaktır. Bu nedenle toplam süre DNS gecikmesidir.

C. *DNS Mimarisini Modellemek ve Sonuç Gecikmeleri [21]*

DNS mimarisi DNS sorgularına cevap veren DNS sunucuları hiyerarşisinden oluşur. Hiyerarşinin en üstünde Kök DNS sunucular bulunur. Yerelde çözümlenmeyen çoğu DNS sorguları öncelikle bu Kök DNS sunucularından birine yönlendirilir. DNS solucanlarının hızla yayılmasından dolayı DNS sorgularının sayısı dramatik olarak artar ve Kök DNS sunucuda fazla yüke (overloading) neden olarak dar boğaz (bottleneck) oluşmasını sağlarlar. Kök DNS sunucularının işlem güçleri sınırlıdır. Kök DNS sunucularının sınırlı veri üretme davranışı üzerinde çalışmışlar ve onları M/M/1/K kuyruklama sistemi olarak modellemişlerdir.

Kuyruklama sistemi DNS sorgularına hizmet verir ve logaritmik bir servis oranına (μ) sahiptir. K, kuyruk sisteminde olabilecek maksimum kuyruk sayısıdır. Yüksek yük olduğu zamanlarda bütün sorgulara cevap verilemeyecektir ve sorgular atılacaktır [21].

D. *DNS Solucanı Yayılımı [21]*

Kabul edilen sorgular için kuyruk sisteminin beklenen cevap süresi Internetteki tipik DNS kuyruğu tarafından harcanan ortalama süre ile ölçülür. M/M/1/K kuyruk modelinde atılması beklenen DNS sorgusu, solucanın ürettiği DNS sorgusunun yeniden iletimi için iyi bir ölçümdür.

IV. SOLUCAN YAYILMA STRATEJİLERİ

Solucanın Sınır Geçidi Protokolü (BGP) yönlendirme tablolarından sağlanan bilgiler aracılığıyla bulaşması muhtemel makineleri ihmal etmeden araştırma uzayını daralttığı belirtilmiştir [22]. Bu yöntem aracılığıyla yönlendirme solucanın 2-3 kat yayılma hızını arttırdığı bildirilmiştir. BGP Yönlendirme tablolarından elde edilecek coğrafik bilgi veren yönlendirme ön ekleri sayesinde spesifik olarak bir ülkeye ve ülkede İSS gibi şirketlere kolaylıkla saldırı düzenlenebileceği belirtilmiştir. Zou ve arkadaşları tarafından yapılan çalışmada IPV4'ten IPV6'ya geçişin tarama yöntemini kullanan solucanların yayılımını sınırlandıracağını belirtilmektedir [23]. Bir başka endişe ise yalın IPv6 kullanmayan ikili yığın ağlarında IPv4 solucanlarının arama stratejilerinde yapılacak değişiklikler ile IPv6 ağını saldırabilecek solucanların üretilebileceği yönündedir [22].

Bir solucanın hızlı yayılmasını belirleyen faktörler [22]:

- Solucan bulaşmış popülasyon sayısı
- Solucan tarama hızı
- Solucanın bulaşabileceği makine sayısını veren olasılık değeri olarak tespit edilmiştir.

Yönlendirme solucanlarının diğer solucanlara göre neden daha hızlı yayıldığı ile ilgili olarak yapılan sınıflandırmada ilk grup olarak BGP yönlendirme tablolarını kullanan solucanlar gösterilmiştir [23]. 1997-2003 yılında IP adresi kullanım oranının %20'lerden %28,5 olarak arttığı tespit edilmiştir [23]. Bu verinin %28,5 IPv4 adresinin atandığının ve yönlendirilebilir olduğunun bilinmesi açısından önemli olduğu ve BGP yönlendirme tablolarında yer alan ön ekler (prefix) sayesinde adres uzayının %71,4'e indirilebileceği bildirilmiştir [23].

Geleneksel solucanların yayılma hızını arttırmanın yolunun A sınıfı atama verilerinin olduğu belirtilen çalışmada IANA'dan elde edilen 2003 yılı A sınıfı adreslere ait bilgi ile BGP yönlendirme verilerini birleştirerek bir tablodan hareketle, A sınıfı adreslere ait bilgi aracılığıyla solucanların %45.3 oranında alt uzayda çalışarak hedefe ulaşacağı belirtilmiştir. RIPE NNC ve Route View'den elde ettilkleri BGP yönlendirme tablosu ön eklerine ait detaylı bilgiler aracılığıyla her iki kaynaktaki örtüşen verilerin kaldırılması durumunda 140602 ön ek sayısının 62053 düştüğünün gözlemlendiği ve bu sayede yönlendirme solucanlarının ihtiyaç duyacağı depolama alanının düştüğü tespit edilmiştir [23].

BGP ve A Sınıfı yönlendirme solucanlarının alana spesifik olarak kullanılacağından bahsedilen çalışmada [23], BGP ön eklerinin birleştirilmesi yöntemine dayalı yönlendirme solucanlarının tasarımının taranan IP uzayı ile yönlendirme solucanlarının kapasite gereksinimleri arasında denge sağladığı belirtilmiştir. Yapılan örnek bir çalışmada 175 KB'den 24 KB'ye inen depolama kapasitesinin solucana %28,6 dan %30,9'a çıkan taranacak adres uzayı oluşturduğu belirtilmiştir. Solucanların birçok tarama tekniği kullandığı belirtilen çalışmada uniform tarama üzerinde çalışıldığı solucan yayılımını modellemek için basit salgın modelinin kullanıldığı belirtilmiştir. Salgın modelinde (epidemic model) ağ üzerindeki makineleri bulaşmış ya da bulaşması muhtemel olarak iki sınıfa ayrıldığı, bulaşma oranının solucan yayılım hızını belirlediği bildirilmiştir [23].

Solucan yayılımına ait hızın ve ağ örüntüsünün araştırılması, solucanları önleme ve tespit etme mekanizmalarının geliştirilmesi için gereklidir. Manna ve arkadaşları tarafından yapılan bir çalışmada ise rastgele tarama yapan solucanların yanında permütasyon taraması yapan solucanların ciddi bir tehdit olduğu ve arama hızlarını nasıl ikiye katladığı tartışılmıştır [24]. Yönlendirme solucanlarının yayılım hızını belirlemek için salgın modelinin kullanıldığı belirtilen çalışmada, Code Red virüsü, BGP yönlendirme virüsü ve A sınıfı yönlendirme solucanının yayılım hızının karşılaştırıldığı çalışmada IP adres bilgisinin yönlendirme solucanlarının yayılım hızını arttırdığının görüldüğü bildirilmektedir.

TABLO 1
IPv4 Solucanları Bilgi Tablosu

Solucan Adı	Menşei	Etkilenen Platform	Yayılma Aracı	Tespit Yılı	Kodlama Dili	Verdiği Zarar (Milyon Dolar)	IPv6 Ortamlarda Yayılma Olasılığı
Morris	ABD	Unix	İnternet	1988	C	1.00	Bilinmiyor
Happy99	Fransa	Windows	Eposta & Usenet	1999	Assembly	-	Evet
Kak	-	Outlook Express	Javascript	1999	Visual Basic	-	Evet
ExploreZip	İsrail	Windows	MS Outlook	1999	Delphi	1,020.00	Evet
iloveyou	Filipinler	Windows	MS Outlook	2000	Visual Basic	5,500.00	Evet
Code Red	Çin	MS IIS	Subnet	2001	Assembly	2,750.00	DNS Tipi
Nimda	Çin	Windows	İnternet	2001	C++	2,600.00	Bilinmiyor
Sadmind	Çin	Web Sunucusu	İnternet	2001	Perl & Shell	-	Bilinmiyor
Sircam	Meksika	Windows	Eposta	2001	-	3,000.00	Evet
Storm	Rusya	Windows	MS IIS	2001	-	-	Bilinmiyor
Klez	Çin	Windows	Eposta	2001	C++	19,800.00	Evet
Mylife	-	Windows	MS Outlook	2002	Visual Basic	-	Evet
Slammer	-	Windows	UDP Paketi	2003	Assembly	1,200.00	DNS Tipi
Blaster	ABD	Windows	DCOM RPC	2003	C	320.00	Bilinmiyor
Sven	Slovakya	Windows	İnternet	2003	C++	10,400.00	Bilinmiyor
Bolgimo	-	Windows	İnternet	2003	-	-	Bilinmiyor
Sober	Almanya	Windows	Mass Mailer	2003	Visual Basic	-	Evet
Sobig	-	Windows	Eposta	2003	C++	37,100.00	Evet
Welchia	-	Windows	RPC	2003	C++	-	Bilinmiyor
Sasser	Almanya	Windows	İnternet	2004	C++	18,100.00	Bilinmiyor
Blackworm	Asya	Windows	Mass Mailer	2004	Visual Basic	-	Evet
Santy	Güney Amerika	Web Sunucusu	PHPBB	2004	Perl	-	Evet
Caribe	İspanya	Symbian OS	Bluetooth	2004	C++	-	Evet
Witty	Avrupa	Windows	IBM ISS	2004	-	-	Bilinmiyor
Netsky	Almanya	Windows	Eposta	2004	C++	2,000.00	Evet
Mydoom	Rusya	Windows	Eposta	2004	C++	38,500.00	Evet
Bagle	Almanya	Windows	Mass Mailer	2004	-	-	Evet
Agobot	Almanya	Windows	Botnet	2004	C++	-	Bilinmiyor
Samy	Polonya	Myspace	XSS	2005	-	-	Evet
Zotob	Fas & Türkiye	Microsoft	Microsoft-ds	2005	-	-	Bilinmiyor
Stration	-	Windows	Eposta	2006	-	-	Evet
Brontok	Endonezya	Windows	Eposta	2006	-	-	Evet
Conficker	Ukrayna	Windows	İnternet	2008	-	9,100.00	Bilinmiyor
Daprosy	-	Windows	USB & İnternet	2009	-	-	Bilinmiyor
Koobface	Rusya	Facebook	Mesaj Sistemi	2009	-	-	Evet
Stuxnet	-	Windows	Siemens PLC	2010	-	-	Evet
Duqu	İsrail	Windows	Microsoft Word	2011	-	-	Evet

V. KORUNMA METOTLARI VE ALINMASI GEREKEN TEDBİRLER

IPv6 geçişini takip eden süreçte ortaya çıkabilecek solucan tiplerini öngörmek kısmen mümkündür. Tablo 1'de IPv4 için 1988-2011 yılları arasında geliştirilmiş solucanlar yer almaktadır. Bu solucanlar kodlama dili, kodlamayı yapan kişinin ülkesi, yayılma ortamı ve şekli ile küresel ağ da yarattığı maddi zarar bileşenleriyle birlikte verilmiştir. IPv6 solucanlarından etkili bir şekilde korunmak için literatürde geçmiş deneyimlerden faydalanılarak çeşitli yöntemler önerilmiştir [25,26]. Ayrıca, Tablo 1'de solucanların IPv6 ağında yayılma ihtimalleri de değerlendirilmiştir. Bu kapsamda yapılan bir çalışmada Slammer ve Code Red gibi solucanların IPv6 ağında DNS sorgularıyla yayılabilen varyasyonlarının ortaya çıkabileceği önerilmiştir [15]. Bu tip rasgele konuk tarama prensibiyle çalışan solucanlar için literatürde kısıtlı sayıda IPv6 araştırması bulunmakla birlikte gerçek zamanlı testlerin kapalı bir ağ da yapılması ile sonuçların tartışılması gerektiği düşünülmektedir. Buna karşın rasgele ağ taramasının aksine IPv6 ağında Tablo 1'de sunduğumuz solucanların farklı varyasyonlarının e-posta, özel amaçlı yazılımlar ve P2P paylaşım ağları gibi ortamlarda yayılmasının kaçınılmaz olduğu öngörülmektedir.

(1). Derleme zamanı yazılım koruması aslında ideal yazılım üretmek anlamına gelmektedir. Solucanlar yazılım açıklarından faydalanarak kurbanlarını etkilerler. Bu sebeple yazdığımız yazılımlarda yani derleme zamanında solucanlar tarafından kullanılabilecek açıklıkların giderilmesi gerekmektedir. Açıkların büyük çaplı yazılımlar için her zaman mevcut olacağı düşünülmektedir. Bu yazılımlarda en azından bellek taşması (buffer overflow) gibi en güncel sorunlara neden olan açıklıkların giderilmesi sağlanmalıdır.

(2). Bir diğer solucan önleme yolu ise anomali ve yanlış kullanım denetleyici olarak çalışan antivirüs yazılımlarıdır. Bu yazılımlar çalıştırma zamanı koruması olarak nitelendirilir. Yanlış kullanım denetleyicileri bilinen imza tabanlı yöntemlerde oluşmaktadır. Bu yöntem yavaş yayılan solucanlar için oldukça etkilidir. Solucan yayılımlarında hızlı çalışan bir solucan imzası tanımlama yöntemi geliştirilmesi için çalışmalar devam etmektedir [24].

(3). Solucan engellemenin başka bir yolu ise solucanların ağ üzerinde yayılmaları için gerekli olan paketlerin filtrelenmesidir. Bu filtreleme işlemi aslında iki kısımda gerçekleşmektedir. İlk olarak solucanların yarattığı trafiğin normal trafik akışından ayırt edilebilmesi gerekmektedir. İkinci olarak da bir solucanı ağ üzerinde nasıl engellenebileceği ya da en azından nasıl yayılmasının yavaşlatılabileceği üzerinde durulmalıdır [27].

(4). Elbette solucanların engellenmesi için geliştirilmiş antivirüs yazılımları, saldırı tespit sistemleri ve güvenlik duvarları gibi yöntemler sıklıkla kullanılmakla birlikte solucanın eğrisel metotlar ile yayılımını tespit ederek kişilerin ölçeklenebilir önlemler almasını sağlayan metotlarda önerilmiştir [28].

(5). Ağ filtrelemesi için kullanılan yöntemlerden bir tanesi solucanların yayıldıkları adreslerin güvenlik duvarları tarafından kara listeleye alınarak bu adreslere gelen giden trafiklerin engellenmesidir. Bu yavaş yayılan solucanlar için tepki süresinin çok uzaması nedeniyle kabul gören bir teknik değildir zira bu adres listelerinin sürekli olarak güncellenmeleri gerekmektedir. Adres tabanlı filtrelemenin bir diğer sorunu ise tek bir UDP paketi kullanarak yayılma stratejisi geliştirmiş olan solucanların bu filtreleri kandırabilmesidir.

(6). Bazı durumlarda anti virüs yazılımlarının solucan görülmeden önce imzasını tahmin etme olasılığı bulunmaktadır. Bu aslında bir açık kapı bulunduktan sonra bunu kullanacak bir solucanın önceden keşfedilmesi olarak değerlendirebilir. Aslına bakılacak olursa bir yazılım açığı keşfedildikten sonra bunun için gerekli olan işletim sistemi ve anti virüs yazılım güncelleştirmeleri solucanın ortaya çıkışına göre geride kalmaktadır.

(7). Literatürde yeni ortaya çıkan atakları yayılmanın başında tanımlamak için imza gereksinimini ortadan kaldıran yapay sinir ağları temelli saldırı tespit sistemleri önerilmiştir [29]. Bu sayede saldırı sistemin çalıştığı ilk noktada tespit edilerek gereken filtreleme önlemleri alınabilecektir.

(8). Başka bir filtreleme yöntemi ise göreceli olarak basit uygulanabilen Ingress filtrelemedir [31]. Teknik açıdan bakıldığı zaman bir makineden yapılan belirli sayıda tarama isteği oldukça şüpheli bulunmaktadır. Ayrıca IP kandırmacası yoluyla aslında normal olan trafiğe sahip kişilerde bu istenmeyen durumdan etkilenebilirler. Bu sorunu çözmek için şüpheli trafiği durdurmak yerine yavaşlatarak elde edilen sonuçları gözlemlemek ve buna göre hareket etmek gerekmektedir.

(9). Elbette bir solucan sistemleri etkilediği zaman hasarı minimuma indirmek için bazı önlemler almak gerekebilir. Bir solucan yayılmak için daha önceden etkilediği makineyi kullanmaktadır. Bu sayede DDoS atakları gerçekleşmektedir. Bu yöntemle özel bilgilerde kurban makineye açılan arka kapılar sayesinde çalınabilmektedir. Bu tarz bir ağ sorunuyla savaşmanın en basit yolu ağ çevresinde yeni bir topolojik yapı oluşturmaktır. Bu topolojik yapı çerçevesinde kullanıcı ve sunucu makineler sadece belirlenen düğümler üzerinden iletişim kurabilmektedir. Kullanıcılar sunucu ile direkt olarak iletişim kuramadıkları için ağ üzerinde arka kapıların açılması ya da bir solucanın sunucuya ulaşması bu düğümlerde bulunan filtre mekanizmaları yüzünden zorlaşmaktadır [31].

(10). Bütün solucan yayılımı engelleme mekanizmaları benzer özellikleri paylaşmaktadır. Açıkçası gerçekleştirilmeleri için gerekli olan fonksiyonel yapıları ve buna bağlı olarak etkileri logaritmik olarak artmaktadır. Buna yeni yazılım sürümlerinin çıkışıyla solucan bulaşma oranlarının logaritmik

olarak azalması örnek olarak verilebilir. Bu dağılımı son kullanıcılar ve Internet servis sağlayıcılar açısından değerlendirmek istediğimizde; solucan yayılma hızının doğrusal olarak artması onu filtrelemek için gerekli olan mekanizmaların logaritmik olarak artmasına neden olmaktadır. Bu sebeple aşağıdaki denklemde açıklandığı gibi tek bir solucan tipine karşı yazılım geliştirmek yerine solucan yayılımını engellemek için kullanılacak tekniklerin tüm Internet katmanlarına ve yazılım geliştirilmesine uygulanması gerekmektedir [32]. Bu amaçla ağ üzerinde akan trafiğin denetlenmesi ve anomali tespiti için IPFix gibi çözümlerde önerilmiştir [33].

(11). Burada bahsedilen genel metotlar haricinde Tablo 1'de verildiği üzere yeni geliştirilen solucanlar internet adres uzayını taramak yerine Stuxnet gibi özel uygulamalar üzerinden yayılma metotları geliştirmiştir. Bu tip solucanlar internet sürümünden bağımsız işlem yaparak solucan tespitini ve engellenmesini zorlaştırmaktadır. Bununla birlikte Koobface gibi sosyal ağlar üzerinde yayılmaya başlayan solucanlar ise tek seferde milyonlarca kullanıcıyı etkileyebilecek düzeydedir. Solucan dağılımını engellemek ve maddi zararları en az indirmek için kurumsal güvenlik ve kişisel güvenlik unsurlarının birlikte uygulanması gerekmektedir.

Genel olarak bakıldığında bir filtre sistemi geliştirmek için solucanları ortaya çıktıkları anda engellemek için yanıt süresi 10 saniye mertebesinde olan bir sistem geliştirmek gerekir. Bu sistemin kurgulanacağı yer ilk bakışta her kullanıcının bağlı olduğu ve ağın büyük bölümüne hakim olan Internet servis sağlayıcılardır. Bu işlem için ilk kurulum noktası Internet servis sağlayıcılar olarak gözükmesine rağmen akan trafiğin sürekli olarak saldırı tespit sistemlerince solucan örüntülerine karşı izlenmesi mümkün değildir. Bu trafik bilgisinin geri planda işlenerek elde edilen sonuçların değerlendirilmesi mümkündür. Bu amaçla yapılan bir çalışmada IPv6 trafik bilgisinin incelenerek anomali tespitinin yapılabileceği gösterilmiştir [30]. İnternet servis sağlayıcısı tarafında kullanılan vekil sunucularda yanlış pozitifliğin oluşmasına neden olarak bireylerin solucanları tespit edebilmesini oldukça zorlaştırmaktadır. Buna ek olarak çok vektörlü (multi-vector) ve değişken imzalı (polimorfik) solucanların yayılmak için birden fazla yöntem benimsemiş olmaları birçok filtreden geçebilmelerine olanak tanımaktadır. Alternatif olarak bir mobil kullanıcı bilgisayarın güvenlik duvarından geçebilen bir solucan çok rahatlıkla Internet servis sağlayıcı altyapısına ulaşabilmektedir. Sonuç olarak filtrenin ağ da ulaşılabilecek son noktaya konulmasını bir diğer sebebi ise zaten belirli bir trafik örüntüsüne sahip bir filtreleme mekanizmasının solucanları daha kolay ayırt edebileceğidir. Bu işlemi çok farklı trafik örüntüleri olan Internet servis sağlayıcı tarafında yapmak mantıklı değildir.

VI. SONUÇ VE DEĞERLENDİRMELER

Solucan saldırılarından korunmak için literatürde çeşitli yöntemler önerilmiştir. Bu yöntemlerin genel olarak IPv4 ağlarında solucan yayılımını önlemek amacıyla geliştirildiği görülmektedir. Bu sebeple IPv6 ağlarında solucan dağılımlarının öngörülmesi amacıyla balküpü yazılımları kullanılmalıdır. Bu durumda bazı öngörülerde bulunulabileceği gibi IPSec ve beraberinde getirdiği yeni güvenlik özellikleri de dahil olmak üzere geçiş sırasında yeni saldırı tekniklerinin geliştirilmesi kaçınılmazdır. Bu metotlardan bazıları ağın genel yapısını koruma altına almakla birlikte, uçtan uca güvenlik veya sadece yönlendiricilerde ve son kullanıcılarda olmak üzere alt rutinleri de kapsamaktadır. Bu alt sınıfların IP kandırmacası ya da hizmet aksatma atakları gibi yöntemler ile yapıldığı belirlenmiştir. Bu amaçla sürecin getirdiği açıklıkları IPv4'den kazandığımız deneyim ile değerlendirerek korunma metodolojilerinin iyileştirilmesi gerekmektedir.

Bunun yanında Bölüm 2'de verilen solucan dağılımı başlığı ve alt başlıkları dikkat edilerek, koruma teknikleri geliştirilmesi, Bölüm 3'de verilen solucan yayılma modelleri ile Bölüm 4'de verilen solucan yayılma stratejileri dikkate alınarak ağ teknolojilerinin geliştirilmesi ve Bölüm 5'de verilen korunma metotlarının da hayata geçirilmesi ile IPv6 ağlarda yüksek seviyede bir korumanın sağlanması ancak mümkün olabilecektir.

IPv6 ağların bilgisayar ve gömülü bilgisayar sistemleri yanında pek çok uygulamayı destekleyeceği göz önünde bulundurularak, bu ağlarda bulunan farklı sistem, uygulama ve yaklaşımları ve geçiş mekanizmalarının değerlendirilmesi ve bunlara yönelik daha kapsamlı araştırmaların yapılması gereklidir.

IPv6 projesi [4] kapsamında geliştirilen balküpü yazılımı (KOVAN)'nın yapılacak bu tür çalışmalara altyapı oluşturması yapılabilecek yeni pek çok araştırma altyapısı sunması sebebiyle IPv6 ağlarda solucan dağılımı saldırılarının denenmesi ve uygun önlemlerin geliştirilmesine katkılar sağlayacağı değerlendirilmektedir.

VII. TEŞEKKÜR

Bu çalışma, TÜBİTAK-KAMAG 108G100 nolu proje kapsamında desteklenmiştir. Projeye maddi desteklerinden dolayı KAMAG başkanlığına ve projeye verdikleri önem ve destek için Bilgi Teknolojileri ve İletişim Kurumu proje ekibine şükranlarımızı sunarız.

KAYNAKLAR

[1] Ş. Sağıroğlu, O. Bektaş, M. Soysal, "Güvenlik Penceresinden IPv4/IPv6 Karşılaştırılması", 3. Uluslararası Katılımlı Bilgi Güvenliği ve Kriptoloji Konferansı, (132-138), Ankara, 2010

[2] C.E. Caicedo, J.B.D. Joshi, S.R. Tuladhar, "IPv6 Security Challenges," *IEEE Computer Society*, Vol.42, No.2, Pp.36-42, 2009.

[3] K. J. Higgins, İnternet: http://www.Darkreading.Com/Vulnerability-Management/167901026/Security/Perimeter-Security/227300083/Ipv6-Transition-Poses-New-Security-Threats.Html, 13.02.2012

[4] Ulusal IPv6 Protokol Altyapısı Tasarımı Ve Geçişi Projesi, Bağlantı: http://www.ipv6.net.tr/, 28.02.2012.

[5] Ulusal IPv6 Protokol Altyapısı Tasarımı Ve Geçişi Projesi, Dönem 2 Raporu, *TÜBİTAK, KAMAG*, 20.06.2010.

[6] M. Y. Soylu, E. Kızılkaya, A. S. Çetin, C. Gencer, Ş. Sağıroğlu, "IPv4'den IPv6'ya Geçiş için Örnek Bir Karar Destek Sistemi Modeli: GEMKAR", *1. Ulusal IPv6 Konferansı*, Ankara, 2011

[7] Y. Gökırmak O. Bektaş M. Soysal, S. Yiğit, "Sanal IPv6 Balküpü Ağı Altyapısı: Kovan", *Ulusal IPv6 Konferansı*, Ankara, 2011.

[8] D. A. Ray, C. B. Ward, B. Munteanu, J. Blackwell, X. Hong, and J. Li., "Investigating The Impact of Real-World Factors on Internet Worm

Propagation". *In Proceedings of The 3rd International Conference on Information Systems Security* (ICISS'07), 2007.
[9] Z. Chen , C. Ji, "A Self-Learning "Worm Using Importance Scanning", Proceedings Of The 2005 ACM Workshop on Rapid Malcode, Fairfax, VA, USA, November 11, 2005.
[10] C. C. Zou , W. Gong , D. Towsley, "Code Red Worm Propagation Modeling and Analysis", *Proceedings of The 9th ACM Conference on Computer and Communications Security*, Washington, DC, USA , November 18-22, 2002.
[11] D. Moore, C. Shannon , K. Claffy, "Code-Red: A Case Study on The Spread and Victims of An Internet Worm", *Proceedings of The 2nd ACM Sigcomm Workshop on Internet Measurement*, Marseille, France , November 06-08, 2002.
[12] S. Staniford, D. Moore, V. Paxson, N. Weaver, "The Top Speed of Flash Worms", *Proceedings of The 2004 ACM Workshop on Rapid Malcode*, Washington DC, USA, October 29-29, 2004,
[13] C. Wong, S. Bielski, J. M. Mccune, C.i Wang, "A Study of Mass-Mailing Worms", *Proceedings of The 2004 ACM Workshop on Rapid Malcode*, Washington DC, USA, October 29-29, 2004.
[14] S. Antonatos , P. Akritidis , E. P. Markatos , K. G. Anagnostakis, "Defending Against Hitlist Worms Using Network Address Space Randomization", *Proceedings of The 2005 ACM Workshop on Rapid Malcode*, Fairfax, Va, USA, November 11-11, 2005.
[15] A. Kamra, H. Feng, V. Misra and A. D. Keromytis, "The Effect of Dns Delays on Worm Propagation İn An IPv6 Internet", *IEEE Infocom 2005*, Miami, USA, 2005.
[16] X. Yangui, Z. Jiachun, "Worm Detection İn An IPv6 Internet" International Conference on Computational Intelligence and Security, 366-370, *IEEE*, 2009
[17] Y. Tang J. Luo B. Xiao G. Wei, "Concept, Characteristics and Defending Mechanism of Worms", *IEICE Transactions on Information and Systems* Vol.E92-D No.5 (799-809), 2009.
[18] S. M. Bellovin, A. Keromytis, B. Cheswick. "Worm Propagation Strategies in an IPv6 Internet", *Login*, Pages 70-76, 2006.
[19] A. Kamra, H. Feng, V. Misra, A. D. Keromytis. *In Proceedings of IEEE Infocom*, Vol. 4, Pp. 2405 - 2414. 2005.
[20] P. Li, M. Salour, X. Su, "A Survey of Internet worm Detection and Containment", *IEEE Communications Survey*, 1st Quarter 2008, Volume 10, No. 1, 2008.
[21] A. Kamra, H. Feng, V. Misra, A. D. Keromytis. *In Proceedings of IEEE Infocom*, Vol. 4, Pp. 2405 - 2414. 2005.
[22] Q. Zheng, T. Liu, X. Guan, Y. Qu, and N. Wang. "A New Worm Exploiting Ipv4-IPv6 Dual-Stack Networks", *In Proceedings of The 2007 ACM Workshop on Recurring Malcode* (Worm '07). ACM, New York, Ny, USA, 2007.
[23] C. C. Zou, D. Towsley, W. Gong, S. Cai, "Routing Worm: A Fast, Selective Attack Worm Based on IP Address Information", *Principles of Advanced and Distributed Simulation*, 2005.
[24] P.K. Manna, S. Chen, S. Ranka, "Exact Modeling of Propagation For Permutation-Scanning Worms," *The 27th Conference on Computer Communications,* Infocom 2008, *IEEE* , Vol., No., (1696-1704), 13-18 April 2008.
[25] K. Deguang, J. Yoon-Chan, G. Tao, Z. Sencun, L. Peng, X. Hongsheng, "Sas: Semantics Aware Signature Generation For Polymorphic Worm Detection", *International Journal of Information Security*, Vol:10-5, (269-283), Oct 2011.
[26] K. Johannes, K. Stefan, S. Christian, V. Helmut, "Proactive Detection of Computer Worms Using Model Checking", *IEEE Transactions on Dependable and Secure Computing*, Vol: 7-4, (424-438), Dec 2010.
[27] B. Chen, F. Bin-Xing, Z. Jun, Y. Xiao-Chun, "Monitoring Network and Defending Against Worm Attacks", *Dynamics of Continuous Discrete and Impulsive Systems-Series B-Applications & Algorithms*, Volume: 13e-S, (3363-3368), Dec 2006.
[28] M. Avlonitis, E. Magkos, M. Stefanidakis and V. Chrissikopoulos, "Treating Scalability and Modelling Human Countermeasures Against Local Preference Worms Via Gradient Models", *Journal in Computer Virology*, Volume 5, Number 4, (357-364), 2008.
[29] Ş. Sağıroğlu, E. N. Yolaçan, U. Yavanoğlu, "Zeki Saldırı Tespit Sistemi Tasarımı Ve Gerçekleştirilmesi", *J. Fac. Eng. Arch. Gazi Univ.*, Vol 26, No 2, (325-340), 2011.
[30] M. Cai, K. Hwang, J. Pan, C. Papadopoulos, "Wormshield: Fast Worm Signature Generation With Distributed Fingerprint Aggregation" *IEEE Transactions on Dependable and Secure Computing*, Vol. 4, No. 2. (88-104), Apr.-June 2007
[31] D. Ping, N. Akihiro, "DDOS Defense Deployment With Network Egress and Ingress Filtering", *IEEE International Conference on Communications Book Series*, 2010
[32] N. Joukov, T.-C. Chiueh, "Internet Worms As Internet-Wide Threat", Technical Report. *Department of Computer Science, Stony Brook. University*. Stony Brook, NY, USA. 2003 (2003)
[33] Y. Lee, S. Shin, S. Choi, and H.-G. Son. "IPv6 Anomaly Traffic Monitoring with IPfix". *In Proceedings of The Second International Conference on Internet Monitoring and Protection* (ICIMP '07), 2007



Uraz Yavanoğlu Ankara doğumludur. Atılım Üniversitesi Bilgisayar Mühendisliği Bölümünden mezun olmuştur. 2009 yılında Gazi Üniversitesi Mühendislik Fakültesi Bilgisayar Mühendisliği Bölümünden yüksek lisans derecesi almıştır. Aynı bölümde Araştırma Görevlisi olarak çalışmakla birlikte Gazi Üniversitesi Elektrik Eğitimi bölümünde doktora çalışmalarına devam etmektedir. Araştırma konuları arasında yapay sinir ağları, insan bilgisayar etkileşimi ve bilgi güvenliği yer almaktadır.



Suat Özdemir Gazi Üniversitesi Mühendislik Fakültesi Bilgisayar Mühendisliği bölümü öğretim üyesidir. Kablosuz ağlar, güvenlik ve veri madenciliği alanlarında çalışmaları bulunmaktadır.



Şeref Sağıroğlu Gazi Üniversitesi Mühendislik Fakültesi Bilgisayar Mühendisliği Bölümü öğretim üyesidir. Zeki sistem kimliklendirme, tanıma ve modelleme, ve kontrol; yapay sinir ağları ve yapay zeka uygulamaları; sezgisel algoritmalar; endüstriyel robotlar; zeki anten analizi ve tasarımı; internet, web ve bilişim sistemleri ve uygulamaları; yazılım mühendisliği; bilgi ve bilgisayar güvenliği; biometri, elektronik ve mobil elektronik imza ve açık anahtar altyapısı; kötücül ve casus yazılımlar gibi konularında çalışmaktadır. 50'nin üzerinde SCI tarafından taranan uluslararası dergilerde yayımlanmış makalesi, 50'nin üzerinde ulusal dergilerde yayımlanmış makalesi, 100'ün üzeride uluslararası konferans ve sempozyum bildirisi ile ulusal sempozyum, konferans ve çalıştaylarda sunulmuş 100'e yakın bildirisi bulunmaktadır. 3 adet alınmış patenti vardır. 5 adet yayımlanmış kitabı, 2 adet kitapta bölüm yazarlığı bulunmaktadır. 4 kitabında editörlüğünü yapmıştır.

Ulusal ve uluslararası pek çok projeler yürütmüş ve konferanslar düzenlemiş olup, akademik çalışmalarına devam etmektedir.

An Application of Decision Trees in Intrusion Detection

Atilla Özgür,Hamit Erdem

***Abstract*—Easily reachable decision Tree algorithm J48 is trained on widely used Intrusion Detection KDD99 dataset and its results are reported. According to our results ; we conclude that using training KDD99 dataset without any preprocessing gives too good results. Even though Intrusion Detection System's performance on KDD99 dataset should be taken into account, this performance is not gold standard, and should not be thought as Intrusion Detection System will perform equally well in real system.**

***Index Terms*—Security, Intrusion Detection Systems, Machine Learning, Decision Trees,KDD99.**

I. Introduction

IN the new global economy, Information technology (IT) has become a central issue for institutions and governments. As usage of IT increases, IT security becomes increasingly important. Intrusion Detection systems are widely used and important part of any IT security. According to CSI Survey [4] ,IDS usage is over %60 percent. But IDS are still open problem for researchers [21].

The objectives of this research are to show that using *KDD99 dataset without any preprocessing* in IDS research does not imply that proposed IDS will be useful in real systems.

For this purpose this paper has been divided into four parts. The first part deals with Need for Intrusion detection and definition of Intrusion Detection. In second part Decision Trees are explained. Related work is given in third part. In fourth part, we explain KDD99 data set characteristics. Widely used decision tree algorithm of J48 is trained on 10% KDD99 training dataset. Trained algorithm is tested on 10% KDD99 training dataset, full KDD99 training dataset and KDD99 test dataset. In the last part, we compare our results with previous results in literature and assert our claim.

A. Need For Intrusion Detection

Theoretical background of computer viruses were introduced by Neumann in an article "Theory of self-reproducing automata" in 1966. [15] .

From the first known virus in 1971 to 2010, security vulnerabilities are increasing in their size and cost. They cost billions of dollars to government and corporates a like. Cracking which began as a hobby is becoming tool for corporates, mafia and armies. [24], [3]

Atilla Özgür is a PHD Student in the Department of Electrical Engineering, Baskent University
Hamit Erdem is a Associate Professor in the Department of Electrical Engineering, Baskent University

Cyber attacks increase can be seen in figure 1. Figure 1 shows that cyber attacks will not decline in foreseeable future therefore security products , especially intrusion detection systems will gain more and more importance.

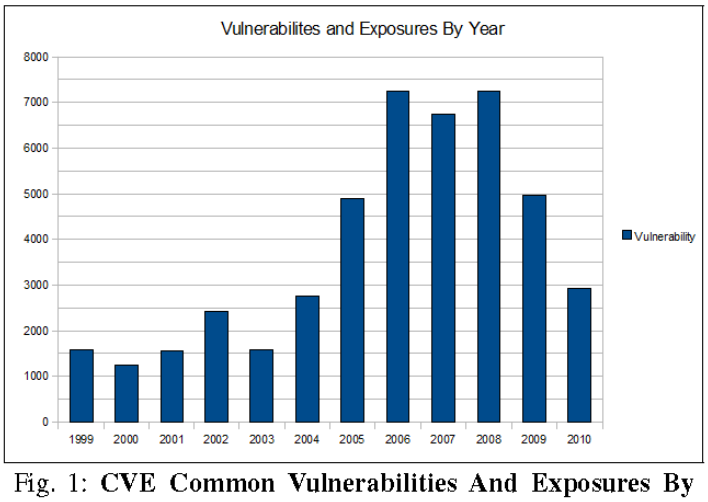


Fig. 1: **CVE Common Vulnerabilities And Exposures By Year**

[1]

B. Intrusion Detection Definition

We will classify Intrusion Detection Systems (IDS) according to NIST Report , Guide to Intrusion Detection and Prevention Systems [20] . According to NIST's guide

> Intrusion detection is the process of monitoring the events occurring in a computer system or network and analysing them for signs of possible incidents , which are violations or imminent threats of violation of computer security policies , acceptable use policies, or standard security practices.

Intrusion Detection systems are classified most of the time in two ways.

- According to deployment of systems
- According to detection methodology.

According to deployment, IDS systems are Network Intrusion Detection and Host Intrusion Detection Systems. While according to detection , Signature based IDS and Anomaly based IDS systems.

Signature based IDS, are similar to virus detection. They keep signatures of well known attacks in their attack databases and classify instances according to this signature.

[1] Note that: CVE Data is from 08-2010 so it does not show all vulnerabilities for 2010 [14] .

While anomaly based systems define what is normal , then classify instances as normal or anomaly (attack).

Intrusion detection problem can be considered as classic classification problem. For example given features of network connection, classify each network connection as normal or attack.

II. Decision Trees

A. Decision Tree-Classification Tree Introduction

Decision Tree or Classification Trees are well known classification method in statistical learning and data mining community. It is called work horse of data mining [25] since it is one of most used method in data mining [27]. Reasons for this :

- Decision Tree is very fast to train and test
- Decision Tree results are very easy to understand by human operators
- Decision Tree results are very easy to visualize
- Decision Tree results can be used to mine rules

in figure 2 , an example classification of well known Iris Dataset [6] with decision tree can be seen. As you can see it is very easy to understand Decision Trees.

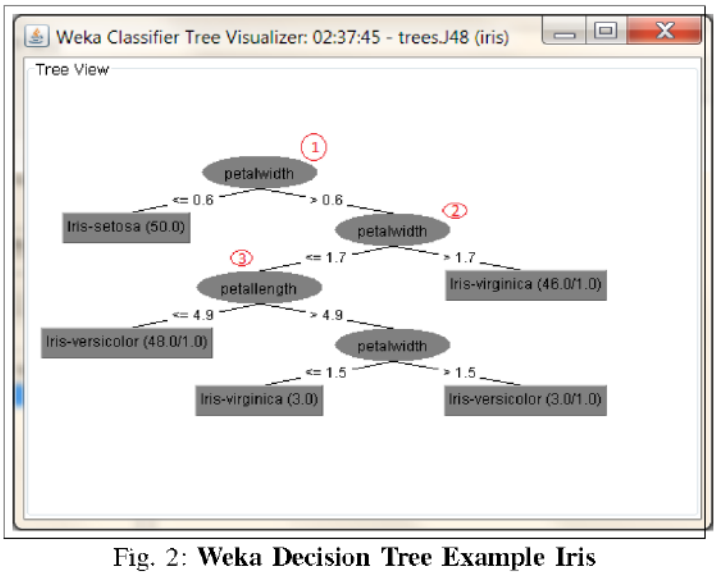


Fig. 2: **Weka Decision Tree Example Iris**

1) Mathematical Definition: Classification and regression are two important problems of statistics. Let x be input feature vector denoted by

$x = x^{(1)}, x^{(2)}, \ldots, x^{(m)}$ where $x^{(m)}$ is m_{th} dimension of x vector and X be domain of x vectors.

Let y be response variables and Y is domain of y. A classification or regression problem is finding a function which maps x values to y such that $f(x) = y$. If y is continuous valued such as house prices then this problem is regression problem on the other hand if y is discrete values for example $y \in S = \{DOS, R2L, U2R, Probe, Normal\}$ then this problem is classification problem. If y is binary valued like $\{0, 1\}$ or $\{attack, normal\}$ then it is binary classification problem.

There can be infinite number of mappings from X to Y. Therefore we need a training set for choosing f(x) among this possibilities. The training set is n number of instances (observations,examples) of (x,y) pairs.

We can also write this problem as

$$\hat{f}\left(\begin{bmatrix} x_1^1 & x_1^2 & \ldots & x_1^m \\ x_2^1 & x_2^2 & \ldots & x_2^m \\ \ldots & \ldots & \ldots & \\ x_n^1 & x_n^2 & \ldots & x_n^m \end{bmatrix}\right) = \begin{bmatrix} y_1 \\ y_2 \\ \ldots \\ y_n \end{bmatrix}$$

We would like to find $\hat{f}$ function which maps X to Y.

2) Graphical Definition: A decision tree partitions input space into linear parts. For example figure 2 node 1, $petalwidth \leq 0.6$ corresponds to figure 3 line 1. Also decision 2 corresponds to line 2 and decision 3 to line 3. When we go to higher dimension visualization becomes impossible but intuition stays same.

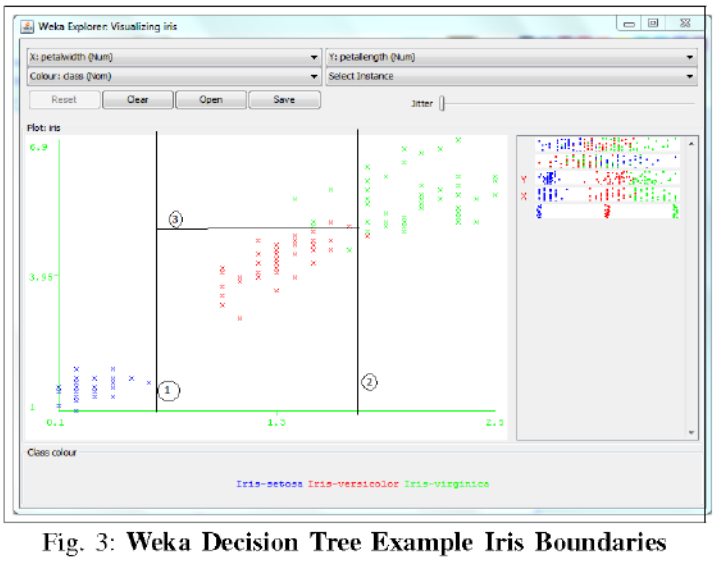


Fig. 3: **Weka Decision Tree Example Iris Boundaries**

B. Decision Tree Algorithm

Constructing a optimal decision tree even for simple task is a NP-Complete [8]. Therefore almost all algorithms use heuristic search algorithms. There are a lot of different algorithms but two families are best known and widely used. These are CART [1] and C4.5 [18] families.

CART is introduced in 1984 by Breiman et al. It is commercialized by Salford Systems and only provided in binary form.

C4.5 is introduced by Quinlan in 1993 [18]. Its predecessor is ID3 algorithm and it is preceded by C5.0. Although source code for both C4.5 and ID3 exists, C5.0 is commercialized and not all of its improvements are published. A java version of C4.5, J48 exists. It is based on source code of C4.5 and published improvements of C5.0 therefore J4.8 (a Java version between 4.5 and 5.0). It is embedded in popular data mining tool weka [7]. This work uses J4.8 in its experiments.

A decision tree algorithm has three major task [12]

1) how to partition data in each step
2) when to stop partitioning
3) how to predict the value of y for each x in a partition.

1) Partition Data: First part is accomplished using a impurity functions. We would like to partition our heterogeneous data to more homogeneous data. Therefore we use functions called impurity function , these functions evaluate heterogeneity, impurity of our data. If our impurity reduce from one node to other node we choose this split.

Impurity functions can be following functions

1) $Entropy = -\sum_{i=1}^{m} p_i log_2(p_i)$
2) $giniindex = 1 - \sum_{j=1}^{2} p_j^2$

using impurity functions they partition input space with following algorithm

Listing 1: Partition Data Pseudo Code

```
impurityReduction = 0
featureToSplit = None
featureSplitValue = None

for (feature in featureVector)
        for (splitPoint in feature)
                tempImpurityReduction = impurity(
                    feature, splitPoint);
                if ( tempImpurityReduction>
                    impurityReduction)
                        impurityReduction =
                            tempImpurityReduction
                        featureToSplit = feature
                        featureSplitValue =
                            splitPoint
```

For every feature , and every point in feature it calculates impurity function and find max impurity reduction. It splits input space according to this feature and split point.

2) Stop Partitioning Data: Most algorithm stop partitioning data according to following.

1) Minumum Number of Instances: If partitioned data is reduced below to given minimum number of instances, stop Partitioning.
2) Maximum tree depth, if a tree depth is bigger than this number stop Partitioning.

But CART [22] and C4.5 [12] does not use this stopping criteria. Instead they fully grow tree then prune it. This gives better training and testing error [22]. Indeed CART and C4.5 are mostly different in their impurity function usage and their pruning strategies [12].

3) Predict Value : Most easy to answer is last one, how to predict: most of the time majority voting is used. That is if node contains 7 attack, 3 normal then this node predicts attack.

III. Related Work

A. Decision Tree-Classification Tree Reviews

Data mining-based intrusion detectors: Wu et al used Decision Trees in their paper [26]. They have compared Decision Trees (C4.5) with Support Vector Machines. They used 10 percent version of KDD99 data set. Their preprocessing is as follows:

> Based on the normal proportion, select each 10,000 group of data where normal proportion is 10%, 20%, 30%, . . ., 90% in training dataset and test dataset; and make remaining data, namely attack data, even and sample them.

They used weka for Decision Trees, libsvm for Support Vector Machines.

They give various Comparison of Detection Rate, False Alarm Rate between SVM,KDD99Winner and Decision Tree (C4.5) and find that Decision Tree is better in most situations. Because of their 10 different experiments, they get widely different results between %40 and %90.

Using an improved C4.5 for imbalanced dataset of intrusion: This article [17] is mostly about KDD-DARPA imbalance problem.

Decision Tree algorithm C4.5 is less sensitive to oversampling but more sensitive to under sampling. To overcome this problem and detect rare attacks they propose a modification to C4.5 which they call PC4.5 (parametrized).

They experiment with KDD99 %10 data set. They use 2 layered architecture. First layer detects the large class (include normal, smurf and neptune), and combine other classes into mix attack. They find that C4.5 is better for first layer detection than other machine learning methods

> For the first level, we use C4.5, Naive Bayes, BayesNet, SVM, KNN to train the set and use ten-cross validation to evaluate. The result demonstrates that C4.5 is more suitable to the datasets than others.

In the second layer they detect 20 classes from mix attack. They compare their PC4.5 with C4.5 in their results, give accuracy , F-Measure and number of leaves (decision tree)

They use weka for their experiments. They do not give accuracy for total but give results for individual attacks, which changes between %58 to %100. They report very good results on DOS and Probe attacks, over %95 percent.

Why machine learning algorithms fail in misuse detection on KDD intrusion detection data set: Sabhani and Serpen [19] shows why machine learning algorithms are unsuccessful, aside from probe and DOS attacks. DOS and probe attacks are statistically similar to each other in Test and Train environments while other attacks are very different. They also review literature and shows that although ML algorithms seems to be successful overall they are not very good on R2L and U2R attacks.

Effective Value of Decision Tree with KDD 99 Intrusion Detection Datasets for Intrusion Detection System

Lee et al [**?**] work's title claim to work in KDD 99 dataset but in article they preprocess DARPA tcp dump data. Since KDD99 also pre-process DARPA tcp dump data, theoretically they should use same features. They only use features from one connection, ignore multiple connections features. This type of pre-processing is not enough to catch all attack in DARPA dumps See [10] for details. They compare their detection rate with those of Lee at al [10]. Their work shows some improvements in DoS and Scan attacks but it loses to R2L and U2R attacks.

	train data set 10 percent	train data set full	test data set full
Total Number of Instances	494021	4898431	311029
Correctly Classified Instances	493931	4897566	285340
Correctly Classified Instance Percentage	99.9818%	99.9823%	91.7406%
Incorrectly Classified Instances	90	865	25689
Incorrectly Classified Instance Percentage	0.0182%	0.0177%	8.2594%
Kappa statistic	0.9997	0.9997	0.87
Mean absolute error	0	0	0.0041
Root mean squared error	0.0029	0.0028	0.0641
Coverage of cases (0.95 level)	99.9874%	99.986%	91.7442%

TABLE I: Summary Results of J48 Classifier

IV. Experiments

KDD-DARPA dataset is a simulated dataset intended to be similar to US Air Force network. First DARPA sponsored IDS event accomplished by MIT Lincoln LAB in 1998. [5]

After one year, in 1999 , they repeated same event with improvements suggested by Computer Security Community. [11] Same dataset is chosen by KDD in their yearly competition. After KDD, intrusion detection system research really took off in knowledge discovery and data mining community. Although its problems widely known [13],[2] KDD99 - Darpa data set is most used data set in Intrusion Detection Data Mining Research [23]

DK99C (DARPA-KDD99 Cup Dataset) is already preprocessed dataset, see Lee [10] for details. Training dataset of KDD99 consists of about 4 million records of 22 attacks and normal instances. This data set is widely imbalanced about 80% of dataset is attack instances. Every attack in this data set belong to 4 major groups.

- R2L - Root to Local
- U2R - User to Root
- DOS - Denial of Service
- Probe - Probing attacks

For more information about used attacks in DK99C see Kendall [9]

Darpa Intrusion Detection and KDD99 dataset is most widely used dataset in IDS literature , Tavallaee et al [23] surveyed 276 studies mostly in indexed journals. Of these studies 67 (%24) employs DARPA, 77 (%28) employs KDD99 , 41 (%15) injects other attacks to this dataset and 86 (%31) does not disclose any data. Only 16 (%6) employs other datasets.

Although Weka [25] can read a lot of different formats, it works best with its own arff format. I have changed provided KD99 data set to arff format , see [16] for details.

After that We train our classifier on 10 percent dataset, see code listing 2. Then we test it on all of our three datasets, see code listing 3

We get following results. Note that results are actually much larger , but we only show summary results as can be seen in table I

V. Results

We train our J48 decision tree on KDD99 Training %10 percent data set and then test its performance on three different data set. These are KDD99 Training %10 percent data set, KDD99 Training full data set and KDD99 Test data set.

First result of Classifier's performance of 99.9818 % is normal. Since this data set is our training data set. We test our classifier performance on our training data set. Effectively this means that we almost memorized this data set.

Second result of Classifier's performance of 99.9823 % is almost unbelievable. We used 10% of this data set to train but our algorithm did not see other 90% of this data. We can only conclude that this other 90% is very similar to used 10%. Indeed it is the case, KDD99 data set consists of is simulated attacks,[9].

Third result of Classifier's performance of 91.7406 % . Here we see a drop in performance. KDD99 test data set's class distribution is different than training data set distribution. Still most of the attacks are similar therefore our classifier is able to attain accuracy of 91.7406 %.

VI. Conclusion

We have shown that it is very easy to get %90 accuracy in KDD99 dataset. We used %10 KDD99 dataset as our training data set and trained J48 classifier on it. After that we tested our classifier on KDD99 full, KDD99 test datasets. We obtained %99 and %91 accuracies. These results with easily obtainable ML Algorithm , Decision Tree, clearly shows simulation nature of KDD99. KDD99 dataset should not be used without preprocessing in IDS research. Although it is still useful as ML test bench as Large Data.

The current study has only examined Decision Tree Learning Algorithm. Therefore further work needs to be done to establish whether other Machine Learning Algorithms show similar behavior.

VII. Appendix

Listing 2: weka command line to save model J48

```
@ECHO OFF
REM -t <file> specifies the training file
REM -T <file> specifies the test file
REM -p <attribute range> for outputting predictions
    (if a test file is present, then for this one,
    otherwise the train file)
REM -d <file> and -l <file> for saving and loading
    serialized models


echo %time%
%java_command% weka.classifiers.trees.J48 -t
    data/kddcupTrainData10PercentCorrrected.arff -d
    "models/J48KddcupTrainData10PercentCorrrected.
    model"
echo %time%
```

```
@ECHO OFF
REM -t <file> specifies the training file
REM -T <file> specifies the test file
REM -p <attribute range> for outputting predictions
    (if a test file is present, then for this one,
    otherwise the train file)
REM -d <file> and -l <file> for saving and loading
    serialized models

echo %time%
%java_command% weka.classifiers.trees.J48 -T
    data/kddcupTrainData10PercentCorrrected.arff -l
    "models/J48KddcupTrainData10PercentCorrrected.
    model"
echo %time%
%java_command% weka.classifiers.trees.J48 -T
    data/kddcupTrainDataFullCorrected.arff -l "
    models/J48KddcupTrainData10PercentCorrrected.
    model"
echo %time%
%java_command% weka.classifiers.trees.J48 -T
    data/kddCupTestDataLabeled.arff -l "
    models/J48KddcupTrainData10PercentCorrrected.
    model"
echo %time%
```

REFERENCES

[1] Leo Breiman, Jerome Friedman, Charles J. Stone, and R.A. Olshen. *Classification and Regression Trees*. Chapman and Hall/CRC, 1984.

[2] S.T. Brugger. Kdd cup'99 dataset (network intrusion) considered harmful. *KDnuggets newsletter*, 7(18):15, 2007.

[3] T.M. Chen and J.M. Robert. The evolution of viruses and worms. *Statistical methods in computer security*, 2004.

[4] CSI. 2010-2011 computer crime and security survey. Technical report, CSI, 2011.

[5] R. K. Cunningham, R. P. Lippmann, D. J. Fried, S. L. Garfinkel, I. Graf, K. R. Kendall, S. E. Webster, D. Wyschogrod, and M. A. Zissman. Evaluating intrusion detection systems without attacking your friends: The 1998 darpa intrusion detection evaluation. Technical report, MASSACHUSETTS INST OF TECH LEXINGTON LINCOLN LAB, 1999.

[6] Ronald Aylmer Fisher. The use of multiple measurements in taxonomic problems. *Annals of Eugenics*, 7:179–188, 1936.

[7] M. Hall, E. Frank, G. Holmes, B. Pfahringer, P. Reutemann, and I.H. Witten. The weka data mining software: an update. *ACM SIGKDD Explorations Newsletter*, 11 (1):10–18, 2009.

[8] L. Hyafil and R.L. Rivest. Constructing optimal binary decision trees is np-complete. *Information Processing Letters*, 5(1):15–17, 1976.

[9] K. Kendall. A database of computer attacks for the evaluation of intrusion detection systems. Master's thesis, MIT - Massachusetts Institute of Technology, 1999.

[10] Wenke Lee and Salvatore J. Stolfo. A framework for constructing features and models for intrusion detection systems. *ACM Trans. Inf. Syst. Secur.*, 3:227–261, November 2000. ISSN 1094-9224. doi: http://doi.acm.org/10.1145/382912.382914. URL http://doi.acm.org/10.1145/382912.382914.

[11] Richard Lippmann, Joshua W. Haines, David J. Fried, Jonathan Korba, and Kumar Das. The 1999 darpa off-line intrusion detection evaluation. *Comput. Netw.*, 34: 579–595, October 2000. ISSN 1389-1286. doi: 10.1016/S1389-1286(00)00139-0. URL http://portal.acm.org/citation.cfm?id=361116.361124.

[12] W.Y. Loh. Classification and regression tree methods. *Encyclopedia of statistics in quality and reliability*, 2008.

[13] J. McHugh. Testing intrusion detection systems: A critique of the 1998 and 1999 darpa intrusion detection system evaluations as performed by lincoln laboratory. *ACM Transactions on Information and System Security*, 3(4):262–294, 2000.

[14] mitre. Cve common vulnerability exposure list, 2010. URL http://cve.mitre.org/cve/.

[15] John Von Neumann. *Theory of Self-Reproducing Automata*. University of Illinois Press, Champaign, IL, USA, 1966.

[16] Atilla Özgür. Converting KDD99 C4.5 Dataset To Weka Arff. Technical report, Baskent University, 2012.

[17] Zhou Quan, Gu Lin-gang, Wang Chong-jun, Wang-jun, and Chen Shi-fu. Using an improved c4.5 for imbalanced dataset of intrusion. In *Proceedings of the 2006 International Conference on Privacy, Security and Trust: Bridge the Gap Between PST Technologies and Business Services*, PST '06, pages 67:1–67:4, New York, NY, USA, 2006. ACM. ISBN 1-59593-604-1. doi: http://doi.acm.org/10.1145/1501434.1501513. URL http://doi.acm.org/10.1145/1501434.1501513.

[18] R. Quinlan. *C4.5: programs for machine learning*. Morgan Kaufmann, 1993. ISBN:1-55860-238-0.

[19] Maheshkumar Sabhnani and Gursel Serpen. Why machine learning algorithms fail in misuse detection on kdd intrusion detection data set. *Intell. Data Anal.*, 8: 403–415, September 2004. ISSN 1088-467X. URL http://portal.acm.org/citation.cfm?id=1293805.1293811.

[20] K. Scarfone and P. Mell. Guide to intrusion detection and prevention systems (idps). *NIST Special Publication*, 800 (2007):94, 2007.

[21] Robin Sommer and Vern Paxson. Outside the closed world: On using machine learning for network intrusion detection. In *Proceedings of the 2010 IEEE Symposium on Security and Privacy*, SP '10, pages 305–316, Washington, DC, USA, 2010. IEEE Computer Society. ISBN 978-0-7695-4035-1. doi: http://dx.doi.org/10.1109/SP.2010.25. URL http://dx.doi.org/10.1109/SP.2010.25.

[22] Dan Steinber. *CART: classification and regression trees*, chapter 10, pages 179–201. CRC, 2009.

[23] M. Tavallaee, N. Stakhanova, and A.A. Ghorbani. Toward credible evaluation of anomaly-based intrusion-detection methods. *Systems, Man, and Cybernetics, Part C: Applications and Reviews, IEEE Transactions on*, 40 (5):516–524, sept 2010. ISSN 1094-6977.

[24] Wikipedia. Timeline of computer viruses and worms. Web, 2010. URL http://en.wikipedia.org/wiki/Timeline_of_computer_viruses_and_worms.

[25] I.H. Witten and E. Frank. *Data Mining: Practical machine learning tools and techniques (Third Edition)*. Morgan Kaufmann Pub, 2011.

[26] S.Y. Wu and E. Yen. Data mining-based intrusion

detectors. *Expert Systems with Applications*, 36(3):5605–5612, 2009.

[27] Xindong Wu, Vipin Kumar, J. Ross Quinlan, Joydeep Ghosh, Qiang Yang, Hiroshi Motoda, Geoffrey McLachlan, Angus Ng, Bing Liu, Philip Yu, Zhi-Hua Zhou, Michael Steinbach, David Hand, and Dan Steinberg. Top 10 algorithms in data mining. *Knowledge and Information Systems*, 14:1–37, 2008. ISSN 0219-1377.

A Two-Layer Fuzzy Genetic Algorithm for Designing Intrusion Detection System

Ghazaleh Javadzadeh, Reza Azmi

***Abstract*— In this paper we propose a two-layer hybrid fuzzy genetic algorithm for designing anomaly based intrusion detection systems. Our proposed algorithm is based on two basic Genetic Based Machine Learning Styles (i.e. Pittsburgh and Michigan). One of the advantages of our proposed algorithm is that, it supports multiple pattern classification; it means that the algorithm is able to detect five classes of network patterns consist of Denial of Service, Remote to Local, User to Root, Probing and Normal class. Our contribution is presenting a two-layer optimization approach based on Pittsburgh style and then combine it with Michigan style in first level. To improve the performance of proposed algorithm, also, we take advantage of memetic approach in second level. We test our algorithm on NSL KDD data set to be able to compare our work with previous ones. We use elitism to keep the efficiency of our algorithm, while using random patterns to produce various generations, in different iteration of genetic algorithm. This leads to faster convergence in the cases that initial random population is far from the optimal result. The simulation results show that our approach can converge to the classification accuracy about 98.2% and 0.5% false alarm, in 50 iterations.**

***Index Terms*—Computational Intelligence, Fuzzy Genetic, Intrusion Detection, Multiple Pattern Classification.**

I. Introduction

Intrusion Detection System (IDS) is a security tool that detects malicious behaviors, also called attacks. IDS monitors and analyzes the data within a computer or a network to detect and alerts the system if a potential attack is in progress. There are several detection methods that IDS use to detect intrusions. Two main detection methods are Signature-based (misuse) and Anomaly-based detection. In Signature based method, IDS compare data traffic with some predefined pattern of attacks, and if they match the traffic, they will be detected as attacks. In this method, rate of false alerts is reduced; however, attacks with new patterns cannot be detected. In Anomaly based detection methods, the traffic patterns detect as an attack if they do not match the normal traffic rules. In fact, a normal traffic rule defined in a system and IDS captures and compares the traffic with it. If a mismatch happens it means that an attack may be in progress. In this method more attacks with new patterns can be detected while we may encounter more false alarms too.

In most of the previous works the detection results in a binary state which means traffic indicates an attack or not. When the system detects an attack, it is very important to be able to recognize the type of that attack, because different type of attacks threat different security aspects. Some attacks disclosure the confidentiality of our assets; while some others altered integrity or availability of them. When we know the attack type, we can pick the most appropriate security mechanism to encounter it. The ability of performing multiple pattern classification is one of the most important features of our proposed algorithm. It means that the algorithm classifies the traffic patterns as normal, and other types of intrusion consist of Probing (PRB), Denial of Service (DoS), and User to Roots (U2R), and Remote to Local (R2L) attacks. Actually the type of attack will be determined in this kind of classification. M.F. Marhusin et al. believe that the continual changing nature of attacks requires a flexible defensive system that is capable of analyzing the enormous amount of traffic in a manner which is less structured [8], so the anomaly based IDS are able to detect new and more types of attacks. The difference between multiple pattern classification and binary pattern classification is illustrated in Fig. 1.

There are two challenging points in designing intrusion detection systems. The first one is the training algorithm of IDS. Recently, Computational Intelligence (CI) techniques have been successfully applied for developing IDS. The characteristic of CI systems, such as adaptation, fault tolerance, high computational speed, and error resilience in the face of noisy information, fit the requirements of building a good intrusion detection model [1]. Among all computational intelligence techniques, we have chosen a mixture of genetic algorithm as an evolutionary computational algorithm and fuzzy system to propose our algorithm. There are two main reasons for using fuzzy in IDS. First, there are many numeric attributes in the collected audit data and various derived many statistical measures. Second, since fuzzy logic deals with imprecise information and essence of the security includes fuzziness because boundaries between normal and abnormal are not well define [9].

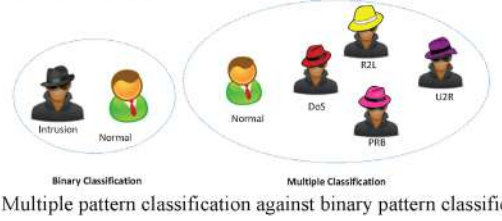


Fig. 1 Multiple pattern classification against binary pattern classification.

Manuscript Received March 8, 2012.

G.J. is with the Computer Department, Sharif University of Technology, International Campus, Kish Island (g-javadzadeh@kish.sharif.edu).

R.A. is with the Computer Department, Alzahra University, Tehran, Iran (azmi@alzahra.ac.ir).

Actually, we present a two-layer hybrid fuzzy genetic algorithm that generates a set of fuzzy rules to classify the network traffic patterns in multiple classification form.

The second challenging point in designing IDS is dataset. It is important to use a good dataset for testing and training the system. We use NSL KDD dataset that is an improved version of KDD Cup99 [10], to test our proposed algorithm.

NSL-KDD is a data set containing numeric and non-numeric values. In this dataset each row indicates a network traffic pattern, and each pattern consists of 41 attributes that are separated by comma from each other. Some important attributes are as follow: duration, protocol type, service, source and destination host, error rate, etc. Each pattern has a label that indicates the type of attack; so we involve a supervised learning in this algorithm.

Before we start using it, we normalized the numerical values of extracted patterns into numbers in interval [0,1]. Four different schemes of attributes normalization are introduced to preprocess the data for anomaly intrusion detection in [11]. We encounter 5 classes of pattern including four attack types and normal patterns. Below we briefly describe these classes:

1)Normal patterns produced by normal and usual behavior of a user such as visiting a web page, streaming a video and so on.

2)Denial of Service (DoS) class contains attacks that by using normal connections and behavior of a user in a massive amount try to down the system. This kind of attacks makes the system unable to service the authorized users.

3)Remote to User (R2L) is a class of attacks that exploit by a bug. These attacks make the remote user to access the account of a local user.

4)User to Root (U2R) class uses some vulnerability that makes the user to be able to gain root access.

5)Probing attack is any kind of effort for information gathering by scanning the target system or network to find its vulnerabilities. These vulnerabilities help the attacker to intrude the system.

The rest of this paper is organized as follows: In Section II Related Work is mentioned. Our proposed algorithm and simulation results are explained in Section III and IV, respectively. Section V is summary and conclusion.

II. RELATED WORK

In the literature, statistical techniques such as Hidden Markov Model, Multivariate Adaptive Regression Splines, Bayesian Classifier and Classification and Regression Tree (CART) have been applied to intrusion detection systems. These statistical approaches usually results in an inflexible detection that is unable to detect an attack if the sequence of events differ a little bit from the predefined profile. The continual changing nature of attacks requires a flexible defensive system that is capable of analyzing the enormous amount of traffic in a manner which is less structured; Using computational intelligence techniques provide this capability for intrusion detection systems.

According to classification mentioned in [1], in order to designing an algorithm for an IDS using computational intelligence we can apply the following techniques: Artificial neural networks, Fuzzy sets, Evolutionary computation, Artificial immune system, Swarm intelligence, Soft computing. Among these techniques Soft Computing has a particular place. In fact, soft computing is the method in which, combination of other computational intelligence techniques are used. As a soft computing technique, we have chosen a mixture of fuzzy system and genetic algorithm. We mention the reason of choosing fuzzy in first section. Also we choose Genetic Algorithm (GA) as an evolutionary algorithm includes search algorithms that are inspired from biological evolution as problem-solving strategy by using some natural mechanism such as selection, crossover, and mutation. As mentioned in [7] GA's are search algorithms that theoretically and empirically have proven to be a great capability in complex space in search and optimization problems, so, are commonly used in pattern classification problems. Also brilliant characteristic of genetic algorithm, such as automatic optimizing, global researching, and adaptability, is the reason for choosing it.

Several Fuzzy Genetic Based Machine Learning (GBML) Algorithms have been proposed for designing fuzzy rule-based systems. Fuzzy GBML algorithms can be classified into two main categories: Pittsburgh and Michigan. Nojima et al. developed two Genetic Based schemes for the design of fuzzy rule-based classification systems [2]. A parallel genetic local search algorithm is presented in [3]. According to that paper, an important solution to reduce the false alarm rate in detection intrusions is fuzzy logic. This algorithm produces fuzzy rules for network intrusion detection systems. The system use Michigan style. In that algorithm, the total population is divided into subpopulations. Each subpopulation contains the same class fuzzy rules. Also M.E. Cintra and H. de Arruda Camargo in [12] named Rule Based definition as one of the most important and difficult tasks in designing fuzzy systems. They introduce a fuzzy rule base generation method using genetic algorithm. That algorithm includes a phase of pre-selection of candidate rules that has been proposed by the authors. The use of a self-adaptive algorithm for the fitness calculation in genetic algorithm is proposed as an improvement of the mentioned method. In these algorithms, we encounter indirect search ability, which reduces the performance.

Another intrusion detection approach that extracts accurate and interpretable fuzzy rules for classification has been proposed in [13]. They use a statistical pattern recognition approach to design an intrusion detection system. These rules are obtained from network traffic data. They evaluated their approach using KDD CUP 99 and compare the results with some well-known classifiers. In that paper fuzzy rule generation strategy is discussed. But, there seems to be no

consensus on the results, since the tests have been done on KDD CUP 99.

Also, a new genetic fuzzy logic method for automatic rule generation has been proposed by the authors of [14]. The algorithm automatically adjusts the crossover rate and the mutation rate using rules based on populations diversity and evolutionary speed. The simulation results in this paper indicate that the algorithm is practical and effective, but the convergence is not fast.

A hybrid algorithm proposed by H. Ishibuchi in [4] that take the advantages of the two fuzzy GBML styles. The base of the algorithm is Pittsburgh style. Also a single iteration of Michigan style is applied to each rule set after that the Pittsburgh style is over. Another hybrid algorithm was proposed in [5] for designing fuzzy rule based systems for pattern classification problem. This algorithm is also a combination of two GBML styles. The experimental results show that, this algorithm has high search ability that Michigan and Pittsburgh styles. To obtain better tradeoff between the accuracy of the system and its complexity, the algorithm should be extend to the multi objective design of fuzzy rule-based classification system.

A genetic fuzzy system is proposed in [15] and the authors compared it with other approaches in intrusion detection systems. As simulation results in literatures show, it seems that because false alarm rate in genetic fuzzy system based intrusion detection is lower than other approaches, IDS which develops using genetic fuzzy systems would be more reliable than other approaches.

So, as the related work indicates fuzzy genetic based algorithms are suitable for developing intrusion detection systems. We decide to propose a fuzzy GBML algorithm that covers the main problems of literature such as false alarm rate, multiple classification support, and convergence speed. We get the main idea of combining two fuzzy GBML styles and propose an algorithm that supports multiple attack classification. Also we try to reduce the false alarm rate while provide fast convergence.

III. PROPOSED ALGORITHM

We propose a fuzzy genetic algorithm that generates a set of fuzzy rules to classify the network traffic patterns in multiple classification form, for designing Intrusion Detection Systems. Our proposed algorithm is a combination of two GBML styles (i.e. Michigan and Pittsburgh); by this means it would be possible to use the advantage of both styles such as direct optimization of rules, high search ability, and at the same time shorter computational time [6]. In fuzzy genetic algorithms, each individual can be a rule or rule set depends on the approach. Pittsburgh style handle the rule sets as individual while rules are considered as individual in Michigan. In subsection *A* the procedure of rule generation is described. This process is one of the important steps in our proposed algorithm. The proposed algorithm is presented in subsection *B*.

A. Fuzzy Rules

In fuzzy genetic algorithms, each individual can be a rule or rule set depends on the approach. Pittsburgh style handle the rule sets as individual while rules are considered as individual

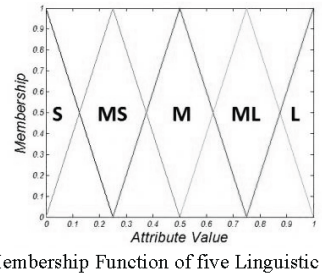


Fig. 2 Membership Function of five Linguistic Values [7].

in Michigan. In this section, the procedure of rule generation is described. This process is one of the important steps in our proposed algorithm.

In our proposed algorithms we use fuzzy rules of the following type:

R_i: if x_1 is A_{i1} & … & x_n is A_{in} then Class C_i with CF_i, (1)

i=1, 2…, n

Where R_i is a fuzzy rule and x_i refers to the ith feature of the corresponding pattern, A_{in} is an antecedent fuzzy set with linguistic label, C_i is a consequent class and CF_i is a rule weight.

In this stage we started to find the class of each rule according to [11]. To do so, the compatibility of antecedent fuzzy rules with the random pattern is calculated by equation (2).

$$\mu_i(x_p) = \mu_i(x_{p1}) \times \ldots \times \mu_{in}(x_{pn}),\ p = 1, 2, \ldots, m \quad (2)$$

Where $\mu_{in}(.)$ is the membership function of A_{in} that achieve from five linguistic values shown in Fig. 2 and m is number of patterns. As shown in Fig. 2 we use five fuzzy partitions as linguistic values. Consequence class of each rule determine according to equation (3).

$$\beta_{Class\hat{n}_i}(R_i) = \max\{\beta_{Class1}(R_i), \ldots, \beta_{Classh}(R_i)\} \quad (3)$$

Where,

$$\beta_{Classh}(R_i) = \frac{\sum_{x_p \in class\ h} \mu_j(x_p)}{N_{Class\ h}} \quad (4)$$

h = 1,2,..5 (number of classes)

Each of the fuzzy rules in the final classification has a certainty grade (class weight), that means the strength of that fuzzy rule and calculated according to:

$$CF_j = \frac{(\beta_{Class\hat{n}_i}(R_i) - \bar{\beta})}{\sum_{h=1}^{5} \beta_{Classh}(R_i)}, \quad (5)$$

Where,

$$\bar{\beta} = \sum_{h \neq h_i} \beta_{Class_h}(R_i) / (5-1) \quad (6)$$

Certainty grade of each fuzzy rule is a number in [0,1] interval that indicates accuracy amount of consequence part of a rule according to the accuracy of antecedent part of that rule. Accordingly, rules can be generated. Also rule sets are a group of rules which can be formed by using above instructions.

After generating N_{pop} rule sets with N_{rule} fuzzy rules as initial population using the above instruction (N_{pop} and N_{rule} indicate the number of rule sets and the number of rules in a rule set respectively), we should evaluate the fitness of each individual. Fitness value for each rule calculated by:

$$fitness(R_j) = w_t * T_p - w_f * F_P \quad (7)$$

Where $T_p$is the number of correctly classified training patterns and F_P is the number of incorrect classified training patterns but the fitness of rule set is just the number of correctly classified patterns. w_t and w_f are the weights of correct or incorrect classification, respectively. In fact, each rule is evaluated by classifying the given training patterns.

B. The Proposed Algorithm

Pittsburgh style is selected as base of our proposed algorithm and at the end of iterations of Pittsburgh we have a single iteration of Michigan in first layer. It should be mentioned that this layer of algorithm is running for each class separately. Initial population is generated according to the random training patterns. N_{pop} rule sets are generated from random patterns of training data set as initial population, according to subsection A. The first layer of our proposed algorithm is illustrated in Fig. 3.

The steps of the first layer of our proposed algorithm are written as follow:

Step 1) Generate N_{pop} rule sets with N_{rule} fuzzy rules.

Step 2) Calculate the fitness value of each rule set in the current population.

Step 3) Generate next generation according to the following portions (experiments show that the following percentage producing best results):
- 80% rule sets of next generation by the selection, crossover and mutation in the same manner as the Pittsburgh-style algorithm.
- 10% of next generation is formed by elite rule set selection
- 5% is elite rule selection among all rule sets (i.e. the best rules of all rule set)
- 5% is the updated patterns from the training patterns that were not chosen in first step.

Step 4) Apply a single iteration of the Michigan style algorithm to each of the generated rule sets.

Step 5) Choose the best rule set in the current population as the result of this iteration.

Step 6) Return to Step 2, if the stopping condition is not satisfied. (shown in Fig. 3 by letter A)

In step 1 to produce an initial population of fuzzy rule sets, we pick N_{pop} training patterns randomly, and generate the antecedent part of several fuzzy rules according to the selected

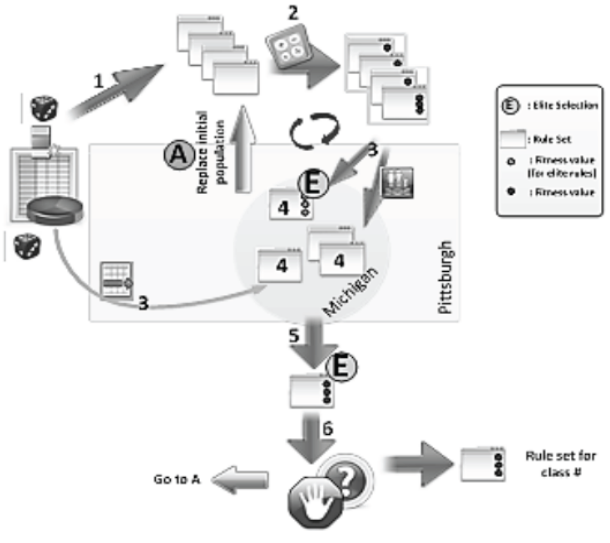


Fig.3 Layer one of the proposed algorithm (Number 1-6 indicates the algorithm steps).

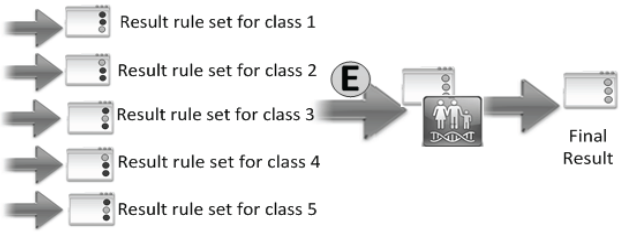


Fig.4 Layer two of the proposed algorithm [7].

patterns. In all steps of the algorithm, the rules that are in the same class of algorithm running for will be accepted.

In step 3 that we apply genetic algorithms, we use tournament selection for selecting the parent rules or rule sets, by this means we give the chance of contribution in forming next generation to the rules or rule sets that have not the high fitness value; it means that we use more number of training patterns in the process rule generation. To achieve the offspring, we use uniform crossover with probability of P_c and mutation with probability of P_m. Each part of individuals is mutated independent of other parts. It means the mutation of a rule do not influence on the mutation probability of other parts.

After producing the next generation we should check the stopping condition. If the pre-specified stopping condition is not satisfied we should return to the step 2, this time instead of starting with a random population, use the newly generated next generation population. In our proposed algorithm, number of iterations is considered as stopping conditions.

Result of the algorithm running for each class is the best rule set which means the rule set with the highest fitness value. The final result of our proposed algorithm is formed as shown in Fig. 4. In this layer, first we choose the best rules of each class, and put them in a rules set. It should be mentioned that the portion of number of rules in the new rule set is equal for all classes. The new rule set will be given to a Michigan style algorithm as its input, and then the final result will be produced.

IV. Evaluation Results

Since the proposed algorithm in [5] is one of the best works that have been done in this domain, we evaluate our proposed algorithm with it. The hybrid algorithm introduced by Ishibuchi in [5] (after here we call it *hybrid algorithm*) is using the combination of Pittsburgh and Michigan styles. So, in this section, first we give a brief description of the hybrid algorithm and then go to the evaluation results of our work.

The hybrid algorithm is like the first layer of our algorithm, but in step 3, it just uses the improved version of individuals. In our proposed algorithm, the random patterns that did not contribute to form the first random generation, is using to produce the next generations. By this means the chance of contributing in rule generation will be given to more number of random patterns. If the initial population forms using improper random patterns, in next iterations the chance of producing the more optimal rules still exists. The detail of the hybrid algorithm is available in [5].

Comparisons of the processes of classification accuracy convergence of each class separately, between our proposed algorithm and hybrid, are presented separately in figures 5 to 9. We can find out that the algorithm behave differently for the pattern of different classes. The reason of this behavior is related to different number of patterns of each class and relevant feature for each class. For example in DOS class that has the high number of training patterns, we get better detection rate. It seems that although our algorithm improves the classification accuracy, but still for the classes that number of training patterns is less, classification accuracy is lower.

Average experimental result over 20 runs is shown in Fig. 10 for all classes together. The vertical axis indicates the classification accuracy and the horizontal axis shows the number of generations that are produced during the algorithm. Since in each iteration a new generation is produced, the number of iterations is equal to the number of generations. Fig. 10 represents that our proposed algorithm converge to the maximum classification accuracy rate on NSL KDD data set faster than the previous hybrid algorithm. Faster convergence leads to reduce the run time. Also, the classification accuracy is higher than previous work. Our proposed algorithm converges in 50 iteration to 98.2% classification accuracy, while the hybrid algorithm converges in 100 iterations.

Totally, our proposed algorithm support multiple classification, higher classification accuracy, and lower false alarm, because of producing better rules (rules with higher fitness value) in comparison with hybrid algorithm. Comparison between different assessment measured are mentioned in Table II, briefly. Also the parameter values that have been used in our algorithm are presented in Table I.

Table I: Parameters values in computer simulation.

Parameter	Value
Number of rule sets	40
Number of rules in each rule set	20
Number of Generations	50
Crossover probability	0.9
Mutation probability	0.1
w_t	0.1
w_f	0.9

Table II: Comparison Results between Hybrid, our proposed algorithm.

Measure \ Approach	Hybrid GBML	Basic IDuFG
True Positive	97.865	98.052
False Negative	0.725	0.511
Recall	99.256	99.481
Precision	97.598	98.701
F-Measure	98.42	99.089
Classification Accuracy	97.891	98.199

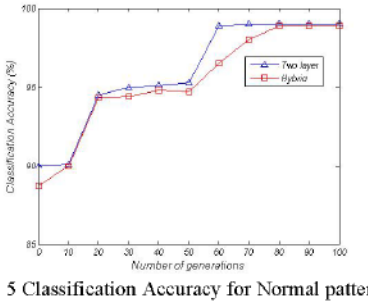


Fig. 5 Classification Accuracy for Normal patterns.

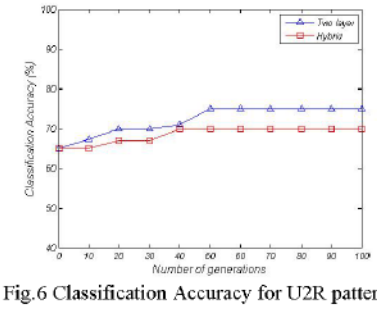


Fig.6 Classification Accuracy for U2R patterns.

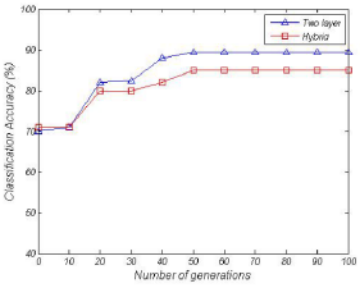


Fig. 7 Classification Accuracy for R2L patterns.

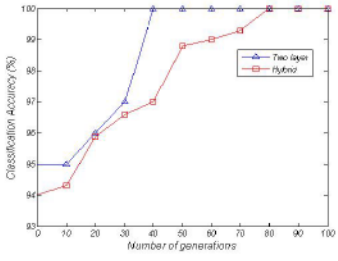


Fig. 8 Classification Accuracy for DOS patterns.

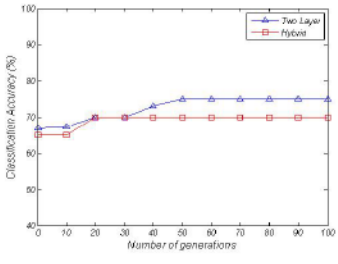


Fig. 9 Classification Accuracy for PRB patterns.

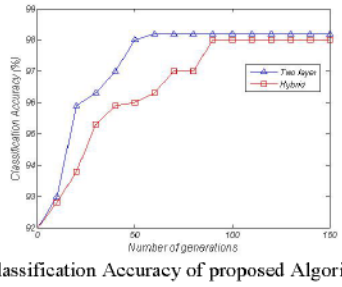


Fig.10 Total Classification Accuracy of proposed Algorithm and Hybrid.

V. SUMMARY AND CONCLUSION

In this paper, we proposed a hybrid fuzzy GBML algorithm as a computational intelligence approach, which supports multiple attack classification. The proposed algorithm is using combination of Pittsburgh and Michigan styles. A two-layer optimization based on genetic algorithm is used to find the optimum rule set. We try to reduce the number of iterations required for convergence by using combination of elite rule sets, elite rules and random training pattern that not use in generation of initial population. Also the false alarm reduction is achieved by using this algorithm. Computer simulations on NSL-KDD data set demonstrate reduction of iterations rather than hybrid evolutionary fuzzy system for intrusion detection. In our proposed algorithm the random patterns that did not contribute to form the next generation, is involving to produce the next generations. By this means the chance of contributing in rule generation will be given to more number of random patterns. If the initial population forms using improper random patterns, in next iterations the chance of moving to the optimal answers still exists. Since the genetic algorithm is a time consuming approach, for future work, we try to reduce the computational time of the algorithm by utilizing the Ant Colony Optimization (ACO) and Particle Swarm Optimization (PSO) instead of genetic algorithm in the first level.

ACKNOWLEDGMENT

Hereby we express our special thanks to Mr. Iman Khalkhali as Web Anomaly-based Intrusion Detection laboratory (WAID) supervisor for his supports during the tests.

REFERENCES

[1] S.X. Wu, W. BanZhaf, "The Use of Computational Intelligence in Intrusion Detection Systems," International Journal of Applied Soft Computing, vol. 10, Issue 1, pp. 1-35, 2009.

[2] Y. Nojima, H. Ishibuchi, I. Kuwajima, "Comparison of Search Ability between Genetic Fuzzy Rule Selection and Fuzzy Genetics-Based Machine Learning," In proceedings of International Symposium on Evolving Fuzzy Systems, Ambleside, 2006.

[3] M. S. Abade, J. Habibi, Z. Barzegar, M. Sergi, "A Parallel Genetic Local Search Algorithm for Intrusion Detection in Computer Networks," International Journal of Engineering Applications of Artificial Intelligence, pp. 1058-1069, 2007.

[4] H. Ishibuchi, T. Nakashima, "Improving the Performance of Fuzzy Classifier Systems for Pattern Classification Problems with Continuous Attributes," IEEE Transactions on Industrial Electronics, vol. 46, no.6, pp. 1057-1068, 1999.

[5] H. Ishibuchi, T. Yamamoto, T. Nakashima, "Hybridization of fuzzy GBML Approaches for pattern classification problems," IEEE Transaction on systems, man, and cybernetics, Japan, vol. 35, pp. 359-365, 2005.

[6] O. Cordon, F. Herrera, F. Hoffmann, L. Magdalena, "Genetic Fuzzy Systems," World Scientific Publishing Publication vol. 19 p.489, 2001.

[7] M. Saniee Abadeh, J. Habibi, E. Soroush, "Induction of fuzzy classification systems using evolutionary ACO-based algorithms," In proceedings of First Asia International Conference on Modeling and Simulation, Phuket, 2007.

[8] M.F. Marhusin, D. Cornforth, H. Larkin, "An Overview of Recent Advantages in Intrusion Detection," In the proceeding of 8th IEEE International Conference on Computer and Information Technology, Sydney, pp. 432-437, 2008.

[9] J. Gomez, D. Dasgupta, "Evolving fuzzy classifiers for intrusion detection," in proceedings of the IEEE information assurance workshop, 2001.

[10] M. Tavallaee, E. Bagheri, W. Lu, and A. Ghorbani, "A Detailed Analysis of the KDD CUP 99 Data Set," IEEE Symposium on Computational Intelligence for Security and Defense Applications (CISDA), Ottawa, pp. 1-6, 2009.

[11] W. Wang, X. Zhang, S. Gombault, S. J. Knapskog, "Attribute Normalization in Network Intrusion Detection," 10th International Symposium on Pervasive Systems, Algorithms, and Networks, Kaohsiung, pp.448-453, 2009.

[12] M. E. Cintra, H. de Arruda Camargo, "Fuzzy Rules Generation using Genetic algorithms with Self-adaptive Selection," IEEE International Conference on Information Reuse and Integration, Las Vegas, pp. 261-266, 2007.

[13] C.H. Tsang, S. Kwong, H. Wang, "Genetic-fuzzy Rule Mining Approach and evaluation of feature selection techniques for anomaly intrusion detection," International Journal of Pattern Recognition Society, pp. 2373-2391, 2007.

[14] H. Zhang, B. Zhang, F. Wang, "Automatic Fuzzy Rules Generation Using Fuzzy Genetic Algorithm," Sixth International Conference on Fuzzy Systems and Knowledge Discovery, Tianjin , pp. 107-112, 2009.

[15] M. S. Abadeh, H. Mohamadi, J. Habibi, "Design and analysis of genetic fuzzy systems for intrusion detection in computer networks," International Journal of Expert Systems with Application, vol. 38, pp. 7067-7075, 2011.

[16] R. Ensafi, S. Dehghanzadeh, M. R. Akbarzadeh, "Optimizing Fuzzy K-means for network anomaly detection using PSO," IEEE, pp. 686-693, 2008.

Radius Regularization using Learning Automata for Spherical Intelligent Anomaly Detectors

Neda Afzali Seresht, Reza Azmi and Boshra Pishgoo

Abstract— **Anomaly detection based on Artificial Immune system (AIS) is now highly regarded among the research community. Nowadays, Clonal selection algorithm is one of the best fields of AIS. In this paper we have assumed anomaly detectors as spherical shape with random central point and variable radius. Detection rate (DR) and false alarm (FA) are influenced by radius of Detectors .Large radiuses would increased both DR and FA and small radiuses would decreased them. So selecting appropriate quantity is an important feature for achieving high accuracy in recognition. The radius of detector is determined based on self-environment. Here we model self-region by a number of spheres with fix radius. The centers of these spheres are determined, using normal data. The radius of self-region spheres has straight effect on detectors radiuses, so by finding the best self-region radius we could have detectors with appropriate radiuses. Our experimental results show that we can gain proper radius by using the advantages of learning automata.**

Index Terms—**Artificial immune systems, clonal selection, learning automata, radius regularization**

I. INTRODUCTION

Intrusion detection is the act of detecting unwanted traffic on a network or a device. Intrusion Detection Systems (IDSs) dynamically monitor the events to detect unwanted activity such as illegal and malicious traffic before they inflict widespread damage.

In general, IDSs fall into two categories according to the location they put in it, namely (i) Network-based Intrusion Detection System (NIDS) and (ii) Host-based Intrusion Detection System (HIDS) [9].NIDS is one common type of IDS that analyzes network traffic for intrusion detection. In contrast, HIDSs analyze network traffic and system-specific settings such as system calls, local security policy, local log audits, and more [5]. HIDSs reside inside an operating system and evaluate its behaviors in order to gain higher detection power than NIDSs.

IDSs is divided into two categories according to the detection methods they employ, namely (i) misuse detection and (ii) anomaly detection. Misuse detection identifies intrusions by matching observed data with pre-defined descriptions of intrusive behavior [4] so it can detect only well-known attacks.

Anomaly detection is orthogonal to misuse detection. It hypothesizes that abnormal behavior is rare and different from normal behavior. Hence, it builds models for normal behavior and detects anomaly in observed data by noticing deviations from these models [4]. So it can detect new types of intrusions.

Artificial immune system (AIS) is a new research field for anomaly detection. This approach is inspired by Human Immune Systems (HIS). The main purpose of HIS is to recognize all cells (or molecules) within the body and categorize them as self or non-self [8]. HIS consists of a collection of lymphocyte cells (T-cells and B-cells) that produce secretion of antibodies as a response to antigens such as bacteria, viruses and tumor cells [7].

AISs have some main branches, namely negative selection, danger theory, Immune network and Clonal selection. In this paper, we use clonal selection algorithm and tune the self-radius parameter using learning automata. We use a self-region environment that has been created by using normal train data. In this case, we have modeled this area by the number of spheres with normal data as its central point and fix radius. We have assumed anomaly detectors as spheres with variable radiuses that have been created out of this area. The detectors radiuses have inverse relation with self-radius. So we have powerful anomaly detectors with high accuracy in recognition by finding appropriate self-region radius. Since using trial and error testing for determining the suitable radius is much slower than the other methods we have decided to use learning automata.

The remainder of this paper is organized as follows: Section 2 reviewed related works on clonal selection. Clonal selection algorithm and learning automata are described in Section 3 in detail. Our purposed algorithm and its implementation are described in Section 4. Finally, section 5 concludes all topics.

II. RELATED WORK

In recent years, artificial immune system inspired by the immune systems has become a notable area in intelligent systems. Research on AIS has led to the development of many different algorithms based on immune principles. Among them, clonal selections were proposed as evaluation algorithms to solve the problem by iteration. Compared to genetic algorithm, the Clonal Selection Algorithm shows a lot

F. Neda Afzali Seresht. is in Operating System Security Lab (OSSL) in Alzahra University in Tehran, Iran (e-mail: n.afzali.s@gmail.com)

S. Reza Azmi. Is Teacher assistant of the computer engineering faculty and founder and director of Operating System Security Lab (OSSL) in Alzahra University in Tehran, Iran (e-mail: azmi@alzahra.ac.ir)

T. Boshra Pishgoo.is head of Operating System Security Lab (OSSL) in Alzahra University in Tehran, Iran (e-mail: Boshra.pishgoo@student.alzahra.ac.ir)

of useful features. It can maintain the best population while improving the convergence rate. The Clonal Selection Algorithm has been widely used in optimization (liked genetic algorithms), pattern recognition and other engineering fields such as network security, data mining and so on. The researches focused on improving the convergence rate, solution stability and accuracy of the solution.

By reviewing the researches in clonal selection field, we can taxonomy them in 3 categories; (i) the researches that consider the main aspects of operation algorithm: Cloning, mutation and selection [16, 6],(ii) the researches that Regulate parameters to achieve high accuracy [2, 13, 10] and (iii) the researches that use clonal selection to optimize the proposed algorithms or their parameters [7,8,11, 9, 4].

In this paper, we want to regularize the self-radius parameter of clonal selection algorithm using learning automata. According to the previous section, self-radius is the parameter that effected on detector radiuses. Detectors with large radius can identify more antigens, so it causes high detection rate, in the other hand, detectors with large radius label every antigen as abnormal, so it increase false alarms. Thus finding the appropriate radius with low false alarms and high detection rate is the important work to gain high accuracy.

III. BACKGROUND

A. Clonal Selection

The clonal selection theory [14] is used by the immune systems to distinguish between self and non-self. In the biological immune system operation, B cells (antibody) play key roles. These cells recognize foreign antigens which attack the organism. The clonal selection establishes the idea that only those cells are selected that can recognize antigens truly. This theory has been shown in Fig.1.

De Castro proposed a clonal selection algorithm (CSA) based on the Clonal selection principle and the affinity maturation process [11].These algorithms also use the idea of memory cells to retain good solutions for problem solving [3].*CLONALG* has global searching ability as it uses the principles of clonal expansion. It has been used to perform the tasks of pattern matching and multi-modal function optimization.

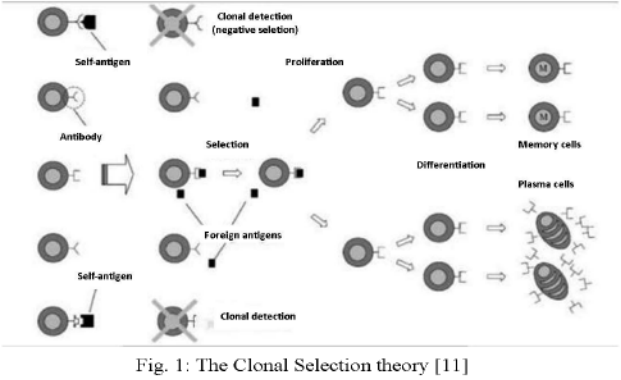


Fig. 1: The Clonal Selection theory [11]

The clonal selection algorithm can be described as follows:

Classic Clonal Selection Algorithm

```
Begin
    Create population randomly.
While (termination criterion not satisfied)
        Calculated the fitness;
        Select n best antibodies;
        Clone these n antibodies;
        Mutate the cloned antibodies;
        Generate new population;
    End
End
```

Fig. 2: Pseudo Code of classic clonal selection algorithm

At first, this algorithm generates N new random antibodies as initial population. These antibodies are our detectors to find abnormal antigens. The fitness (affinity) of each antibody is specified. These antibodies are sorted according to their fitness and then n antibodies that have high fitness are selected.

Cloning is one of the key aspects of AIS. It is the process of producing similar populations of antibodies. The selected n best antibodies will be replicated proportional to their fitness. The Mutation helps antibodies to mutate and improve their fitness. Uniform mutation, Gaussian Mutation or Cauchy mutation can be used as mutation function [2].

For the next iteration we will use these antibodies to create new population and if they are less than N, we generate others randomly. This cycle would be repeated several times to achieve satisfied results; it's clear that the algorithm creates better population in each iteration than previous one.

B. Learning Automata

An *automata* is a machine or control mechanism that is designed to control a process without adequate information. The concept of the learning automaton is defined as a result of the work on modeling observed behavior, choice of actions based on past observations and implementation of optimal strategies in the context of the two-armed bandit problem. A finite number of actions can be run in a random environment [15]. The actions are chosen according to a specific probability distribution. This probability distribution is updated by the environment that responses the automata.

Learning automata has the variable structure which represented by a quintuple $\{\psi, a, b, A, G\}$ where: $\psi(n)$ is state of automata that can be represented by $\psi = \{\psi 1, \ldots, \psi\}$,$a(n)$ is output of automata that can be represented by $a=\{a_1, \ldots, a_r\}$,$b(n)$ is input to automata that can be represented by $b=\{b1, \ldots, bm\}$,A is the learning algorithm, $G[.]$, is the output function which: $a(n)=G[\psi(n)]$; n indicates the iteration number and $pj(n)$ is action probability; the probability that automaton is in state j at iteration n.

The automata schema can be described as follow:

If a (n) = a_i and for j != i; (j=1 to r)

$pj(n+1) = pj(n) - g\,[pj(n)]$ when b(n)= 0. (1)

$pj(n+1) = pj(n) + h\,[pj(n)]$ when b(n)= 1. (2)

In order to preserve probability measure,

$\Sigma\ pj\ (n) = 1$, for j = 1 to r [10,12] . (3)

IV. PURPOSED ALGORITHM

In this section we describe our purposed algorithm step by step. In this algorithm we first follow basic clonal selection and then use automata in it to achieve our goal. Our algorithm is described in Fig. 3.

Our Proposed Algorithm

1) Generate *N* initial population (randomly in first iteration)
2) Using automata to find the best safe-radius
3) Updating the detection radius
4) Calculating the fitness
5) Sorting *N* detectors based on fitness descending
6) Selecting *n* best detector with high affinity
7) Cloning this n detector
8) Mutating this cloned based on its fitness
9) Generating new population

Fig. 3: Pseudo code of our proposed algorithm

After generating *N* antibody randomly in first iteration, we use 5 automata to determine best self-radius. Each automaton needs an initial radius to work. This radius is provided with a coefficient of primary self-radius. So automata start their work with fair probability and different initial radiuses. Then each automaton randomly selects one action. At the first action it increases self-radius, at the second action it does not change self-radius and at the third action it decreases self-radius. Based on selected action, the initial self-radius is changed and the radiuses of detectors are influenced too. In this step we calculate the accuracy of system, using new detectors with new radiuses. If these new detectors have higher accuracy than previous ones; the probability of selected action will be increased, otherwise it will be decreased. In each iteration, the automaton has been worked with a new self-radius. So among five new self-radiuses, at the end of each iteration the best radius is selected based on detection rate of system with it and it will be introduced as a next self–radius. This process is shown in Fig. 4. In this experiment we determined w={100, 10, 1, 0.1, and 0.01}.

To obtain the detector fitness, rewarded and punished technique can be used. Therefor if the detector correctly found an antigen, it has been rewarded and its fitness has been increased, otherwise the fitness has been decreased.

When fitness of each detector was calculated, we must sort detectors based on their fitness descending to select *n* best detectors. These *n* detectors were cloned. Cloning is one of the key aspects in AIS. The number of clones for each detector can be calculated by equation (4) that defined in [2]:

$$N_c = \sum_{i=1}^{n} round(\frac{\beta * N}{i}) \quad (4)$$

Where *Nc* is the Number of clones generated from each simulated cell; *N* is The size of Antibody Pool (detector), *n* is the Number of antibodies with highest affinities and β is a multiplying factor. Round (.) is the operator that rounds its argument towards the closest integer. Clone size of each selected detector is represented by each term of this sum. The number of clones that are generated for detectors with higher fitness, which is placed on top of the sorted fitness array; are more than bottom detectors [2].

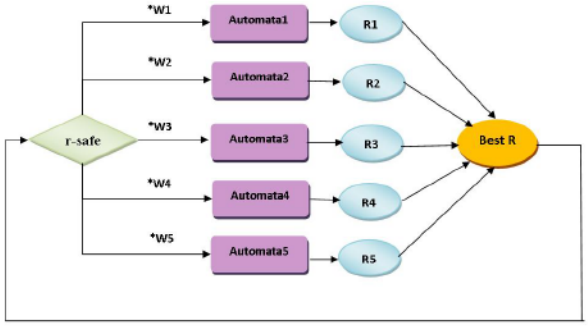


Fig. 4: Structure of proposed algorithm using learning automata

In this step we should perform mutation process on the cloned detectors. In this paper, mutation rate is calculated by equation (5).

$$Mutation\ Rate = exp\,(-fitness) \quad (5)$$

After this step, we should check the population number. If it was less than *N*, we'd have to generate additional detectors randomly; if not, we should remove additional detectors. The next iteration will be started with this new population.

V. EXPERIMENTAL RESULTS

So as to proof our claim, we should evaluate our proposed algorithm. We need a set of normal and abnormal patterns together with their labels (normal or abnormal label).We examined our purposed algorithm in 2 datasets.The first of them is dataset of system calls that has been generated by using a secure architecture. The process of dataset generation is described in [1] in details. Each pattern of this dataset have some suitable features the number of system calls, access mode and flag arguments, Pid, Uid and Gid to distinguish between normal and abnormal behaviours.

The second dataset is NSL_KDD99 that has special version of KDD Cup99 dataset.Each pattern of this dataset has 41 features: 38 numeric features and 3 Non-numeric features. In this examination we only use 19 important features based on [5].

We used three criteria for evaluating detection results of our anomaly detection system. These criteria are Accuracy

The process of self-radius regularization for the different radiuses is shown in Figure 6. As illustrated in this figure, automata starts its work with an initial radius as the self-radius and after a lot of fluctuation (18 times) achieves the proper radius. As indicated in this figure, all initial self-radiuses coverage to the best range of self-radiuses that has been introduced by trial and error process and colored in TABLE III.

TABLE III: The results of classic clonal selection in NSL-KDD99 dataset

Self-radius	ACC	FA	DR
0.6	0.5013	0	0
0.5	0.5063	0	0.0101
0.4	0.5013	0	0
0.3	0.05542	0	0.1061
0.2	0.06297	0	0.2576
0.1	0.8967	0.0201	0.8131
0.06	0.9270	0.0352	0.8889
0.05	0.9320	0.0402	0.9040
0.04	0.9295	0.0503	0.9091
0.03	0.09244	0.0704	0.9192
0.02	0.9093	0.1106	0.9293
0.01	0.8992	0.1156	0.9141
0.003	0.08892	0.1457	0.9242
0.002	0.8866	0.1759	0.9495
0.001	0.8917	0.1508	0.9343

TABLE IV: The results of our proposed algorithm in NSL-KDD99 dataset

Primate self-radius	Regularized self-radius
0.6	0.0646
0.5	0.06928
0.4	0.0598
0.3	0.0386
0.2	0.0585
0.1	0.0447
0.01	0.0507
0.001	0.0259
0.0001	0.0198

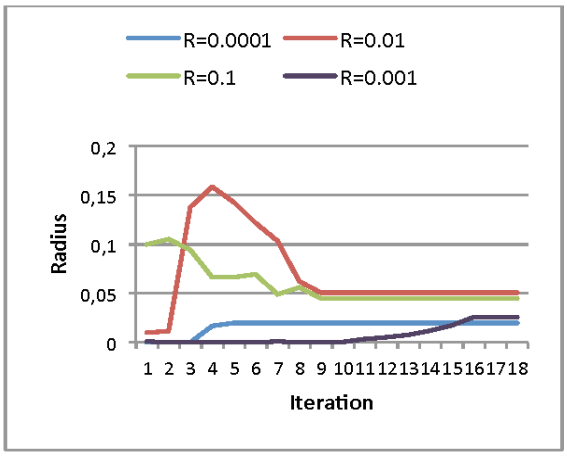


Fig. 6: The result of our proposed algorithm with different primary radiuses in NSL-KDD99 dataset

VI. CONCLUSION

In this paper, an automatic way to regularize self-region radius of clonal selection algorithm by automata is proposed. Since the clonal selection algorithm is one of the important fields of Anomaly detection based upon AIS, finding appropriate self-region radius can highly effects on its accuracy. Finding this element by trial and error testing is time consuming; in addition there is no guaranty that we can find the best element to obtain maximum accuracy.. Based on experimental results we can achieve the appropriate self-region radius by using automata through the algorithm that is represented in this article this automata starts the process with different radiuses and adjusts them by using the accuracy and will provide the best one as an output.

ACKNOLEDGMENTS

We wish to acknowledge the support of this work through Iran Telecommunication Research Center (Contract Number = ت/500/6085).

REFERENCES

[1] R. Azmi, B. Pishgoo, H. Nemati, "Hypervisor-based Intrusion Detection Using Artificial Immune Systems": 8th International Iranian ISC Conference on Information Security and Cryptology, pp. 147-153, (2011), (In Farsi).

[2] S. Chittineni and S.M. Krishna, "Design of Fixed and Ladder Mutation factor based Clonal Selection Algorithm(FMCSA and LMCSA) forsolving uni-modal and multimodal functions": Applied Computational Intelligence and Soft Computing Volume 2011 (2011), Article ID 210918,, pp 1-8

[3] S. Chitra, B. MadhuSudhna and M. Rajaram," Investigation of data clustering preprocessing algorithm on independent attributes to improve the performance of CLONALG": International Journal on Computer Science and Engineering, Vol. 2(1), 2010, pp 8-11

[4] SH.Ding and SH.X.Li,"Clonal Selection Algorithm for Feature Selection and Parameters Optimization of Support Vector Machines": Second International Symposium on Knowledge Acquisition and Modeling, 2009.

[5] D.M. Farid, J. Darmont, N. Harbi, H.H. Nguyen, M.Z.Rahman,"Adaptive Network Intrusion Detection LearningAttributeSelectionandClassification":InternationalConference onComputer Systems Engineering (ICCSE09),Bangkok,Thailand,December 2009

[6] Y.Hang, J.Li-Cheng and G.Mao-Guo," Clonal Selection Function Optimization Based on Orthogonal Experiment Design", Journal of Software, Science Press. pp 950-967,2010.

[7] T.Huntsberger, "Clonal Selection Based Artificial Immune System for Generalized Pattern Recognition": *Proceedings of the 2001 Congress on. Evolutionary Computation, 2001.*

[8] K.Lakshmi and S.Vasantharathna and C.Muniraj," Clonal Selection Based Artificial Immune System to Solve the Unit Commitment Problem in Restructured Electricity Sectors",, *IEEE International Conference on Power and Energy (PECon),2010.*

[9] J.Ma and Y.Shou,"Study on Immune Clonal Algorithm and Its Application": Second International Conference on Intelligent Computation Technology and Automation, 2009.

[10] A. H. Momeni Azandaryani and M. R. Meybodi., "A Learning Automata Based Artificial Immune System for Data Classification": *Applied in Computer Conference, 2009. CSICC 2009. 14th International CSI.*

[11] E. Nabil, A. Badr and I. Farag,"A P System Design using Clonal Selection Algorithm": Studia UNIV. Babes_{Bolyai, Information, Volume LVI, Number 1, 2011.

[12] K.S.Narendra, "Learning Automata-A survey": IEEE Transactions on System, Man, AND Cybernetics, VOL. SMC-4, NO. 4, 1974.

[13] A.Rezvanian and M.R.Meybodi," LACAIS: Learning Automata Based Cooperative Artificial Immune System for Function Optimization":*Springer-Verlag Berlin Heidelberg , IC3 2010, Part I, CCIS 94, pp. 64–75, 2010.*

[14] L.Ruochen, D.Haifeng and J.Licheng, "Immunity Clonal Strategies": *Proceeding in ICCIMA '03 of the 5th InternationalConference on Computational Intelligence and Multimedia Applications IEEE Computer Society , 2003.*

[15] Cem.Unsul, "Intelligent Navigation of Autonomous Vehicles in an Automated Highway System: Learning Methods and Interacting Vehicles Approach": Remarks: Thesis (Ph. D. in Electrical Engineering)--Virginia Polytechnic Institute and State University, 1997

[16] L.Zhang,M.Gong and L.Jiao," Improved Clonal Selection Algorithm based on Baldwinian learning": *(IEEE World Congress on Computational Intelligence). IEEE Congress on Evolutionary Computation, 2008. CEC 2008.*

Topic-Based Probabilistic Approach to Criminal Network for Suspect Investigation

Arzu Kakışım, İbrahim Soğukpınar

Abstract— **Specifying the suspicious groups, gathering information of all suspects and clarifying connections between them before the occurrence of possible next crimes, are crucial duties for the maintenance of security of the community. An investigator manually gets information about the criminal events and evaluates the suspects according to their criminal probability by creating a network. In this work, a new approach is proposed for the problem of criminal probabilistic network analysis. Proposed method is achieved by combination of Probabilistic Author-Topic (AT) model and method of Social Network Analysis. AT model is applied to extract valuable topics and probabilities of each author directly from text documents. A criminal probabilistic network is constructed to assist suspect investigation by the use of probabilities of suspects and relationships among them. A corpus was generated with combining of Kos, Enron and Nips databases and experimental results have been presented.**

Keywords: Criminal Probabilistic Network Analysis, Author-Topic Model, Suspect Investigation, Text Mining.

I. INTRODUCTION

THE aim of maintaining the public order and safety of the community can only be achieved through the deactivation of the potential criminals before they commit another crime. Therefore, to catch the criminals and resolve the criminal events, investigators analyze crime scene using eyewitness statements and evidences. All the data, which are obtained during the analysis, are kept in the databases of public security agencies and they are used to create criminal profiles. These profiles are particularly utilized to solve criminal events in the future. For instance, K. Baumgartner, S. Ferrari and G. Palermo [9] have developed a system which is based on such information of the potential criminals as age, occupational and sexual data, through the use of certain crime scene data and Bayesian network model. In the light of the criminal profiles and known or estimated relations among offenders, criminal networks are be constructed by investigators. Individuals in criminal networks might be offender or innocent. Thus, these people are evaluated as suspicious ones since the event is currently in the phase of investigation. Definitely, all suspects have to be regarded as innocent individuals before their guilt is proved. Therefore, analyzing these criminal networks with targeting the correct entity is main goal to identify the correct criminals. A variety of methods could be used to solve the criminal networks through the utilization of partial information of offenders. For example Z. Xia [3] has used the belief propagation method and extended MPFS algorithm to pick the individuals who have to be primarily investigated among the suspicious people in a criminal network.

Crime investigators labor to solve a certain case by determining individuals' possibilities for being criminal and deepening the investigation by focusing specific suspects on the ground of these possibilities. This method can produce successful results for small criminal networks, but the process is highly time-consuming in case of further information and a greater network. Therefore, a criminal possibility has to be allocated to each member of the network and relationships among the suspects should be rigorously clarified in order to decide the suspects who would be primarily investigated. For making this estimation correctly, investigators need suspect profiles and a variety of data which are similar to the crime scene variables.

With the intense use of internet, virtual communities and user profiles come into existence in the cyber world. People usually hold such profiles more than one. And they leave some traces as a result of their virtual actions while surfing the internet. These traces may be e-mails, blogs, writings in the chat log, bill of sale of a cinema ticket or lists of visited places. Furthermore, people keep crucial part of data especially in the hard-disks of their computers. Thus, when a suspect is arrested, such traces are investigated to obtain information about her/him. Getting information from these ragged data, however, proved so time-consuming mission. Against such problems, various methods have been developed to automatically extract short descriptions belonging to text collections [12], [14], [2], [13], [1]. These methods have been used for significant tasks such as classification and summarization.

In this work, a new approach has been proposed for the criminal probabilistic network analysis problem. In the proposed method, criminal probabilistic network is constructed for suspect investigation using social network and AT model [1] in which suspects have probabilities related to topics extracted from text collections of suspects. This work is aimed to enhance the concept of Social Network Analysis (SNA) using a probabilistic approach.

Rest of the paper is organized as follows: In Section 2, related works are mentioned. Section 3 presents proposed method. Case study and experiments are presented in Section 4. Section 5 concludes the paper with the discussion of future works.

II. LITERATURE REVIEW

Many different methods have been developed in the field of crime investigation since analyzing criminal networks is a crucial task to preserve national and transnational security. For example, Chen et al. [10], [11], [15] improved an application that could identify criminal associations from a large amount of databases at police departments. In addition, J. Xu and H. Chen's another work [16] is related to the topology of dark networks. As it can be seen in their study, social network analysis methods can be applied for criminal networks. For example, C. Yang and T. Ng [17] use information at blogs and propose a topic-specific exploration mechanism which uses the relations between bloggers to construct the web-log social networks. R. Al-Zaidy, B. C. M. Fung, and A. M. Youssef [6] present a frequent community approach to identify criminal communities. Their method discovers the criminal communities from textual data and gives the information of location, telephone and topics of documents of communities. In addition, methods like [5], [7] apply to solve problem of community detection. G. L'Huillier, S. A. Rios, H. Alvarez, and F. Aguilera [4] proposed a topic-based system according to virtual communities of interests. They used LDA topic modeling technique in conjunction with SNA techniques to build topic-based dark network and define relationships according to information of users' posts. McCallum, X. Wang and A.C. Emmanuel [13], present the Author-Recipient-Topic (ART) model which is similar to Author-Topic model. This model is a directed graphical structure and differentiated from AT model using information of author and set of recipients relevant to a message.

In our proposed approach, as a distinct one from these methods, we constructed a topic-based criminal probabilistic network according to criminal probability of suspects and their relationships using Author-Topic model. Short descriptions, in a word, topics, are obtained from text documents of suspects to investigate a specific event. Then, some topics are chosen in the light of information of the event under investigation. And then, these chosen topics will help us to construct our network.

III. PROPOSED METHOD

The main problem of criminal probabilistic network is to describe criminal probability of each suspect, and the other one is to extract relationships between them. Firstly, suspects' documents are collected and clustered according to certain features. Some clusters specially give clues concerning the event under investigation. For this task, previously known and clustered documents are used.

This section is divided into three parts: Notation, Author-Topic Modeling and Network Modeling.

A. Notation

D is a set of all suspects' documents and defined by $D = D_1 \cup D_2 \cup \ldots \cup D_S$, where S represents the Sth suspects. D_1 is a set of first suspect's documents and represents $D_1 = \{d_{11}, d_{12}, \ldots, d_{1k}\}$. Each one of d documents holds its owner information and k is number of documents belonging to the first suspect. A document is a sequence of n words denoted by $\mathbf{w} = (w^1, w^2, \ldots, w^n)$ and w^n is the nth word in the document. Words are represented by an item from a vocabulary indexed by $\{1, \ldots, V\}$. Finally, a corpus consists of m documents and defined by $D = \{w^1, w^2, \ldots, w^m\}$. Authors of each document are known previously and the set of suspects of document d is defined s_d, where s represents suspect.

B. Author-Topic Modeling

In the Author-Topic Model which is a highly generative type, each word w is related to an author and a topic. "Each author is represented by a probability distribution over topics and each topic is represented as a probability distribution over words for that topic" [1]. Firstly, the process randomly chooses an author for each word in the document. Then, this author selects a topic from multinomial distribution over topics represented by θ and ensamples a word from the multinomial distribution over words represented by φ, associated with that topic. At the beginning of this process, T topics are assumed. The following sequence of AT model is represented as described by [8].

1) For each suspect $s \in \{1, \ldots, S\}$ choose $\theta_s \sim$ **Dirichlet** (α)
   For each suspect $t \in \{1, \ldots, T\}$ choose $\varphi_t \sim$ **Dirichlet** (α)
2) For $d \in D$
   Given the vector of suspects s_d
   For i=1... number of words in the dth documents (N_d)
   Conditioned on s_d, choose $x_{di} \sim$ **Uniform** (s_d)
   Conditioned on s_d, choose $z_{di} \sim$ **Discrete** ($\theta_{x_{di}}$)
   Conditioned on s_d choose $w_{di} \sim$ **Discrete** ($\varphi_{z_{di}}$)

Θ and φ have a symmetric Dirichlet prior with hyper parameters α and β. These parameters are given at the beginning of this process and correlate with number of words and topics.

Depending on θ and φ, the probability of the corpus is

$$P(w|\theta, \varphi, s) = \prod_{d=1}^{D} P(w_d|\theta, \varphi, s_d). \quad (1)$$

The probability of the words in each document is

$$P(w_d \mid \theta, \varphi, s) = \prod_{i=1}^{N_d} P(w_{di}|\theta, \varphi, s_d). \quad (2)$$

The final goal is to estimate θ and φ random variables. Several methods have been developed for estimating the posterior distribution for these variables. This paper is based upon Gibbs Sampling which is a form of Markov chain Monte Carlo model [18].

C. Network Modeling

Criminal probabilistic network is constructed according to probabilities of suspects and relationships among them. Nodes of graphs represent suspects and relations between them are symbolized by the graph edges. Using AT model, T number topics are generated from text collections and some topics are chosen from a certain topic's set $t' = \{t'_1, \ldots, t'_N\}$ according to investigator's query $Q = \{q_1, q_2, \ldots, q_q\}$ which consists of some important words about the event. Author probabilities of

selected topics are used to evaluate criminal probabilities. For example, t^{th} topic containing author probabilities is defined $\{p_{t,1}, p_{t,2}, \ldots, p_{t,S}\}$, where $p_{t,1}$ represents the first suspect of probability belonging to $\mathbf{t_1}$topic. Each suspect who is allocated to a certain topic is correlated with such a value that could give the information about his/her criminal probability's place in the rank of those of all the suspects who are allocated to the same topic. The probabilities are re-evaluated using the rank of author probability which is defined $r_{t,s}$. **For instance, when topic 130 is analyzed in Table 2, rank of suspect 18 and 19 is 20 and 19 respectively.** By this way, set of criminal probabilities is defined as $\boldsymbol{P} = \{P_1, P_2, \ldots P_S\}$, where P_1 is criminal probability of the first suspect and can be calculated by (3)

$$P_i = \frac{\sum_{j=1}^{N} p_{j,i}\, r_{j,i}}{SxN}; 1 < i \leq S, 1 < j \leq N \qquad (3)$$

After criminal probabilities are computed, we choose maximal probability and set it to 0.92 to be able to position the values between 0.1 and 0.99 as far as possible.

To find associations between suspects, the documents of suspects can be analyzed. The similarities between suspects can be measured using Kullback Leibler (KL) divergence function, Euclidian distance, Jensen-Shannon divergence. In this study, cosine similarity method which is a measure of similarity between two vectors, have been used. The similarity between s_1 and s_2 depends on topic distributions $\theta_{s_1}$and θ_{s_2} and gives information relationship's degree, R.

$$sim = \frac{\sum_{i=1}^{T} \theta_{s_1}\ \theta_{s_2}}{\sqrt{\sum_{i=1}^{T}(\theta_{s_1})^2}\sqrt{\sum_{i=1}^{T}(\theta_{s_2})^2}} \qquad (4)$$

Algorithm 1 presents the pseudo-code which creates our criminal network according to important topics. After similarity values are obtained, we use a threshold to distinguish strong relationships.

IV. EXPERIMENTAL RESULTS

In this section, some experiments have been conducted and results have presented and discussed. Different datasets have used to implement the proposed method. We preferred Kos, Nips and Enron databases to obtain various documents regarding different fields and to make difference among the suspects. First six suspects have only Kos documents and each one has different 300 Kos documents. But, first three suspects have also same 100 documents. Suspect 7, 8, 9 and 10 have only Nips documents and they do not share any documents. Table 1 also shows distribution of the documents of each suspect. We described $S = 20$ suspects and our collection contains $D = 6300$ documents, 1245678 word tokens and 33518 words in the vocabulary V. $T = 100$ topics are extracted using
AT model previously described in Section B. According to our query, $t' = 11$ topics are chosen and criminal probabilities are evaluated.

Algorithm 1. Topic-Based Criminal Probabilistic Network

Input: $D, V, T, s, \alpha, \beta, s_d$
Output: $G(C, E)$
1: P, t, $\theta \leftarrow$ AT (s, $s_d, T, N_d, \alpha, \beta$) (section B);
2: $t' \leftarrow$ be defined by investigator, $\mathbf{1} \leq s(t') \leq s(t)$;
3: For each $i \in s$
4: For each $j \in t'$
5: $Pi \leftarrow$ (Equation 3 in section C)
6: End For
7: End For
8: Initialize $C = \{\ \}$, $E = \{\ \}$;
9: For each $i \in s$
10: $C \leftarrow C \cup i$;
11: For each $j \in s, i \neq j$
12: $R_{i,j} \leftarrow sim(\theta_i, \theta_j)$ (section C);
13: If $R_{i,j} \geq threshold$
14: $E \leftarrow E \cup R_{i,j}$
15: End if
16: End For
17: End For

Table 1. Distribution of Kos, Nips and Enron documents for each suspect.

KOS	NIPS	ENRON
300 documents for each of $s_1, s_2, s_3, s_4, s_5, s_6$ suspects.	50 documents for each of s_7, s_8, s_9, s_{10} suspects.	200 documents for each of s_{11}, s_{12}, s_{13} suspects.
100 shared documents for s_1, s_2, s_3 suspects.	Not shared	100 shared documents for s_{11}, s_{12}, s_{13} suspects.
KOS&ENRON	**NIPS&KOS**	**KOS& ENRON&NIPS**
300 Kos and 200 Enron documents for each of s_{14}, s_{15} suspects.	100 Kos and 50 Nips documents for each of s_{16}, s_{17}suspects.	400 Kos, 200 Enron and 50 nips documents for each of s_{18}, s_{19}, s_{20} suspects.
Not shared	50 shared documents for each of s_{16}, s_{17}suspects.	150 shared documents for s_{18}, s_{19}, s_{20} suspects.

Investigators can use several approaches like query mechanism to choose topics. In our study, we have selected some topics which involve such words like "attack, December, Guatemala, getaway, election, financial, Citibank" according to our event scenario. In Table 2, we illustrate author-topic and topic-word distribution of selected topics. There are ten words and six authors associated with each topic. For example, Topic 145 and topic 395 at the top of Table 2, describe different two events related to Guatemala. They are related to robbery and escape respectively.

Table 3 shows the criminal probabilities of suspects. Suspect 3 and suspect 16 have high probabilities. Because these suspects are assigned to a topic with high probability and they associate more than one topic with greater ranks.

Value of similarity between, for example, suspect 1 and suspect 2 who have some shared documents, reaches to 0.95.

Topic 334		**Topic 393**		**Topic 394**	
WORD	**PROB**	**WORD**	**PROB**	**WORD**	**PROB**
MEETING	0.03493	HOUSTON	0.03708	EXPERT	0.04658
DEAL	0.03020	CITIBANK	0.02560	ANDERSON	0.02543
FINANCIAL	0.02139	EQUIPMENT	0.02296	CONCILIATOR	0.02463
DIRECTOR	0.01278	ASSESSOR	0.01754	BERMUDA	0.01660
TRADER	0.01202	ALIENATE	0.01612	APPROVAL	0.01365
TERM	0.01202	ASSET	0.01505	CORPORATION	0.01339
GETTING	0.01174	HOTRATE	0.01476	CHART	0.01312
MIKE	0.01108	ABSORBED	0.01391	MONEY	0.01312
PRICES	0.01060	ESPERA	0.01326	BANK	0.01232
OFFICE	0.01051	FUNERAL	0.01291	CONCILIATORY	0.01124
AUTHOR	**PROB**	**AUTHOR**	**PROB**	**AUTHOR**	**PROB**
Suspect 15	**0.22798**	**Suspect 20**	**0.23996**	**Suspect 3**	**0.93077**
Suspect 18	**0.16887**	**Suspect 16**	**0.17426**	**Suspect 2**	**0.03127**
Suspect 8	**0.15079**	**Suspect 10**	**0.15702**	**Suspect 1**	**0.02896**
Suspect 7	**0.12221**	**Suspect 17**	**0.10580**	**Suspect 16**	**0.00611**
Suspect 19	**0.10112**	**Suspect 11**	**0.07495**	**Suspect 18**	**0.00177**
Suspect 20	**0.09198**	**Suspect 18**	**0.05923**	**Suspect 9**	**0.00061**
Topic 357		**Topic 281**		**Topic 202**	
WORD	**PROB**	**WORD**	**PROB**	**WORD**	**PROB**
ELECTION	0.01813	DEUTSCHE	0.03436	FUNDAMENTAL	0.02743
ACCIDENTAL	0.01648	ABATE	0.02518	GETAWAY	0.02015
DIETRICH	0.01566	DEFENDING	0.02401	AWARENESS	0.01744
ADJOURNED	0.01566	BORDERING	0.02362	DROPPED	0.01710
KERRY	0.01500	BODE	0.01991	CHARACTER	0.01575
CLASS	0.01335	COON	0.01816	HAMAS	0.01287
GLANCE	0.01335	COMFORT	0.01484	BANGED	0.01219
DEMOCRATIC	0.01137	RELATION	0.01445	BARREL	0.01202
MONEY	0.01088	FIRE	0.01328	ELVIS	0.01117
REPUBLICAN	0.01055	MURDER	0.01328	DROVE	0.01033
AUTHOR	**PROB**	**AUTHOR**	**PROB**	**AUTHOR**	**PROB**
Suspect 16	**0.99942**	**Suspect 4**	**0.69999**	**Suspect 10**	**0.93224**
Suspect 13	**0.00019**	**Suspect 3**	**0.08428**	**Suspect 13**	**0.02436**
Suspect 1	**0.00002**	**Suspect 20**	**0.05762**	**Suspect 1**	**0.01406**
Suspect 2	**0.00002**	**Suspect 2**	**0.05184**	**Suspect 2**	**0.01139**
Suspect 3	**0.00002**	**Suspect 19**	**0.04090**	**Suspect 3**	**0.00962**
Suspect 4	**0.00002**	**Suspect 1**	**0.02438**	**Suspect 4**	**0.00589**
Topic 130		**Topic 145**		**Topic 395**	
WORD	**PROB**	**WORD**	**PROB**	**WORD**	**PROB**
ATTACK	0.02330	BALLINGER	0.03390	GETAWAY	0.05660
COMPANY	0.02176	DIETRICH	0.02884	HUNGTINGTON	0.04505
JENNIFER	0.00537	GUARDING	0.02625	FACES	0.03778
DECEMBER	0.01041	BELONGED	0.02191	IMPASSE	0.02752
ARNOLD	0.00970	CANOPY	0.02150	DROVE	0.02155
BOMB	0.00970	ALARM	0.01995	SHOT	0.01999
FUTURES	0.00923	GUATEMALA	0.01871	CHINA	0.01727
GLOBAL	0.00923	ENDICOTT	0.01726	GUATEMALA	0.01649
SOURCING	0.00911	ROBBERY	0.01716	BATTLED	0.01415
MANAGER	0.00828	GAMBOT	0.01571	ARNOLD	0.101311
AUTHOR	**PROB**	**AUTHOR**	**PROB**	**AUTHOR**	**PROB**
Suspect 18	**0.36088**	**Suspect 17**	**0.36330**	**Suspect 13**	**0.43223**
Suspect 19	**0.22038**	**Suspect 11**	**0.35085**	**Suspect 18**	**0.20946**
Suspect 20	**0.21915**	**Suspect 13**	**0.13739**	**Suspect 17**	**0.11841**
Suspect 15	**0.18210**	**Suspect 12**	**0.06354**	**Suspect 12**	**0.09309**
Suspect 14	**0.01542**	**Suspect 16**	**0.03364**	**Suspect 11**	**0.07719**
Suspect 7	**0.00185**	**Suspect 19**	**0.02013**	**Suspect 16**	**0.04487**

Table 2. Nine example topics with ten most relevant words and six authors with their probabilities extracted from the Kos, Enron and Nips databases.

Table 3. Criminal probabilities and relationships for criminal probabilistic network.

Suspects	**Probabilities**	**Relationships**
1	0.144	2,3,4,5,6,14,15,19,20
2	0.216	1,3,4,5,6,14,15,19,20
3	0.91	1,2,4,5,6,14,15,19,20
4	0.576	1,2,3,5,6,14,15,19,20
5	0.025	1,2,3,4,6,14,15,19,20
6	0.036	1,2,3,4,5,14,15,19,20
7	0.083	8
8	0.648	7
9	0.024	-
10	0.891	11,12,13,16,17,19,20
11	0.387	10,12,13,16,17
12	0.153	10,11,13,16,17
13	0.504	10,11,12,16,17
14	0.072	15,20
15	0.765	14,19,20
16	0.92	10,11,12,13,17,19,20
17	0.486	10,11,12,13,16,19,20
18	0.648	19
19	0.452	1,2,3,4,5,6,14,15,10,16,17,18,20
20	0.837	1,2,3,4,5,6,14,15,10,16,17,19

But, as indicated in Table 4, having shared documents is not always important to find high values of similarity. Suspect 1 and suspect 6 do not have any shared documents but their value of similarity is 0.9187 as they include documents from group of same dataset. Because the similarities are measured using the topic assignments of authors. For example, suspect 19 and 20 are assigned 2951 and 1950 times respectively to topic 130.

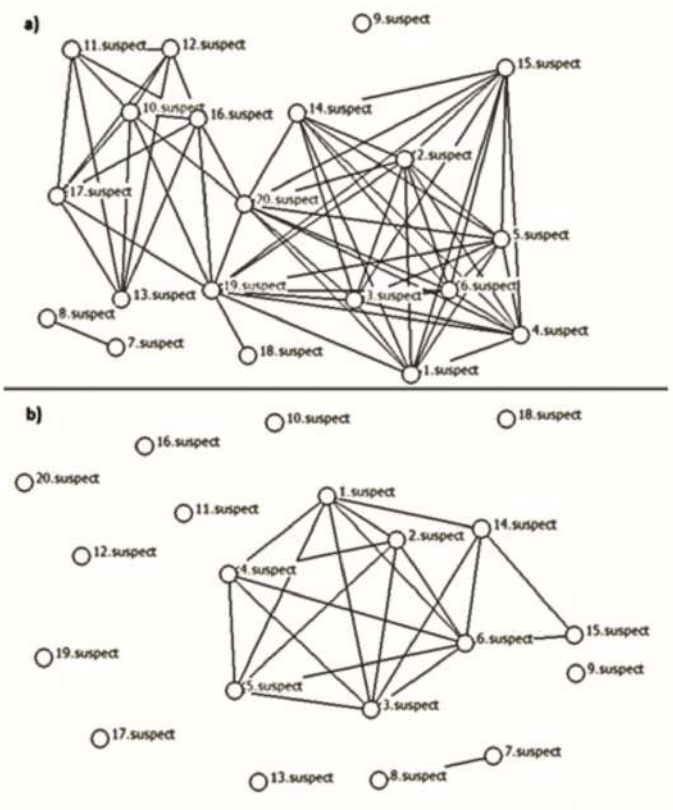
Figure 1 is the visualization of the criminal probabilistic network as threshold is 0.5 and 0.8. This network has 20 members and the number of edge depends on the threshold. Suspect 19 and 20 have the most intense relations whereas threshold is 0.5. In terms of intensity of relations, the other suspects such as 1, 2 and 3 follow them. According to social network dynamics [10], the number of relations shows how active a suspect is. Therefore, suspect 19 and 20 are evaluated as a leader or hub in the network. Specially, suspect 20 has high relationship and criminal possibility. Then, it can be primarily investigated to analyze the criminal network. By using different threshold values, groups in the network can be discovered according to density of relationships. For instance, as threshold is 0.8, a group consisting of suspects 1, 2, 3, 4, 5, 6, 14 and 15 is formed.

In our study, we have primarily aimed to construct the topic-based criminal probabilistic network. The obtained network may be used for solving the problem of choosing the next investigate suspects. Based on the experiment, some problems are discussed. Primarily, measuring the effectiveness of the proposed method depends on real datasets belonging to the suspects. Whereas relations among the suspects are being clarified, mutual information among them should also be

revealed. In this way, common values on which their relations are based will be more easily understood.

Figure 1. Visualization of the 20-member criminal probabilistic network.

a) threshold=0.5, b) threshold = 0.8 (section C).



V. CONCLUSION

In this paper, we present a new approach to criminal network analysis using suspect probabilities. Text documents of suspects can give cues of a specific event for crime investigators. None of previous studies on criminal network analysis focused on creating a criminal probabilistic network. But, regarding the suspects, crime possibilities of them have to absolutely be taken into account. Network which is formed in our study in respect of the short descriptions about the documents acquired, criminal probabilities is calculated and clarified relationships among the suspects by the use of Author-Topic Model. We used a corpus which was generated with combination of Kos, Enron and Nips datasets. With using the corpus, we constructed criminal probabilistic network.

This study suggests several different directions for future work. Firstly, we will enhance this method by using individuals' text documents which are obtained from their hard-disks. Secondly, a method will be proposed for the problem of determining the next suspects who will be primarily investigated in criminal probabilistic network which is obtained from our method. Finally, we will redefine

Table 4. Some similarities among the suspects according to cosine similarity method.

	3	5	6	8	9	11	13	15	18	20
1	0.9	0.87	0.91	0	0	0	0	0.78	0.31	0.56
2	0.9	0.87	0.89	0	0	0	0	0.77	0.30	0.56
3	1	0.88	0.91	0	0	0	0	0.79	0.30	0.56
4		0.91	0.86	0	0	0	0	0.77	0.29	0.55
5		1	0.85	0	0	0	0	0.76	0.29	0.55
6			1	0	0	0	0	0.80	0.29	0.52
7				0.91	0.41	0	0	0.24	0.28	0.07
8				1	0.44	0	0	0.23	0.27	0.07
9					1	0	0	0.13	0.15	0.03
10						0.56	0.64	0	0.35	0.51
11						1	0.66	0	0.38	0.38
12							0.63	0	0.38	0.36
13							1	0	0.43	0.42
14								0.84	0.35	0.49
15								1	0.41	0.51
16									0.45	0.67
17									0.47	0.60
18									1	0.49
19										0.69
20										1

measures of social network dynamics such as node, group and link measures to analyze the network.

REFERENCES

[1] Mark Steyvers, Padhraic Smyth, Michal Rosen-Zvi, and Thomas Griffiths. 2004. Probabilistic author-topic models for information discovery. In Proceedings of the tenth ACM SIGKDD international conference on Knowledge discovery and data mining (KDD '04).

[2] David M. Blei, Andrew Y. Ng, and Michael I. Jordan. 2003. Latent dirichlet allocation. J. Mach. Learn. Res. 3 (March 2003), 993-1022.

[3] Z. Xia. 2008. Fighting criminals: Adaptive inferring and choosing the next investigative objects in the criminal network. Know.-Based Syst. 21, 5 (July 2008), 434-442.

[4] Gaston L'Huillier, Sebastián A. Ríos, Hector Alvarez, and Felipe Aguilera. 2010. Topic-based social network analysis for virtual communities of interests in the Dark Web. In ACM SIGKDD Workshop on Intelligence and Security Informatics (ISI-KDD '10). ACM, New York, NY, USA, Article 9, 9 pages.

[5] Ding Zhou, Eren Manavoglu, Jia Li, C. Lee Giles, and Hongyuan Zha. 2006. Probabilistic models for discovering e-communities. In Proceedings of the 15th international conference on World Wide Web (WWW '06). ACM, New York, NY, USA, 173-182.

[6] Rabeah Al-Zaidy, Benjamin C. M. Fung, and Amr M. Youssef. 2011. Towards discovering criminal communities from textual data. In Proceedings of the 2011 ACM Symposium on Applied Computing (SAC '11). ACM, New York, NY, USA, 172-177.

[7] Z.Xia and Z. Bu. 2012 Community detection based on a semantic network. Knowledge-Based Systems, 26, pp. 30-39.

[8] Michal Rosen-Zvi, ChaitanyaChemudugunta, Thomas Griffiths, Padhraic Smyth, and Mark Steyvers. 2010. Learning author-topic models from text corpora. ACM Trans. Inf. Syst. 28, 1, Article 4 (January 2010), 38 pages.

[9] K. Baumgartner, S. Ferrari, and G. Palermo. 2008. Constructing Bayesian networks for criminal profiling from limited data. Knowledge-Based Systems 21, 563-572.

[10] Jennifer Xu and Hsinchun Chen. 2005. Criminal network analysis and visualization. Commun. ACM 48, 6 (June 2005), 100-107.
[11] Jennifer J. Xu and Hsinchun Chen. 2004. Fighting organized crimes: using shortest-path algorithms to identify associations in criminal networks. Decis. Support Syst. 38, 3 (December 2004), 473-487.
[12] S. Deerwester, S. Dumais, T. Landauer, G. Furnas, and R. Harshman. 1990. Indexing by Latent Semantic Analysis. Journal of the American Society of Information Science, 41(6):391-407.
[13] A. McCallum, X. Wang, and A.C. Emmanuel. 2007. Topic and Role Discovery in Social Networks with Experiments on Enron and Academic Email. Journal of Artificial Intelligence Research 29 (2007).
[14] T. Hofmann.1999. Probabilistic Latent Semantic Indexing. Proceeding of the Twenty-Second Annual International SIGIR Conference.
[15] H. Chen, H. Atabakhsh, T. Petersen, and Chuck Violette. 2004. COPLINK center: information and knowledge management for law enforcement. In Proceedings of the 2004 annual national conference on Digital government research (dg.o '04). Digital Government Society of North America, Article No: 16 , 2 pages.
[16] J. Xu and H. Chen. 2008. The topology of dark networks. Commun. ACM 51, 10 (October 2008), 58-65.
[17] C. C. Yang and T. D. Ng. 2007. Terrorism and crime related weblog social network: Link, content analysis and information visualization. In IEEE International Conference on Intelligence and Security Informatics (ISI), pages 55-58.
[18] Mark Stevyers and Tom Griffths. 2007. Handbook of latent semantic analysis : A road to meaning.

Bilişim Suçlarında Delillendirme

Ç. Ülküdemer

Özet— **Bu çalışma, bir adli olaydaki bilişim delillerinin taşıması gereken temel özellikler, kopya çıkarma aşamasında karşılaşılan temel problemler ile dikkat edilmesi gereken konular, kopya çıkarma aşamasında delilin bütünlüğü ve güvenilirliğine yönelik suistimallerin nasıl yapıldığı ile bu suistimallerin tespitinin mümkün olup olmayacağı hususlarını kapsamaktadır.**

Anahtar Kelimeler— **Bilişim suçları, bilişim suçlarına müdahale, elektronik delil, kopya çıkarma, imaj alma, adli kopya, adli bilişim, arama ve el koyma.**

Evidences in IT Crimes

Abstract— **This paper covers the fundamental properties of IT criminal evidences, the problems while getting the digital image of evidences and the important topics related IT criminal. Also includes, abusement of evidence integrity and reliability and if it is possible to understand the integrity problems.**

Index Keywords— **IT crimes, IT crimes incident response, digital evidence, digital image, IT law, criminal investigation on IT crimes.**

I. GİRİŞ

Bilişim teknolojilerinin günlük hayatta kullanımının her geçen gün artarak yaygınlaşması, bilişim sistemlerinin kullanımında suistimallerin artmasına ve bilişim suçlarının oluşmasına neden olmaktadır. Bilişim suçunun konusu bazen araç olarak kullanılan bir bilişim sistemi olabileceği gibi, hedef olarak seçilen bir bilişim sistemi de olabilmektedir. Özellikle internet üzerindeki pek çok platformun hayatımızı kolaylaştıran imkânlar sunması da, suçlular için bu platformları oldukça cazip hale getirmektedir. Bilişim sistemlerinin uzaktan erişim yöntemleri ile kullanılabilmesi, bilişim sistemlerine yapılan kaynağı belirsiz saldırılar, verilere izinsiz erişme, değiştirme ya da silme/bozma gibi durumlarda delillerin toplanması, incelenmesi ve faillerin tespiti adli bilişim uzmanlarının işini her geçen gün zorlaştırmaktadır.

Bilişim sistemlerindeki temel sorunlardan birisi, verinin oluşturulduğu tarih-saat bilgisinin sonradan değiştirilebilmesi ve istenilen tarih-saat bilgisi ile yeniden oluşturulabilmesidir. Bu nedenle delile müdahale aşamasında, adli kopyası (imaj) alınan sistemin tarih-saat bilgisinin güncel tarih-saat bilgisi ile karşılaştırılmasının yapılması ve bu hususun arama el koyma tutanağına yazılması gerekmektedir. Ayrıca, bir sistemde veriler kopyalanırken, kopyalanan verilere ait erişim, değiştirilme, silinme, taşınma, aidiyet, yetki v.b. gibi bilgilerin de kopyasının alınması gerekmektedir. Zira, bilişim sistemlerindeki verilerin çeşitli teknik ve yöntemlerle manipüle edilmesi mümkündür. Bu nedenledir ki, bilişim sistemlerinin adli kopyasının alınması, olaya müdahale (incident response) metotları ile yapılmalı, aksi halde yapılan işlemlerde delilin bütünlüğü ve güvenilirliği şüpheli duruma düşmekte ve delil niteliğini kaybetmektedir.

Bir bilişim sisteminin adli incelemesinde delillerin bulunabileceği alanlar şunlardır:

- Fiziksel alanlar:
  - Manyetik alanlar,
    - Sabit diskler,
    - ZIP kasetler,
    - Floppy disketler.
  - Optik alanlar,
    - CD-R,
    - DVD-R, DVD+R, DVD-RAM,
    - BLUERAY.
  - NAND ve NOR alanlar,
    - USB bellekler,
    - SSD'ler,
    - Diğer bellekler (SD, MMC, MS, xD v.b.)
    - RAM'ler.
- Mantıksal alanlar:
  - Dosya sistemleri,
    - ReFS, NTFS, FAT32, FAT 16,
    - Ext2, Ext3, Ext4,
    - HPFS, HFS+, CDFS.
  - İşletim sistemleri,
    - MS Windows,
    - Linux/Unix/Free BSD,
    - MacOS,
    - Mobil (gömülü) sistemler.
  - Uygulamalar,
    - Veri tabanları,
    - İnternet uygulamaları,
    - Office dosyaları,
    - Diğer dosyalar.
- Ağlar:
  - Yerel Ağlar (LAN),
  - Uzak/Geniş Ağlar (WAN),
  - Özel Sanal Ağlar (VPN).

II. BİLİŞİM SİSTEMLERİNDE ORTAMLAR VE İNCELEMELER

A. İşletim Sistemleri

İşletim sistemini çekirdek modunda çalışan bir yazılım olarak tanımlamaktan daha fazla bir şey söylenemez, ki bu her zaman doğru değildir. İşletim sistemi hem programcılara aygıtları yönetebileceği bir komut seti sağlar hem de bu aygıtları kontrol eder [1].

Bu nedenle işletim sistemlerinin çalışma mantığı ve diğer aygıtlarla nasıl bir etkileşim içerisinde olduğu programcıya göre değişen bir kavramdır ve *her sistem kendi bütünü içerisinde incelenmelidir.*

Bir işletim sisteminde verilerin, özellikle değiştirilme, silinme dışında kaybolması ancak;

- Doğal felaketler: Yangın, sel, deprem vb.,
- Donanım ya da yazılım hataları: CPU hataları, disk okuma/yazma hataları, iletişim hataları, yazılım hataları vb.,
- İnsan hataları: Hatalı komut/girdi, hatalı bilişim sistemi etkileşimleri, bilerek/bilmeyerek hatalı program çalıştırma ile mümkündür [2].

Bu nedenle işletim sistemlerindeki komutların özellikleri ve sonuçları adli incelemeyi gerçekleştirecek uzmanlar tarafından tarafsız, önyargısız, varsayımsız olarak incelenmelidir. Bu hususları yerine getirebilmek için bilimsel bir inceleme metot ve yöntemi oluşturulmalı ve oluşturulan bu metot ve yöntem her zaman denetime açık ve kontrol edilebilir olmalıdır.

Günümüzde yaygın olarak kullanılan işletim sistemleri Windows, Linux, Unix, OsX ve BSD'dir. Ancak tüm bu işletim sistemlerinin bir türevinin cep telefonu, tablet vb. araçlarda da kullanıldığını unutmamak gerekir.

İşletim sistemleri belirli ölçülerde özelleştirilebilmekte ve yaygın kullanılan komutlar farklı amaçlar için de kullanılabilmektedir. Bu nedenle inceleme esnasında, kullanılan komutların dosya bütünlük değerleri (hash value), orijinal hali ile karşılaştırıldıktan sonra içerik analizi yapılmalıdır. Linux işletim sistemine özel olarak bu karşılaştırmaları yapan en yaygın araçlardan biri GPL lisans ile açık kaynak kodlu olarak dağıtılan *rootkithunter* projesidir [3].

İşletim sistemlerinin kullanıcılar tarafından özelleştirilmesi, suç işleyenler tarafından da kötüye kullanılabilmekte ve özellikle işletim sisteminin kapatılması esnasında delil niteliği taşıyacak pek çok verinin silinmesi için programlanabilmektedir. Bu nedenle, adli bilişim eğitimlerinde uzman adaylarına olaya ilk müdahalenin nasıl yapılacağı anlatılırken, genellikle sistemleri normal kapatma (shutdown) yerine fişinin çekilmesi (power off) tavsiye edilmektedir [4].

Bu tavsiyenin kabul edilebilir gerekçeleri olsa da, sistemlerin düzgün kapatılmaması yazılımsal ve donanımsal sorunlara yol açıp veri delillerin bozulmasına hatta kaybolmasına sebep olabilir.

Adli kopyanın çıkarılması ile ilgili diğer temel bir sorun ise; adli kopyası alınacak optik depolama aygıtlarının (CD, DVD, BlueRAY) kopyasının fiziksel ya da mantıksal olarak hangi yazılım ve sürümü ile alındığının ve kopyalama neticesinde oluşan elektronik imzanın arama-el koyma tutanağı ve bilirkişi (expertiz) raporlarına detaylı olarak yazılmamasıdır. Zira, adli bilişim incelemelerinde delilin doğrulanma (verification) aşamasında, adli kopyaların elektronik imzalarının adli bilişim yazılımları ile kontrolü yapılmaktadır. Adli kopyanın alındığı yazılım haricinde başka bir yazılım kullanıldığında, farklı bütünlük değerleri hesaplanabilmektedir. Bu durum, optik disklerin yapısı, verilerin yazılma formatı, adli kopyaların fiziksel ya da mantıksal olmasının adli bilişim yazılımları tarafından farklı işleme tabi tutulması ve bu alandaki standardın tam olarak sağlanamamasından kaynaklanmaktadır [5]. Bu nedenle, doğrulama yapılırken aynı yazılım ve sürümü ile yapılması önerilmektedir.

B. Dosya Sistemleri

Bir verinin bir işletim sistemi üzerinde yazılması/okunması için geliştirilmiş algoritmik düzene dosya sistemi denilmektedir [6].

Farklı amaçlar için geliştirilmiş onlarca dosya sistemi mevcuttur. En yaygın kullanılan dosya sistemleri: NTFS, FAT, EXT-3, HFS'tir. Bunlar, yaygın kullanılan işletim sistemlerinin ön tanımlı dosya sistemleridir. Tüm dosya sistemleri disk üzerinde veriyi farklı bir şekilde barındırırlar ve inceleme sırasında bu verilerin nasıl bulunduğunun, kopyalama, değiştirme, taşıma ve silme işlemleri sırasındaki hareketlerinin iyi bilinmesi gerekmektedir.

5271 sayılı Ceza Muhakemesi Kanunu'nun (CMK) 134. maddesi ile Adlî ve Önleme Aramaları Yönetmeliği'nin 17. maddesinde bir bilgisayar sisteminde arama, kopyalama ve el koymanın nasıl yapılacağı belirtilmiştir. Gerekli tedbirlerin alındığı zaruri haller hariç, şüphelinin veri depolama aygıtları üzerinde canlı inceleme yapılmamalıdır. Ayrıca, delil üzerinde değişikliğe yol açacak ve delili şüpheli hale getirecek işlemlerden kaçınmalı, mümkünse delilin adli kopyası iki farklı diske alınmalı ve inceleme bu kopyalardan biri üzerinde yapılmalıdır. Böylece, taşınma ve inceleme esnasında oluşabilecek hata, zarar ve bozulmaların önüne geçilmelidir.

Hemen tüm dosya sistemleri *META DATA* (üst veri) adı verilen bilgiler üzerinde dosyanın oluşturulma, değiştirilme, son erişim, son çıktı alma v.b. bilgiler bulunmaktadır. Tüm bu veriler dosya sisteminin bir parçası olduğundan ve belirli bir sistematikte saklandığından değiştirilmesi mümkündür.

Bu nedenle, *pratikte dosya sistemi üzerindeki veriyi adli kopya (imaj) alma aşamasında bile değiştirmek mümkündür.*

Delilin güvenilirliğini sağlamak için *donanımsal yazma önleme sistemlerinin* (write blocker) adli kopya alma esnasında mutlaka kullanılması gerekmektedir.

Adli kopya alma esnasında *yazılımsal yazma önleme teknikleri* de mevcuttur. Yazılımsal çözümler, BIOS üzerindeki INT13h kodunu engelleyerek bunu gerçekleştirmektedir. Ancak, BIOS kontrollerini etkisiz hale getirmek mümkün olduğundan yazılımsal önleme teknikleri pek tercih edilmemektedir [7].

Adli kopya (imaj) alma işlemi, dosya sistemi üzerindeki her biti/bloğu sırası ile bir dosya/disk üzerine yazmak için kullanılmaktadır. Adli kopya almak için kullanılan en yaygın yöntemlerden birisi açık kaynak kodlu *dd* yazılımıdır. Pek çok adli kopya alma yazılımının da uyguladığı yöntem bu yazılımdan türemiştir. EnCASE, FTK Autopsy gibi ticari adli inceleme yazılımlarının kendi adli kopya alma sistemleri de mevcuttur.

Disk üzerindeki okuma hataları adli kopya alma sistemi tarafından görmezden gelinerek, okunabilen ilk alandan son alana kadar adli kopyalama işlemi yapılır. Bu hatalar veri alanları arasındaki ilişkileri bozabilir. Örneğin, veri silinmediği halde disk üzerinde gözükmez ve META DATA alanında da silinme tarihi yer almaz. Bu durum, verinin silindiği ve META DATA bilgisinin de bilerek ve isteyerek (delil saklama maksatlı) değiştirildiği şeklinde yorumlanmamalıdır.

Özetle, dosya sistemleri birbirleri ile ilintilendirilmiş çeşitli tablolardaki ilişkisel yapılardan yararlanarak veriye ulaşırlar. Bir nedenle referans tabloları hasar görürse (genellikle disk okuma/yazma hataları sonucu) veri silinmediği halde, dosya sistemi üzerinde ulaşılamaz duruma gelebilir. Bu dosyalar adli inceleme yazılımları ile diskin adli kopyasının incelemesinde görülebilirler, çünkü adli inceleme yazılımları referans tablolarında yer almayan dosyaları da gösterebilmektedir. Bu dosyalar gerçekte silinmediğinden, silinme tarihleri meta data tablosundaki ilgili alanlarda işaretlenmezler ve genellikle 0000.00.00 olarak tespit edilir. Bu durumda *delilin sağlıklı bir şekilde elde edilemediği* unutulmamalıdır.

C. Uygulama ve Veri Tabanları

Uygulamalar, genellikle verilerin oluşturulduğu, veri tabanları ise uygulamalara bağlı olarak bu verilerin saklandığı yerlerdir. Uygulamalar ile oluşturulan verilerin adli incelemesinde genellikle verinin oluşum tarihi ve saati önemlidir. Tarih ve saatin bilgisayarın BIOS'u üzerinden işletim sistemine aktarıldığı, sonrasında ise uygulamaya gönderildiği unutulmamalıdır. Zaman sunucuları (NTP) ya da ara uygulamalar ile işletim sistemi açıldıktan sonra saati değiştirmek mümkün olsa bile bu durum kötüye de kullanılmaktadır.

Uygulamaların oluşturacağı bir verinin ya da sistem kaydının oluşma zamanı, bilerek ve isteyerek sadece bilgisayarın saati değiştirilerek de değiştirilebilir. Bu nedenle inceleme sırasında sistem saatine asla güvenilmemelidir. 5651 sayılı İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanun'da sistem kayıtlarının zaman damgası ile tutulmasının gerekçesi de bundan kaynaklanmaktadır.

Üçüncü bir tarafça sabitlenmeyen hiç bir zaman verisi olay zamanını sabitlemez. Suçlular tarafından bilerek ve isteyerek zaman verilerinin değiştirilmesi özellikle ağ üzerinden yapılan saldırı olaylarının seyrini tamamen değiştirebilecek sonuçlar yaratmaktadır.

Bütün bunlardan hareketle, uygulama incelemelerinde aynı koşullarda uygulamanın algoritmik tepkileri ve oluşturdukları verilerin karakteristik özellikleri, bağlı bulunduğu veri tabanı ve diğer bileşenlerle birlikte değerlendirilmeli, ancak incelemeye konu olan dosyalardaki zamanlara ve verilere güvenilmemelidir.

Uygulamaların / veri tabanlarının verileri nasıl sildiği, değiştirdiği ya da nereye nasıl bir formatta kaydettiği adli inceleme açısından çok daha önemlidir. Uygulamaların verileri kurtarılamayacak şekilde silmesi ile ilgili durumlara çok nadir rastlanmakla birlikte, çoğunlukla bu sorunun cevabı dosya sistemlerinde aranmalıdır.

D. Bellek ve Takas Alanları

Belleklerin yönetimi işletim sistemlerinin sorumluluğundadır. Bellekler bir uygulamanın çalışması sırasında geçici verilerin yazıldığı ya da değişken bilgilerinin tutulduğu alanlardır. Kullanıcı bellek alanları 3 parçadan oluşmaktadır:

- Code Segment (Kod Kesimi)
- Data Segment (Veri Kesimi)
- Stack Segment (Yığın Kesimi)

Tüm bu veri alanları, kullanıcı kabuk bilgilerini taşıdığı gibi aynı zamanda parolaların ya da kullanıcılar ile ilgili önemli verilerin barındırıldığı yerlerdir. İşletim sistemi üzerinde kullanıcılar arasındaki paylaşımlar da buralarda yapılmaktadır [8].

Takas alanları bir depolama ünitesi üzerinde bellek gibi kullanılan yapılardır. Windows işletim sisteminde bu alana *Sanal Bellek* (virtual memory), Unix/Linux ve türevi işletim sistemlerinde *Swap* adı verilir.

Fiziksel bellekler (RAM) elektrik olmadığı sürece bilgi depolayabilecek bir özelliğe sahip değildirler. Bu nedenle bilgisayar her açıldığında yeniden sıfırlanır.

Bir bilgisayar belleğinin adli incelemesi yapılacak ise sistem kapatılmadan ya canlı olarak yapılması ya da belleğin adli kopyası alındıktan sonra yapılması gerekir. Olaya müdahale esnasında sistemlerin belleğinin adli kopyasının

alınmaması yaygın olarak yapılan hatalardan birisidir.

Takas alanları veri depolama alanları üzerinde durduğu için bu alanlar bilgisayar kapatıldıkran sonra da incelenebilir. Tabi ki bilişim ortamındaki tüm veriler gibi bu alanlardaki verilerin de yeniden üretilmesi, değiştirilmesi ya da silinmesi mümkündür.

E. Ağ İncelemeleri

Ağ incelemeleri, bilgisayar incelemelerinden daha farklı ele alınması gereken bir kavramdır. Ağ üzerinde gelen paketlerin gerçek zamanlı kaydı ile mümkündür. Günümüzde özellikle uzak bağlantıların bir film izler gibi (SSH, RDP, VNC, Telnet, ICA) izlenebildiği ve kayıt edilebildiği sistemler vardır ve adli incelemeler için de bu sistemlerden faydalanılmaktadır [9].

Ağ incelemelerinde, suçu ya da suistimali delillendirmek için gerçek zamanlı ağ trafiği yeterli bir zaman aralığı boyunca kopyalanmalı ve inceleme bu kopya üzerinde adli bilişim imkânları ile yapılmalıdır. Ağ incelemelerinde, gerçek zamanlı yapılmamış kayıtların dışında delil elde etmek mümkün değildir. Ancak ve ancak *gerçek zamanlı olarak kayıt edilen deliller kesin delil niteliği taşır*.

F. Verilerin Kesinliği ve Zaman Damgası

Bilişim sistemlerinde olay anında ayrıca kaydedilmeyen (ki bu ağ bağlantıları için geçerlidir) hiç bir veri kesin delil niteliği taşımaz. ***Bilişim ortamında bütün veriler değiştirilebilir, silinebilir ve yeniden oluşturulabilir.***

Bu nedenle gerçek zamanlı olarak kayıt edilen ağ verileri zaman damgası ile damgalandıktan sonra saklanmalıdır. Zaman damgası ile damgalanan veriler, sadece verinin zaman damgası alındıktan sonra değişmediğinin ispatı için kullanılabilir.

G. Delil saklama ile ilgili işlemler

Bilişim delilleri bağlı bulunduğu sistemler ile birlikte saklanmalıdır. Hangi kablonun nereye bağlı olduğu, hangi sistemlerin açık olduğu inceleme esnasında çok önemlidir. Özellikle bağlandıkları noktalar ayrıca işaretlenmeli, fotoğraf ve video ile kayıt altına da alınarak yapılan tüm işlemler tutanağa geçirilmelidir.

Bilişim ortamlarında veri saklama ortamlarının çoğu manyetik alan kullanarak veri kaydettiğinden, bu tarz medyaların antistatik bir ortamda saklanması gerekmektedir.

Diskler mutlaka iki farklı diske adli kopya alındıktan sonra alınan kopyalardan biri üzerinden incelenmelidir.

Bilişim sisteminin her açılıp kapanması sırasında verilerin değişebileceği ya da silinebileceği unutulmamalıdır.

III. SONUÇ

Bilişim sistemlerindeki veriler silinebilir, değiştirilebilir ya da yeniden oluşturulabilir. Bu nedenden ötürü gerçek zamanlı olarak kaydedilmemiş hiç bir veri kesin delil olarak değerlendirilmemelidir. Sistemlerin saatlerinin değiştirilmesi dosyalar üzerinde yapılan işlem zamanlarını güvenilmez yapar. Ancak, delile müdahale aşamasında adli bilişim metot ve tekniklerinin usulüne uygun olarak yerine getirilmesi ve yapılan her türlü işlemin kayıt altına alınması elektronik delilin güvenilirliğini sağlayabilir.

Dosya meta dataları bir çok yazılım tarafından değiştirilebildiği için tamamen bu verilere dayanılarak hüküm verilemez, ancak meta data verileri ana delilleri destekleyen yan deliller olarak kullanılabilir.

Veri depolama aygıtlarının adli kopyalarının alınması esnasında donanımsal yazma önleme sistemlerinin kullanılmaması, delilin güvenilirliği ve bütünlüğü konusunda şüpheye neden olur ve alınan kopya delil niteliği taşımaz.

KAYNAKLAR

[1] Andrew S. Tanenbaum, *Modern Operating Systems, 3/E,* Prentice Hall, pp 1-4, 2007.
[2] Andrew S. Tanenbaum, *Modern Operating Systems, 3/E,* Prentice Hall, pp 9-6, 2007.
[3] RootkitHunter, http://www.rootkit.nl/projects/rootkit_hunter.html
[4] Semih Dokurer, Kriminal Polis Laboratuvarı, *Bilişim Suçları ve Adli Bilişim Sunumu* , Wormy, pp 20, 2005.
[5] Christopher Marberry and Philip Craiger, *Factors Affecting One-Way Hashing of CD-R Media*, IFIP Int. Conf. Digital Forensics, pp 1-13 2007.
[6] Daniel Grosshans, *File systems: Design and Implementation*, Prentice Hall, pp1,5, 1986.
[7] Brain Carrier, *File System Analysis*, Addison Wesley Professional, pp 49-50, 2005.
[8] Graham Glass, *UNIX For Programmers and Users* , Prentice Hall, pp 533, 1993.
[9] Shell Control Box, http://www.balabit.com/network-security/scb/features

Ç. Ülküderner 2003 yılında bilgisayar mühendisi olarak mezun oldu. 2007 yılında 'Kablosuz Ağlarda Güvenlik' üzerine yazdığı tezi ile birlikte yüksek mühendis ünvanını aldı. TÜBİTAK'ta uzun yıllar sistem yöneticisi olarak çalıştı sonra, Hacettepe Üniversitesi Bilişim Hukuku yüksek lisans programında ders verdi.

Yurt içi ve yurt dışında bilgi güvenliği ile ilgili pek çok projede yer aldıktan sonra Profelis Bilişim adındaki şirketini kurdu. Halen şirketin yönetcisi olarak meslek hayatına devam etmektedir.

Siber Güvenlik Makro Analiz Modeli Önerisi ve Türkiye'nin Analizi

Hakan ŞENTÜRK, Celal Zaim ÇİL, Şeref SAĞIROĞLU

***Özet*— 21'inci yüzyılın en kritik güvenlik tehdidi olan siber güvenlik konusundaki saldırı haberleri ile ülkelerin siber savunma amacıyla icra ettiği çeşitli faaliyetler yazılı ve görsel medyada sürekli olarak yayımlanmaktadır. Ancak, yazarların bilgisi dahilinde, ülkeler tarafından yapılan faaliyetlerin kapsamlı bir metodoloji altında incelenmesine yönelik bir çalışma yada model bulunmamaktadır. Bu bildiri, literatürdeki bu boşluğu gidermeyi amaçlamaktadır. Çalışma kapsamında, ülkelerin siber güvenlik durumlarının analiz edilebilmesi amacıyla yedi temel gösterge ve ilgili alt göstergeleri kapsayan bir analiz modeli önerilmiş, önerilen model kullanılarak Türkiye'nin siber güvenlik analizi yapılmıştır.**

***Anahtar Kelimeler*—Siber güvenlik, siber güvenlik analizi, siber savaş, siber tehdit.**

***Abstract*—The cyber attack news regarding the most critical security threat of the 21st century as well as the cyber security activities that the countries perform in order to defend their cyberspace are continuously published in print and visual media. Yet, to the knowledge of the authors, there is no formal study or a model, where the various cyber security activities of the countries can be analysed by following a comprehensive methodology. This paper aims to fill this gap in the literature. In this paper, in order to analyse the countries' cyber security postures, a cyber security macro analysis model that consists of seven main indicators and related sub-indicators is proposed and Turkey's cyber security analysis is performed using the proposed model.**

***Keywords*—Cyber security, cybersecurity analysis, cyber warfare, cyber threat.**

Bu bildirinin ihtiva ettiği hususlar, yazarların şahsi görüşleri olup, kurumlarının resmi görüşlerini yansıtmamaktadır.

I. GİRİŞ

Siber güvenliği, Uluslar arası Telekomünikasyon Birliği (ITU), "Siber ortamda, kurum, kuruluş ve kullanıcıların varlıklarını korumak amacıyla kullanılan; araçlar, politikalar, güvenlik kavramları, güvenlik teminatları, kılavuzlar, risk yönetimi yaklaşımları, faaliyetler, eğitimler, en iyi uygulamalar ve teknolojiler bütünüdür." şeklinde tanımlamaktadır.

Devletlerarası düzeyde ilk kez 2007 yılında gerçekleşen Estonya Siber Savaşından günümüze kadar olan dönemde, Rusya-Gürcistan (Güney Osetya Anlaşmazlığı), K.Kore-ABD, Çin-Hindistan ve son olarak İran nükleer tesislerinin hedef alındığı Stuxnet saldırısı gibi pek çok siber saldırı olayı gerçekleşmiştir. Bu saldırılar, siber savaşların şiddetinin zamanla daha da artacağını, bu nedenle 21'inci yüzyılda siber uzayın güvenliğinin sağlanmasının kritik önemi olduğunu ortaya çıkarmıştır. Nitekim Birleşik Krallık Kabine Ofisinin Haziran 2009'da "Birleşik Krallık Siber Güvenlik Stratejisi" adıyla hazırladığı raporda, ilgi çekici bir saptama yapılarak, milli güvenlik için 19'uncu yüzyılda denizlerin, 20'nci yüzyılda hava sahasının tehdit altında olduğu ve emniyetinin alınmasının önem arz ettiği, 21'inci yüzyılda ise siber uzayda avantajlı konuma geçilmesi gerektiği ifade edilmiştir [1].

Bu gelişmelere paralel olarak ülkelerin de siber güvenlik alanında önüne geçilemez bir rekabet içerisinde oldukları gözlemlenmektedir. Her geçen gün, çeşitli ülkelerin savunma ve hatta saldırı amacıyla siber birimler teşkil ettiği, farkındalığın artırılması ve siber tehdide karşı konulabilmesi amacıyla siber güvenlik eğitim, sempozyum ve tatbikatlarının icra edildiği bilgileri medyada yer almaktadır.

Ülkelerin siber güvenlik faaliyetlerinin bir metodoloji izlenerek analiz edilebilmesi amacıyla bir model önerilen bu çalışmada; ikinci bölümde araştırmanın amacı, kapsamı ve izlenen metodoloji ortaya konulmuştur. Siber güvenlik makro analiz modelinin önerildiği üçüncü bölümde, belirlenen yedi temel gösterge ve her bir gösterge kapsamında incelenebilecek hususlar incelenmiştir. Son bölümde ise önerilen model kullanılarak Türkiye'deki durum analiz edilmiştir.

II. ARAŞTIRMANIN AMACI; KAPSAMI VE METODOLOJİ

Çalışmanın amacı; değişen güvenlik anlayışı içerisinde, siber savaşa karşı stratejik planlamanın rolünün önemini vurgulamak ve ülkelerin siber güvenlik analizlerinin yapılabilmesi için bir model önerisi sunmaktır. Çalışmada, siber güvenlik alanında literatür taraması yöntemi kullanılarak, makro seviyede ülkelerin siber güvenlik durumlarının analiz edilebilmesi amacıyla aşağıda listelenen yedi temel gösterge ve ilgili alt göstergeleri kapsayan bir analiz modeli önerilmiştir.

Manuscript received March 11, 2012.

Bilg.Y.Müh. Hakan ŞENTÜRK, Kara Harp Okulu Savunma Bilimleri Enstitüsü, Ankara. (Tlf: 312-414-2631; e-mail: hsenturk@hvkk.tsk.tr).

Prof.Dr. Celal Zaim ÇİL, Çankaya Üniversitesi Elektronik ve Haberleşme Mühendisliği, Ankara (e-mail: czaimcil@cankaya.edu.tr).

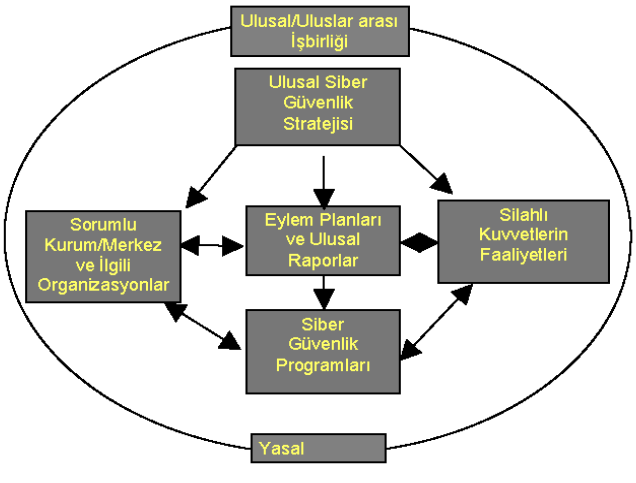
Prof.Dr. Şeref SAĞIROĞLU, Gazi Üniversitesi Bilgisayar Mühendisliği, Ankara (e-mail: ss@gazi.edu.tr)

1- Ulusal Siber Güvenlik Stratejisi
2- Eylem Planları ve Ulusal Raporlar
3- Yasal Mevzuat
4- Sorumlu Kurum/Merkez ve İlgili Organizasyonlar
5- Siber Güvenlik Programları
6- Silahlı Kuvvetler Siber Güvenlik Faaliyetleri
7-Ulusal/Uluslararası İşbirliği

Çalışmanın ikinci bölümünde ise önerilen modelin rehberliğinde belirlenen göstergeler doğrultusunda Türkiye'nin siber güvenlik analizi yapılmış, zafiyet noktaları tespit edilerek alınması gereken tedbirler belirlenmiştir. Önerilen makro analiz modeli kullanılarak yapılan Türkiye'nin analizinde sadece açık kaynaklarda erişime açılan stratejik planlar, resmi raporlar ve diğer stratejik eylem ve uygulamalar ele alınmış; değerlendirmeler, başka plan, rapor ya da doküman olmadığı varsayımı üzerine yapılmıştır.

III. SİBER GÜVENLİK MAKRO ANALİZ MODELİ

Bir ülkenin makro seviyede siber güvenlik durumunun ve yürütülen faaliyetlerin analizi maksadıyla önerilen model Şekil 1'de görülmektedir. Model, ulusal siber güvenlik stratejisinden yola çıkarak birbiriyle yakın etkileşimde olan eylem planları, sorumlu kurumlar, güvenlik programları ve silahlı kuvvetler faaliyetlerini kapsamakta olup; birbirini bütünleyen bu hususlar; genel çerçevede şart kriter olan yasal mevzuat ve ulusal/ulusal işbirliği unsurları ile tamamlanmaktadır.



Şekil 1. Siber Güvenlik Makro Analiz Modeli.

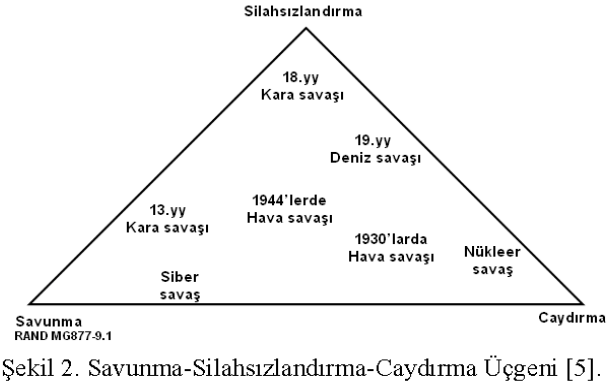
Modelin yedi ana göstergesi ve her ana gösterge kapsamında incelenebilecek hususlar sonraki maddelerde açıklanmaktadır.

A. Ulusal Siber Güvenlik Stratejisi

Makro düzeyde siber güvenliğin en önemli boyutu stratejik planlamayı da kapsayan stratejik yönetimdir. Bu nedenle, ilk ana gösterge olarak ulusal siber güvenlik stratejisi belirlenmiştir. Bu amaçla bir ülkenin siber güvenlik stratejisi geliştirip geliştirmediği öncelikle incelenmelidir.

Siber güvenliğin sağlanmasının ana savunma hedefi olduğu siber savaşların, 21'inci yüzyılın kritik savaş çeşidi olacağı açıktır. Bu nedenle, siber savaşlara yönelik strateji geliştirmek hayati öneme sahiptir. Siber savaşlarla geleneksel savaşların kıyaslamasını yapan Marsan, siber savaşı konvansiyonel savaşlardan ayıran farkları "İlk mücadelenin kazanılmasının önemi, siber savaşların hızı, gizliliği, kullanılan teknikler, amaç ve hedefleri" şeklinde belirleyerek geleneksel harp stratejilerinin siber savaşlara uygulanamayacağı sonucuna varmıştır [2].

Siber saldırılar gün geçtikçe daha teknik bir hal almaktadır ve uygulanan taktik ve teknikler ile çoğu zaman saldırının ana kaynağını belirlemek imkânsızlaşmaktadır [3]. Sonuçta siber savaş, geleneksel savaşların bilinen doğasının dönüşüm geçirmiş halidir [4]. Bu durumda; geleneksel stratejilerin siber savaşlarda uygulanması da mümkün olmayacaktır. ABD ile Sovyetler Birliği arasındaki nükleer caydırıcılık örneğinde olduğu gibi "…siber saldırı yeteneklerinin güçlenerek artması siber savaşları da önleyebilecek midir?" sorusuna Libicki, kimin saldırdığının bilinememesi, saldırganların kapalı sistemleri bulunan küçük ülkeler olduğunda, saldırıyı yapana ve kaynaklarına tehdit teşkil edilememesi ve aynı saldırı taktiğinin tekrarlanması halinde etkisiz kalması sebepleriyle olumsuz cevap vermiştir [5].



Şekil 2. Savunma-Silahsızlandırma-Caydırma Üçgeni [5].

Kaçınılmaz bir tehdit karşısında, hedef ülkenin başvurabileceği üç temel strateji bulunmaktadır: Savunma, Silahsızlandırma ve Caydırma. Libicki kitabında geçmişten günümüze kullanılan harp nevilerinin hangi yöntem ile bertaraf edilebileceğini Şekil 2'de sunulan Savunma-Silahsızlandırma-Caydırma (Defend-Disarm-Deter) üçgeni üzerinde açıklamıştır. Görüldüğü üzere Libicki, siber savaş için karşı tarafın silahsızlandırılmasının mümkün olmadığını, caydırma stratejisinin yukarıda belirtilen nedenlerle nükleer savaşta olduğu gibi işe yaramayacağını, "En iyi savunma, saldırıdır" sözünün de her durumda geçerli olamayacağını belirterek sonuçta siber savaş için uygulanacak en iyi stratejinin savunma olacağını ifade etmiştir. Sonuç olarak siber tehdide karşı konulması için yapılması gereken ilk şey stratejik hedefleri ve hedeflere ulaşılması gereken tedbirleri kapsayan [6] bir Ulusal Strateji Belgesi hazırlamaktır.

Dünyada Siber Güvenlik Stratejileri:

Siber güvenliklerinin sağlanması maksadıyla atılması gereken ilk adım olarak belirlenen ulusal strateji belirlenmesi konusunda dünyadaki durum incelendiğinde, başta ABD

olmak üzere pek çok ülkenin stratejisi belgesi bulunduğu görülmektedir.

ABD Ulusal Siber Strateji dokümanı; "Siber Uzayın Güvenliğinin Sağlanması için Ulusal Strateji" adıyla Şubat 2003 tarihinde yayımlanmıştır [7]. Taslağı halka açıklandıktan sonra ulus çapında binlerce insan ve çok sayıda kamu ve özel kuruluşun katkılarıyla oluşturduğu belirtilen ulusal strateji dokümanında, siber uzayın güvenliğinin sağlanmasının federal ve eyalet hükümetleri ile tüm Amerikan halkı ve özellikle özel sektörün, kamu ve özel sektör işbirliğinin çabalarıyla mümkün olacağının altı çizilmiştir. Strateji dokümanıyla siber güvenliğin sağlanması ana sorumluluğu ABD İç Güvenlik Bakanlığı (Department of Homeland Security-DHS)'na verilmiş olup, bu strateji dokümanının, ABD anavatanının korunması için hazırlanan "Ulusal Strateji" dokümanının tamamlayıcı unsuru olduğu belirtilmiş ve üç temel stratejik hedef belirlenmiştir. Bir diğer strateji dokümanı olan "Kapsamlı Ulusal Siber Güvenlik İnisiyatifi" (Comprehensive National Cybersecurity Initiative-CNCI), 2008 yılında Bush yönetimince "GİZLİ" gizlilik derecesinde hazırlanmış ancak; 2010 Mart ayında bir bölümünün gizlilik derecesi indirgenerek kamuya açılmıştır. Dokümanda; askeri, sivil ve hükümet bilgisayar ağları ve sistemlerinin ve kritik altyapıların korunması ile siber savaşa karşı izlenilecek saldırgan stratejilere ilişkin hükümetin kapsamlı stratejisini kapsayan 12 adet direktif yer almaktadır [8].

İngiltere siber güvenlik stratejisi Haziran 2009'da "Birleşik Krallık Siber Güvenlik Stratejisi" adıyla yayımlanmıştır. Dokümanda; siber uzayda emniyet, güvenlik, esneklik ve çabuk iyileşebilirlik ana temalarına değinilmiş, 21.yüzyılın en büyük güvenlik riskinin siber taarruzlara yönelik tehdit olduğu, bu kapsamda, uluslar arası koordinasyon gerektiği, merkezi bir Siber Güvenlik Ofisi kurulması, mevcut doktrinel, politik ve hukuksal düzenlemelerdeki boşlukların belirlenerek adreslenmesi gerektiği belirtilmiştir [9].

Almanya siber güvenlik strateji belgesinde; kritik bilgi altyapılarını koruma ve ulusal kamu sistemlerinin güvenliği vurgulanarak Ulusal Siber Güvenlik Konseyi ve Ulusal Siber Müdahale Merkezi kurulması gerektiği belirtilmiştir [10].

2009'da yayımlanan Avustralya siber güvenlik stratejisinde, tehdit farkındalığı ve müdahale, kültürel değişim ve ulusal güvenliğe tehdit teşkil edebilecek tüm elektronik sistemlerinin güvenli ve çabuk iyileşebilir olması gerektiği hususları öncelikle ele alınmıştır [11].

Fransa siber güvenlik stratejisi belgesinde, dünyada siber savunma süper gücü olunması, ulusal bağımsızlıkla ilgili bilginin korunumu, kritik altyapıların korunması ve siber uzayın güvenliğin sağlanması stratejik hedefler olarak belirlenmiştir [12].

Hollanya siber güvenlik strateji belgesinde; kamu-özel sektör ortaklığı ile kurumlar ve uluslar arası işbirliklerine önem verilmiştir [13].

Hindistan siber güvenlik stratesjisinde; yasal çerçeve, güvenlik olayları erken uyarı ve müdahale sistemi, dijital adli tıp merkezleri kurulması ile araştırma geliştirme ve uluslar arası işbirliği hususları vurgulanmıştır [14].

Önerilen modelin ilk ana göstergesi olan ulusal strateji kapsamında değerlendirilebilecek alt göstergeler; siber güvenliğin sağlanması sorumluluklarının kamu kurum ve kuruluşlarına açıkça dağıtılmış olup olmadığı, belirlenen strateji kapsamında stratejik hedeflerin öncelik derecelerine göre tespit edilip edilmediği, belirlenen stratejik hedeflere ulaşılması için gerekli eylem planları ve yol haritaları yapılıp yapılmadığıdır. Ayrıca ulusal strateji belgesinde, askeri, sivil ve hükümet bilgisayar ağları ve sistemleri ile kritik altyapıların korunması ve siber savaşa karşı izlenilecek saldırgan stratejilere ilişkin hükümetin kapsamlı stratejisini kapsayan aşağıda örnek olarak verilen direktiflerin de yer alıp almadığı incelenmelidir.

- Kamu ağlarının güvenli entegrasyonunun sağlanarak tek bir ağ yapısında saldırı tespit ve önleme sistemleri ile korunması ve yönetilmesi ve internet vb. harici bağlantılarının güvenli hale getirilmesi.
- Siber güvenlik teknolojileri alanında Ar-Ge ihtiyaçlarının tespiti ile finansal/yönetsel anlamda teşvik ve koordine edilmesi.
- Siber güvenlik eğitimlerinin ulusal eğitim-öğretim sistemine entegre edilerek yaygınlaştırılması.
- Siber güvenlik problemine çözüm olması amacıyla caydırıcı strateji ve programların tanımlanıp geliştirilmesi.
- Kritik altyapıların siber güvenliğinin sağlanması için eylem planları oluşturulması, bu amaçla kamu ve özel sektör işbirliğinin sağlanması.

B. Eylem Planları ve Ulusal Raporlar:

Belirlenen ulusal strateji doğrultusunda tespit edilen stratejik hedeflere ulaşılması amacıyla stratejik seviyede planlar yapılmalıdır. Önerdiğimiz modelin bu boyutu kapsamında, ulusal çapta stratejik etki yaratacak plan ve raporların incelenmesi yapılır. Bu kapsamda örnek olarak, hükümet kurumlarının ve bakanlıkların düzenli periyodlarla hazırlamış oldukları strateji planları ele alınabilir. Bu planlarda stratejik amaçlar belirlenir ve amaçların yerine getirilmesini izleme ve değerlemede kullanılacak performans göstergeleri tespit edilir. Siber güvenlik planlarının da hükümet kurumları ve bakanlıklar tarafından, gerek bağımsız bir doküman olarak olarak hazırlanıp hazırlanmadığı gerekse de mevcut stratejik planlara dahil edilip edilmediği hususu incelenmelidir. Özellikle gizlilik dereceli bilgi işleyen kamu kurum ve kuruluşlarının siber güvenlik planlarının hazırlanmasında ABD Ulusal Standartlar ve Teknoloji Enstitüsü (National Institute of Standards and Technology-NIST) 800-18 Federal Bilgi Sistemleri için Güvenlik Planları Geliştirme Rehberi [15] veya benzeri ulusal veya uluslar arası rehber dokümanlardan faydalanılmış olması hazırlanan planların kalitesine işaret eden bir alt gösterge olarak değerlendirilebilir.

Ayrıca, siber güvenlik alanında faaliyet icra eden ulusal kamu kurum ve kuruluşları ile özel sivil toplum kuruluşları ve çeşitli dernekler tarafından hazırlanan; ülkenin bilgi ve iletişim teknolojileri altyapısı, güvenli/güvensiz yazılım ve donanım raporları ve benzeri alanlarda ülkenin siber güvenlik durumu ve buna ilişkin tavsiyeleri içeren ulusal

raporların sayısı da bu boyutta incelenmesi gereken bir diğer göstergedir.

Bu ana gösterge kapsamında değerlendirilebilecek bir diğer husus, ulusal standart ve rehber dokümanlardır. Özellikle kamu kurum ve kuruluşlarının bilgi sistemlerinin korunması, ilgili güvenlik süreç ve organizasyonlarının oluşturulmasına rehberlik edecek standart ve raporların hazırlanarak ulusal çapta uygulanmasının sağlanması gerekmektedir. ABD'de bu sorumluluk NIST'e verilmiş olup 800-53 "Federal Bilgi Sistemleri ve Organizasyonları için Tavsiye Edilen Güvenlik Kontrolleri" [16], "Risk Yönetimi Çerçevesinin Federal Bilgi Sistemlerine Uygulanma Rehberi" [17] ve daha pek çok ilgili NIST yayını örnek olarak verilebilir.

C. Yasal Mevzuat:

Önerilen analiz modelinin temel taşlarından birisi olan yasal mevzuat, düzenlenmediği takdirde ülkelerin, siber güvenliklerinin sağlanmasında en önemli problem sahası olarak ortaya çıkmaktadır. Bu ana gösterge kapsamında incelenebilecek alt göstergeler:

- Ülkenin kamu bilgisayar ağlarının güvenliğinin sağlanması amacıyla bir yasa mevcut mudur?
- Özel sektör ve son kullanıcıların siber güvenliğinin ve aynı zamanda bireysel haklarının korunmasına yönelik yasal düzenlemeler yapılmış mıdır?
- Ulusal ve uluslar arası ISO 27001, PCI, HIPAA, SOX, COBIT gibi güvenlik standartlarına uygunluk yasal düzenlemelerle mecburi hale getirilmiş midir? Bu uygunluğun denetlenmesinden sorumlu kurum/kuruluşlar belirlenmiş midir, gerekli denetim mekanizmaları geliştirilmiş midir?
- Bilişim suçlarının yargılanması için özel yasa bulunmakta mıdır?
- Ülkenin siber savaşlara hazırlık anlamında siber saldırı kullanımını düzenleyen yasal çerçeve mevcut mudur?
- Bu gösterge kapsamında incelenmesi gereken diğer bir husus, son dönemde akademik çevrelerde tartışılmaya başlayan güvenliğin sistem geliştirme sırasında sağlanmasına yönelik yasal düzenlemelerdir. Hali hazırda, ürün geliştiren firmalar, ürünlerin kullanımından dolayı kayba uğrayan müşterilerine karşı bir yasal sorumluluk altında bulunmamaktadır. Bu nedenle, geliştirme süreçlerinde güvenlik için gerekli altyapıya önem vermemektedirler. Siber saldırılar da, bu tür ürünlerin açık noktaları hedef alınarak gerçekleştirilmektedir. Yasal düzenlemelerle ürün geliştirenlerin ihtiyaç analizi, sistem tasarımı, kodlama ve test-kabul gibi tüm ürün geliştirme süreçlerinde belirlenen güvenlik standart ve kriterlerine uymaları zorunlu hale getirilebilir [6].

Ayrıca yapılacak yasal düzenlemelerin uluslar arası arenada geçerliğinin sağlanması gerekmektedir. Gerek 2007 Estonya, gerekse 2008 Gürcistan siber saldırılarında görülen, yaygın olarak kullanılan dağıtık hizmet dışı bırakma saldırılarının dünya üzerindeki pek çok farklı ülkedeki ele geçirilmiş bilgisayarlar üzerinden yapıldığıdır. Temmuz 2009'da ABD ve G.Kore hükümet sistemlerine karşı gerçekleştirilen dağıtık hizmet dışı bırakma saldırılarının kontrol edildiği sunucu bilgisayarın, K.Kore veya Çin'de değil, Miami/Florida'da olduğunun tespit edilmesi [18] siber saldırı ve savunma alanındaki yasal mevzuatın kritik önemine işaret etmektedir. Bu ve benzeri durumlarda, ele geçirilmiş bilgisayar sahibinin, örneğin, evinin aranması, bilgisayarına el konulması vb. yasal işlemleri düzenleyecek uluslar arası geçerliği olan mevzuata ihtiyaç duyulmaktadır. Bu paralelde bir diğer husus, ABD'nin "Siber Saldırı Yeteneklerinin Edinimi ve Kullanımı Konusunda Teknoloji, Politika, Hukuk ve Etik Hususlar" raporunda belirtildiği üzere; siber saldırılar için yasal rejim zemininin Birleşmiş Milletler Sözleşmesindeki "Kuvvet Kullanımı (Use of Force)" ve "Silahlı Saldırı (Armed Attack)" olması, Savaşçıl Davranış ve Savaşa Yönelik Uluslar Arası hukuk kurallarının siber saldırılara uygulanması gerektiğidir [19].

D. Sorumlu Kurum/Merkez ve İlgili Organizasyonlar

Bu ana gösterge ile ülkenin siber güvenliğinin sağlanması amacıyla gerekli teşkilat yapılarını oluşturup oluşturmadığı incelenmelidir. Bu kapsamda, aşağıdaki belirtilen örnek organizasyonların varlığı incelenebilir:

- Ulusal anlamda siber güvenliğin sağlanması için bir sorumlu kurum/birim belirlenmiş veya oluşturulmuş mudur?
- Ulusal siber güvenliğin sağlanmasından sorumlu kurum veya kuruluşun siber güvenlik yapılanması mevcut mudur?
- Siber güvenlik alanında gerekli koordinasyon ve işbirliğinin sağlanması için bir merkez/birim kurulmuş mudur?
- Siber güvenlik alanında ulusal standartları belirleyen bir kurum/enstitü mevcut mudur?
- Kamu ve özel sektör kurumları bilgi sistemlerinin korunmasına yönelik, ilgili güvenlik süreçlerinin ve organizasyonların oluşturulmasında rehber dokümanlar yayımlayan bir kurum/enstitü mevcut mudur?
- Ulusal anlamda siber güvenlik faaliyetlerini yönlendiren bir koordinasyon kurulu mevcut mudur?
- Ülkede Bilgisayar Olaylarına Acil Müdahale Ekibi-BOME merkez(ler)i mevcut mudur? BOME'nin amacı saldırıya uğramış bilgisayar sistemleri ve ağlarına yönelik acil durum desteği sağlamaktır. Bazı BOME'ler gelecekte meydana gelebilecek siber saldırıların önlenmesi ve bilgisayar ağlarındaki zafiyetlerin ortaya çıkarılması alanında da faaliyet gösterebilmektedir.
- Her kamu kurum ve kuruluşun kendi BOME'si var mıdır?
- BOME'lerin faaliyetlerini yönetecek ve yönlendirecek merkezi bir koordinasyon merkezi mevcut mudur?
- Siber saldırıların önceden tespiti amacıyla faaliyet gösteren merkez(ler) mevcut mudur?
- Siber saldırıların kriminal analizi ve soruşturulması amacıyla faaliyet gösteren merkez(ler) mevcut mudur?
- Siber güvenlik alanında araştırma-geliştirme yapan eğitim kurumları mevcut mudur?
- Siber saldırıların analizi ve gözlemlenmesi ile savunma yöntemleri geliştirilmesi amaçlarıyla balküpü ve benzeri aldatma sistemlerine sahip laboratuarlar mevcut mudur?

- Kritik altyapıların korunması ve/veya ulusal çapta siber savunma amacıyla hükümet-özel sektör işbirliğinin geliştirilebilmesi amacıyla bir merkez mevcut mudur?
- Siber güvenlik odaklı lisans/yüksek lisans seviyesinde eğitim öğretim sağlayan, teknoloji geliştirme odaklı araştırmalara öncülük yapan enstitüler veya araştırma merkezleri mevcut mudur?
- Güvenli yazılım ve donanım ürünlerinin akreditasyonunu sağlayan bir kurum/kuruluş mevcut mudur?

E. Siber Güvenlik Programları

Bu ana gösterge kapsamında, belirlenen eylem planlarının gerekli program ve projelere dönüştürülme durumları, kamu ve özel sektör bilgi sistemlerinin korunması için gerekli programların uygulanılıp uygulanılmadığı, ulusal düzeyde bilinçlendirme, farkındalığı artırma ve eğitim programları yapılıp yapılmadığı ve yürütülen programların değerlendirilmesinin ne ölçüde yapılabildiği hususları incelenmelidir. Bu kapsamda incelenebilecek alt göstergeler aşağıdadır:

- Siber güvenlik teknolojileri alanında Ar-Ge teşvik programları mevcut mudur?
- Kritik altyapıların korunmasına yönelik risk yönetimi, zafiyet analizi, araştırma-geliştirme ve benzeri program(lar) mevcut mudur?
- Ulusal çapta, bireysel bilgisayar kullanıcılarının farkındalığının artırılması ve siber tehditlere, sistem açıklıklarına yönelik çeşitli uyarıların yapıldığı bir sistem/portal vb. mevcut mudur?
- Siber güvenlik konusunda farkındalığı artırıcı sosyal (Örn. ABD'de uygulanan siber güvenlik farkındalık ayı) veya eğitim amaçlı faaliyetler mevcut mudur?
- Siber güvenlik bilgilendirme ve eğitim programları mevcut mudur?
- Siber güvenlik alanında görev yapan personelin eğitim seviyelerini artırmaya yönelik periyodik eğitim, burs, sertifikasyon vb. programlar mevcut mudur?
- Siber güvenlik odaklı lisans/yüksek lisans seviyesinde eğitim öğretim sağlayan, teknoloji geliştirme odaklı araştırmalara öncülük yapan programlar mevcut mudur?
- Siber saldırıların analizi ve gözlemlenmesi ile savunma yöntemleri geliştirilmesi amaçlarıyla balküpü ve benzeri aldatma sistemlerine sahip laboratuarlar oluşturma amaçlı programlar mevcut mudur?
- Siber saldırı istatistiklerinin kayıt edildiği bir ulusal veri tabanı programı mevcut mudur?
- İşletim sistemleri ve uygulama yazılımlarındaki zafiyetlerin, güvenlik açıklarının ve benzeri bilgilerin kayıt altına alındığı ulusal veri tabanı programı mevcut mudur?
- Siber güvenlik alanında konferans ve sempozyumlar düzenlenmekte midir? Bu tür faaliyetlerin ve faaliyetlere katılım sağlayan kamu kurum/kuruluşları ile katılımcı sayıları kıyaslama amacıyla değerlendirilebilir.
- Ulusal çapta siber güvenlik tatbikatları düzenlenmekte midir? Bu tür tatbikatlar ile katılım sağlayan kamu ve özel sektör kurum ve kuruluşların sayıları kıyaslama amacıyla değerlendirilebilir.
- Uluslar arası siber güvenlik etkinliklerine katılım sağlanmakta mıdır? Bu alt gösterge altında, akademik konferans vb. akademik faaliyetler, siber güvenlik tatbikatları, siber güvenliğin sağlanması ve kritik altyapıların korunmasına yönelik uluslar arası toplantı ve organizasyonlara katılım seviyesi ayrı ayrı değerlendirilebilir.
- Planlanan programların izleme-değerlendirilmesini yapmakla görevli bir kurum belirlenmiş midir? İzleme ve değerlendirme hangi sıklıkla, ne kadar etkinlikle icra edilmektedir?

F. Silahlı Kuvvetler Siber Güvenlik Faaliyetleri

Bu ana gösterge, siber güvenliğe, 21'inci yüzyılın savaş türü olan siber savaş boyutu açısından yaklaşılarak belirlenmiştir. McAfee 2009 Sanal Kriminoloji Raporu'nda, 2007 yılında yayımlanan rapordan sonra, ülkelerin sadece birbirlerinin siber uzay faaliyetleri hakkında bilgi toplamakla kalmayıp, gelişmiş siber saldırı teknikleri geliştirdikleri, saldırı amaçlı hazırlık yapan ülkelerin başında özellikle Çin, Rusya, ABD, İsrail ve Fransa'nın bulunduğu belirtilmiştir [20]. Kuzey Kore, İran, Tayvan, Brezilya [21] ve Hindistan'ın [22] da siber saldırı programları bilinmekte olup bir analiz çalışmasında ABD'nin siber saldırı güç puanı 8, siber savunma güç puanı ise 1; K.Kore'nin ise 2 ve 7 olarak belirlenmiştir [23].

Siber uzayda çalışan tüm elektronik sistemlere karşı askeri tedbir alınması gerektiği [24], sadece savunma değil saldırı amaçlı yetenek geliştiren ülkeler de olduğu değerlendirildiğinde, ülkelerin silahlı kuvvetlerinin bu bağlamdaki aşağıda belirtilen faaliyetleri analiz edilmelidir.

- Silahlı kuvvetlerin siber güvenlik strateji belgesi ve eylem planı mevcut mudur?
- Silahlı kuvvetlerin savunma ve saldırı amaçlı siber güvenlik teşkilatlanması mevcut mudur? Bu alt gösterge kapsamında, üst seviyede koordinasyon veya yönlendirme kurulu, BOME ekipleri, siber komutanlık ve alt birimleri olup olmadığı incelenebilir.
- Siber güvenlik alanında ihtisaslaşmış bir personel yapılanması mevcut mudur?
- Siber güvenlik alanında ihtisas eğitimi sağlayan askeri eğitim-öğretim kurumu mevcut mudur?
- Siber savunma ve saldırı amaçlı harekat doktrin, konsept veya uygulama usulleri dokümanı mevcut mudur?
- Siber savunma ve saldırı amaçlı yetenek geliştirme programları yürütülmekte midir?
- Silahlı kuvvetler tarafından ulusal çapta icra edilen faaliyetlere katılım sağlanmakta mıdır? Bu alt gösterge kapsamında akademik, politik veya tatbikat gibi teknik faaliyetlere katılım durumu ve seviyesi ayrı ayrı incelenebilir.

G. Ulusal/Uluslar arası İşbirliği

Ulusal çapta icra edilen faaliyetlerin tek bir merkezden yönetilmesi ve gerekli koordinasyonun sağlanması, yürütülen faaliyetlerin ortak bir amaca hizmet etmesi, etkilerinin toplam faydayı artıracak şekilde sinerji yaratması, ayrıca

uluslar arası alanda devam eden faaliyetlere katılım sağlanarak, gerekli işbirliği ve koordinasyonun sağlanması, ulusal siber güvenliğin yapı taşlarından birisidir.

Ulusal ve uluslar arası işbirliğine, başta kritik altyapıların korunması olmak üzere, siber saldırılara müdahale, siber saldırıların tespiti, gözlemlenmesi ve analiz edilmesi ve siber güvenlik teknolojileri alanında araştırma ve geliştirme faaliyetleri gibi pek çok alanda ihtiyaç duyulmaktadır. Nitekim, ABD "Siber Uzay Politika Gözden Geçirme Raporu"'nda da, siber güvenlik konusunda milli diyalog gerektiği, bu kapsamda kamu - özel sektör ve diğer ülkelerle birlikte hareket etmenin şart olduğu belirtilmektedir [25]. Bu nedenle belirlenen gösterge kapsamında; yukarıda belirtilen alanlarda işbirliğine yönelik faaliyetler incelenmelidir.

V. TÜRKİYE'NİN SİBER GÜVENLİK ANALİZİ

Bu bölümde, önerilen yedi ana kategoride Türkiye'nin 2002-2012 yılları arasındaki dönemde gerçekleştirilen faaliyetleri ile mevcut durumu analiz edilmiş, zafiyet noktaları tespit edilerek öneriler sunulmuştur.

A. Ulusal Siber Güvenlik Stratejisi

Türkiye'nin Ulusal Siber Güvenlik Stratejisi adı altında bir belgesi bulunmamakla beraber "Ulusal Sanal Ortam Güvenlik Politikası" dokümanının bu kapsamda incelenebileceği değerlendirilmiştir. Başta Cumhurbaşkanlığı, Başbakanlık ve Genelkurmay Başkanlığı olmak üzere toplam 19 kurum/kuruluşun katkısıyla Temmuz-Kasım 2008 tarihleri arasında hazırlanan ve Ocak 2009'da Başbakanlığa teslim edilen [33] Ulusal Sanal Ortam Güvenlik Politikası'nın amacı, ülkemizi sanal ortamdaki saldırılara karşı hazır hale getirecek ve sanal ortamda yaşanacak sorunların ardından hızlı geri dönüşü sağlayacak sanal ortam güvenlik adımlarını belirlemektir. Politika kapsamında belirlenen strateji adımları aşağıdaki şekildedir:

- Yasal Düzenlemeler
- Ülke Yeteneklerinin Geliştirilmesi
- Ulusal Bilgisayar Olaylarına Müdahale Organizasyonu
- Bilgilendirme ve Bilinçlendirme Çalışmaları
- Ulusal Kritik Bilgi ve İletişim Sistem Altyapılarının Güvenliği
- Uluslararası Eşgüdüm
- Kurumsal Bilgi ve İletişim Sistemleri Güvenliği
- Ulusal Sanal Ortam Güvenlik Stratejisi'nin Hazırlanması

Politika dokümanında belirtilen strateji adımlarının hayata geçirilmesi sürecinin henüz tamamlanmadığı, bu bağlamda Ulusal Sanal Ortam Güvenlik Stratejisi'nin de henüz yayımlanmadığı bilinmektedir.

B. Eylem Planları ve Ulusal Raporlar:

Devlet Planlama Teşkilatı tarafından günümüze kadar, "e-Türkiye Girişimi Eylem Planı-2002", "e-Dönüşüm Türkiye Projesi Kısa Dönem Eylem Planı (2003–2004)", "e-Dönüşüm Türkiye Projesi 2005 Eylem Planı", "Bilgi Toplumu Stratejisi (2006-2010)","Bilgi Toplumu Stratejisi Eylem Planı (2006-2010)" adlı politika belgeleri yayımlanmıştır. "Bilgi Toplumu Stratejisi ve Ek'i Eylem Planı" 11/07/2006 tarihli ve 2006/38 sayılı Yüksek Planlama Kurulu Kararı'yla onaylanmış olup, 28/07/2006 tarihli ve 26242 sayılı Resmi Gazete'de yayımlanarak yürürlüğe girmiştir. Bu dokümanda siber güvenlik ile ilişkili olduğu belirlenen aşağıda açıklanan beş eylem maddesi bulunduğu tespit edilmiştir.

1-"Güvenlik ve Kişisel Bilgilerin Mahremiyeti" kategorisinde belirlenen 88'inci maddesinde, 2007 yılı başlangıç tespit edilerek 24 aylık süre içerisinde bir Ulusal Bilgi Sistemleri Güvenlik Programı (UBGP) hazırlanması sorumluluğu TUBİTAK-UEKAE'ne verilmiştir.

2-"Bilgi Güvenliği ile İlgili Yasal Düzenlemeler" başlıklı 87'nci stratejik eylem maddesi, aşağıdaki iki hususu dikte ettirmekte olup gerçekleştirme sorumluluğu Adalet Bakanlığı'na verilmiştir.

"- Ülke güvenliğini ilgilendiren bilgilerin elektronik ortamda korunması ve devletin bilgi güvenliği sistemlerinin geliştirilmesi amacına uygun yasal altyapıyla ilgili düzenleme yapılacak ve uygulamaya konulacaktır.

- Kişisel Verilerin Korunması Hakkında Kanun Tasarısı Taslağı yasalaştırılacaktır." [26].

3-"Vatandaş Odaklı Yaklaşım" kategorisi 27'nci eylem maddesi gereği, Kamu kurumları İnternet sitelerine içerik, güvenlik, kimlik yönetimi ve kullanılabilirlik standardizasyonu sağlanması zorunluluğu getirilmiştir. Bu madde kapsamında, "Kamu Kurumları İnternet Siteleri Standartları ve Önerileri" isimli bir kılavuz oluşturulmuş ve 27/01/2009 tarihinde gerçekleştirilen bir toplantı ile kamu kurumlarına tanıtılmıştır. Bu amaçla, www.kakis.gov.tr isimli internet sitesi hizmete açılmış, barındırma hizmetine ilişkin çalışmalar ise sürmektedir.

4-"Bilgi ve İletişim Teknolojilerinin İş Dünyasına Nüfuzu" kategorisi 26'ncı eylem maddesi olan "e-Ticaret Güvenlik Altyapısı" kapsamında Türk Standartları Enstitüsü tarafından daha önce ilgili kuruluşlar ile birlikte hazırlanmış olan e-ticaret güvenlik alt yapısı raporunda saptanan güvenlik gereklerinin Qweb sistemi ile entegre edilmesi çalışmaları devam etmektedir.

5-"Sosyal Dönüşüm" kategorisi 10'ncu eylem maddesi olan "İnternet Güvenliği" maddesi kapsamında Adalet Bakanlığı tarafından, 5651 Sayılı İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanunun uygulama sonuçları izlenmeden yeni bir çalışma yapılması öngörülmediği, eylemin tamamlanmış olarak değerlendirildiği belirtilmiştir [27].

Sağlık Bakanlığı'nın 2010-2014 Stratejik Planı'nda, yasal mevzuat bölümünde açıklanan siber güvenlik hususları bulunmaktadır. Milli Eğitim Bakanlığı, İçişleri Bakanlığı ve Kültür ve Turizm Bakanlığı 2010-2014 stratejik planlarında stratejik amaç ve hedefler kapsamında siber güvenlik konusu ele alınmamıştır. Devlet Planlama Teşkilatı'nın 2009-2013, Savunma Sanayii Müsteşarlığı'nın (SSM) 2007-2011 dönemi stratejik planları ve SSM'nin 2009-2016 Sektörel Strateji Dokümanı incelenmiş olup siber güvenliğe yönelik herhangi bir husus bulunamamıştır.

Ulusal raporlar kapsamında; açık kaynak taraması sonucunda yukarıda açıklanan Ulusal Sanal Ortam Güvenlik

Politikası ile DPT Strateji Dokümanı ve Eylem Planı haricinde bu kategoride değerlendirilecek bir resmi kurum/kuruluş raporu bulunamamıştır. Ancak; her ne kadar kurumunun görüşlerini yansıtmasa da Bilgi Teknolojileri ve Koordinasyon Dairesi Başkanlığı personeli tarafından hazırlanan 2009 tarihli "Siber Güvenliğinin Sağlanması: Türkiye'deki Mevcut Durum ve Alınması Gereken Tedbirler Raporu"nda, Ulusal Siber Güvenliğin sağlanmasına ilişkin tavsiyeler sunulmuştur [28].

C. Yasal Mevzuat

Bilişim alanındaki suçlar, Türk Ceza Kanunu'nun 10. bölümünde yer almakta olup aşağıdaki üç maddede tanımlanmıştır:

- Bilişim sistemine girme suçunu düzenleyen 243. madde
- Sistemi engelleme, bozma, verileri yok etme veya değiştirme suçunu düzenleyen 244. madde
- Banka veya kredi kartlarının kötüye kullanılması suçunu düzenleyen 245. madde

5809 sayılı "Elektronik Haberleşme Kanunu" ile; bilgi güvenliği ve haberleşme gizliliğinin gözetilmesi, izinsiz erişime karşı şebeke güvenliğinin sağlanması, hizmet kalitesi de dahil olmak üzere standartlar ve spesifikasyonlara uyumluluk, elektronik haberleşme sektörüne yönelik olarak, millî güvenlik, kamu düzeni veya kamu hizmetinin gereği gibi yürütülmesi amacıyla mevzuatın öngördüğü tedbirlerin alınması görevleri Bilgi Teknolojileri ve İletişim Kurumu'na verilmiştir [29].

Elektronik Haberleşme Güvenliği Yönetmeliği, 20 Temmuz 2008 tarihli ve 26942 sayılı Resmi Gazete'de yayımlanmıştır. Yönetmelik kapsamında işletmecilere, 20 Temmuz 2010 tarihine kadar TS/ISO 27001 Bilgi Güvenliği Yönetim Sistemi belgesi alma yükümlülüğü getirilmiştir.

5070 Sayılı "Elektronik İmza Kanunu" ile güvenli e-imza ile ilgili teknik kriterlerin belirlenmesi ile Elektronik Sertifika Hizmet Sağlayıcıların yetkilendirilmesi ve denetlenmesi,

5651 Sayılı "İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanun" ile internet aktörlerinin düzenlenerek (içerik, yer, erişim ve toplu kullanım sağlayıcılar) içerik denetimi yapılması,

Elektronik Ticaretin Düzenlenmesi Hakkında Kanun Tasarısı ile istek dışı elektronik ileti konusunda ikincil düzenleme yapma yetkisi,

Telekomünikasyon Sektöründe Kişisel Bilgilerin İşlenmesi ve Gizliliğinin Korunması Hakkında Yönetmelik ile haberleşmenin gizliliği, trafik verilerinin işlenmesi, yer verisinin tespiti,

İstek Dışı Mesajlar Hakkında Tebliğ Taslağı ile basit ve ücretsiz bir yolla yığın SMS'i reddetme usullerinin belirlenmesi,

22 Ağustos 2011 tarihinde yürürlüğe girmesi beklenen, ancak gelen tepkiler üzerine üç ay ertelenen İnternetin Güvenli Kullanımına İlişkin Usul ve Esaslar Taslağı ile işletmecilerin güvenli internet hizmeti sunmasına yönelik yükümlülüklerinin belirlenmesi,

23 Ekim 2010 tarihinde resmi gazetede yayımlanan Kamu Kurum ve Kuruluşları ile gerçek ve tüzel kişilerine elektronik haberleşme hizmeti içinde kodlu veya kriptolu haberleşme yapma usul ve esasları hakkında yönetmelik ile, 5809 sayılı Kanunda belirtilen istisnai kurumlar haricindeki tüm kamu kurum ve kuruluşları ile gerçek ve tüzel kişilerin kodlu ve/veya kriptolu haberleşme yapabilmesinin izine tabi tutulması [30] amaçlanmıştır.

DPT Strateji Dokümanının "Bilgi Güvenliği ile İlgili Yasal Düzenlemeler" başlıklı 87'nci stratejik eylem maddesi, Ülke güvenliğini ilgilendiren bilgilerin elektronik ortamda korunmasını ve devletin bilgi güvenliği sistemlerinin geliştirilmesi amacına uygun yasal altyapıyla ilgili düzenleme yapılmasını ve uygulamaya konulmasını, ayrıca kişisel verilerin korunması hakkında kanun tasarısı taslağının yasalaştırılmasını dikte ettirmektedir. Bu kapsamda; Kişisel Verilerin Korunması Kanunu Tasarısı 22 Nisan 2008 tarihinde TBMM Başkanlığına arz edilmiş, ancak halen onaylanamamıştır [31].

"Ulusal Bilgi Güvenliği Teşkilatı ve Görevleri Hakkında Kanun Tasarısı" taslağı hazırlanmış olup halen Adalet Bakanlığı'nın tasarı ile ilgili komisyon kurulması yönündeki hazırlık çalışmaları devam etmektedir. Tasarının amacı; Ulusal güvenliği ilgilendiren, askeri, istihbari, dış ilişkiler, ekonomik, teknolojik, bilimsel, ticari ve diğer çok gizli, gizli, özel, hizmete özel ve tasnif dışı gizlilik derecesini kapsayan bilgilerin korunması, devletin bilgi güvenliği faaliyetlerinin geliştirilmesi, gerekli politikaların üretilmesi ve belirlenmesi, kısa ve uzun dönemli planların hazırlanması, kriter ve standartların saptanması, haberleşme ve bilgi sistemlerinin teknolojisine uyumunun sağlanması, uygulamanın takip ve denetimi, kamu ve özel kurum ve kuruluşları arasında koordinasyonun sağlanması amacıyla bir teşkilatın kurulması ve bu teşkilatın görevlerine ilişkin usul ve esasları düzenlemektir.

Ulusal ve uluslar arası standartlara uygunluk ve denetimi kapsamında Sağlık Bakanlığı 2010-2014 Stratejik Planı'nda 2.7.3.numaralı e-Sağlık sistemi oluşturulması stratejik hedefi kapsamında bakanlık ve taşra teşkilatı bilgi sistemlerinin TS ISO/IEC 27001 güvenlik gereksinimleri standartlarına göre güvenliği sağlanacağı kayıt altına alınmıştır [32].

Kritik altyapıların korunmasına yönelik mevcut durumda bir yasal mevzuat çalışması bulunmamakla beraber, Ulusal Sanal Ortam Güvenlik Politikası hazırlık çalışmaları ve Başbakanlık Kanunlar ve Kararlar Genel Müdürlüğü bünyesinde oluşturulan e-Mevzuat Çalışma grubunun, 7 Ağustos 2009 tarihi itibarıyla hazırladığı "e-Devlet ve Bilgi Toplumu Kanun Tasarısı Taslağı", bu alanda bugüne kadar yapılan mevzuat çalışmalarıdır [33].

Siber suçların analizi kapsamında, 3'üncü Bilgi Güvenliği ve Kriptoloji Konferansı sonuç bildirgesinde, ülkemizde "Adli Bilişim Kurumu veya Enstitüsü"nün kurulması ve adli bilişim konusunda ülkemiz için bir ulusal yönetişim modeli ve uygulama çerçevesinin belirlenmesinin gerekli olduğu tespit edilmiştir [34].

Siber Güvenlik Hukuku Çalıştayı 2012 sonuç bildirgesinde, mevcut mevzuat değerlendirildiğinde yukarıda

açıklanan kanunlar ve ilgili yönetmeliklerle siber güvenlik hukuku altyapısının desteklendiği fakat sadece bu düzenlemelerle günümüz ihtiyaçlarının tümüyle karşılanmasının mümkün olmadığı sonucuna varılmıştır [35].

D. Sorumlu Kurum/Merkez ve İlgili Organizasyonlar

Ulusal Bilgi Güvenliği Teşkilatı, ilgili kanun teklifi onaylanmadığından oluşturulamamıştır. Mevcut durumda Türkiye'nin siber güvenliğinin sağlanması sorumluluğu TÜBİTAK'a verilmiştir. Taslağı hazırlanan Ulusal Bilgi Güvenliği Teşkilatı kanun tasarısı onaylanarak yürürlüğe girmesi halinde, Başbakanlığa bağlı Ulusal Bilgi Güvenliği Üst Kurulu ile tüzel kişiliğe sahip genel bütçeli Ulusal Bilgi Güvenliği Kurumu Başkanlığı kurulacaktır.

Kritik altyapıların korunması amacıyla ulusal çapta kurulan bir merkez mevcut değildir.

Ulusal Bilgi Sistemleri Güvenliği Programı kapsamında kurulan TR-BOME Koordinasyon Merkezi'nin görevi ülke genelinde kurum ve kuruluşlara bilgisayar güvenlik olaylarına müdahale yeteneği kazandırmak ve gerçekleşen siber güvenlik olaylarına müdahale etmektir [36].

TR- BOME tarafından BOME kurulum danışmanlığı, olay müdahale koordinasyonu ile alarm ve uyarı hizmetleri sağlanmaktadır. Merkezde, siber güvenliğe ilişkin kamu kurum ve üniversite bilgi işlem personeline eğitimler düzenlenmekte, uygulamalı konular için laboratuar ortamından faydalandırılmaktadır. Merkez tarafından kurumlara teknik güvenlik testleri uygulanmakta olup pek çok kamu kurum ve kuruluşuna da BOME kurulumu tamamlanmıştır.

Türkiye'de hali hazırda biri hükümet tarafından işletilen (TR-BOME) biri de TÜBİTAK'ın araştırma ve eğitim amacıyla işletilen (ULAK-CSIRT) akredite olmuş iki adet BOME bulunmaktadır. Ayrıca TR-BOME, uluslararası alanda da etkin olarak faaliyet göstermektedir. TR-BOME ile NATO NCIRC (NATO Computer Incident Response Capability) arasında 2007 yılında "Personel değişimi, NATO Siber Savunma Tatbikatı'na katılım, müşterek olay müdahale ile açıklık denetimi, NCIRC gizli ağına, teknik açıklık veritabanına ve alarm-uyarılara erişim ve zararlı kod analiz desteği" konularını kapsayan mutabakat zaptı imzalanmıştır [37]. TR-BOME, 09-13 Kasım 2008 tarihlerinde düzenlenen "International Cyber Defense Workshop, Fall 09 - ICDW09" tatbikatında ülkemizi temsil etmiş, ayrıca siber savunma tatbikatı olan NATO Cyber Coalition 2009 Exercise etkinliğine aktif katılım göstermiştir. Sonuçta, BOME kurulması konusunda Türkiye açısından durum olumludur.

Sanal Ortam Savunma Merkezi (SOSAM); Ulusal Bilgi Sistemleri Güvenliği Programı kapsamında Ankara'da kurulmuş olup bünyesinde gerçek ve balküpü ismi verilen tuzak sistemler bulunmaktadır. Faaliyetleri; kamu kurumlarına ait kritik sistemleri hedef alan tehditlerin tespiti, genel saldırı profillerinin belirlenmesi ve raporlanması, tespit edilen tehditler ile ilgili uyarılar yayınlayarak önlem alınmasını sağlamak, botnetlerin tespiti ve bertaraf edilmesidir [38].

E. Siber Güvenlik Programları

Devlet Planlama Teşkilatı Bilgi Toplumu Stratejisi ve Ek'i Eylem Planı 88'inci maddesi gereği Ulusal Bilgi Sistemleri Güvenlik Programı (UBGP) hazırlanması dikte ettirilmiştir. TÜBİTAK-UEKAE tarafından gerçekleştirilen e-Dönüşüm Türkiye Projesi 2005'in devamı olan program kapsamında;

- Koordinasyon alanında, Ulusal Bilgisayar Olayları Müdahale Ekibi (BOME) Koordinasyon Merkezi'nin kurulması,
- Eğitim alanında, kamu kurumları bilgi işlem personeline bilgi sistemleri güvenliği eğitimleri verilmesi,
- Dokümantasyon alanında, kamu kurumları için bilgi sistemleri güvenliği ile ilgili kılavuz dokümanların hazırlanması ve kurulacak Bilgi Güvenliği Portalı (Kapısı) aracılığı ile paylaşılması,
- Yönetim alanında, pilot kurumlara Bilgi Güvenliği Yönetim Sistemi (BGYS) kurulması,
- İzleme alanında, Sanal Ortam Savunma Sistemi'nin kurulması kararlaştırılmıştır [38].

Bilgi Toplumu Stratejisi Eylem Planı Beşinci Değerlendirme Raporu'nda programların uygulama durumları aşağıdaki şekilde belirtilmiştir. Eğitim projesi kapsamında, üniversite personeline bilgi güvenliği eğitimleri verilmiştir. Kurumlarda BOME kurulmasını sağlamak ve BOME personeline teknik yeterlilik kazandırmak amacıyla hazırlanan Kullanıcı Bilinçlendirme Eğitimi, BOME Kurulum ve Yönetim Eğitimi, Olay Müdahale ve Sistem Analizi Eğitimi'nin internet üzerinden ücretsiz olarak verilmesi için ön çalışmalar başlamıştır. Bilgi Güvenliği Yönetim Sistemi (BGYS) pilot projeleri kapsamında, Başbakanlık, Adalet Bakanlığı, Muhasebat Genel Müdürlüğü ve Sayıştay Başkanlığı'nda risk analizi çalışmaları tamamlanmıştır.

Kritik altyapıların korunmasına yönelik resmi bir program mevcut değildir.

Ulusal Bilgi Güvenliği Kapısı projesi kapsamında; "http://www.bilgiguvenligi.gov.tr/" web adresi üzerinden güvenlik konularında teknik yazılar, standart ve kılavuz dokümanlar, güvenlik bildirileri yayımlanmaktadır.

Ayrıca, özel sektör eğitim kurumları tarafından da çok sayıda siber güvenlik eğitimleri sağlanmaktadır. Örneğin, Bilgi Güvenliği Akademisi tarafından ilk kez Temmuz 2011 tarihinde düzenlenen siber güvenlik yaz kampı kapsamında 20 üniversite öğrencisine, beş hafta boyunca yoğun bir eğitim verilmiştir [39]. Eğitim kapsamında "CEHTurkiye.com" gibi gönüllü hizmet veren programlar da oldukça olumludur. CEHTurkiye.com, bilgi güvenliği kapsamında bilişim gönüllülerine destek vermek için bilgi birikimini ve tecrübelerini paylaşan etik hackerların oluşturduğu bir bilgi güvenliği kütüphanesidir [40].

Halkın eğitimi ve farkındalığı artırmak kapsamında Avrupa'da 2004 yılından beri düzenlenen "Güvenli İnternet Günü" etkinliği Türkiye'de ilk kez 23 Şubat 2010'da düzenlenmiştir. Ayrıca, Telekomünikasyon İletişim Başkanlığı tarafından Ulaştırma ve Milli Eğitim Bakanlığı işbirliği ile öğrencileri ve velileri internette yer alan tehlikelerden korumaya yönelik ve bilgi teknolojilerinin

doğru kullanılabilmesi amacıyla faydalı bilgilerin yer aldığı "Güvenli İnternet Kullanımı İçin Tavsiyeler" adlı bir kitapçık yayınlanmıştır [41].

Konferans ve Sempozyumlar kapsamında; Türkiye'de yeterli sayıda konferans ve sempozyumun düzenlendiği değerlendirilmektedir. Örnek olarak, beşincisi 17-19 Mayıs 2012 tarihlerinde düzenlenecek olan, ana teması Siber Güvenlik ve Savunma olarak belirlenen ve konferans serilerinde sunulan tüm bidiri ve sunumların www.iscturkey.org adresinde açık olarak kamuoyu ile paylaşılan Uluslar Arası Bilgi Güvenliği ve Kriptoloji Konferansı, altıncısı Haziran 2011'de düzenlenen Kamu Kurumları Bilgi Teknolojileri Güvenlik Konferansı, ikincisi Eylül 2011'de icra edilen Ulusal Siber Güvenlik Çalıştayı, Ocak 2012'de icra edilen Siber Güvenlik Hukuku Çalıştayı, Aralık 2011'de icra edilen Siber Güvenlik Konferansı, IV. Uluslararası Bilgi Güvenliği ve Kriptoloji Konferansında 2010 yılında düzenlenen Siber Savunma Çalıştayı ve Aralık 2009'da gerçekleştirilen Sayısal Ortamda Savaş Sempozyumu verilebilir.

Siber Güvenlik Tatbikatları kapsamında; Bilgi Sistemleri Güvenliği Tatbikatı'nın ikincisi bir takım olumsuzluklar nedeniyle iki kez ertelenerek Ulusal Siber Güvenlik Tatbikatı 2011 ismiyle 25-28 Ocak 2011 tarihleri arasında gerçekleştirilmiştir. Finans, elektronik haberleşme, eğitim ve savunma sektörleriyle TSK, adli ve kolluk birimleri ve çeşitli bakanlıkların ilgili birimlerinin temsilcilerinden oluşan 41 kamu ve özel sektör kurum/kuruluşunun katılımıyla gerçekleştirilen tatbikat kapsamında; dağıtık servis dışı bırakma saldırıları, web sayfası güvenlik denetimi vb. içeren 450'nin üzerinde yazılı senaryo değerlendirilmiştir. İlk BOME tatbikatı ise 20-21 Kasım 2008 tarihlerinde sekiz kamu kurum ve kuruluşunun katılımıyla, "BOME 2008 Bilgi Sistemleri Güvenliği Tatbikatı" ismiyle icra edilmiştir [42].

F. Silahlı Kuvvetler Siber Güvenlik Faaliyetleri

Açık kaynaklarda, TSK'ya ait siber güvenlik planı, programı, projesi ve teşkilat değişikliği tespit edilememiştir. Ancak, farkındalığın artırılması faaliyetleri kapsamında icra edilen konferanslara, sempozyumlara ve tatbikatlara TSK'nın katılımının sağlandığı bilinmektedir.

G. Ulusal/Uluslar arası İşbirliği

Bu kapsamda, işbirliğiyle gerçekleştirilen en önemli örneğin, 2009 yılında BTK koordinatörlüğünde işletmecilerin de işbirliğiyle tüm Türkiye'de uygulanan "Yığın E-posta ile Mücadele Projesi" olduğu görülmektedir. En iyi uygulamalara örnek olarak verilebilecek olan proje sonucunda yığın e-posta mesaj yayan IP sayısının %99 civarında düşüş gösterdiği ve işletmecilerin yaydığı günlük yayılan mesaj sayısının 6,5 milyar düzeyinden 394 milyon düzeyine indiği görülmüştür [41].

Ancak, ulusal ve uluslar arası işbirliği amacıyla kritik altyapıların korunması başta olmak üzere pek çok alanda yapılması gereken hususlar bulunmaktadır. 23 Şubat günü Ankara'da birçok kurumun katılımıyla gerçekleştirilen "Türkiye'nin Siber Güvenlik Yol Haritası" konu başlıklı e-Devlet Yuvarlak Masa Toplantıları'nın 13.sü sonucunda öne çıkan kamu, özel sektör ve birey arasında farkındalık ve güvene dayalı işbirliği hususları bu değerlendirmeyi destekler yöndedir [43]. Uluslar arası işbirliği kapsamında olumsuz durumumuza bir örnek ise 1-2 Kasım 2011 tarihlerinde Londra'da düzenlenen 60 ülkenin katılımıyla gerçekleşen Siber Uzay Konferansı'na Türkiye'nin katılmaması olarak verilebilir [44]. Konferansta siber tehdide karşı, küresel çapta koordineli müdahale gerektiği vurgulanmıştır [45].

H. Bulguların Yorumlanması ve Öneriler

Türkiye'de internete erişim imkânı olan hane oranı %42,9'a yükselmiştir [46]. 2011 yılında yapılan bir araştırmaya göre Türkiye nüfusunun %14'ü akıllı telefon sahibi olup mobil cihazlarından internete bağlananların oranı ise %66'dır[47]. Türkiye, Dünya'da "Botnet"lere ev sahipliği yapan ülkeler sıralamasında sekizinci, yığın e-posta üretiminde beşinci (2008'in son beş ayında ikinci), 2007'de 15. sıradan 2008'de 9. sıraya çıkarak kötü niyetli faaliyetlerin toplamının %3'ünün kaynağı durumundadır. Bu kapsamda en hızlı yükselen ülke konumundadır [48]. Bu farkın, büyük oranda 2006 yılında başlatılan Bilgi Toplumuna Dönüşüm Sürecine geçişte gerekli güvenlik mekanizmalarının kurulmamasından kaynaklandığı, dönüşüm süreci tamamlandığında gerekli siber güvenlik tedbirlerinin alınmaması durumunda Türkiye'nin sıralamasının negatif yönde daha da yükselebileceği değerlendirilmektedir. İnternet'te yer alan kiralık Botnet ilanlarında Türkiye 40 ABD doları / 1000 bilgisayar ile "ucuz botnet" ligindedir. Sonuç olarak Türkiye'nin elindeki mevcut bilgisayar parkı (sanal asker), kendi takdiri dışında kendisine karşı kullanılabilecek kuvvetli bir silaha dönüşmüş durumdadır [49] ve Türkiye olası bir siber savaşta risk altındadır.

Ulusal strateji bağlamında; hali hazırda Türkiye'nin siber güvenliğin sağlanmasına yönelik resmi bir stratejisi bulunmaması nedeniyle, taslak olarak hazırlanarak TÜBİTAK-UEKAE tarafından Ocak 2009'da Başbakanlığa gönderilen "Ulusal Sanal Ortam Savunma Stratejisi" belgesinin gözden geçirilerek, farklı tarafları da içine alacak şekilde tekrar düzenlenerek acilen onaylanması, belirlenen stratejik hedeflerin diğer kamu kurum/kuruluşlarına yaygınlaştırılması gerektiği değerlendirilmektedir. Taslak olarak hazırlanan strateji belgesinin adından yola çıkarak savunmaya yönelik olacağı anlaşılmaktadır, her ne kadar bu konuda stratejilerin ağırlıkla savunmaya yönelik düşünülmesi gerekmekle birlikte, siber savaşın bir savaş türü olduğunun bilincine varılmalı; bu paralelde saldırı amaçlı olarak da yetenek geliştirilmesi gerektiği değerlendirilmektedir. Aralık 2011'de ABD'de imzalanan Ulusal Savunma Yetki Kanunu ile siber saldırı amaçlı operasyonlara yetki tanınmıştır [50].

Eylem planları ve ulusal raporlar bağlamında; ABD'de olduğu gibi, özellikle sorumluluk alanında kritik altyapıların bulunduğu her Bakanlık kendi Siber Güvenlik Stratejik Planı'nı oluşturmalıdır. Kritik altyapıların korunmasının

siber savaşta hayati öneme sahip olduğu kabul edildiğinde, özel sektör sahipliğinde ve kontrolünde olan bu altyapıların korunmasına ilişkin devletin rol ve sorumluluğu açıkça ortaya konmalı, bir kamu-özel sektör işbirliği modeli geliştirilmeli, kritik altyapıların korunması için müşterek (kamu-özel sektör) BOME merkezleri oluşturulmalı ve kurulan mekanizmalar deneme tatbikatlarında test edilmelidir. Yapılan analizde bu konuda pek çok eksiklik olduğu gözlemlenmiştir. Ayrıca yapılan akademik çalışmaların hükümet seviyesinde bir farkındalık ve etki yaratmaktan uzak kalması nedeniyle, başta TÜBİTAK ve Bilgi İletişim Kurumu olmak üzere kamu ve özel araştırma kurum/kuruluşlarının çeşitli analiz ve tavsiyeler içeren raporlar yayınlamaları teşvik edilmelidir.

Yasal Mevzuat bağlamında; taslağı hazırlanan Ulusal Bilgi Güvenliği Teşkilatı kanun teklifi vakit geçirilmeden gözden geçirilerek onaylanmalı, ulusal anlamda siber güvenliği yönetecek bir üst düzey organ oluşturulmalıdır. Bu organ vasıtasıyla, yapılması gereken gerek mevzuat değişikliklerinin gerekse de köklü diğer değişikliklerin çok daha kısa sürede ve kolaylıkta gerçekleştirilebileceği değerlendirilmektedir. Türk Ceza Kanununda tanımlı olan üç maddelik bilişim suçlarının ileri teknoloji kullanılan saldırı tekniklerini de içerecek şekilde genişletilmesi, Avrupa Konseyine üye bir ülke olarak Avrupa Siber Suçlar Sözleşmesinin onaylanarak iç hukuka uyarlanması gerekmektedir. Daha güvenli sistemler geliştirebilmek ve dolayısıyla sistem açıklıklarından kaynaklanan saldırıların sayısını azaltabilmek amacıyla, yasal düzenlemelerle sistem geliştirme safhasında, ürün geliştiren firmaların ihtiyaç analizi, sistem tasarımı, kodlama ve test-kabul gibi tüm ürün geliştirme süreçlerinde belirlenecek güvenlik standart ve kriterlerine uymaları zorunlu hale getirilmelidir [6]. Ayrıca, internet servis sağlayıcılarına bilgi güvenliği ihlallerini önleme yetkisi ve yükümlülüğü verilmesi [51] de düşünülmesi gereken bir diğer husustur.

Sorumlu Kurum/Merkez ve İlgili Organizasyonlar bağlamında; üst düzeyde Ulusal Bilgi Güvenliği Teşkilatı kurulmasına ilişkin kanun tasarısının yasalaşmasından sonra kurulacak teşkilatlanma bünyesinde kritik altyapı bulunduran Bakanlıkların kendi içerisinde kriz yönetimi ve olay müdahale amaçlı siber güvenlik merkezleri kurmaları gerektiği değerlendirilmektedir.

Siber Güvenlik Programları bağlamında; DPT Eylem Planı 88'inci madde doğrultusunda gerekli programların gerçekleştirilme çalışmaları devam etmektedir. Devlet Ar-Ge teşviklerinin siber güvenlik teknoloji alanlarında da kullanılabilecek şekilde düzenlenmesi ve ulusal çapta gerçekleştirilebilecek bir teknoloji yol haritası uygulaması sonucunda belirlenecek kritik siber teknolojilerinin milli olarak geliştirilmesinin sağlanması hedeflenmelidir. Üzerinde önemle durulması gereken bir diğer husus ise; siber güvenlik konusunda farkındalık yaratmak ve gerekli eğitimleri sağlamaktır. Siber güvenlik alanında eğitimlerin ilköğretimden başlamak üzere yüksek lisansa kadar her seviyede verilmesi amacıyla Milli Eğitim Bakanlığı eğitim müfredatları güncellenmelidir. Siber güvenlik konusunda yetişmiş insan gücü ve istihdama önem verilmelidir, 7 Şubat 2012'de gerçekleştirilen Savunmada Bilişim Konferansı sonuç bildirgesinde belirtildiği üzere bu alanda bir Mükemmeliyet Merkezi kurulabilir [52]. Siber güvenlik teknolojileri alanında Ar-Ge amaçlı akademik programlara öncelik verilmeli, Ar-Ge bütçesinin bir kısmının bu alanda kullanılması sağlanmalıdır. ABD İleri Savunma Araştırma Projeleri Ajansı (DARPA) 2012 yılı siber güvenlik araştırma bütçesini yüzde 50 oranında artırarak 208 milyon dolara çıkarmıştır [53]. Özellikle kamu bilgi sistemlerine yönelik yapılacak güvenlik testlerinin ulusal bir otorite tarafından oluşturulan güncel ulusal güvenlik politikalarına uygun olarak yapılması gerekmektedir[54]. Konferans ve sempozyumlar açısından umut verici görünen durum, siber güvenlik tatbikatları açısından ise yeterli görünmemektedir. Tatbikatların düzenlenmesindeki problemlerin aşılması sağlanabilse de tatbikatın sonuçları açısından içinde ilgili kamu kurum ve kuruluşlarının bulunduğu durumun olumsuz olduğu görülmektedir.

Silahlı Kuvvetler Siber Güvenlik Faaliyetleri bağlamında; açık kaynakta TSK'ya ait doğrulanmış, herhangi bir siber güvenlik planı, programı, projesi ve teşkilat değişikliği tespit edilememiştir. Ancak başta ABD olmak üzere pek çok ülkenin Siber Komutanlıklar kurmakta olduğu, bu birliklerde hem savunma hem de saldırı amaçlı harekâtlar icra edilmesinin planlandığı, ülkelerin personel politikalarında, teşkilatlarında değişiklikler yaptıkları, siber savaş eğitimleri sağladıkları, bu amaçla personel ihtisaslarını yeniden düzenledikleri, bilinmektedir.

Ulusal/Ulusal İşbirliği bağlamında; başta kritik altyapıların korunması olmak üzere pek çok alanda, hükümetin kritik altyapıları işleten özel sektör kuruluşlarıyla işbirliği yapması ve bunun sürdürülebilirliğinin sağlanması gerekmektedir. Siber saldırıların önceden tespiti, gözlemlenmesi, analizi ve saldırılara müdahale konusundaki tüm faaliyetler, sorumlu kılınacak bir merkez tarafından yönlendirilmelidir.

VI. SONUÇ

Sistemlerin kapalı olmaktan çıkıp açık, çevrim-içi hale geldiği, teknolojinin hayatın her alanını kontrol ettiği bir ortamda siber saldırı teknikleri, şüphesiz bir bireye, gruba, şirkete, kuruma veya ülkeye zarar vermek için kullanılabilecek en etkili ve en ucuz yöntemdir. Bu nedenle siber tehditlerin artacağı şüphesizdir.

Gelecekteki tüm askeri ve politik anlaşmazlıkların siber yönü olacağında yaygın bir görüş bulunmaktadır. Bu nedenledir ki, siber savaşa yönelik stratejisi ve merkezi bir savunma ve yanıt yeteneği olmayan ülkeler zayıf kalacaktır [55].

Ülkelerin siber güvenlik faaliyetlerinin bir metodoloji izlenerek analiz edilebilmesi amacıyla önerilen modelde, belirlenen yedi temel gösterge ve her bir gösterge kapsamında incelenebilecek hususlar incelenmiştir. Son bölümde ise önerilen model kullanılarak Türkiye'deki durum analiz edilmiştir.

Yazarların bilgisi dahilinde literatürde benzer bir çalışma olmaması nedeniyle önerilen makro analiz modelinin bu alanda yapılacak sonraki çalışmalara ışık tutacağı, önerilen modelin geliştirilerek gerek bireysel olarak gerekse de kıyaslama yöntemiyle birden fazla ülkenin siber güvenlik analiz durumlarını incelemede kullanılabileceği, değerlendirilmesi yapılan yedi ana göstergedeki sonuçların görsel olarak da farklı şekillerde kolaylıkla gösterilebileceği değerlendirilmektedir.

Türkiye'nin siber güvenlik analizi kapsamında; henüz ulusal bir strateji belgesinin yayımlanmadığı, ulusal anlamda tüm siber güvenlik faaliyetlerini yönlendirecek bir koordinasyon kurulunun bulunmadığı, bu nedenle yapılmakta olan pek çok plan ve programın etkinliğinin kısıtlı olduğu, ulusal siber güvenliğin sağlanması için zaruri olan yasal mevzuat ve ulusal/uluslar arası işbirliği konusunda da eksiklikler bulunduğu görülmektedir.

Önemini her geçen gün artıran siber savaşın kullanıldığı teknolojiler, nükleer teknoloji gibi birkaç ülkenin tekelinde bulunmamaktadır. Bütün ülkeler veya belli gruplar tarafından bu teknoloji kullanılarak siber saldırılar icra edilebilmektedir. Siber silah üretimi konusunda henüz erken olduğunu düşünmek açık bir yanlıştır [56]. Bu nedenle, başta ABD olmak üzere bu alanda hazırlıklarını yoğun şekilde sürdüren NATO ve diğer ülkelere paralel olarak, siber tehdit odaklı siber savaşa Türkiye'nin ve dolayısıyla TSK'nın da kendisini hızlı bir dönüşümle adapte edecek çalışmalara ivedilikle başlanması gerektiği değerlendirilmektedir. Siber tehdidin, "Kırmızı Kitap" olarak bilinen Milli Güvenlik Siyaset Belgesi'ne tehdit algısı olarak girmesi de bu konuda en üst düzeyde atılmış olumlu bir adımdır.

Ülke olarak, 21'nci yüzyılın savaş ortamı olan, ülkeleri ayıran sınırların ortadan kalktığı, siber uzayda siber güvenlik cephesindeki yerimizi sağlamlaştırabilmemiz adına, çalışmada belirtilen önerilerin ivedilikle dikkate alınması gerektiği değerlendirilmektedir.

KAYNAKÇA

[1] UK Kabine Ofisi, "Cyber Security Strategy of the United Kingdom", Haziran 2009, <http://www.cabinetoffice.gov.uk/media/216620/css0906.pdf/>
[2] Marsan, Carolyn Duffy, "10 Things You Didn't Know About Cyber Warfare", Network World, June 08, 2009 <http://www.networkworld.com/news/2009/060809-cyberwarfare.html/>
[3] Gökpınar, E. Serdar. "Şebekeler (Ağ Yapılar) ve Savaş", Sayısal Ortamda Savaş Sempozyumu, Ankara, 10 Aralık 2009
[4] Arquilla, John., Ronfeldt, David, "In Athena's Camp, Preparing for Conflict in the Information Age Ch.2 : Cyberwar is Coming", RAND Corporation, 1997
[5] Libicki, Martin C. "Cyberdeterrence and Cyberwar", RAND Corporation, 2009
[6] Mulligan, Deirdre K., Schneider, Fred B., "Doctrine for Cybersecurity", 15 May 2011
[7] US White House, "The National Strategy to Secure Cyber Space", February 2003
[8] US White House, "The Comprehensive National Cybersecurity Initiative", <http://www.whitehouse.gov/cybersecurity/comprehensive-national-cybersecurity-initiative/>
[9] UK Office of Cyber Security, "Cyber Security Strategy of the United Kingdom: Safety, Security and Resilience in Cyber Space", June 2009, <http://webarchive.nationalarchives.gov.uk/+/http://www.cabinetoffice.gov.uk/media/216620/css0906.pdf/>
[10] Cyber Security Strategy for Germany, February 2011, <http://www.cio.bund.de/SharedDocs/Publikationen/DE/Strategische-Themen/css_engl_download.pdf?__blob=publicationFile/>
[11] Australian Government Cyber Security Strategy, ISBN: 978-1-921241-99-4, 2009, <http://www.ag.gov.au/Documents/AG%20Cyber%20Security%20Strategy%20-%20for%20website.pdf/>
[12] French Network and Information Security Agency (FNISA), "France's Strategy : Information Systems Defence and Security", February 2011, <http://www.enisa.europa.eu/media/news-items/Information_system_security_France_strategy.pdf/>
[13] Netherlands National Cyber Security Strategy : Success Through Cooperation, 2011, <http://www.enisa.europa.eu/media/news-items/dutch-cyber-security-strategy-2011/>
[14] Sağıroğlu, Şeref, Prof.Dr., "Siber Güvenlik ve Türkiye", Siber Güvenlik Çalıştayı, 29 Eylül 2011, Ankara
[15] US National Institute of Standards and Technology (NIST), Special Publication 800-18, "Guide for Developing Security Plans for Federal Information Systems", February 2006
[16] US National Institute of Standards and Technology (NIST), Special Publication 800-53, "Recommended Security Controls for Federal Information Systems and Organizastions", August 2009
[17] US National Institute of Standards and Technology (NIST), Special Publication 800-37, "Guide for Applying the Risk Management Framework to Federal Information Systems", February 2010
[18] Carr, Jeffrey., "Inside Cyber Warfare : Mapping the Cyber Underworld", ISBN : 978-0-596-80215-8, 2010
[19] Owens, William A., Dam, Kenneth W. and Lin, Herbert S., "Technology, Policy, Law, and Ethics Regarding U.S. Acquisition and Use of Cyberattack Capabilities", The National Academies Press, Washington, D.C., 2009
[20] McAfee, "Virtual Crimonology Report, 2009" <http://www.mcafee.com/uk/local_content/reports/virtual_criminology_report/uk_virtual_criminology_09_report.pdf>
[21] Jancewzski, Lech J., Colarik, Andrew M., "Cyber Warfare and Cyber Terrorism", ISBN : 978-1-59140-992-2, 2008
[22] Gürkaynak, Muharrem., İren, Adem Ali., "Reel Dünyada Sanal Açmaz: Siber Alanda Uluslararası İlişkiler", Süleyman Demirel Üniversitesi,İktisadi ve İdari Bilimler, Fakültesi Dergisi, Y.2011, C.16, S.2, s.263-279.
[23] Clarke, Richard. A., "Cyberwar: The Next Threat to National Security and What to Do About It", ISBN-13: 978-0061962233, 20 April 2010
[24] Keggier, J., Mahon, T., "Preparing for Cybergeddon", Armada International, s: 34-36, 01 Nisan 2009.
[25] US White House, "Cyberspace Policy Review", May 2009
[26] DPT Bilgi Stratejisi Ek'i ve Bilgi Toplumu Eylem Planı, 2006
[27] DPT Bilgi Toplumu Stratejisi Eylem Planı (2006-2010) Değerlendirme Raporu, Rapor No:5, Ankara Mart 2010.
[28] Ünver, Mustafa., Canbay, Cafer., Mirzaoğlu, Ayşe Gül., "Siber Güvenliğinin Sağlanması: Türkiye'deki Mevcut Durum ve Alınması Gereken Tedbirler Raporu", Mayıs 2009
[29] 5809 sayılı Elektronik Haberleşme Kanunu, Yayımlanma Tarihi 10 Kasım 2008
[30] Kamu Kurum ve Kuruluşları ile Gerçek ve Tüzel Kişilerine Elektronik Haberleşme Hizmeti İçinde Kodlu veya Kriptolu Haberleşme Yapma Usul ve Esasları Hakkında Yönetmelik, Yayımlanma Tarihi 23 Ekim 2010
[31] T.C.Başbakanlık Kanunlar ve Kararlar Genel Müdürlüğü, Sayı:B.02.0.KKG.0.10/101-902/1812, 22 Nisan 2008.
[32] T.C.Sağlık Bakanlığı 2010-2014 Stratejik Planı, Yayın No:788, Syf.77, ISBN:978-975-590-315-6
[33] Karabacak, Bilge., "Kritik Altyapılara Yönelik Siber Tehditler ve Türkiye için Siber Güvenlik Önerileri", Siber Güvenlik Çalıştayı, 29 Eylül 2011, Ankara
[34] 3'üncü Uluslararası Katılımlı Bilgi Güvenliği ve Kriptoloji Konferansı, 25-27 Aralık 2008, Ankara, <http://www.iscturkey.org/2010/2008/index.php?id=sonuc>
[35] Siber Güvenlik Hukuk Çalıştayı, 26-27 Ocak 2012, Ankara, <http://www.iscturkey.org/calistay/2/>
[36] Tatar, Ünal., "Siber Tehditler Karşısında Türkiye TR-BOME Çalışmaları", İstanbul Bilgi Güvenliği Konferansı, 10 Haziran 2009

[37] Eriş, Mehmet., "Türkiye Bilgisayar Olayları Müdahale Ekibi Koordinasyon Merkezi" 3. TÜBİTAK-UEKAE Bilgi Teknolojileri Güvenlik Konferansı Sunumu, 06 Haziran 2008
[38] Bircan, Bahadır., "SOSAM (Sayısal Ortam Savunma Merkezi)", 3. TÜBİTAK-UEKAE Bilgi Teknolojileri Güvenlik Konferansı, 06 Haziran 2008
[39] Bilgi Güvenliği Akademisi web sitesi, erişim tarihi 09 Mart 2012, <http://blog.bga.com.tr/duyurular/bga-siber-guvenlik-kampi-ilk-mezunlarini-verdi/>
[40] CEH Türkiye web sitesi, erişim tarihi 09 Mart 2012, <http://www.cehturkiye.com/index.php/ceh-turkiye-hakkinda/>
[41] Ulaşanoğlu, M.Emin., Yılmaz, Ramazan., Tekin, M.Alper., "Bilgi Güvenliği : Riskler ve Öneriler", Ağustos 2010
[42] TÜBİTAK Web Sitesi, <http://www.tubitak.gov.tr/sid/0/cid/21886/index.htm;jsessionid=122D58093787 8F69C4C9D54A5A49B706/>
[43] Interpromedya Haber Merkezi, "Farkındalık Olmadan Siber Güvenlik Olmaz", <http://www.bthaber.com.tr/?p=10979/>
[44] Tettersall, Aynur., Düven, Alpaslan., "Rusya ve Çin: Siber Uzay Konferansı'na karşı", <http://www.dha.com.tr/haberdetay.asp?Newsid=230255>
[45] Conference on Cyberspace, 1-2 November 2011, London, <http://www.fco.gov.uk/en/global-issues/london-conference-cyberspace/>
[46] Bensghir, T.Kaya., Prof.Dr., "E-Dönüşüm ve E-İmza Uygulamaları", TODAİE e-Devlet Merkezi Uygulamalı E-İmza Semineri, 16-17 Kasım 2011, Ankara
[47] Starcom MediaVest Group (SMG) Connected web sitesi, erişim tarihi 09 Nisan 2012, "Türk Tüketicisinin Akıllı Telefon Kullanımı", <http://smgconnected.com/turk-tuketicisinin-akilli-telefon-kullanimi/>
[48] Symantec "Global Internet Security Threat Report, Trends for 2008. Vol. XIV", April, 2009
[49] Üneri, Mert., "Bilgisayar Güvenliği ve İnternet", Temmuz 2009, <http://www.bilgitoplumu.gov.tr/Documents/1/Icra_Kurulu/090715_IK27.ToplantisiInternetVeBilgisayarGuvenligi.pdf/>
[50] Hoover, Nicholas J., "Defense Bill Approves Offensive Cyber Warfare", Information Week, 05 January 2012
[51] Özenç, Köksal, Alkan, Mustafa, Acarer, Tayfun, "Uluslararası Ülke Güvenliğinde Hukuki ve Teknik Yaklaşım", 3'üncü Uluslararası Katılımlı Bilgi Güvenliği ve Kriptoloji Konferansı, 25-27 Aralık 2008, Ankara
[52] Savunmada Bilişim Konferansı, 07 Şubat 2012, <http://www.interpromedya.com.tr/savunmadabilisim/?p=777/>
[53] Hoover, Nicholas J., "DARPA Boosts Cybersecurity Research Spending 50%", Information Week, 07 November 2011
[54] Vural, Yılmaz., Sağıroğlu, Şeref, Prof.Dr., "Ülke Bilgi Güvenliği", 3'üncü Uluslararası Katılımlı Bilgi Güvenliği ve Kriptoloji Konferansı, 25-27 Aralık 2008, Ankara
[55] Anıl, Süleyman., "Cyber Security in NATO and Nations", Sayısal Ortamda Savaş Sempozyumu, Ankara, 10 Aralık 2009
[56] Gündoğan, Mete, Prof.Dr., "Siber Silah Endüstrisi ve Türkiye", Siber Güvenlik Konferansı, 22 Aralık 2011, Ankara.

Operating System Evaluation Using Choquet Integral in Terms of Cyber Threats

K. Göztepe* A.Ejder**

Abstract— **Operating system (OS) selection is a critical decision that can significantly affect future competitiveness and performance of an organization. It is increasingly valuable in today's current administration and businesses because of its ability to integrate the information. An operating system, especially with the weakness in security can lead to serious financial losses. The aim of this study is to develop a decision model based on choquet integral that select the appropriate operating system for critical computer systems by taking subjective judgments of decision makers into consideration. Proposed approach is based on choquet integral method. Choquet integral method is used in determining the weights of the criteria by decision makers and then rankings of the operating systems. Numerical study has also been demonstrated.**

***Index Terms*—Operating systems, choquet integral, decision making, cyber threats.**

I. INTRODUCTION

The quick evolution of IT force system security professionals to a competitive environment. Government agencies, enterprises, and even individuals, are confronted by technology replacement decisions more frequently as technology upgrades speed up. Because of this, it becomes necessary to take decisions more often for the update of the technology. Government agencies, enterprises, firms and organizations should consider the changes and update the information technologies. One of these technology-related changes occur in operating systems. Operating system is system software responsible for the direct control and management of the hardware, basic system operations and operation of applications. It provides links to the memory, input/output devices and file system [1],[2].

Operating system choice is crucial for companies or organizations in terms of IT infrastructure reliability [3]. Selection Choice of operating systems should be considered a variety of criteria. Choquet integral has been used for that reason in this case.

Corresponding author :
*Kerim Göztepe,(I.E.Ph.D). War Colleges Command, Army War College, Dept. of Combat Tactics, Yenilevent, 34330, Pbx: +90 212 398-0100, İstanbul-Turkey, e-mail: kerimgoztepe@yahoo.com.

**Ahmet Ejder, War Colleges Command, Army War College, Dept. of Combat Tactics, Yenilevent, 34330, Pbx: +90 212 398-0100, İstanbul-Turkey, e-mail: a ejders@yahoo.com.

II. KEY FEATURES OF OPERATING SYSTEMS

An OS should ensure tasks and service management features in order to meet enterprise computing needs. Tanenbaum [2] and Galvin [1] categorize these features as follows: Process Management, Storage Management, Protection and Security, Distributed Structure and Software Features (Fig.1).

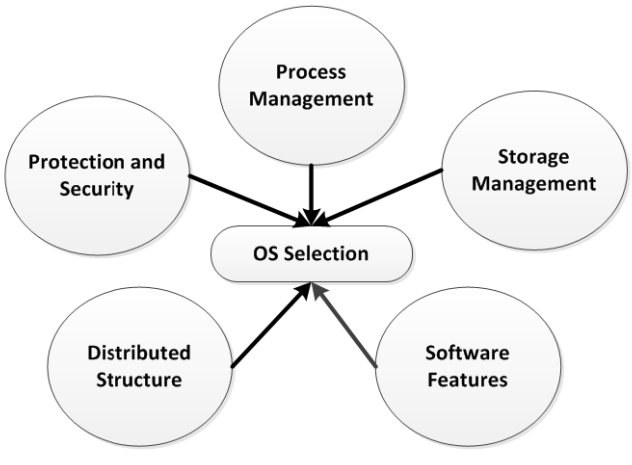


Fig. 1. Main features of an operating system.

A. Process Management (PM)

A Process is an instance of a computer program. It is being sequentially executed by a computer system. PM has the ability to run several computer programs concurrently [4]. Most modern operating systems support processes that have multiple threads.

B. Storage Management (SM)

Main memory is usually too small to accommodate all the data and programs permanently. Thus, the computer system must provide secondary storage to back up main memory. Today's computer systems use disks as the primary on-line storage medium for information. The file system provides the mechanism for on-line storage and access to both data and programs residing on the disks [4],[5].

C. Protection and Security (PS)

Protection is an internal problem. However, security must consider both the computer system and the environment. To defend the processes from cyber threats is essential for the operating systems. Protection refers to a mechanism for controlling the access of programs, processes, or users to the resources. These are determined by the computer system [2],[5]. Computer resources must be guarded against cyber

terrorists, cyber activists and special cyber attack teams.

D. Distributed Structure *(DS):*

A distributed system is a collection of processors that do not share memory or a clock. Instead, each processor has its own local memory, and the processors communicate with one another through communication lines such as local area or wide are networks. Main topics related with distributed structure are network structures, distributed system structures, distributed file systems and distributed coordination. It is important to know that it is sometimes impossible to determine the exact events order in a distributed system. Timestamps and mutual exclusion can be used to provide a consistent event ordering [2],[5].

E. *Software Features (SF)*

An operating system must provide applications and tools, bugs and coding, graphical user interface, availability and support criteria [3]. Programming Interface provides several ways for developers to access to system resources such as kernel objects, I/O devices and etc. Graphical User Interface takes advantage of the computer's graphics capabilities to make interacting user and operating system easier. Applications and tools must be always available and should be supported by developers in order to satisfy user requests [2],[5]. In this study, operating system's software features are evaluated for their specialities.

III. CHOQUET INTEGRAL

The choquet integral method can be seen as a fuzzy integral method based on any fuzzy measure that provides an alternative computational structure for aggregating information. Sugeno [6] introduces the concepts of fuzzy measure and fuzzy integral to express the grades of importance for criteria, which is useful to model the preference structure. Fuzzy measures, according to Sugeno, are obtained by replacing the additive requirement of classical measures with weaker requirements of monotonicity (with respect to set inclusion) and continuity. Sugeno and Terano [7] incorporate the λ-additive axiom to reduce the difficulty of collecting information. In literature choquet integral has been used in different studies and applications [8],[9],[10],[11].

A. Fuzzy Measure

Fuzzy measure g is a set function defined on the power set β(X) of X and satisfies the following properties [12],[13]:

If there are two criteria such as A and B;

$$g:\beta(X)\rightarrow[0,1]$$

$$g(\varnothing)=0, \qquad g(X)=1 \quad \text{(Boundary conditions)} \quad (1)$$

$$\text{if } A,B\in\beta(X) \quad \text{and} \quad A\subset B \quad \text{then} \quad g(A)\le g(B) \quad \text{(Monotonicity)} \quad (2)$$

$$In\ \beta(X),\ if\ A_1\subset A_2\subset A_3\subset A_4\subset,\ldots,$$
$$and\ \mathbf{U}_{i=1}^{\infty}A_i\in\beta(X),$$
$$then\ lim_{i\to\infty}g(A_i)=g(\mathbf{U}_{i=1}^{\infty}A_i)$$
(Continuity from below) (3)

$$In\ \beta(X),\quad if\ A_1\supset A_2\supset A_3\supset A_4\supset,\ldots,$$
$$and\ \mathbf{I}_{i=1}^{\infty}A_i\in\beta(X),$$
$$then\ lim_{i\to\infty}g(A_i)=g\left(\mathbf{I}_{i=1}^{\infty}A_i\in\beta(X)\right)$$
(Continuity from above) (4)

A λ-fuzzy measure g_λ is a fuzzy measure with the following property:

$$\forall A,B\in\beta(X),\quad A\cap B=\varnothing \quad (5)$$
$$g_\lambda(A\cup B)=g_\lambda(A)+g_\lambda(B)+\lambda g_\lambda(A)g_\lambda(B)$$
where $\lambda\in(-1,\infty)$ (6)

If $X=\{x_1,x_2,\ldots,x_n\}$ fuzzy density $g_i=g_\lambda(\{x_i\})$ will have the following form: (7)

$$g_\lambda(\{x_1,x_2,\ldots,x_n\})=\sum_{i=1}^{n}g_i+\lambda\sum_{i_1=1}^{n-1}\sum_{i_2=i_1+1}^{n}g_{i_1}g_{i_2}+\ldots \quad (8)$$
$$+\lambda^{n-1}g_1g_2,\ldots,g_n$$

$$=\frac{1}{\lambda}\left|\prod_{i=1}^{n}(1+\lambda g_i)-1\right| \quad for\ -1\le\lambda<\infty \quad (9)$$

If $\lambda>0$ then $g_\lambda(A\cup B)>g_\lambda(A)+g_\lambda(B)$. This means that the evaluation of the set {A,B} is larger than the sum of evaluations for sets {A} and {B}. *It is called* ***superadditivity***. i.e., the multiplicative effect exists in {A, B}.

If $\lambda<0$ then $g_\lambda(A\cup B)<g_\lambda(A)+g_\lambda(B)$ This means that the evaluation of the set {A, B} is smaller than the sum of evaluations for sets {A} and {B}, i.e., the substitutive effect exists in {A, B}. *It is called* ***subadditivity***.

If $\lambda\neq0$ indicates that the λ-fuzzy measure g_λ is ***nonadditivity*** and there is interaction between A and B.

If $\lambda=0$ then $g_\lambda(A\cup B)=g_\lambda(A)+g_\lambda(B)$. This means that the evaluation of the set {A, B} equals the sum of evaluations for sets {A} and {B} It is called additivity. If $\lambda=0$ indicates that the λ-fuzzy measure g_λ is additive, and there is no interaction between A and B.

The fuzzy measure is often used with fuzzy integral for the purpose of aggregating information evaluation.

B. Fuzzy integral

Let h be a measurable function from X to [0,1]. Assuming that $h(x_1) \geq h(x_2) \geq \cdots \geq h(x_n)$ then a fuzzy integral is defined as follows [6],[14],[15].

$$(C)\int h dg = h(x_n)g(H_n) + [h(x_{n-1}) - h(x_n)]g(H_{n-1}) + \ldots + [h(x_1) - h(x_2)]g(H_1)$$
$$= h(x_n)[g(H_n) - g(H_{n-1})] + h(x_{n-1})[g(H_{n-1}) - g(H_{n-2})] + \ldots + h(x_1)g(H_1) \quad (10)$$
$$where\ H_1 = \{x_1\}, H_2 = \{x_1, x_2\}, \ldots\ldots, H_n = \{x_1, x_1, \ldots, x_n\} = X$$

The basic concept of Eq. (2) can be illustrated as shown in Fig.2. Furthermore,

if λ=0 and $g_1 = g_2 = \cdots = g_n$ then $h(x_1) \geq h(x_2) \geq \cdots \geq h(x_n)$ is not a necessary condition. (11)

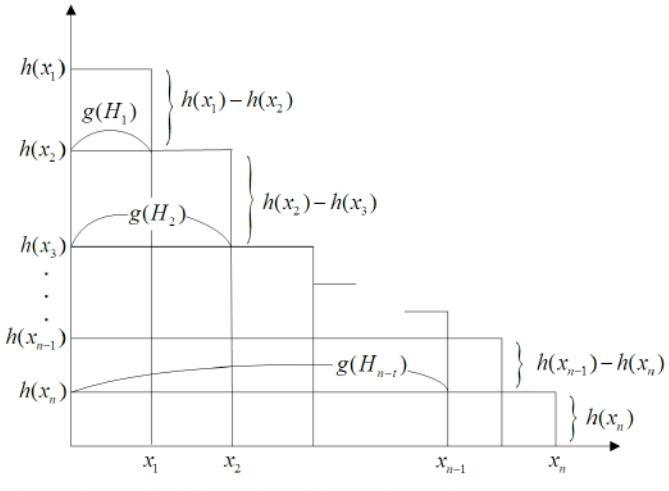


Fig. 2: The graphical illustration of choquet integral.

IV. A NUMERICAL SAMPLE

Five popular and widely used operating systems evaluated in this section. These are Ubuntu (UBT), Ms-Win (WIN), MAC, Fedora (FED) and Slackware (SLACK). Evaluation process made according to process management, storage management, protection and security, distributed structure and software features. Evaluation steps are given below (see also Appendix A).

Step1: Making pairwise comparison matrices.
A pairwise matrix calculated in order to find weight values of operating systems. Pairwise table is given below(Table1).

TABLE I
PAIRWISE COMPARISON TABLE

	PM	SM	PS	DS	SF	weights
PM	1	3	1	2	2	0.2927
SM	0.333	1	0.5	1	0.5	0.1115
PS	1	2	1	3	3	0.3240
DS	0.5	1	0.333	1	1	0.1248
SF	0.5	2	0.333	1	1	0.1467

Pairwise comparison is a widely used judgement method either for deriving criteria-weights or for evaluating alternatives according to a given criterion [16],[17].

Step 2. Determining interaction degree.
Interaction degree λ is used in the evaluation. λ=3 in model.

Step 3. Obtaining results.
Obtained results from proposed example are given in Appendix A. Evaluation scores for operating system criteria are; {PM} 0.1668, {SM} 0.0557, {PS} 0.1890, {DS} 0.0629, {SF} 0.0751. Here, PS criteria got the high score then others.

Step 4. Choquet integrated values
Operating system experts gave score to each OS for Ubuntu, MS-Win, Mac, Fedora and Slackware (Table2). Operating systems have been evaluated over 10. For instance, Ubuntu scores are PM=8, SM=7, PS=8, DS=8, SF=6 as seen Table 2.

TABLE II
CHOQUET INTEGRATED VALUES

OS	PM	SM	PS	DS	SF	Choquet Integrated Values
UBT	8	7	8	8	8	7.80898
WIN	7	6	8	7	7	6.99803
MAC	8	5	7	8	9	7.08872
FED	8	6	8	8	8	7.61796
SLACK	6	8	8	7	6	6.66806

Ubuntu OS received the highest score, 7.808, at the end of the calculation process.

Step 5. Sensitivity analysis.

From the coloured graph (Fig 3), Mac OS (Blue line) is most preferred OS when $\lambda < 0.5$. If λ value increases, $\lambda > 0.5$, then Ubuntu OS gets high score. Ubuntu is the best OS between $10 > \lambda > 0.5$ values. If λ value remains between $6 > \lambda > 0.5$, OS order of preference will be the same. When λ is $8 > \lambda > 6$, Win OS will be third one.

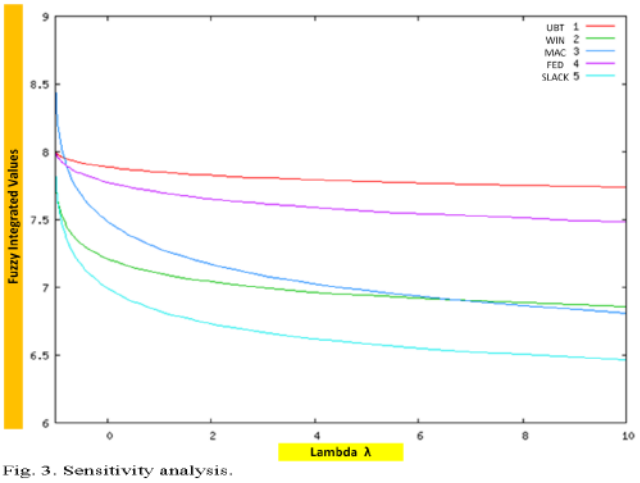


Fig. 3. Sensitivity analysis.

V. Conclusion

Today the number and impact of cyber-threats are increasing rapidly. Selection of appropriate operating system has vital importance for organizations, government agencies, and enterprises. A firm may have some positive results in its interested competition area. It is possible to get better results in costs, time-efficiency and increased work performance by using suitable OS. In this paper, choquet integral is used for evaluating selected operating systems. Pairwise matrices calculation for determining the weights of the criteria and priority values of operating systems has been done by choquet integral method. Although choquet integral has complex calculation procedure, it is a useful approach for evaluating multiple criteria alternatives. Choquet integral is one of the outranking methods for multi-criteria decision-making and can be used for ranking alternatives. This approach enables experts and users to select more suitable operating system for a specific purpose and requirement.

The researchers may compare the performance of choquet integral with other meta-heuristics (e.g. genetic algorithm, artificial neural network, fuzzy neural networks) specifically to test whether choquet integral approach has any advantage in operating system evaluation.

APPENDIX

Appendix A: Main steps of λ Fuzzy Measure and Fuzzy Integral, and Choquet Integral Evaluation Scores is given.

REFERENCES

[1] S. Galvin, Operating System Concepts, 4th Edition. Addison Wesley, Reading, MA, 1994.
[2] A.S. Tanenbaum, Operating Systems: Design and Implementation. Prentice Hall, Englewood Cliffs, NJ, 1987.
[3] E. Tolga, M. Levent Demircan, C. Kahraman, Operating system selection using fuzzy replacement analysis and analytic hierarchy process, Int. J. Production Economics , 97 pp.89-117, 2005.
[4] G.D. Knott, A proposal for certain process management and inter-communication primitives. *SIGOPS Operating Systems Review*, 8(4), pp.7-44, 1974.
[5] S. Ballı and S. Korukoğlu, Operating System Selection Using Fuzzy Ahp And Topsis Methods, Mathematical and Computational Applications, Vol. 14, No. 2, pp. 119-130, 2009.
[6] M. Sugeno, Theory of fuzzy integrals and its applications, PhD Thesis, Tokyo Institute of Technology, 1974.
[7] M. Sugeno and T.Terano, A model of learning on fuzzy information, Kybernetes 16 (3), pp. 157-166, 1977.
[8] L. Berrah, G. Mauris and J. Montmain, Monitoring the Improvement of an Overall Industrial Performance Based on a Choquet Integral Aggregation", The International Journal of Management Science, 36, pp. 340-351, 2008.
[9] T. Demirel, N. Ç. Demirel, and C. Kahraman, Multi-criteria Warehouse Location Selection Using Choquet Integral, Expert Systems with Applications, 37(5), pp.3943-3952, 2010.
[10] P. Meyer, M. Roubens, On the Use of the Choquet Integral with Fuzzy Numbers in Multiplecriteria Decision Support, Fuzzy Sets and Systems, 157, pp.927-938, 2005.
[11] H.H. Tsai, I.Y. Lu, The Evaluation of Service Quality Using Generalized Choquet Integral, Information Sciences, 176, pp.640-663, 2006.
[12] Z. Wang, G.J. Klir, Fuzzy Measure Theory, Plenum Publishing, Corporation, New York, 1992.
[13] E. Takahagi, λ Fuzzy Measure Identification Methods using λ and Weights, 2005.
[14] K. Ishii and M. Sugeno, A model of human evaluation process using fuzzy measure. International Journal of Man-Machine Studies 22, pp.19-38, 1985.
[15] M. Grabisch, T. Murofushi, M. Sugeno, Fuzzy Measures and Integrals, Physica-Verlag, New York, 2000.
[16] T.L. Saaty, The Analytic Hierarchy Process, McGraw-Hill, Inc., New York, USA, 1980.
[17] T.L. Saaty, Decision making with dependence and feedback: the analytic network process, RWS Publications, Pittsburgh, 1996.
[18] E. Takahagi, An intermediate Evaluation Method among Maximum, Average and Minimum using Fuzzy Measure and Choquet Integral and its Applications, Methodologies for the conception, design, and application of intelligent systems; proceedings of the 4th International Conference on Soft Computing 1, World Scientific, pp.299-302, 1996.

APPENDIX A

Infrastructure of main steps; λ Fuzzy Measure and Fuzzy Integral [18]

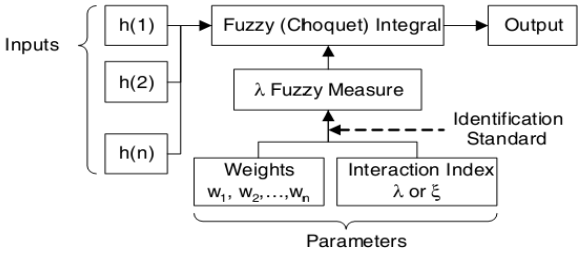


Table III
Identified Fuzzy Measure for OS Criteria

Sets	Fuzzy Measure
{}	0
{PM}	0.166869
{SM}	0.0557408
{PM,SM}	0.250515
{PS}	0.189054
{PM,PS}	0.450566
{SM,PS}	0.276409
{PM,SM,PS}	0.581652
{DS}	0.0629981
{PM,DS}	0.261405
{SM,DS}	0.129274
{PM,SM,DS}	0.360859
{PS,DS}	0.287783
{PM,PS,DS}	0.598719
{SM,PS,DS}	0.391648
{PM,SM,PS,DS}	0.75458
{SF}	0.0751959
{PM,SF}	0.279709
{SM,SF}	0.143511
{PM,SM,SF}	0.382224
{PS,SF}	0.306899
{PM,PS,SF}	0.627405
{SM,PS,SF}	0.41396
{PM,SM,PS,SF}	0.788062
{DS,SF}	0.152406
{PM,DS,SF}	0.395571
{SM,DS,SF}	0.233632
{PM,SM,DS,SF}	0.51746
{PS,DS,SF}	0.427899
{PM,PS,DS,SF}	0.808979
{SM,PS,DS,SF}	0.555195
{PM,SM,PS,DS,SF}	1

Siber Güvenlik Persfektifinden Makineler Arası İletişim Uygulamalarının İncelenmesi

Alper ÖZBİLEN, İlhami ÇOLAK, Şeref SAĞIROĞLU

***Özet*—Makineler arası (M2M) iletişim uygulamaları, geçmişten bu yana belirli iş süreçlerini otomatize etmek, uzak istasyonlardan sıcaklık, seviye, hız, konum vb. gibi çeşitli değerleri okumak maksadıyla uzun yılardır farklı isimlerde kullanılmaktadır.Ancak günümüzde, otomasyona ve uzak erişime duyulan ihtiyacın fazlalaşmasıyla birlikte M2M uygulamalar, artık eski hizmet sınırlarını aşarak, taşımacılık, ev elektroniği, sağlık gibi çok farklı alanlarda da kullanıma başlamıştır. Önümüzdeki yıllarda uzaktan yönetilebilen sayaç, klima, buzdolabı, fırınlı ocak ve motorlu taşıtlar gibi ürünlerin sayısının katlanarak artacağı tahmin edilmektedir. Kritik işlemleri icra eden bölgesel ve ulusal otomasyon altyapılarında ise geçmiş özel telsiz ağlar yerine, ticari mobil ve sabit şebekelerin kullanımını artması beklenmektedir. Yakın gelecekte M2M uygulamalarına yönelik siber saldırılar, toplum sağlığı ve insan hayatını etkileyebilecek katastrofik problemlere üretme potansiyeline sahip olacaktır. Özellikle, haberleşme ortamı olarak gömülü SIM kart ve uydu modüllerini kullanan sistemler, hesap verebilirliği kısıtlayan siber vakalara neden olabilecektir.**

***Anahtar Kelimeler* — Siber Güvenlik, Makineler Arası İletişim, Telekomünikasyon**

***Abstract*—Machine to Machine communication applications have been used with different names for different purpose to automate particular tasks such as collecting temperature, level, speed, position data since a long time. Today, with the increase in the need for automation and remote access, M2M applications are now beyond the borders of the old services, and are started to be used in various areas like transportation, home electronics, health care. In the following years, it is estimated to grow exponentially in the number of products such as remotely manageable utility-meter, air-condition, refrigerator, cooker and motor vehicles. Automation systems that perform critical operations in the regional and national scale infrastructures are expected to increase the use of commercial mobile and fixed networks as a communication platforms instead of private wireless networks. In the near future, cyber attack on M2M applications may lead to catastrophic problems that affect public health and human life. Particularly, systems that uses a embedded SIM card and satellite modules as a medium of communication platforms cause cyber incidents that could restrict accountability.**

A.Özbilen, Bilgi Güvenliği Derneği, Maltepe/Ankara, Türkiye (alper@ozbilen.net)
Prof. Dr. İ. Çolak, Gazi Ünv. Teknoloji Fakültesi Elektrik-Elektronik Mühendisliği Bölümü, Ankara, Türkiye (icolak@gazi.edu.tr)
Prof. Dr. Ş. Sağıroğlu, Gazi Ünv. Mühendislik Fakültesi Bilgisayar Mühendisliği Bölümü, Ankara, Türkiye (ss@gazi.edu.tr)

***Index Terms*—Cyber Security, Machine to Machine Communication, Telecommunicatiom**

I. GİRİŞ

Makine'den Makineye (M2M) iletişim, arada herhangi bir insan unsuru olmadan makine üzerine gömülü veya entegre cihazlar arasında, kablolu veya kablosuz erişim ortamları üzerinden kurulan iletişimi temsil etmektedir. Birbiriyle haberleşen makineler, kullanım alanı ve servise bağlı olarak belirli bir alanda yer alabileceği gibi dünya üzerinde dağıtık bir yapıda da yerleşik bulunabilmektedirler [1]

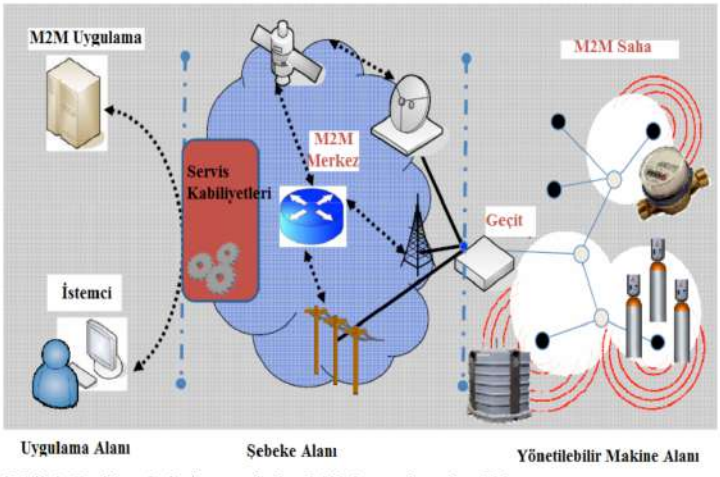
Makine'den Makineye (M2M) iletişim uygulamaları, iletişim pazarında yeni ivme kazanan bir hizmet modeli olarak görülse de, geçmişi, uzun yıllardır otomasyon sistemlerinin uzak birimlerinin yönetiminde kullanılan telemetri sistemlerine dayanmaktadır.Bu yönüyle geçmiş ve şimdili telemetri sistemlerinin kendisi veya devamı sistemler olarak da isimlendirilebilir.

II. MAKİNELER ARASI İLETİŞİM

M2M uygulamaları, tipik olarak, uzaktan yönetim ve ölçüm verilerinin toplanması gibi amaçlarla bilgisayar tabanlı akıllı sensör ve aktüatörler ile doğrudan sabit veya mobil cihazlar üzerinden kullanılabilmektedir.

Geçmişteki M2M uygulamaları daha çok belirli endüstriyel kontrol süreçlerini izlemek ve yönetmek için oluşturulur ve iletişim için ağırlıkla telemetri olarak da adlandırılan özel tahsisli veya kamuya açık frekans bantları seçilirdi. Son birkaç yılda M2M uygulamaların çeşitlenmesi ve gündelik kullanım alanları içersine de girmesiyle hücresel mobil şebekeler gibi ticari telekomünikasyon altyapıları üzerinden kullanımının arttığı görülmektedir.

Şekil 1'de hücresel, uydu ve kablolu şebekeler üzerinden yapılan M2M saha uygulamalarının şematik gösterimi yer almaktadır.



Şekil 1. Farklı şebekeler üzerinden M2M uygulamaları [2]

M2M uygulamalarında bağlanabilirlik, ev ve ofisi gibi kişisel kullanım alanları için IEEE 802.15, Ultra-wideband (UWB), Zigbee ve Bluetooth erişim teknolojileri ile ; kampus, site ve endüstriyel tesis gibi yerel alanlarda PLC (Power Line Communication), Wi-Fi ve Femtocell gibi erişim teknolojileri ile sağlanabilmektedir [3]. Ancak şehir, bölge veya ülke ölçeğinde verilecek servisler için kişisel veya yerel alanda bağlantı sağlayan erişim teknolojileri beklenildiği üzere yetersiz kalacaktır. Şehir ve ülke ölçeğinde erişilebilen uygulamalar için xDSL başta olmak üzere düşük maliyetli kablolu bağlantı hizmetleri; alternatif olarak da uydu veya GSM, GPRS, CDMA, WiMax, LTE gibi hücresel tabanlı kablosuz altyapılar kullanılabilmektedir [3].

M2M uygulamalarının, özel haberleşme altyapıları yerine GSM hat ve modülleri gibi farklı uygulamalar için standardizasyon sağlayan, cüzi ücretlerle elde edilebilen, ulusal ve/veya uluslararası ölçekte erişebilirlik ve yönetilebilirlik sağlayan sistemlere kayması ile M2M pazarının da büyüyeceğini öngörmek mümkündür. Örneğin, önceleri M2M, elektrik şebekelerinin ana çatılarındaki belirli altyapı elementleri uzaktan kumanda etmek veya ölçüm verilerine ulaşmak için kullanılırken, bugün akıllı sayaçlar ve üzerlerindeki M2M modülleri sayesinde nihai tüketicilere ait veriler dahi izlenebilir hale gelebilmiştir. M2M uygulamalar, geçmişten bu yana otomasyon altyapısı kullanan ve şebekeleri sağlıklı yönetebilmek için buna ihtiyaç duyan elektrik, su, gaz gibi temel ve kritik altyapılar için önemli olmakla birlikte, artık eski hizmet sınırlarını aşarak, sağlık, ulaşım ve tüketici elektroniği gibi farklı alanlarda hizmet alanların memnuniyetini arttırabilmek için kullanıma başlamıştır.

M2M, çoğunlukla uygulama seviyesinde farklılaşan servisler olmakla birlikte, erişim ve bağlanabilirlik alanında, ETSI (European Telecommunications Standard Institute), 3GPP (The Institute of Electrical and Electronics Engineers), TIA (Telecommunications Industry Association), GSMA (GSM Association), OMA (Open Mobile Alliance) ve IEEE (Institute of Electrical and Electronics Engineers) gibi kuruluşlar bünyesindeki çeşitli erişim standartları grupları, M2M standardizasyonuyla ilgili çalışmalar yürütmektedir. Bu kuruluşlar, M2M için frekans girişiminden ağ katman mimarilerine kadar farklı alanlarda standardizasyon çalışmalarına başlanmış bulunmaktadır. Ayrıca farklı kuruluş ve topluluklar da konuyu farklı açılardan ele almaktadırlar. Örneğin, 3GPP ağırlıklı olarak sistem mimarisi odaklı bir standardizasyon yaklaşımını benimserken, ETSI'nin uygulama odaklı bir standardizasyona gittiği görülmektedir [4-5].

M2M uygulamalar için yeni standartların oluşturulmasına ihtiyaç olup olmadığı konusu çeşitli tartışmalara neden olmaktadır. Konu, bugünkü ticari haberleşme şebekelerinin insandan insana (H2H) iletişim orijinli olarak geliştirildiği ve bu yönüyle M2M'nin gereksinimleriyle örtüşmeyebilecek mimaride olduğu şekliyle ele alındığında, ayrı bir standardın oluşturulması gerektiği yönündeki tezler kuvvet kazanmaktadır. Şüphesiz ki M2M güvenlik gereksinimi yönüyle de H2M iletişimden farklılaşmaktadır. H2H iletişim için birinci öncelik iletişimin devamlılığını ve içeriğinin gizliliğini sağlamak iken, M2M'de içeriğin değiştirilmemesi, başka bir ifadeyle bütünlüğünün korunması ayrıca önem taşımaktadır.

III. M2M Pazarı ve Geleceği

ABI Research 2010 yılında, 2014 yılı içerisinde dünya genelinde 225 milyon cihazın hücresel ağlar üzerinden erişilebilir olacağı tahmininde bulunmuştur. M2M ticari pazarında verilen hizmetlere ilişkin bugünkü durum Tablo 1'de yer almaktadır.

TABLO 1
M2M TİCARİ PAZARINDA VERİLEN HİZMETLERE İLİŞKİN DURUM [3]

Bölge	Servis Sağlayıcı	Servise Başlama Yılı	Klasik Uygulama
Avrupa	Vodafone	2002	Lojistik
	Orange	2004	Araç Kontrol
Japonya	Docomo	2004	Ağ uygulamaları
A.B.D	Sprint, Verizon	2004	e-market
Çin	China Telecom	2007	Smart home
	China Mobile	2006	Taşımacılık
	China Unicom	2006	Deprem İzleme

Telekomünikasyon altyapı ürün tedarikçilerinden Ericsson, 2020 yılı için, endüstriyel sistemler, çevrimiçi ev araç gereçler, ulaşım sistemleri ve taşıtlar, akıllı sayaç ve okuyucular gibi farklı alanlardaki ürün ve sistemleri kapsayan ve M2M uygulaması ile birbirine veya bir merkeze bağlanan ürünlerin sayısının 50 milyarı bulacağını öngörmektedir [4]. Farklı ancak daha önemli bir tahminde, Tablo-2'de yer alan, küresel ölçekte veri altyapı ürünleri tedarikçilerinden olan Cisco Systems Inc'nin mobil veri trafiği tahminleridir[6]. Tablo 2'den görüleceği gibi küresel veri trafiğindeki artış oranının video uygulamalarından sonra M2M uygulamalarında olması beklenmektedir.

TABLO 2
2013-2016 YILLARI MOBİL VERİ TRAFİĞİ TAHMİNİ [6]

	2013	2014	2015	2016
Uygulama	(Terabayt/ Ay)			
Data	549559	864122	1349825	2165174
File sharing	154601	204617	261235	361559
Video	1545713	2917659	4882198	7615443
VoIP	12491	15485	22976	35792
Gaming	24388	40644	77568	118330
M2M	92150	172719	302279	508022

Telefon ve internet kullanımı gibi insanlar arası veya insandan makinelere doğru iletişimde, telekomünikasyon pazarı açısından en önemli kısıt, pazarın insan sayısıyla sınırlı olmasıdır. Örneğin 70 milyon nüfuslu bir ülkede tek bir telekomünikasyon operatörün için ulaşılabilecek en yüksek abone değerinin en fazla ülke nüfusu olan 70 milyon ile sınırlı kalması beklenir. Oysa bir kişinin doğrudan veya dolaylı olarak kullanabileceği akıllı cihaz sayısı her geçen gün artabileceğinden, araba, klima, elektrik sayacı vb. ürünler için ayrı ayrı iletişim pazarı oluşturulabilecektir. Oluşacak bu pazarın boyutları, hizmetin sunulabileceği insan sayısıyla değil her bir insanının hayatına girebilecek cihaz ve makine sayısıyla sınırlı olacaktır. Bu nedenle, ağırlık mobil operatörlerde olmakla birlikte telekomünikasyon operatörlerinin, sınırları sürekli genişleyebilecek bu pazarı sürekli büyütecek servis ve uygulamalarını ardı ardına sunmaya başlayacaklarını öngörmek zor olmayacaktır.

IV. TEKNİK DÜZENLEME BOYUTUYLA M2M

M2M uygulamalarının yoğun olarak kablosuz ağlar üzerinden ve özellikle ticari hücresel ağlar üzerinden kullanımının yaygınlaşacağı öngörülmektedir. Bu itibarla, M2M model ve uygulamalarının, ulaşılabilecek hacim de göz önünde bulundurulduğunda spektrum düzenlemelerini etkilemesi kaçınılmaz görülmektedir. Örneğin, sayaç, motorlu taşıt veya ev elektroniği türündeki ürünlerin üzerindeki M2M birimlerinin 10 ile 30 yıl aralığında ömrü olduğu düşünülürse,milyarlarca M2M aygıtının iletişim modüllerinin yenilenme maliyetinin çok yüksek olacağı ve dolayısıyla M2M aygıtlarında bulunan iletişim modüllerinin yenilenme ihtiyacı duyulmadan 10-30 yıllık süre zarfında çalışması gerekmektedir. Bu da hücresel mobil operatörlerinin şebekelerinde 2G teknolojisinin 2030 yılına kadar aktif kullanmasını durumunu ortaya çıkaracak ki düzenleyici kurumların mevcut kullanılan spektrum lisansının ötesinde 20 yıl sonrası için taahhütte bulunabilmeleri mümkün görülmediği gibi böyle bir taahhüttün ileride farklı sorunları da beraberinde getirmesi olasıdır [7].

Kaynak kullanımı boyutuyla, spektruma ilaveten numaralandırma veya adresleme konusu da önemli bir husus olarak ortaya çıkmaktadır. Zira M2M cihazlar, bir şebeke içinde çalışabilmek için adresleme, kimliklendirme ve tanımlama için bir veya birden fazla numaraya ihtiyaç duyabilecektir. Bu numaralar, E.164 formatında telefon numarası, E.212 IMSI numarası veya IPv4-IPv6 numaraları olabilecektir.

2G ve 3G hücresel mobil şebekeler üzerinden yapılan iletişim, mobil telefon numaralarının (MSISDN) kullanımını gerektirdiğinden, bu şebekeler üzerinden verilecek M2M uygulamaları, zaten kısıtlı olan numara kaynaklarının daha hızlı tükenmesine de sebebiyet verecektir. Telefon numaralarının tükenmesine yönelik olarak çözüm önerileri bulunmaktadır. . Bunlar [8]:

- Yeni telefon numara aralıklarının arttırılması
- M2M aygıtları için, E.164 standardına uygun numara yerine daha çok karakterden oluşan numaralandırma politikasını uygulamak
- M2M aygıtların aynı anda sistemde aktif olmadığı değerlendirildiğinde, birden çok M2M aygıta aynı telefon numarasının atanması
- E.164 standardına göre, hiçbir ülkeye atanmamış olan bir prefiksin tüm dünyada M2M aygıtları için tahsis edilmesi
- 4G teknolojisinin yaygınlaşması ile, Aygıtların telefon numara ihtiyaçlarının ortadan kaldırılması

Yukarıda yer alan önerilerin, beraberinde getireceği olumlu ve olumsuz etkilerle birlikte çokça tartışılmaya muhtaç olduğu görülmektedir.

V. M2M UYGULAMALARıNDA İLETİŞİM GÜVENLİĞİ

M2M kullanan sistemlerde güvenlik temel olarak, ağ katmanlarını içeren erişim seviyesindeki güvenlik ve uygulama seviyesindeki güvenlik olarak temel iki kategoriye ayrılabilir. Örneğin, birimler arası bağlantı için erişim teknolojisinin klasik telemetri sistemlerinin mi yoksa hücresel tabanlı GSM, GPRS, EDGE, UMTS sistemlerin mi kullandığı güvenlik açısından önemli farklar taşımaktadır. Hücresel şebekelerdeki 2N'den (2. Nesil) 3N'ye ve her ara kademe mobil teknoloji geçişlerde iletişim güvenliği ve şifreleme kapasitesi daha da artığı [9] görülmektedir.

M2M uygulamasının kritikliğine bağlı olarak, sistem altyapısında kullanılan işletim sistemi, uygulama yazılımı, donanım ve haberleşme protokolleri de hayati önen taşımaktadır. Örneğin, bölgesel veya ulusal ölçekte gaz, petrol, su iletim ve dağıtım şebekelerinde gerçek zamanlılık kriterinin güvenlik gereksinimleriyle birlikte sağlanması gerekecektir. Çoğu zaman gerçek zamanlı iletişim ve güvenlik şartlarını birlikte sağlamak mümkün olmayabilmektedir. Özellikle kritik uygulamalarda kullanılan, gerçek zamanlı hayati fonksiyonlar icra eden birçok sensör ağlarındaki ekipmanlar, yüksek kaynak tüketimi gerektiren güvenlik servislerinin ihtiyaçlarını karşılayamamaktadır [10].

ETSI ve 3GPP gibi standardizasyon kuruluşlarının çalışmaları olmakla birlikte M2M uygulamalarına yönelik bugün için net bir güvenlik standardı bulunmamaktadır. Aslında güvenlik ihtiyacının yönetilecek uygulamanın kritikliğine bağlı olması, bu konuda tek bir güvenlik

standardının oluşturulmasının da doğru olmayacağı sonucunu doğuracaktır.

İnternet iletişimde kullanılan SSL dahil her türlü güvenlik mekanizmalarını M2M haberleşmesi için de kullanmak mümkündür. Elbette ki uygulamanın hangi sıkılıkta güvenliğe sahip olacağı, yukarıda ifade edildiği gibi sahip olunan donanımsal kaynağa bağlıdır. Uygulama seviyesinde kullanılabilecek güvenlik özellikleri, uygulamanın doğasına ve geliştiricilerin yordamına bağlı olarak ciddi farklılıklar arz edebilir. Uygulamaya kıyasla ağ katmanlarını içeren bağlantı seviyesinde kullanılabilecek güvenlik mekanizmaları, kullanılan erişim tekniğine bağlı olarak daha standart bir yapıda olacaktır.

VI. M2M VE SİBER RİSKLER

Günümüzde en yaygın M2M uygulaması 'uzaktan sayaç okuma' projeleri olarak karşımıza çıkmaktadır. Literatürde [11-12] de M2M uygulamalarına ilişkin siber tehditler daha çok bu alan üzerinde tartışılmaktadır. Örneğin elektrik sayaçlarının uzaktan takibi uygulamalarında, dışarıdan yapılabilecek yetkisiz müdahalelerle akan verinin bütünlüğünün bozulması neden olabilecektir [11]. Bu tür durumlar da anlık güç tüketimlerinin yanlış hesaplanması ve yönetilmesi de dahil olmak üzere birçok probleme sebebiyet verebilecektir

M2M uygulamalarına ilişkin en önemli siber tehdit, sisteme veya haberleşme ortamlarına yapılacak yetkisiz erişimler olarak görülmektedir. Tipik internet ve intranet uygulamalarında güvenlik önceliklendirmesi çoğu durumda gizlilik, bütünlük ve erişilebilirlik şeklinde sıralanırken, uzaktan sayaç okuma gibi M2M uygulamalarda erişilebilirlik, bütünlük ve gizlilik şeklinde önceliklendirilecektir [12]. Diğer yandan uzaktan bir komut icra eden ve hatalı komut işlenmesi durumunda can ve mal güvenliğini riske atacak uygulamalarda yetkisiz erişimlere karşı 'bütünlük kontrolü' birinci sırayı alacak, erişilebilirlik ve gizlilik ikinci derece önemli sayılabilecektir.

Genel olarak M2M sistemlere yönelik saldırılar aktif ve pasif saldırılar olarak sınıflandırılabilirler. Pasif saldırılar, M2M sistemlerinin çalışmasına zarar vermeyen ancak bilginin kopyasının iletişim kanalından çalınmasına imkan veren saldırılardır. İletişimi kesmemesi ve açıktan bir zarar vermemesi nedeniyle pasif saldırıları tespit etmek çoğu durumda güçtür. Aktif saldırılar ise, bir veri veya komutu değiştirmek suretiyle sistemi bozmaya, işlevini doğru olarak icra edemez hale getirmeye yönelik saldırılardır. Aktif saldırılar ayrıca, iç ve dış saldırılar olarak da ikiye ayrılırlar. Genelde dış saldırılar belirli ve dar alanda zarar verirken, iç saldırılar daha yıkıcı olabilmektedir. Genel güvenlik yaklaşımı, dış kaynaklı saldırılara karşı tedbir almak yönündedir. Ancak bir dış saldırı neticesinde başka sistem bileşenlerine erişebilen bir iç bileşenin ele geçirilmesi, dış kaynaklı başlayan saldırının iç kaynaklı olarak devam etmesine ve böylece tahribatını arttırmasına neden olabilecektir [1]. Bu sebeple, M2M sistem tasarımı ve güvenlik yaklaşımlarında, sadece içeriyi dışarıdan değil, içeriyi içeriden koruyacak erişim kısıtlamalarının da etkin hale getirilmesine ihtiyaç duyulacaktır.

M2M uygulamalarına hazır olarak tasarlanan ve üretilen ürünlerin üzerine gömülü gelen SIM kart ve modülleri birkaç açıdan diğer bağlantı türlerinde daha avantajlı bulunmaktadır. Zira bu tür ürünler herhangi bir yapılandırma ve ilave bağlantı işlemi gerektirmeden hazır M2M bulutuna dahil olabilmektedir. İkinci önemli avantaj ise hücresel şebekelerin mobil iletişim için tasarlanmış olup mobil ürünler üzerinden kullanılabilecek yegane servis durumundan olmalarıdır. Ancak gömülü SIM kart kullanımı ve bunların uluslararası bir alandan yönetilebilir olması ülkelerin kendi hakimiyet alanlarındaki fiziki varlıkların siber güvenliğini riskli duruma getirecektir. Önümüzdeki yıllarda üzerinde gömülü SIM kart bulunduran klima, buzdolabı, fırınlı ocak, televizyon ve motorlu taşıtlar gibi ürünlerin sayısının çok daha artacağı beklemektedir. Bu ve benzer ürünlerin her ne kadar müşteri lehine veri toplama gibi amaçları olsa da, sistemin kötü niyetli kişi veya grupların kontrolüne geçmesi gibi riskler herhangi bir sorunun yaşanması durumunda insan hayatına dahi mal olabilecek katastrofik etkilerinin ortaya çıkabilmesine neden olabilecektir. Daha ötesinde, global M2M uygulamalarının ülkeler arası ortaya çıkabilecek siber savaşların umulmadık silahları olarak kullanılmaları uzak bir ihtimal olarak varsayılsa bile teknik açıdan yararlanılabilecek imkanlar arasındadır. Tüm bunların uzağında, iyi niyetli sistem güncelleme veya uzaktan arıza onarımı gibi, kullanıcının bilgisi dışından yapılabilecek çalışmaların ne tür sorunlarla sonuçlanabileceğini önceden kestirmek de mümkün olmayacaktır. Bu bağlamda sadece siber korsanların yetkisiz erişimleri değil, uluslararası ölçekte yönetilen ve kritik sistem ve cihazları kumanda edebilen M2M uygulamaları da siber riskler olarak değerlendirilebilir.

M2M uygulamaları için gömülü modül veya kart kullanımı ve bunların öntanımlı şifreleme anahtarı veya önyüklü sertifikalar kullanmaları, bu yetkilendirme mekanizmalarının da erişim sağlayıcı, servis sağlayıcı veya erişmesi gerekiyorsa kullanıcı tarafından değiştirilememesi sonucunu doğuracaktır ki bu da yetkilendirme mekanizmalarının kırılganlaşmasına sebebiyet verecektir. Bu yönüyle M2M yetkilendirmesinin ihtiyaç duyulduğunda şifre ve/veya sertifikaları değiştirilebilir güvenlik mekanizmalarına dayanmasının uygun olacağı değerlendirilmektedir.

VII. SONUÇ VE ÖNERİLER

Endüstriyel otomasyon uygulamaları, belirli bir yapı içerisindeki altyapı bileşenlerinin icra ettikleri görevlere ilişkin konum, hız, basınç, sıcaklık, ağırlık, çeşitli elektriksel değerler başta olmak üzere farklı verileri uzak birimlerden okuyan, toplayan ve hesaplamak suretiyle merkezden komutlar üreten sistemlerdir. Bu yönüyle, bugün M2M olarak isimlendirilen uygulamalar geçmişte ağırlıklı olarak dağıtık yapılı endüstriyel otomasyon sistemlerinde kullanılmaktaydı. Bugün ise, uzaktan izleme ve kumanda etme ihtiyacının birçok farklı iş süreçlerinin vazgeçilmez parçası haline geldiği görülmektedir. İnternet ağlarının ve mobil şebekelerin yaygınlaşması ve elde edilebilirlik maliyetlerinin düşmesiyle birlikte de uzaktan erişim ve yönetim ihtiyacı kolay ve ucuz olarak karşılanabilir hale gelmiştir. Ortaya çıkan ihtiyaç ve imkanlardaki bu genişlemeyle birlikte, endüstriyel tesis ve

altyapılar gibi daha dar bir alana işaret eden 'otomasyon' ifadesi yerine sağlık, ulaşım, güvenlik ve hatta ev içi uygulamaları da kapsayan M2M ifadesi son birkaç yılda daha sık kullanılmaya başlanmıştır.

M2M uygulamalar, esasında İnsandan İnsana (H2H) veya İnsandan Makineye (H2M) iletişim için geliştirilmiş mobil telekomünikasyon şebekeleri üzerinden çalıştırılacağından, makinelere yönelik saldırıla karşı kalıtsal bazı açıklıklar içerecektir. Bu nedenle, M2M standardizasyon çalışmalarında gizlilik, bütünlük ve sürekli erişilebilirliği her şartta mümkün kılacak yöntemlerin geliştirilmesi veya var olan şebekelere adapte edilmesine ihtiyaç duyulacaktır.

Klasik otomasyon sistemlerinde haberleşme altyapısı olarak bugünkü yaygın uygulamalarının aksine, özel oluşturulmuş telemetri sistemleri kullanılmaktaydı. Bugünün iş dünyasının farklı ihtiyaçlarına bağlı olarak ise, 'esnek bağlanabilirlik' önemli bir değer ve aynı zamanda güvenlik tehdidi olarak ortaya çıkmaktadır. Örneğin, dünya çapında aynı ürünü satan ve ürüne ait çeşitli verileri müşteri memnuniyeti ve takibi gibi amaçlarla tek merkezden yönetmek isteyen uluslararası şirketler, mobil hücresel şebekeler arasındaki uluslararası dolaşımı kullanarak bu amaçlarına belirli bir maliyet karşılığında kolaylıkla ulaşabilecektir.

Doğrudan internet vasıtasıyla veya hücresel şebekeler üzerinden yapılabilecek ulusal veya uluslararası veri dolaşımıyla M2M uygulamaları, teknik imkanlar açısından sınırsız ticari uygunluk ve maliyetler açısından sınırlı hale gelmiştir. Makineler arası veri aktarım ihtiyacının nispeten kısıtlı olduğu göz önünde bulundurulursa, veri aktarımdan kaynaklı maliyetlerin doğrudan internet şebekesine bağlı sistemler için sıfıra yakın, hücresel şebekelere bağlı sistemler içinse sıfırın biraz üzerinde olabileceği söylenebilir. Bu nedenle M2M uygulamaların sadece belirli bölge veya ülkeler kapsamında değil uluslararası dolaşımlar marifetiyle dünya çapında uygulamalar hale gelmesi de beklenmektedir. Uluslararası dolaşımlar üzerinden yönetilen kritik M2M uygulamalar, siber savaş veya siber korsanlık gibi vakaların ortaya çıkması durumunda ilk hedef alınabilecek uygulamalar arasında olabilecektir. Bu yönüyle, elektrik, su, gaz gibi kritik altyapılara izleme ve yönetim sistemlerinin; motorlu taşıt, fırınlı ocak gibi tüketicilerin can ve mal emniyetini doğrudan ilgilendirebilecek ürünlerin uluslararası dolaşım ile başkaca bir ülke sınırları içerisinde yönetilmemesinin yaşamsal önem sahip olduğu değerlendirilmektedir.

Ülkelerin ithal ettikleri ve üzerinde gömülü olarak gelen SIM kart veya uydu haberleşme modülleri taşıyan ürünlere yönelik, gümrük süreçleri de dahil olmak üzere ilave inceleme süreçleri geliştirmeleri bir zorunluluk olarak ortaya çıkmıştır. Nitekim, dünya çapındaki büyük otomobil, sayaç, beyaz eşya ve elektronik üreticileri, ürünleri üzerine gömülü olarak kendi ülkelerine ait bir mobil operatörün SIM kartlarını yerleştirme yoluna gidebilecektir. Bu durumda, bu ürünleri ithal eden ve pazar konumunda bulunan diğer ülkeler, kontrolü başka bir ülkeden yapılan ürünleri satın almış durumuna düşeceklerdir. Bu itibarla, uluslararası tedarikçilerinin marka itibarlarını zedelememek adına her türlü tedbiri alacağı ve uzaktan izleme, veri toplama ve yönetme fonksiyonlarını hiçbir sorun oluşmaksızın tüketicilerin lehine kullanacağı varsayımının tartışmaya açılmasının faydalı olacağı değerlendirilmektedir.

M2M uygulamalarını diğer veri aktarım ve iletim servislerinden farklı hale getiren yanı da, tarafların çokluğu ve sorumluluğun tanımlanması meselesidir. Örneğin tipik uzaktan sayaç okuma örneği ele alınırsa, taraflar şu şekilde sıralanabilir: M2M modül üreticisi, şebeke operatörü, servis sağlayıcı, abone ve kullanıcılar. Burada uygunsuz bir kullanım veya yönetimden zarar görebilecek birden fazla taraf olabilecek ve sorumluluğun tespiti veya üstlenilmesi meselesini problemli hale gelebilecektir.

M2M uygulamalar ile birçok şirket tüketicilere ait bir takım özel sayılabilecek verileri anlık veya gecikmeli olarak toplayabilecektir. Örneğin, akıllı elektrik sayaçları üzerinden tüketicinin ne zamanlar evinde olduğu, hangi gün ve saatlerde yoğun tüketim olduğu hatta evinde hangi tür elektrik makineyi ne zaman kullandığı gibi kişisel sayılabilecek verileri görme imkanı olacaktır. Bir motorlu taşıt uygulamasında kullanıcıların güzergah konum verileri öğrenilebilecektir. Bu nedenle, kişisel verilerin korunması yönündeki mevzuat çalışmalarına M2M uygulamalarından elde edilecek verilerin saklanması ve işlenmesi hususları da dahil edilmelidir.

Ticari mobil şebekeler üzerinden sunulacak M2M uygulamalarında kullanılacak cihaz sayısının çeşitli kaynaklarda öngörüldüğü gibi dünya çapında milyarlar mertebesine ulaşmasıyla birlikte, hem spektrum kullanımı hem de adresleme uzaylarındaki yetersizlik yönüyle yeni problemlerin ortaya çıkması muhtemel görülmektedir. Bu nedenle, ulusal ve uluslararası düzenleyicilerin spektrum kullanımı ve hangi adres uzayının (telefon, IP numaraları vb.) ne şekilde kullanılabileceği yönünde yeni düzenlemelere gitmeleri gerekebilecektir.

M2M uygulamaları, hem barındırdığı terminal sayısı ve coğrafi dağınıklı göz önünde alındığında, genel ve hatalı bir güvenlik yaklaşımı olan içerideki bileşenleri sadece dış ağlardan koruma yerine, içerideki bileşenlerin de en az dışarıdakiler kadar tahripkar olabileceği varsayımıyla yetkilendirme kısıtları uygulanmalıdır.

Sonuç olarak, M2M uygulamalar, adresleme ve numaralandırma, frekans gibi kıt kaynak kullanımı, ulusal veya uluslararası dolaşım, yetkilendirme ve kullanıcı mahremiyeti konularında henüz çözüm bekleyen soruları beraberinde getirmiştir. Bu sorunlara karşı önerilen çözüm önerilerinin henüz tartışılma safhasında olduğu görülmektedir. M2M uygulamalar, bugün ulaştığı kullanım hacmi ve ivme dikkate alındığında, ülkelerin siber güvenliğini ve kritik tesislerde kullanımlarıyla birlikte halkın can ve mal güvenliğini, ülke ekonomilerini doğrudan etkileyebilecek uygulamalardır.

KAYNAKLAR

[1] R. Lu, X. Li, X. Liang, X. Shen, X. Lin "GRS: The Green, Reliability, And Security Of Emerging Machine To Machine Communications", Communications Magazine IEEE, Vol. 49 Issue:4 On page(s): 28 - 35, ISSN: 0163-6804, April 2011

[2] "Machine to Machine Communication", ETSI, February 2011, Available:http://www.etsi.org/WebSite/document/EVENTS/ETSI%20M2M%20Presentation%20during%20MWC%202011.pdf

[3] M. Chen, J. Wan, F. Li,"Machine-to-Machine Communications: Architectures, Standards and Applications",KSII Transactions On Internet and Information Systems Vol. 6, NO. 2, Feb 2012

[4] V. Galetić, I. Bojić, M. Kušek, G. Ježić, S. Dešić, D. Huljenić, "Basic principles of Machine-to-Machine communication and its impact on telecommunications industry", MIPRO, 2011 Proceedings of the 34th International Convention, On page(s): 380 - 385,ISBN: 978-1-4577-0996-8, Opatija, Issue Date: 23-27 May 2011
[5] K. C. Soong, A. Tseng, M. Z. Xiang "Global Wireless Machine-to-Machine Standardization", Internet Computing, IEEE, Volume: 15 Issue: 2, On page(s): 64 - 69, ISSN: 1089-7801, Issue Date: March-April 2011
[6] Cisco Visual Networking Index: Global Mobile Data Traffic Forecast Update, 2011–2016, Available:http://www.cisco.com/en/US/solutions/collateral/ns341/ns525/ns537/ns705/ns827/white_paper_c11-520862.html
[7] "Machine-To-Machine Communicatıons: Connectıng Billions Of Devices", Working Party on Communication Infrastructures and Services Policy, OECD Report, 30-Jan-2012
[8] D. Boswarthick, O. Hersent, O. Elloumi, "M2M Communications:A Systems Approach", John Wiley & Sons, ISBN: 9781119994756, 15 MAR 2012
[9] J. Quirke, "Security in the GSM system", 1st May 2004, Available:http://www.it.iitb.ac.in/~kavita/GSM_Security_Papers/Security%20in%20the%20GSM%20system%2001052004.pdf
[10] J.A. Stankovic,T.E.Abdelzaher,C. Lu, L. Sha,J.C. Hou "Real-time communication and coordination in embedded sensor networks", Proceedings of the IEEE,Volume: 91 Issue: 7 On page(s): 1002 - 1022, ISSN: 0018-9219, July 2003
[11] T. Baumeister, "Literature Review on Smart Grid Cyber Security", December 2010, Available:http://csdl.ics.hawaii.edu/techreports/10-11/10-11.pdf
[12] J. Liu, Y. Xiao, S. Li, W. Liang, C. L. P. Chen, "Cyber Security and Privacy Issues in Smart Grids", Communications Surveys & Tutorials, IEEE, Volume: PP Issue:99 On page(s): 1 - 17 ISSN: 1553-877X, Ocak 2012

A. ÖZBİLEN
1980 Antakya doğumludur. Gazi Üniversitesi Elektrik-Elektronik Mühendisliğinde lisans ve yüksek lisans eğitimini tamamladı ve doktora öğrenimine devam etmektedir. Türk Telekom A.Ş Ankara Bilişim Ağları Müdürlüğü ve Türk Telekom A.Ş Genel Müdürlüğü Uluslararası İlişkiler Dairesi Başkanlığında Telekom Uzman Yardımcısı unvanıyla görevler aldı, halen Bilgi Teknolojiler ve İletişim Kurumu'nda uzman olarak görevini sürdürmektedir. "Denetim Sistemleri ve Kritik Altyapı Güvenliği" üzerine akademik çalışmalarına devam eden yazarın bu konular üzerine çeşitli dergilerde yayınlanmış makaleleri ve konferans bildirileri bulunmaktadır.

Güvenli Q Sürü Bellek Yazılım Yongası Üreten Dilbilim Örneği

Prof. Dr. Fevzi Ünlü
Ege Üniversitesi ve Yaşar Üniversitesi
Bilgisayar Bilimleri ve Uygulamalı Matematik Emekli Öğretim Üyesi
Bornova, İzmir

Abstract—In this paper a TASIM genetic, RCR formatted, secure I@I ∈ I@I$^+$ producing Q ∈ Q$^+$ swarm memory software chip generating formal grammar model is introduced. This formal grammar model is generating all Q swarm memory models which have n different communication channels controllable only 1 control variable.

***Özet**—Bu bildiride TASIM genetik, RCR formatlı, güvenli I@I ∈ I@I$^+$ sürü internet sürüsünü üreten Q ∈ Q$^+$ sürü bellek sürüsü yazılım yongalarını oluşturan bir biçimsel dilbilim örneği tanıtılacaktır. Bu biçimsel dilbilim modeli sadece 1 denetim değişkeni ile denetlenebilir n bildirişim kanalına sahip her Q sürü bellek modelini üretebilmektedir.*

***Anahtar Sözcükler**-BTN, tamra, ramta, anten, bellek, rator, cab, rand, RCR formatlı Q$^+$, RCR formatlı biçimsel dil ve dilbilim, Bildirişimli Matematik.*

I. GİRİŞ

Yazar 1972 yılından günümüze kadar; güvenli, uzaktan programlanabilir, TASIM[1] genetik, genişletilebilen ve büzülebilen yazılım yongası[2] bellek yapıları üzerinde çalışılmaktadır. 1976 yılında, sadece 3 yapıbilim[3] kuralından oluşan TASIM biçimsel dili üretildi ve yayınlandı. Kaynak[1]. Amaç bu dili kullanarak bildirişim[4] yapan yazılımsal bellek yapılarını üretmek, programlamak ve optimize[5] ederek kullanmaktı. Önce, K = Kip[2] = {0, 1} kümesi üzerinde 2-değerli mantığı T: TASIM dilinde üretilen yazılım yongalarına programlayan teknik gerçekleştirildi. Kaynak[2, 3]. Sonra N doğal sayılar kümesinden alınan her n değeri için, n ≥ 1 ve n ∈ N olmak üzere, K = Kip[n] = {0, 1, 2, ... n-1} kümesi üzerinde tanımlanan n-değerli mantık tasarımı TASIM ve TASIM genetik olan biçimsel dillerde çalışıldı. Kaynak[4-6]. Güvenli BTN[6] kavramı algılandı. Yalın BTN oluşumlarından tümleşik olarak optimize edilmiş BTN oluşumları üretme yolları arandı, bulundu, tanımlandı ve CITALOG[7] adı altında yayınlandı. Kaynak[7]. Doğada, yaşama şansını yakalayan her canlının bir güvenli bilgi olduğu düşünüldü. Sanal kanser oluşumu bir biçimsel kavram olarak ele alındı. Kaynak[8]. Doğanın istenildiğinde istenilen güvenli bilgiyi üretme gücüne sahip olduğu algılandı. Güvenli bilgi üretme ve saklama yolları arandı, belli kısıtlarlar içinde bulundu ve yayınlandı. Kaynak[9-20]. Güvenli bilgi kavramının anlatımını çok kolaylaştıracak olan Bildirişimli Matematik bilim dalı kuruldu. Kaynak[12, 22]. Güvenli I@I sürü internet üreten güvenli Q sürü bellek yapılarının tasarımı ve onları uzaktan programlama yöntemleri çalışıldı, bulunarak yayınlandı. Kaynak[20-22]. Bu gün gelişigüzel seçilen her K = Kip[n] = { 0, 1, 2, ... n-1} kümesi üzerinde; n, m ≥ 1 ve n, m ∈ N olacak biçimde seçilen; m değişkenli, n mantık değerli, ü[m, n] sayıda, biçimsel mantık fonksiyonunun tasarımının yapılarak; TASIM dilinde üretimi yapılmış olan güvenli Q sürü bellek yazılım yongalarına programlanması, hemen anında mümkün olmaktadır. Yazar, inanılması zor olanı başarmıştır. Bu gerçekten bilim adına bir evrimdir. Bir Türk bilim adamı tarafından, yaşam boyu özverili çalışma karşılığında gerçekleştirilmiştir. Öz ve yoğun olarak Kaynak [23-24] içeriğinde yayınlanmıştır. Yapılan yayınların içeriği, Bilgisayar Bilimcileri tarafından çok iyi bilinen LISP dilinin çekirdek dilbilimine, n-değerli mantık kavramına ve özdevinim teorisine; bilgi genetiğini biçimsel olarak analiz ve sentezleyebilen dilbilim anlamında bağımlıdır. Yani oldukça güçlü bir alt yapıya sahiptir. Kaynak[25, 26, 27].

Biçimsel olarak, sözü yerinde söylemek gerekirse, her n-değerli Kip[n] mantığının iyi algılandığı; güvenli bilgi çağının kapısı, I@I sürü internet üreten Q sürü bellekleri ile ustaca açılmıştır. Kaynak[23, 24]. Araştırmacılar, araştırırken; gözlemlerinde karşısına çıkan, her kapalı veya açık çevre ortamında oluşmuş çok farklı özelliklere sahip tik BTN oluşumlarını artık güvenli bilgi yapısı olarak algılamalıdır. Çünkü düşünsel olarak, evrenin kendisi bir güvenli tik BTN oluşumudur. Tik alt BTN oluşumları arasında açık veya kapalı biçimde bildirişim kurmayı gerçekleştiren; tıpkı "Yer Çekimi

[1] *TASIM: Tidy Automatic Sequential Information Processing Mechanism.*
[2] *Yonga: Chip.*
[3] *Yapıbilim: Syntax.*
[4] *Bildirişim: Çok katmanlı, çok yönlü, ıtkaz ve yoğun biçimde yapılan biçimsel iletişim.*
[5] *Optimize: Amaca en uygun biçimde minimize veya makimize edilmiş.*
[6] *BTN: Bilgi Tabanlı Nesne. KBO.*
[7] *CITALOG: Compact and Integrated TASIM Logic. Bu çalışma yazarın zorla kendi ülkesinde işsiz bırakıldığı ve bu nedenle yurt dışında çalışmak zorunda kaldığı zor yılların ürünüdür.*

Yasası" gibi bir "Bildirişime Çekim Yasası" vardır. Onu anlayıp anlatmak için çaba gösterilmelidir.

Yazar sadece evrenin güvenli olan kesiminde yaşanabildiğini düşünerek, güvenli BTN kavramını çok geniş anlamda düşünmüştür. Bunun için gözlenebilir veya algılanabilir bildirişim çözünürlüğüne sahip olan, sayılabilir çokluktaki TASIM genetik tik BTN öbeklerini matematik nesnesi olarak ele almıştır. TASIM tarafından üretilen her Q sürü bellek yongasını, bir tik BTN gibi algılamıştır. Onu *tamra, ramta, anten, bellek, rator, cab, rand, RCR formatlı Q, RCR formatlı biçimsel dil ve dilbilim* kavramları aracılığında anlatmıştır. Kaynak[23, 24]. Tik BTN öbeklerini değişen ve değişmeyen kesimlerine ayırarak; sayılabilir BTN değişenlerini, sayılabilir BTN değişmezleri ile ifade etmiştir. Her yaşam katmanında, biçimselliğini değiştiren akıllı BTN yaşamı; güvenli değişim kavramını algılayarak, giydirilen farklı güvenlikli giysisi ile koruma altına alınmak istenmiştir. Bu gün güvenlik giysisi giymiş her biçimsel BTN yaşamı, bir I@I sürü internet modeli biçiminde doğayı veya daha geniş anlamda evreni biçimsel olarak iyi anlamak için zaman tünelinde evrensel zamanın ne olduğunu biçimsel olarak tanımlayabilmek için kendi amacı doğrultusunda ilerliyor.

Biçimsel bildirişimde kullanılan, her BTN oluşumunun bir Kip[n] biçimsel mantık öbeği kuralları altında oluşmuş BTN yazılım yongası olduğu algılanmıştır. Güvenli bildirişimde, biçimsel Kip[n] mantığının programlanacağı TASIM genetik BTN oluşumların kullanılmasının kaçınılmaz olduğu idrak edilmiştir. Ön görülen amaca erişme yolunda, çok katmanlı, derin ve tıkız biçimde gündeme getirilen; tümleşik olarak gözlenebilir veya gözlenemez tik BTN sürü bellek oluşumlarının, bildirişim yapan değişik küme-biçimli oluşumlarının yeni sürümleri; kavramsal olarak, yaşamın algılanan evrensel gündemine yenidenlikli[8] olarak taşınmıştır.

Bir TASIM genetik biçimsel dilbilimin, bir TASIM genetik biçimsel dilinde oluşturduğu; yenidenlikli, biçimsel sürü bellek oluşumlarını iyi algılayıp; "Bildirişime Çekim Yasası" kuralları eşliğinde güvenli olarak modelleyen yeni teknikler bulunmuştur. Daha farklı olanları bulunabilir. Bu yazıda, bilgi işleme sürecinde bildirişimi güvenli anten ve anten sinyalleri ile gerçekleştiren, bilgi işlerken biçimsel ham bilgi kodunu değişik tik BTN yazılım belleklerinde saklayabilen ve gerektiğinde kullanıma açabilen, yazılım biçiminde oluşturulan Q sürü bellek yapılarının oldukça kolay olan tasarımı bir dilbilim desteğinde yapılmıştır. Farklı olanları yapılabilir görülmektedir. Q sürü bellek yapılarını, istediğimiz amaç doğrultusunda anında üretip, programlayıp ve kullanıma sunma doğrultusunda biçimsel I@I sürü bellek oluşumlarını gerçekleştiren BTN oluşumları uzun bir süre için gündemde olacaktır.

Bunun için, Q sürü bellek modelleme süreçlerinin tasarımını ve anlatımını kolaylaştıracak; çok katmanlı olarak, değişik durumlara duyarlı; öğrenilmesi, öğretilmesi ve kullanılması kolay; dil ve dilbilim alt yapısına ihtiyaç vardır. Bu bildiri, bunun için; teorik anlamda, güvenli bildirişim yapan, TASIM genetik, 1 değişkenli yazılım olarak gündemde olan Q sürü bellek üretimini bir algoritma aracılığında gerçekleştirilen; $\underline{L} = \underline{L}[\underline{G}]$ biçimsel dilini ve onu üreten $\underline{G}$ dilbiliminin alt yapılarını ve özelliklerini; biçimsel olarak anlatacaktır.

Anlatımda, Kaynak[1-27] içeriğinde geliştirilen alt BTN bilgi yapıları ve bu alt yapıların anlatımını çok kısaltan, biçimsel bildirişim kavramları biliniyor varsayılacaktır.

II. Kip[n], n ∈ N

Eğer $K_n = \{0, 1, 2, \ldots (n-1)\}$, $n \in N$, rakamlardan oluşan bir biçimsel dil alfabesi ise ve aşağıda ortaya konulan Tanım 1 içeriğinde verilen belitleri[9] sağlıyorsa bu K_n 'ye bir $K = K[n] = Kip[n]$, $n \in N$, denir.

Tanım 1: Aşağıda verilen belitleri sağlayan bir boş olmayan K_n kümesi vardır. Rakamlar kümesi diye adlandırılır. Belitler:

B0: $0 \in K_n$;

B1: Bir en küçük $k = \underline{0}$ elamanı vardır öyle ki bu elaman için $\underline{0} = 0$ geçerlidir.

B2: Her $k \in K_n$ için bir tek $k^* \in K$ vardır. Bu $k^* \in K$ elemanına k elemanının ardılı denir.

B3: Dokuz diye adlandırılan bir en büyük $k = \underline{k}$ elamanı vardır öyle ki bu elaman için $\underline{k}^* = 0$ geçerlidir.

B4: Eğer K_n kümesinin gelişi güzel seçilmiş bir S alt kümesi varsa ve onun için:

(i) $0 \in S$;

(ii) $k \in S$ olduğunda $k^* \in S$ oluyorsa;

O zaman $S = K_n$ olur.

Tanım 2: Tanım 1 içeriğinde verilen belitleri gerçekleyen her K_n kümesine bir Kip[n] rakamları alfabesi denir. Elamanları K_n kümesinin elamanları ile bire-bir eşlenebilen her semboller kümesine bir K_n kümesine denk ve K_n rakamları ile sayılabilen KRA[n] alfabesi denir.

Sonuç 1: $KRA[\|<alfabe>\| = n] \equiv Kip[n] = Mod[n]$, $n \in N$.

Örnek: (a) $KRA[\|<\{a, b, c\}\| = 3] = \{a, b, c: a < b < c\} = \{<a, 0>, <b, 1>, <c, 2>\} \equiv Kip[3] = Mod[3]$ gerektirir $a \equiv 0$, $b \equiv 1$ ve $c \equiv 2$. Bu $KRA[3] = \{a, b, c\}$ alfabesinden üretilen bir biçimsel dilde $bbac_3 \equiv 1102_3$ olarak algılanır.

Kural: KRA[n] alfabelerinin harfleri farklı görüntüye sahip olabilir ama her harfin Kip[n] içinde denk olduğu ancak bir rakam vardır.

Tanım 3: (a) Her sonlu sayıda terminal im[10] kümesine bir **terminal alfabe** denir. Bu bildiride $\underline{A}$ ile temsil edilecektir.

(b) Her sonlu sayıda terminal olmayan im kümesine bir **terminal olmayan alfabe** denir. Bu bildiride $\underline{B}$ ile temsil edilecektir.

[8] *Yenidenlikli: Recursive.*

[9] *Belit: Aksiyom.*

[10] *İm: Rakam, harf, sembol veya karakter oluşumlarına verilen genel ad.*

Tanım 4: (a) Her tik giysili im bir **tik im** olarak adlandırılır. Bu nedenle tik im onu oluşturan alt parçalarına ayrılamaz. Her terminal im bir tik imdir.

(b) Her tik giysisiz im bir **tok im** olarak adlandırılır. Tok im onu oluşturan alt parçalarına kolaylıkla ayrılabilir. Her terminal olmayan im bir tok imdir.

Tanım 5: Yatay doğrultuya benzer bir doğrultuda görüntülenen imler dizisine bir **imdizi** denir. Hiç imi olmayan imdizi bir **boş imdizi** veya **hiçlik temsil eden imdizi** olarak adlandırılır. Hiçlik imdizi ε ile temsil edilir. Bir imdizinin ölçümü onu oluşturan im sayısı ile ölçülür. Bir imdizi içinde bulunan im sayısına o imdizinin uzunluğu denir. İmdizi uzunluğu ‖...‖ işleci ile ölçülür. **‖<imdizi>‖ = <imdizi>-uzunluğu olarak algılanır.**

Örnek: Eğer $\underline{A}$ = {a, b, c} ise "**baba**" $\underline{A}$ 'dan elde edilmiş bir imdizidir. Bu imdizinin uzunluğu **‖<baba>‖ = 4 olarak bulunur.**

Tanım 6: Bir imdizi, $\underline{A}$ 'nın **imlerinden, yenidenlikli olarak kullanılabilen, "." birleştirme[11] işleci kullanarak oluşturulur.**

Örnek: a.b.a = aba, <kara>.<deniz> = <kara deniz> = karadeniz, bir $\underline{A}$ = {a, b, d, **i, n,** z} **alfabesinden "." aracılığında elde edilmiş olan im dizilerdir.**

Tanım 7: (a) K_n = Kip[n] = {0,1, 2, ... (n-1)} kümesi, n farklı rakam içeren bir terminal alfabe olarak ele alındığında: ${}^{k}K_n$ kümesi bu alfabeden elde edilen k uzunluklu Kip[n] sayılarını ihtiva eder. Öyle ise:

(i) ${}^{k}\omega_n$ rakam dizisine, ${}^{k}K_n$ kümesinden alınan ve **k** uzunluğunda olan **n-ce doğal sayısı** denir.

(ii) ${}^{k}K_n$ kümesine K_n kümesinden elde edilen k uzunluğunda n-ce sayılarının kümesi denir. Bu ${}^{k}K_n = \{ {}^{k}\omega_n : \| {}^{k}\omega_n \| = k, k \in N\}$ kümesi aslında bir **k-uzunluklu n-ce doğal sayı** sürüsüdür. Elamanları, k ve n sayılabilir olduğunda sayılabilirdir.

(iii) Bir ${}^{k}K_n = \{ {}^{k}\omega_n : \| {}^{k}\omega_n \| = k, k \in N\}$ k-uzunluklu n-ce doğal sayı sürüsü verildiğinde aşağıdakiler geçerlidir:

0. ${}^{0}K_n = \{\varepsilon\}$. Bu kümede her sayı sıfır rakamdan oluşur.

1. ${}^{1}K_n = \{0_n, 1_n, 2_n, \dots, (n-1)_n\}$. Bu kümede her sayı 1 n-ce rakamından oluşur.

2. ${}^{2}K_n = \{00_n, 01_n, 02_n, \dots, 0(n-1)_n, 10_n, 1_n, 12_n, \dots, 1(n-1)_n, \dots, (n-1)0_n, (n-1)1_n, (n-1)2_n, \dots, (n-1)(n-1)_n\}$. Bu kümede her sayı 2 n-ce rakamından oluşur.

...

k. ${}^{k}K_n = \{00\dots00_n, 00\dots01_n, 00\dots02_n, \dots, 00\dots0(n-1)_n, 00\dots10_n, 00\dots11_n, 00\dots12_n, \dots, 00\dots1(n-1)_n, \dots, (n-1)(n-1)\dots(n-1)0_n, (n-1)(n-1)\dots(n-1)1_n, (n-1)(n-1)\dots(n-1)2_n, \dots, (n-1)(n-1)\dots(n-1)(n-1)_n\}$. Bu kümede her sayı k n-ce rakamından oluşur.

(iv) ${}^{k}K_n$ kümesi verildiğinde: (a) $K_n^{+} = \bigcup_{k=1}^{\infty} {}^{k}K_n$ kümesine K_n = Kip[n] kümesinin "+" küme kapanışı denir. Bu "+" küme kapanışı ε dışında bütün k ∈ N uzunluklu n-ce sayı sürüsünü ihtiva eder. Yani sonsuz sayıda n-ce sayısından oluşur. (b) $K_n^{*} = \bigcup_{k=0}^{\infty} {}^{k}K_n$ kümesine K_n = Kip[n] kümesinin "*" küme kapanışı denir. (c) $K^{+} = K^{*} \setminus \{\varepsilon\}$ olduğunu görünüz. Burada "\" küme farkı işlecini temsil etmektedir. (d) K_n^{*} kümesinin her alt kümesine bir **n-ce sayma dili** denir.

Teorem 1: Eğer $\underline{A} \equiv {}^{k}K_n = \{ {}^{k}\omega_n : \| {}^{k}\omega_n \| = k\}$ ise,

$$\#[\underline{A}] = \#[\{ {}^{k}\omega_n : \| {}^{k}\omega_n \| = k\}] = \ddot{u}[k, n] = 1 + (n-1)\sum_{r=0}^{k-1} n^{r}.$$

İspat: $\#[\underline{A}] = \#[\{\|00\dots0\|=k, \|00\dots1\|=k, \dots \|(n-1)(n-1)\dots(n-1)\| = k\}] = 1 + <(n-1)(n-1)\dots(n-1)>_n = \ddot{u}[k, n] = 1 + (n-1)\sum_{r=0}^{k-1} n^{r}$.

Örnek 1: $A \equiv {}^{4}K_2 = \{ {}^{4}\omega_2 : \| {}^{4}\omega_2 \| = 4\}$ olsun.

(a) $\#[A] = \#[\{ {}^{4}\omega_2 : \| {}^{4}\omega_2 \| = 4\}] = \#[\{0000_2, 0001_2, 0010_2, 0011_2, 0100_2, 0101_2, 01102, 0111_2, 1000_2, 1001_2, 1010_2, 1011_2, 1100_2, 1101_2, 1110_2, 1111_2\}] = 16$. Bu sonuç 2-ce sayma dilinde yapılan ileri doğru sayma yöntemi ile bulunmuştur.

(b) $\ddot{u}[4, 2] = 1 + (2-1)\sum_{r=0}^{4-1} 2^{r} = 1 + 1(2^{0} + 2^{1} + 2^{2} + 2^{3}) = 1 + 1 + 2 + 4 + 8 = 16$. Bu sonuç ü[4, 2] formülü kullanılarak bulunmuştur. Kaynak[23,24].

Örnek 2: $A \equiv {}^{3}K_4 = \{ {}^{3}\omega_4 : \| {}^{3}\omega_4 \| = 3\}$ olsun. (a) $\#[A] = \#[\{ {}^{3}\omega_4 : \| {}^{3}\omega_4 \| = 3\}] = \#[\{ 000_4, 001_4, 002_4, 003_4, 010_4, 011_4, 012_4, 013_4, 020_4, 021_4, 022_4, 023_4, 030_4, 031_4, 032_4, 033_4, 100_4, 101_4, 102_4, 103_4, 110_4, 111_4, 112_4, 113_4, 120^{4}, 121_4, 122_4, 123_4, 130_4, 131_4, 132_4, 133_4, 200_4, 201_4, 202_4, 203_4, 210_4, 211_4, 212_4, 213_4, 220_4, 221_4, 222_4, 223_4, 230_4, 231_4, 232_4, 233_4, 300_4, 301_4, 302_4, 303_4, 310_4, 311_4, 312_4, 313_4, 320_4, 321_4, 322_4, 323_4, 330_4, 331_4, 332_4, 333_4\}] = 64$. Bu sonuç 4-ce sayma dilinde yapılan ileri doğru sayma yöntemi ile bulunmuştur. (b) $\ddot{u}[3, 4] = 1 + (4-1)\sum_{r=0}^{3-1} 4^{r} = 64$. Bu sonuç ü[4, 2] formülü kullanılarak bulunmuştur.

Tanım 8: (i) $\underline{A}$ bir sayılabilir terminal imlerinin alfabesi, (ii) $\underline{B}$ bir sayılabilir terminal olmayan imlerin alfabesi, (iii) $\underline{KK}$ bir sayılabilir üretim kuralları kümesi ve (iv) $\underline{\Sigma}$ bir cümle veya sayı üretme kayıtsayarı olsun. Her $\underline{G} = <\underline{A}, \underline{B}, \underline{KK}, \underline{\Sigma}>$ sıralı dörtlüsüne bir **biçimsel BTN oluşturma dilbilim**[12] denir. **Çevremizde gözlediğimiz her oluşum, doğa tarafından böyle bir dilbilim ile bir dilde BTN olarak oluşturulmuş bir kelimedir. Doğayı doğru anlamak istiyorsak bu sözünü ettiğimiz $\underline{G}$ ve $\underline{L}$ adlı iki kavramı iyi anlamak zorundayız**

III. BTN

[11] *Birleştirme: Concatenation.*

[12] *Dilbilim: Gramer.*

Her BTN oluşumu bir biçimsel dilbilim ile korunan, bir imdizi oluşumudur. Bunu biçimsel olarak ortaya koymak için aşağıdaki tanımı yapacağız.

Tanım 9: (i) Her tik[13] terminal im veya tik resim bir biçimsel[14] bilgiyi temsil etsin. Böyle sayılabilir çokluktaki tik terminal imlerinin alfabesi A olsun. Belli kurallarla ondan seçilen bir alt alfabe de AA olsun. AA'nın tik öğeleri, belli bir amacı gerçekleştirmek için bir G dilbiliminin üretim kuralları altında bir imdizi olarak bir araya gelmiş olsunlar. Eğer bu imdizi uzaktan bildirişim yapabilen belli teknikleri kullanarak; bilgiyi algılayan, toplayan, değerlendiren, işleyen, kullanan, pazarlayan, alan, satan, depolayan, dönüştüren veya benzeri eylemleri biçimsel olarak yürütebilen; bir biçimsel imdizi sistemi olarak örgütlenebilmişlerse bu imdizi sistemine bir **BTN** denir. (ii) Genelde gelişi güzel seçilerek, bir nD uzayında görüntülenen her tik BTN, n farklı bileşenden oluşabilir. Biz bu bildiride **başlık, boyunluk, bedenlik, bacaklık ve kuyrukluk** adlı beş tik bileşenden oluşan BTN modelini çalışacağız. Her bileşenin giysisini şeffaf ve şeffaf olmayan biçimde bir iki durumlu maske giysisi olarak algılayıp kullanacağız.

(a) BB bir tik BTN olsun. Bu tik BB 'nin her bileşenine bir şeffaf giysi giydirilmiş olduğunu kabul edelim. Bu durumda, her BB BTN oluşumu bir 5B= bbbbb bileşen uzayında açık olarak, bir sütun veya satır vektörü kullanılarak aşağıda verildiği gibi temsil edilebilinir. Yani:

$BB = = < b\leftarrow b_0, b\leftarrow b_1, b\leftarrow b_2, b\leftarrow b_3, b\leftarrow b_4 >^T = <b_0\ b_1\ b_2\ b_3\ b_2 >^T = bbbbb^T = \begin{matrix} b \\ b \\ b \\ b \\ b \end{matrix}$ olur. Şimdi, Δ bir giysi maskesi vektörü olsun. $\Delta^T = < bGMF\leftarrow\delta_0, bGMF\leftarrow\delta_1, bGMF\leftarrow\delta_2, bGMF\leftarrow\delta_3, bGMF\leftarrow\delta_4 >^T = <\delta_0\ \delta_1\ \delta_2\ \delta_3\ \delta_4 >^T = \delta\delta\delta\delta\delta^T = \begin{matrix} \delta \\ \delta \\ \delta \\ \delta \\ \delta \end{matrix}$ olarak temsil edilebilinir.

Burada Δ tanımı içinde izlenen "GMF" bir kısaltılmış kelimedir. "Giysi maskesi formatı" anlamında kullanılmıştır. "←": Tik atama veya kayıtlama işlecidir.

Teorem 2: Bir giysi maskesi formatı, GMF kavramının iyi algılandığı her bilgi işlem ortamında, bir Δ giysi maskesi vektörü 5Bh[15], $h \in \{1, 2, 3, 4, 5\}$ GMF vardır.

İspat: Kabul edelim ki: (i) Δ bir 5B giysi-maskesi formatı vektörü olsun.

(ii) Eğer Δ içinde, i^{th} GMF bileşeni $\delta_i = 0$ olduğunda giydirildiği b_i = "-" oluyor ve bu bileşenini görülmez yapıyorsa ve yine i^{th} GMF $\delta_i = 1$ olduğunda giydirildiği b_i = "+" oluyor ve bu bileşeni görülür yapıyorsa, $\Delta =< \delta_0, \delta_1, \delta_2, \delta_3, \delta_4 > = \delta\delta\delta\delta\delta$, [5]K[2] genetiktir. Yani ü = ü[5, 2] = 1 + (2-1)($2^0 + 2^1 + 2^2 + 2^3 + 2^4$) = 1 + 1(1+2+4+8+16) = 1+ 31 = 32 GMF tasarımı yapılabilir. Çünkü $\delta_i \in \{0, 1\}$ gerektirir bbbbb ∈ GMF = {-----, ----+, ---+-, ---++, --+--, --+-+, --++-, --+++, -+---, -+--+, -+-+-, -+-++, -++--, -++-+, -+++-, -++++, +----, +---+, +--+-, +--++, +-+--, +-+-+, +-++-, +-+++, ++---, ++--+, ++-+-, ++-++, +++--, +++-+, ++++-, +++++} görüntü maskesi formatının kod kümesidir. ‖GMF‖ = 32 olduğunu sayarak görebiliriz.

Örnekler:

(i) Eğer δδδδδ= 00000 ise bbbbb = ----- olur ve tik BB BTN hiç görülmez.

(ii) δδδδδ=00110 ise bbbbb= --++- olur ve BB BTN oluşumu yalnız bedenlik ve bacaklık bileşeni ile görülür.

Teorem 3: Her yeni tasarımda δδδδδ = 00100 kodu 3D1[16] uzayında 5B1: Bedenlikli imdizi olan BB BTN üretir.

İspat: Her yeni BB BTN tasarımı bir biçimsel dilbilim aracılığında bir biçimsel dilde yapılır. Bu dilbilimin A alfabesinde yer alacak tik imler 00100 formatlı olacaklardır. Bu GMF altında sadece 1 bileşen görüntüleneceğinden biz sadece 5B1: Bedenlik bileşenli imdizileri 3D1 boyutunda dizilmiş olarak göreceğiz.

Örnek: Her satır bir 3D1 boyutlu uzaydır.

Teorem 4: Her yeni tasarımda δδδδδ = 00110 kodu 3D1 uzayında 5B2: Bacaklıklı ve bedenlikli imdizi BB BTN üretir.

İspat: Yeni tasarımlar bir biçimsel dilbilim aracılığında bir biçimsel dilde yapılır. Bu dilbilimin A alfabesinde yer alacak tik imler, 00110 giysi maske formatlı olacaklardır. Bu giysi maske formatı altında sadece 5B2 bileşen görüntüleneceğinden biz sadece o iki bileşenli imdizileri göreceğiz. Bu imdiziler, bacaklıklı ve bedenlikli olacaktır.

3.1 RCR Formatlı BTN Oluşumları

Bu kesimde F = <$F_0\leftarrow$Rator, $F_1\leftarrow$Cab, $F_2\leftarrow$Rand> = <Rator, Cab, Rand> = <R, C, R> = RCR formatlı BB BTN üreten bir dilbilim çalışılacaktır.

Tanım 10: (i) <t> = t 'ye başlangıç durumunda, BSK gibi görev yapmaya programlanmış iki durumlu bir tik **tamra** anteni denir.

(ii) <r> = r 'ye başlangıç durumunda, BAK gibi görev yapmaya programlanmış iki durumlu tik **ramta** anteni denir.

(iii) <t, r> = <tr> = tr 'ye her başlangıç durumunda, t tik tamra anteni BSK olarak ve r tik ramta anteni BAK olarak programlanmış iki tikli tik anten sistemi denir. Bundan sonraki her durum değişikliğinde tikler görevlerini değiştirirler. Bunun anlamı gelişigüzel seçilen bir durumda biri bilgi salarken diğeri o bilgiyi alır. Yani biri konuşurken diğeri onun konuşmasını kesmeden dinler. BSK, BAK, tamra ve ramta kavramları Kaynak[23, 24] içeriğinde verilmiştir.

(iv) $<t_0, t_1, t_2, \ldots, t_{(n-1)}> = < t_0\ t_1\ t_2 \ldots t_{(n-1)} > =$

[13] *Tik: Alt kesimlerine ayrılamayan bilgi dokusu.*
[14] *Biçimsel: Formal. Yapısı, anlamı, kullanımı %100 kesinlik derecesi ile algılanabilen, yorumlanabilen, kullanılabilen.*
[15] *5B: 5 Bileşenli. 5Bh: 5 Bileşenden h bileşeni görüntüleyen.*
[16] *D:Dimension. 3D1: 3 boyutlu uzayının yalnız bir boyutunu kullanan alt uzay.*

$t_0\ t_1\ t_2 \ldots\ t_{(n-1)}$ = ttt… t oluşumuna K_n **genetik n-li tamra anten sistemi** denir.

(v) $x \in K_n$ 'ye n durumlu veya K_n = Kip[n] kümesinden değer alan K_n **genetik denetim değişkeni** denir.

(vi) $R = <t_0, t_1, t_2 \ldots t_{(n-1)}> <x> = < t_0\ t_1\ t_2 \ldots\ t_{(n-1)}> <x> = t_0\ t_1\ t_2 \ldots t_{(n-1)}\ x$ = "ttt… tx" oluşumuna K= K[n] = Kip[n] **genetik bildirişimi denetleyebilir rator sistemi** denir. Denetim değişkeni ve rator kavramı Kaynak[23, 24] içeriğinde çalışılmıştır.

(vii) (a) <r(n-1), … , r2, r1, r0> = < r(n-1)… r2 r1 r0> = rn-1… r2 r1 r0 = "rrr… r" oluşumuna K= K_n = Kip[n] **genetik ramta anten sistemi** denir.

(b) s ∈ K= K_n = Kip[n] oluşumuna n durumlu veya K_n **genetik olarak denetlenebilir sabit** denir.

(c) <sr(n-1), … , sr2, sr1, r0> = < sr(n-1)… sr2 sr1 sr0> = srn-1… sr2 sr1 sr0 = "srsrsr… sr" oluşumuna K= K_n = Kip[n] **genetik bildirişimi denetlenebilir sabit sistemi** denir.

(d) c: Her evrede veya katmanda bildirişimleri algılayan denetleyebilen ve yönlendirebilen cab veya BÇDM adı olsun. O zaman CR = <csr(n-1)… csr2, csr1, csr0> = < csr(n-1)… csr2 csr1 csr0> = "csrn-1… csr2 csr1 csr0 = "csrcsrcsr… csr" oluşumuna bir K= K_n = Kip[n] **genetik bildirişimi denetlenebilir sabit birlikleri rand sistemi** denir.

(viii) Q = RCR = "ttt… txcsr… csrcsrcsr" oluşumuna bir Q = **< K= K_n = Kip[n], x, n; 5Bh > Q sürü bellek modeli** denir.

Kural: Q her zaman her yerde, bir T genetik RCR formatlı BTN oluşumudur.

Teorem 5: Her Q = < K= K_n = Kip[n], x, n; 5Bh> Q sürü bellek oluşumu 5×(4×n + 1) tik belekten oluşur.

İspat: Bir Q = < K_n, x, n; 5Bh> Q sürü belleği verilmiş olsun. Q içeriğinde: (i) ‖rrr… r‖ = n, (ii) ‖csr… csrcsrcsr‖ = 3n, ve (iii) ‖x‖ = 1 olduğunu biliyoruz. Bunlar gerektirir ‖Q‖ = 5×‖rrr… r‖ + 5×‖x‖+ 5×‖csr… csrcsrcsr‖ = 5×(n+1+3×n) = 5×(4×n+1) olur. Burada her tik eleman en az bir merkez belliği olan 5 bileşenden oluşmaktadır.

3.2 RCR Formatlı Biçimsel Dil Üreten Biçimsel Dilbilim

Bu kesimde RCR formatlı biçimsel dil üreten biçimsel dilbilim çalışılacaktır.

Tanım 10: Eğer P_1 = "<K = K_n = Kip[n], x, n; 5Bh>" = "< K_n, x, n; 5Bh> " anlamında algılanırsa:

1. $Q_0 = P_1$ $Q_0[x]$ = "txcsr" BTN oluşumuna bir Q = < K_1, **x, 1; 5B1: <--+--> > Q kök-sürü bellek** denir.

2. $Q_1 = Q_1[x] = Q_0[x \leftarrow Q_0[x]]$ = t<x←Q_0[x]>csr = "ttxcsrcsr" BTN oluşumuna bir Q = **<K_2, x, 2; 5B1: <--+--> > Q kök-sürü bellek** denir.

3. $Q_{(n-1)} = Q_{(n-1)}[x] = Q_{(n-2)}[x \leftarrow Q_0[x]]$ = "ttt …ttxcsrcsr…csrcsrcsr" BTN oluşumuna **bir Q = <K_n, x, n; 5B1: <--+--> > Q kök-sürü bellek** denir.

4. $Q^{+n} = Q^{+n}[x]$ = { $Q_0[x]$, $Q_1[x]$, $Q_2[x]$, … $Q_{(n-1)}[x]$ } kümesine **bir n-ary <K_n, x, n; 5B1: <--+--> > Q kök-sürü bellek "+n" küme kapanışı** denir.

5. $Q^+ = Q^+[x]$ = { $Q_0[x]$, $Q_1[x]$, $Q_2[x]$, … $Q_{(n-1)}[x]$, … } kümesine **bir <K_∞, x, ∞; 5B1: <--+--> > Q kök-sürü bellek "+" küme kapanışı** denir.

6. Bir Q^+ = **<K_∞, x, ∞; 5B1: <--+--> > Q^+ kök-sürü bellek "+" küme kapanışının** her sonlu alt kümesine bir L = L[G] = **<K_n, x, n; 5B1: <--+--> > L [G] kök-sürü bellek biçimsel dili** denir. Burada GMF = <--+--> ≡ <00100> = GMC: "Görüntü maskesi kodu" olarak algılanacaktır.

Örnek: Eğer "y" bir tik tamra anteni BTN oluşumu, "a" bir K_1 kümesinden değer alan bir tik denetim değişkeni BTN oluşumu, "r" bir tik yöresel BÇDM BTN oluşumu, "ı" bir tik sabit BTN oluşumu ve "k" bir tik ramta anteni BTN oluşumu ise o zaman:

1. Q = Q_0[a] = "yarık" bir Q = <K_1, a, 1; 5B1: <--+--> > Q bir kök-sürü bellek örneğidir.

2. Q = Q_1[a] = "y<a←yarık>rık" = "yyarıkrık" bir Q = <K_2, a, 2; 5B1: <--+--> > Q kök-sürü bellek örneğidir.

3. Q = Q_2[a] = "yy<a←yarık>rıkrık" = "yyyarıkrıkrık" = "yyyarıkrıkrık" bir Q = <K_3, a, 3; 5B1: <--+--> > Q kök-sürü bellek örneğidir.

4. $Q^{+3} = Q^{+3}$[a] = { Q_0[a] = "yarık", Q_1[a] = "yyarıkrık", Q_2[a] = "yyyarıkrıkrık"} kümesi bir Q^+ = <K_3, a, 3; 5B1:<--+-->> Q kök-sürü bellek "+3" küme kapanışı örneğidir.

5. $Q^+ = Q^+$[a] = { Q_0[a] = yarık, Q_1[a] = yyarıkrık, Q_2[a] = yyyarıkrıkrık, … , $Q_{(n-1)}$[a] = "yyy… yarık… rıkrıkrık" … } kümesi bir Q^+ = <K_∞, a, ∞; 5B1: <--+--> > Q kök-sürü bellek "+" küme kapanışı örneğidir.

6. L = {"yyarıkrık", "yyyarıkrıkrık"} bir L = <K2|3, a, 2|3; 5B1: <--+--> > L[G] kök-sürü bellek biçimsel dilidir.

Teorem 6: Her n ≥1 için bir k ∈ K_n = Kip[n] kök-sürü bellek biçimsel dilini "5B1: Bedenlik" formatında türeten bir biçimsel dilbilim vardır.

İspat: Her n ≥ 1 bir için K_n = Kip[n], n ∈ N, verilmiş olsun. Kabul edelim ki A: Tikler alfabesi, B: Toklar alfabesi, KK: BTN türetme kuralları kümesi ve Σ: "<tik> | <tik ve tok>" imdizi BTN oluşumlarının geçici kayıt-sayar kütüğü olsun. "5B1: Bedenlik" formatının geçerli olduğu her ortamlarda, G = { A = {x, c, s, t, r }; B = { X, L, RCR, Σ }; KK = { K_0: L = { }, K1: Σ ‖ X, K2: X ‖ tXcsr, K3: X ‖x, K4: RCR = [Σ], K5: L = L ∪ {[RCR]}, K6: x→X}, Σ } biçimsel dilbilimini göz önüne alalım. Bu dilbilim Q = <K_n, x, n; 5B1:<--+-->>Q, n ∈ N, sürü bellek türü BTN oluşumlarının kapanışı olan Q^+ = <K_n, x, n; 5B1:<--+-->>Q^+ kök-sürü bellek "+" küme kapanışını ve onun bir alt kümesi olan her L = L[G] kök sürü bellek biçimsel dilini üretir. Biz burada bir örnek olarak L = L[G] = <K_3, x, 3; 5B1: <--+-->> L[G] ={Q_0=Q_0[x] = "txcsr", Q_1=Q_1[x] = "ttxcsrcsr", Q_2=Q[x] = "tttxcsrcsrcsr" } biçimsel dilinin G dilbiliminin KK kurallarını kullanarak bir L = <K_n, x, n; 5B1:<--+-->>L[G] biçimsel dil biçimini üreteceğiz. Bunu yaparken aşağıda verilen **Algoritma A1** ve **İzlence A1** anlatımlarını kullanacağız.

Algoritma A1: A0: Başla. A1: N doğal sayılar kümesinden gelişi güzel bir n ≥ 1 sayısı seç ve Kip[n] kümesini oluştur. A2: k = 0 atamasını yap. A3: Σ = { }, L = { }, RCR = { } atamalarını yap. A4: K1 kuralını kullan. A5:

K2 kuralını kullan; A6: K3 kuralını kullan. A7: K4 kuralını kullan. A8: K5 kuralını kullan. A9: K6 kuralını kullan. A10: Eğer k < n-1 ise, o zaman k = k + 1 yap ve A5 adımına git. A11: Dur.

İzlence A1: İA0:Başla. İA1: N doğal sayılar kümesinden, n = 3 sayısını seç ve K3 = Kip[3] = { 0, 1, 2} kümesini oluştur. İA2: k = 0 atamasını yap. İA3: $\underline{\Sigma}$ = { }, $\underline{L}$ = { } ve $\underline{RCR}$ = { } atamalarını yap. İA4: K1 kuralını kullan. $\underline{\Sigma} \xrightarrow{K_1} X$ ve [Σ] = X üretilir. İA5: K2 kuralını kullan. $\underline{\Sigma} \xrightarrow{K_1} X \xrightarrow{K_2}$ tXcsr ve [Σ] = tXcsr üretilir. **İA6:** K3 kuralını kullan. $\underline{\Sigma} \xrightarrow{K_1} X \xrightarrow{K_2}$ tXcsr $\xrightarrow{K_3}$ txcsr ve [Σ] = txcsr üretilir. **İA7:** K4 kuralını kullan. $\underline{RCR} \xrightarrow{K_4}$ [Σ] = txcsr. [$\underline{RCR}$] = txcsr üretilir. **İA8:** K5 kuralını kullan. $\xrightarrow{K_5} \underline{L} = \underline{L} \cup \{ [\underline{RCR}] \} = \{ \} \cup \{$ txcsr$\} = \{$ txcsr $\}$ üretilir. **İA9:** K6 kuralını kullan. $\underline{\Sigma} \xrightarrow{K_1} \ldots \xrightarrow{K_6}$ tXcsr. [Σ] = tXcsr. [$\underline{L}$] = { txcsr} olur. **İA10:** k = 0 < 3-1 = 2 doğru olduğundan, k = k + 1 = 1 olur ve İA5 adımına gidilir. **İA5:** K2 kuralını kullan. $\underline{\Sigma} \xrightarrow{K_1} \ldots \xrightarrow{K_6}$ tXcsr $\xrightarrow{K_2}$ ttXcsrcsr üretilir. **İA6:** K3 kuralını kullan. $\underline{\Sigma} \ldots \xrightarrow{K_2}$ ttXcsrcsr $\xrightarrow{K_3}$ ttxcsrcsr ve [Σ] = ttxcsrcsr üretilir. **İA7:** K4 kuralını kullan. $\underline{RCR} \xrightarrow{K_4}$ ttxcsrcsr, [Σ] = [$\underline{RCR}$]= ttxcsrcsr üretilir. **İA8:** K5 kuralını kullan. $\underline{L} \xrightarrow{K_5} \underline{L} \cup \{$ [$\underline{RCR}$] $\} = \{$ txcsr $\} \cup \{$ttxcsrcsr $\} = \{$ txcsr, ttxcsrcsr $\}$ üretilir. **İA9:** K6 kuralını kullan. $\underline{\Sigma} \xrightarrow{K_1} \ldots \xrightarrow{K_6}$ ttXcsrcsr ve [Σ] = t_tXcsrcsr türetilir. **İA1:** k = 1 < 3-1 = 2 doğru olduğundan, k = k + 1 = 2 olur ve İA5 adımına gidilir. **İA5:** K2 kuralını kullan. $\underline{\Sigma} \xrightarrow{K_1} \ldots \xrightarrow{K_6}$ ttXcsrcsr $\xrightarrow{K_2}$ ttt Xcsrcsrcsr türetilir. **İA6:** K3 kuralını kullan. $\underline{\Sigma} \xrightarrow{K_1} \ldots \xrightarrow{K_2}$ tttXcsrcsrcsr $\xrightarrow{K_3}$ tttxcsrcsrcsr ve [Σ] = tttxcsrcsrcsr üretilir. **İA7:** K4 kuralını kullan. $\underline{RCR} \xrightarrow{K_4}$ [Σ] = tttxcsrcsrcsr ve [$\underline{RCR}$] = tttxcsrcsrcsr türetilir. **İA8:** K5 kuralını kullan. $\underline{L} \xrightarrow{K_5} \underline{L} \cup \{[\underline{RCR}]\} = \{$ txcsr, ttxcsrcsr$\} \cup \{$tttxcsrcsrcsr$\} = \{$txcsr, ttxcsrcsr, tttxcsrcsrcsr$\}$ üretilir. **İA9:** K6 kuralını kullan. $\underline{\Sigma} \xrightarrow{K_1} \ldots \xrightarrow{K_3}$ tttxcsrcsrcsr $\xrightarrow{K_6}$ tttXcsrcsrcsr ve [Σ] = tttXcsrcsrcsr üretilir. **İA10:** k = 2 < 3-1 = 2 yanlış olduğundan, bir sonra ki adıma gidilir. İA11: Dur; elde edilir. Burada $\underline{L} = \underline{L[G]} = <K_3, x, 3; 5B1: <--+-->> \underline{L[G]} = \{Q_0=Q_0[x] =$ txcsr, $Q_1=Q_1[x] =$ ttxcsrcsr, $Q_2 = Q_2[x] =$ tttxcsrcsrcsr $\}$ kök-sürü bellek biçimsel dilinin bir biçimsel $\underline{G}$ dilbilimi ile türetilebilirliği **Algoritma A1** ve **İzlence A1** ile ortaya konulmuştur.

IV. SONUÇLAR, ÖNERİLER VE ELEŞTİRİLER

Bildirişimli matematiğin bilgi güvenliği için RCR formatlı Q^+ kök-sürü bellek "+" küme kapanışının altyapılarını türeten $\underline{L}$ biçimsel dil ve $\underline{G}$ biçimsel dilbilim örneği bu bildiri içeriğinde çalışılmıştır. Elde edilen Q kök sürü belleği I@I kök sürü internet modelinin güvenli modellenmesinde kullanıma hazırdır.

I@I sürü internet modeli BTN oluşumlarının içinde bulunduğumuz çok yakın bir süreçte günlük yaşamın gündemine geleceği ve gündemde olacağı beklenmektedir.

BTN aracılığında, sistematik bilgi oluşumlarına "bildirişim yapabilen yazılım sistemi olarak bakılması," zamanlama yönünden çok derin ve içerikli anlatımın yapılabileceğini gündeme getirmiştir. Ürettiğimiz her biçimsel Q sürü bellek oluşumu sonlu sayıda başka uzaktan programlanabilir biçimsel Q sürü bellek biçiminden oluşturulmuş BTN yazılım yongasıdır. Her m denetim değişkenli K = Kip[n] mantık bilgisine duyarlı olan Q sürü bellek yazılım yongası m, n ≥ 1 ve m, n ∈ N olduğunda m×(4×n+1) tik alt Q sürü bellek yongasını farklı birleşimde kullanarak bilgi güvenliği sağlamayı gerçekler. İleride çok denetim değişkenli Q sürü bellek yapılarının ürettiği I@I sürü internet ortamlarında, sonsuza yakın güvenli bilginin biçimsel Kip[n] mantığının denetiminde nasıl kolayca toplumun açık kullanımına sunulabileceğini göreceğiz.

Evrende, tıpkı yerçekimi yasası gibi, bir **"Bildirişime Çekim Yasası"** vardır. Bu yasanın gereği olarak, her Q BTN sürü bellek modeli bir Q BTN sürü bellek modeli gurubu ile bildirişim kurabilmektedir. Bu biçimsel bildirişimin, sonsuz mertebesinde sayılabilir frekanslar kümesinin birinden seçilen, bir frekans ile yapılmasının mümkün olduğunu gösterir. Bundan dolayı, bu algılama yeryüzünde güvenli açık bildirişimin gerçekleştirilmesi açısından son derece önemli görülen bir algılamadır.

KAYNAKLAR

[01] F. Ünlü: Kuramsal λ-Tasımlaması, *Atatürk Üniversitesi Basımevi,* Erzurum, 1976.

[02] F. Ünlü: A TASIM Logic Realization of Boolean Algebra, *DIRASAT: A Research Journal, the University of Jordan, VIII (7): pp67-76, Amman, 1986.*

[03] F. Ünlü: TASIM Logic Realizations in Logic Design, *DIRASAT VIV (12): pp61-80, Amman, 1987.*

[04] F. Ünlü: Multi-Valued CITALOG Closure, *Proceeding of the 10th National Computer Conference, King Abdulaziz University, 28 February -2 March, pp 537-547, Jeddah, Kingdom of Saudi Arabia, 1987.*

[05] F. Ünlü: An Optimal Logic Software Construction Engineering Technique by Boolean Type of Algebra on CITAWIROM Closure, *The Final Report of Research Project No. 1409/048, King Abdulaziz University, Office of Vice Presidency, Post-Graduate Studies & Academic*

Research, Scientific Research Council, Jeddah, Kingdom of Saudi Arabia, 1989.

[06] F. Ünlü: A Construction Engineering Technique For Generating An Algebraic Closure of Software Minimizing CITAWIROM Based On Automata, Virtual Machines and Language, *The Final Report of Research Project No. 1410/150, King Abdulaziz University, Office of Vice Presidency, Post-Graduate Studies & Academic Research, Scientific Research Council, Jeddah, Kingdom of Saudi Arabia, 1989.*

[07] F. Ünlü: CITALOG: Compact and Integrated Tasim Logic Closure, *Journal of King Abdulaziz University, Science, Vol. 2 pp 117-136, Jeddah, 1990.*

[08] F. Ünlü: FTD Grammar Graph, *International Journal of Computer Mathematics,* 2003, Vol. 80(1) pp1-9.

[09] F. Ünlü: Soyut Canlı Oluşumunda Kanserli ve Kansersiz Yaşam Biçimi, Journal of Yasar University, 1(4), pp303-318, 2006.

[10] F. Ünlü: us-Crop Based Compact Memory, *International Journal of Contemporary Mathematical Science, Volume 1, No. 5-8, pp 317-325, 2006.*

[11] F. Ünlü: A Remote Programming Technology on a Remote VDM Clustering in λ-Calculus, *International Mathematical Form, Vol. 1, No. 13-16, pp 671 - 685, 2006 .*

[12] F. Ünlü: Plemvanal: A Communicating Commuting Mathematics Generator Type, *International Mathematical Form, Vol. 1, No. 13-16, pp 671 – 685 , 2006 .*

[13] F. Ünlü: W-Pencereli W-Bilim Tasarım Teknolojilerinin W@W Desenleri, *Journal of Yasar University, 3(10), pp1185-1212, 2008.*

[14] F. Ünlü: G-Form Memory GENBIOM KBO Description, *Journal of Yasar University, 4(15), pp2327-2335, 2009.*

[15] F. Ünlü: Communicating e-Economy in us-Culture, *Journal of Yasar University, 4(15), pp2419-22433, 2009.*

[16] F. Ünlü: TASIM Günlüğü A: TASIM, *Journal of Yasar University, 4(16), pp2539-2556, 2009.*

[17] F. Ünlü: Communicating TASIM °T-Genetic Quantum KBO Memory Modules Closure, *Journal of Yasar University, 4(16), pp2611-2636, 2009.*

[18] F. Ünlü: T-genetic RCR-U Form, *INISTA 2010, ID 16, pp 1-5, Kayseri, Turkey, 2010.*

[19] F. Ünlü: Biçimsel TASIM Dilbilimi, AYSU 2010, ID 5, pp 1-5, Kayseri, 2010.

[20] F. Ünlü: Remote Programmable Mobile Communicating Global TASIM-T E-Business Modules Controllable by One Control Variable, *ICBME 2009, Vol. II, pp 90-103,Yasar University, Izmir.*

[21] F. Ünlü: A Formel Property Dependent United Business System Design and Programming, ICBME 7-9 October 2010 e-Proceeding, Yasar University, Izmir, Turkey.

[22] F. Ünlü: Bildirişimli Matematik, 9. Matematik Sempozyumu, 20-22 Ekim 2010 Karadeniz Teknik Üniversitesi, Trabzon.

[23] F. Ünlü: Q ve Q^+ Sürü Bellekli I@I Modeli Tasarımında Kullanılan T Genetik Altyapı Elamanları, *XVI. Türkiye 'de İnternet Konferansı. Bildiri No. 3, 30 Kasım-2 Aralık 2011, Ege Universitesi, İzmir.*

[24] F. Ünlü: Bildirişimli Matematiğin <T<x>, 1, n> Q Sürü Bellekli 3D I@I İnternet Sürüsü. *XVI. Türkiye'de İnternet Konferansı. Bildiri No. 4, 30 Kasım -2 Aralık 2011, Ege Universitesi, İzmir.*

[25] P. Linz, *Introduction to Formal Languages and Automata,* Fourth Edition, Jones and Bartlett Publishers, London, 2006.

[26] R. L. Causey, *Logic, Sets, and Recursion,* Second Edition, Jones and Bartlett Publishers, Inc., London, 2006.

[27] W. Lark, *LISP 1.5 Primer,* Dickenson Publishing Inc. California, 1968.

Cycle Counting For Information Security in I@I Swarm Internet Generating Q Swarm Memory

Prof. Dr. Fevzi Ünlü
Retired Professor of Computer Science and Applied Mathematics
Ege University & Yasar University, Izmir

***Özet*—*Bir Q^+ kümesinden gelişigüzel alınan bir Q sürü belleği, LOS ve RDS ile adlandırılan iki farklı durumda bulunur. LOS durumunda Q belliğinin, bildirişim yapaya uygun olan tamra ve ramta anten çiftleri bulunur ve bildirişim yaparken kullanacakları frekanslar onlara atanır. Atanan bu frekanslar Q sürü belleği RDS durumuna geçtiğinde kullanılır. Devirli sayma CC bir Q sürü belleği LOS durumunda iken, onun yapısında bulunan ve bildirişim yapmaya muktedir olan, tamra ve ramta anten çiftlerini bularak eşleyen ve hangi frekanslarda bildirişim yapacaklarını bulan bir sayma işlemi biçimidir. Bir Kip[n], n ∈ N, dilinde CC ile bulunan frekans kodları, bir I@I sürü internet modeli üreten Q sürü bellek modeli RDS durumunda iken; onun yapısında bulunan tamra ve ramta antenlerinin bildirişim yapmada kullanacağı en uygun frekanslardır. Yazar bunun için, bu bildiride, bir Q sürü belleği LOS durumunda iken; CC tekniği ile onun RDS durumunda güvenli bildirişim yapmaya muktedir olacak tamra ve ramta anten çiftlerine atanacak olan, en uygun bildirişim frekanslarını bulma çalışmasını yapmaktadır.*

Abstract— A Q of Q^+ swarm memory closure can be in two distinguishable states. They are namely called LOS and RDS of Q. Cycle counting CC is a process for pairing and marking the communicating tamra and ramta antennas appearing in a Q of Q^+ while Q in LOS by the same frequency codes in a Kip[n], n ∈ N. Frequency codes are used to realize the observe able and secure optimal communicational activities in the I@I swarm internet model generating Q swarm memory model while it is in RDS. Author is studding CC techniques in order to code securely communicating pairs of the tamra and ramta antennas while Q is in LOS. The basic supporting information can be found in Ünlü at all and [1-14].

Index Terms— Cycle counting, internet, I@I, ITC, IRC, KBO, LOS, memory, N, Q, RCR, RDS, security, swarm.

I. INTRODUCTION

I@I and Q are tic RCR formatted KBOs with a pair of ITC and IRC systems. Tamra and ramta antenna systems in the rator and rand of a distributed communicating I@I swarm internet model generating Q swarm memory model are responsible from ITC and IRC. They were studied in Ünlü at all. I@I and Q can be in two different states. Namely they are called randomly distributed state RDS and linearly ordered state LOS. For designing formally optimal communicational algorithms to realize information processing in a distributed Q swarm memory model software chip, some cycle counting CC models were needed for pairing and marking the communicating tamra and ramta antennas while Q in LOS. A set of suitable CC models are found to mark tamra and ramta antennas on Q in LOS in ordered to be used in RDS in this paper. Basic background information is available in [1-14].

II. FOUNDATION

In this section the main tools of communicating antenna resource cycle counting models in a distributed Q of Q^{+n} swarm memory closure for generating an distributed I@I of $I@I^+$ swarm internet closure are shortly introduced by using DTS: Descriptive Text Sequence [1-14] for the sake of easy readability. The reader should read each DTS in the given order in order to grasp the notion of different cycle counting process types.

DTS-1: Brief words

01. KBO: "Knowledge Based Object,"
02. ITC: "Information Transmitting Channel,"
03. IRC: "Information Receiving Channel,"
04. TIC | tic: "undividable tiny compact and dense information construct,"
05. CIC | cic: "Coarse easily dividable into other compact and dense tic information construct,"
06. Rator: "Operator" | "Operator register,"
07. Rand: "Operand" | "Operand register,"
08. @ | CAP | cap: "Communicational Attraction and Process Controlling Center,"
09. RCR: Rator Cab Rand. It is used to generate RCR formatted symmetric KBO software model.
10. I@I: Internet @ Internet.
11. N: The set of natural number.
12. LOS: Linearly Ordered State.
13. RDS: Randomly Distributed State.
14. CC: Cycle Counting.
15. ISTS: Information Sensing and Transmitting State.
16. ISRS: Information Sensing and Receiving State.

DTS-2: Tics, IDC, P_1 and P_2

1. (i) t: tic tamra antenna resource, (ii) x or y: tic control variable resource, (iii) @: cab: tic cap resource, (iv) c: tic constant resource, and (v) r: tic ramta antenna resource. They are used in the construction of a tic RCR formatted Q KBO construction.

2. IDC = {0000, 0001, 0010, 0011, 0100, 0101, 0110, 0111, 01000, 1001, 1010, 1011, 1100, 1101, 1110, 1111}. Where IDC stands for "Image Dress Code" in which "1" represents observe able component while "0" represents none observe able component in a vector representation of a tic KBO.

3. P_1: A property vector which has only 1 control variable x in its structure. P_2: A property vector which has only 2 control variables x and y in its structure.

DTS-3: P_1 and P_2 form design and meaning of P_1 and P_2

1. P_1 = <C, T; K = K[n] = Kip[n], x, n; 4B: bbbb ∈ IDC> is a form design.

Meaning of P_1 = <C: Communicating, T: TASIM genetic; K = Kip[n] = {0, 1, 2 … n-1}, x: 1 control variable named by x, n ≥ 1 and n ∈ N; 5B: bbbb ∈ IDC >.

2. P_2 = <C, T; < K = Kip[m], K = Kip[n] >, <x, y>, <m, n>: m, n ≥ 1 and m, n ∈ N; 5B: bbbb ∈ IDC > is a form design.

The meaning of P_2 = <C: Communicating, T: TASIM genetic; < K = K[m] = Kip[m] = {0, 1, 2, … , m-1}, K = K[n] = Kip[n] = {0, 1, 2, … , n-1} >, <x, y>: 2 control variables named by x and y, <m, n>: 2 natural number named by m and n such that m, n ≥ 1 and m, n ∈ N; 4B: bbbb ∈ IDC > is a form design.

2.1 Cycle Counting Models

Different cycle counting models are introduced in the following different text boxes.

DTS-4: FRCC

Definition 1: A proper forward counting is generated by using only numerals appearing in **K** = K[n] = Kip[n] such a way that all numbers are generated in length 1 in the order of n-tuple cycles is called a **forward regular cycle counting** on K = K[n] = Kip[n]. It is briefly represented by FRCC[n]. Where, "n-tuple" meaning is "a sequence that it contains n element in it".

Theorem 1: There is one forward regular n-tuple cycle counting FRCC[n].

Proof: 0, 1, 2, 3 … (n-1), 0, 1, 2, 3 … (n-1), 0, 1, 2, 3 … (n-1), 0, 1, 2, 3 … is forward regular cycle counting FRCC[n].

Example 1: If n = 8, then 8–tuple K = K[8] = Kip[8] = {0, 1, 2, 3, 4, 5, 6, 7} ≡ "0 | 1 | 2 | 3 | 4 | 5 | 6 | 7" is obtained. FRCC [8] is carried in the length 1 vocabularies in the order of 8-tuple cycles by using 8 numerals in K = K[8] = Kip[8]. Hence 0, 1, 2, 3, 4, 5, 6, 7, 0, 1, 2, 3, 4, 5, 6, 7 … is a forward regular cycle counting FRCC[8].

DTS-5: BRCC

Definition 2: The reverse counting process of FRCC[n] is called backward regular cycle counting by n-tuple on K = Kip[n]. It is briefly represented by BRCC[n].

Theorem 2: There is one backward regular n-tuple cycle counting BRCC[n].

Proof: "(n-1), (n-2) … 3, 2, 1, 0, (n-1), (n-2) … 3, 2, 1, 0, (n-1), (n-2) … 3, 2, 1, 0…" is backward regular n-tuple cycle counting BRCC[n] on K = K[n] = Kip[n] .

Example 2: If n = 8. K = Kip[8] = {0, 1, 2, 3, 4, 5, 6, 7} ≡ "0 | 1 | 2 | 3 | 4 | 5 | 6 | 7", then "7, 6, 5, 4, 3, 2, 1, 0, 7, 6, 5, 4, 3, 2, 1, 0 …" is a BRCC[8] on K = Kip[8].

DTS-6: Root Cycle of FRCC

Definition 3: The first n-tuple of FRCC[n] or BRCC[n] is called the root cycle of FRCC[n] or BRCC[n]. They are briefly represented by RC-FRCC[n] and RC-BRCC[n].

Theorem 3: There is only one root cycle of FRCC[n] or BRCC[n] on K = K[n] = Kip[n].

Proof: (a) "0, 1, 2, 3 … (n-1)" is the root cycle of FRCC[n] on K = K[n] = Kip[n]. (b) "(n-1), (n-2) … 3, 2, 1, 0" is the root cycle of BRCC[n] on K = K[n] = Kip[n].

Example 3: (a) "0, 1, 2, 3, 4, 5, 6, 7" is the root cycle of FRCC [8] on K = K [8] = Kip [8]. (b) "7, 6, 5, 4, 3, 2, 1, 0" is the root cycle of BRCC[8] on K = Kip[8].

DTS-7: Root cycle of FBRCC

Definition 4: The concatenation of the root cycles of RC-FRCC[n] and RC-BRCC[n] on a K = Kip[n] is briefly represented by RC-FBRCC [2×n].

Theorem 4: There is only one RC-FBRCC [2×n] on K = K[n] = Kip[n].

Proof: "0, 1, 2, 3 … (n-2), (n-1)". "(n-1), (n-2) … 3, 2, 1, 0" = **"**0, 1, 2, 3 … (n-2), (n-1), (n-1), (n-2) … 3, 2, 1, 0" is RC-FBRCC [2×n] on K = Kip[n].

Example 4: (a) **"**0, 1, 2, 3, 4, 5, 6, 7, 7, 6, 5, 4, 3, 2, 1, 0" is RC-FBRCC [2×8] on K = Kip [8].

Definition 5: RC-FBRCC [2×n] = "0, 1, 2, 3, … , n-2, n-1, n-1, n-2 … 3, 2, 1, 0 " is also called the root cycle of the forward and backward mirror cycle counting RC-FBMCC [2×n] by 2 × n-tuple on K = Kip[n].

2.2 Image Designs for Forward Regular Mirror Cycle Counting

DTS-8: Numerical Image A, B and C

(a)"IA: Image A" is a RC-FRCC[n] on K = Kip[n]. It observes itself in the mirror as RC-BRCC[n] on K = Kip[n]. "IB: Image B" is RC-BRCC[n] on K = Kip[n]. It observes itself in the mirror as RC-FRCC[n] on K = Kip[n]. "IC: Image C" is RC-RMCC[n] on K = Kip[n]. It observes itself in the mirror as a RC-RMCC[n] on K = Kip[n]. Hence:

(b) IA = "0, 1, 2, 3… n-2, n-1" ‖ "n-1, n-1, n-2 … 3, 2, 1, 0 " = IB ⇔ "IA ‖ IB and IB ‖ IA". It implies that IC = RC-RMCC[n] = "0, 1, 2, 3 … n-2, n-1, n-1, n-2 … 3, 2, 1, 0" ‖ "0, 1, 2, 3 … n-2, n-1, n-1, n-2 … 3, 2, 1, 0" = RC-RMCC[n] = IC ⇔ IC ‖ IC.

Where, "**‖**" **is double sided mirror.**

DTS-9: Observer O

Assuming "O" is a remote observer to observe the action of IA and IB together on its own mirror, while IA and IB are looking into their mirrors. Following cases are possible:

(i) If IA is looking into its mirror with its eye-detectors, then it observes itself as IB.

(ii) If IB is looking into the mirror with its eye-detector then it observes itself as IA.

(iii) If O, observes IA and IB together while they are looking into mirror, then O observes IA and IB images in its own eye mirror as RC-RMCC[n] on K = Kip[n].

DTS-10: IC as an observer

Theorem 5: Assume that IC is RC-RMCC[n] on K = Kip[n]. IC observes itself in its mirror.

Proof: Let us assume that "||" is a two sided eye detectible mirror. Assume that IC is RC-RMCC[n] on K = Kip[n]. It implies that IC = "0, 1, 2, 3, ... (n-1), (n-1), (n-2) ... 3, 2, 1, 0" || "0, 1, 2, 3 ... (n-1), (n-1), (n-2) ... 3, 2, 1, 0" = IC⇔ IC || IC.

Example 5: Let us assume that "||" is a two sided eye detectible mirror and IC = "0, 1, 2, 3, 4, 5, 6, 7, 7, 6, 5, 4, 3, 2, 1, 0" is RC-RMCC [8] on K = Kip [8]. This implies that IC = "0, 1, 2, 3, 4, 5, 6, 7, 7, 6, 5, 4, 3, 2, 1, 0" || "0, 1, 2, 3, 4, 5, 6, 7, 7, 6, 5, 4, 3, 2, 1, 0" = IC⇔ IC || IC.

DTS-11: Relation between RC-FRCC and RC-BRCC

Theorem 6: If RC-FRCC[n] is the root cycle of a forward regular cycle counting by n-tuple on K = Kip[n] and RC-BRCC[n] is the root cycle of a backward regular cycle counting by n-tuple on K = Kip[n]. Then

(i) RC-FRCC[n] observes RC-BRCC[n] in the mirror.

(ii) RC-BRCC[n] observes RC-FRCC[n] in the mirror.

Proof: Assume that RC-FRCC[n] is the root cycle of a forward regular cycle counting by n-tuple on K = Kip[n] and RC-BRCC[n] is the root cycle of a backward regular n-tuple cycle counting by n-tuple on K = K[n] = Kip[n]. Then:

(i) RC-FRCC[n] = "0, 1, 2, 3 ... (n-2), (n-1)" || "(n-1), (n-2), ..., 3, 2, 1, 0" = RC-BRCC[n] in the mirror.

(ii) RC-BRCC[n] = "(n-1), (n-2) ... 3, 2, 1, 0" || "0, 1, 2, 3, ..., (n-2), (n-1)" = RC-FRCC[n] in the mirror.

Example 6: (i) If IA = RC-FRCC [8] = "0, 1, 2, 3, 4, 5, 6, 7" || "7, 6, 5, 4, 3, 2, 1, 0" = RC-BRCC [8] = IB.

(ii) If IB = RC-BRCC [8] = "7, 6, 5, 4, 3, 2, 1, 0" || "0, 1, 2, 3, 4, 5, 6, 7" = RC-FRCC [8] = IA.

DTS-12: Rator and rand part of a RC-RMCC

Definition 6: Let us assume that RC-RMCC[m] = "0, 1, 2, 3, ..., m-1, m-1 ... 3, 2, 1, 0" is given for m ≥ 1 and m ∈ N. (a) The first m section of RC-RMCC[m] is called a rand part of RC-RMCC[m]. (b) The second m section of RC-RMCC[m] is called a rator part of RC-FRMCC[m]. (c) If an "o_i" is the ith tic tab memory component, injected in front of each ith numeral for using "$i \rightarrow < o_i\ i >$" transformation, in the rand part of the RC-RMCC[m]; then the new RC-RMCC[m] is called as an **m black hole tab tic memories injected into RC-RMCC[m]**. It is briefly represented by RC-BHIRMCC[m]. Where, "o" is an extendable and contractible tic black hole memory. It can't be observed by any technology for time being. Only T can store very dense, observable, T genetic, communicating, forward and backward regular mirror cycle countable tic information in it.

Theorem 7. There is at least one RC-BHIRMCC[m] for m ≥ 1 and m ∈ N.

Proof: Let us assume that "0, 1, 2, 3 ... m-1, m-1 ... 3, 2, 1, 0" is a RC-RMCC[m] for each m ≥ 1 and m ∈ N. The construction of "0, 1, 2, 3 ... m-1, o_{m-1}, m-1, o_{m-2}, m-2 ... o_3, 3, o_2, 2, o_1, 1, o_0, 0" is an m black hole tab memories injected RC-BHIRMCC[m].

Example 7: "0, 1, 2, 3 ... 7, o_7, 7, o_6, 6 ... o_3, 3, o_2, 2, o_1, 1, o_0, 0" is 8 black holes injected RC-BHIRMCC [8].

DTS-13: Mixed and Smooth Complex RMCC

Definition 7: Let assume that A = A [m, o] = "0, 1, 2, 3 ... m-2, m-1, o_{m-1}, m-1, o_{m-2}, m-2 ... o_3, 3, o_2, 2, o_1, 1, o_0, 0" is a RC-BHIRMCC[m] and B_i = B[n_i] is a RC-RMCC [n_i]. C = C [m, n = <n_0, n_1, n_2 ... n_{m-1}>] = A [m, $o_i \leftarrow B_i$ = B[n_i]] is called a **mixed complex RMCC[<m, n= <n_0, n_1, n_2 ... n_{m-1}>>]**. Further: If $\forall n_i$ = s, then RMCC [<m, n = <m x s >] is called **a smooth complex RMCC [m, n = <m x s>]**. The first one is briefly represented by MCRMCC [<m, n= <n_0, n_1, n_2 ... n_{m-1}>>]. The second is briefly represented by SCRMCC [m, n = <m × s>].

Theorem 8: (a) There is at least one SCRMCC [m, n = <m × s>].

Proof: Consider: (i) A = A[m, o] = "0, 1, 2, 3 ... m-1, o_{m-1}, m-1, o_{m-2}, m-2 ... o_3, 3, o_2, 2, o_1, 1, o_0, 0" is a SCRMCC[m, n = <m × s>] for each m ≥ 1 and m ∈ N. Consider $\forall B_i$ [s ← n] = B[n] = "0, 1, 2, 3 ... n-1, n-1 ... 3, 2, 1, 0" is a RC-RMCC[n] for each n ≥ 1 and n ∈ N. Construct C = C[m, <m × n>] = A[m, o:$\forall o_k \leftarrow$ B[n]] = "0, 1, 2, 3 ... m-2, m-1, o_{m-1}←B [n], m-1, o_{m-2}←B[n], m-2 ... o_3←B[n], 3, o_2←B[n], 2, o_1←B[n], 1, o_0←B[n], 0" = "0, 1, 2, 3, ..., m-2, m-1, "0, 1, 2, 3, ..., n-1, n-1, ..., 3, 2, 1, 0", m-1, "0, 1, 2, 3, ..., n-1, n-1, ..., 3, 2, 1, 0", m-2, ..., "0, 1, 2, 3, ..., n-1, n-1, ..., 3, 2, 1, 0", 3, "0, 1, 2, 3, ..., n-1, n-1, ..., 3, 2, 1, 0", 2, "0, 1, 2, 3, ..., n-1, n-1, ..., 3, 2, 1, 0", 1, "0, 1, 2, 3, ..., n-1, n-1, ..., 3, 2, 1, 0", 0 " is a SCRMCC[<m, <m x n >>].

DTS-14: Smooth and complex RMCC

Example 7: Consider A[8, o] = "0, 1, 2, 3, 4, 5, 6, 7, o_7, 7, o_6, 6, o_5, 5, o_4, 4, o_3, 3, o_2, 2, o_1, 1, o_0, 0" is 8 black hole tab memories injected RC-BHIRMCC [8]. Let assume that $\forall B_i$ [s ← n = 8] = B[8] = "0, 1, 2, 3, 4, 5, 6, 7, 7, 6, 5, 4, 3, 2, 1, 0" is a RC-RMCC[8]. Construct C = C[<8, <8×8>] = A[8, $\forall o_i \leftarrow$ B[8]] = "0, 1, 2, 3, 4, 5, 6, 7, "0, 1, 2, 3, 4, 5, 6, 7, 7, 6, 5, 4, 3, 2, 1, 0", 7, "0, 1, 2, 3, 4, 5, 6, 7, 7, 6, 5, 4, 3, 2, 1, 0", 6, "0, 1, 2, 3, 4, 5, 6, 7, 7, 6, 5, 4, 3, 2, 1, 0", 5, "0, 1, 2, 3, 4, 5, 6, 7, 7, 6, 5, 4, 3, 2, 1, 0", 4, "0, 1, 2, 3, 4, 5, 6, 7, 7, 6, 5, 4, 3, 2, 1, 0", 3, "0, 1, 2, 3, 4, 5, 6, 7, 7, 6, 5, 4, 3, 2, 1, 0", 2, "0, 1, 2, 3, 4, 5, 6, 7, 7, 6, 5, 4, 3, 2, 1, 0", 1, "0, 1, 2, 3, 4, 5, 6, 7, 7, 6, 5, 4, 3, 2, 1, 0", 0" is a SCRMCC [8, <8 × 8>].

Theorem 8: There is at least one MCRMCC [<m, n = <n_0, n_1, n_2 ... n_{m-1}>].

Proof: Assume A = A [m, o] = "0, 1, 2, 3 ... m-2, m-1, o_{m-1}, m-1, o_{m-2}, m-2 ... o_3, 3, o_2, 2, o_1, 1, o_0, 0" is a RC-BHIRMCC [m] for m ≥ 1 and m ∈ N. Assume B_{m-1}[1] = "0, 0", B_{m-2}[2] = "0, 1, 1, 0" ... B_2[m-2] = "0, 1, 2, 3 ... m-3, m-3 ... 3, 2, 1, 0", B_1[m-1] = "0, 1, 2, 3 ... m-2, m-2 ... 3, 2, 1, 0", B_0[m] = "0, 1, 2, 3 ... m-1, m-1 ... 3, 2, 1, 0". Construct C[m, <1, 2, 3 ... m>] = "0, 1, 2, 3 ... m-2, m-1, "0, 0", m-1, "0, 1, 1, 0" m-2 ... "0, 1, 2, 3 ... m-3, m-3 ... 3, 2, 1, 0", 2, "0, 1, 2, 3, ..., m-2, m-2, ..., 3, 2, 1, 0", 1, "0, 1, 2, 3, ..., m-1, m-1, ..., 3, 2, 1, 0" 0". It is a MCRMCC [<m, <1, 2, 3 ... m>>].

Example 8: "0, 1, 2, 3, "0, 1, 2, 2, 1, 0", 3, "0, 1, 1, 0", 2, "0, 1, 2, 3, 3, 2, 1, 0", 1, "0, 1, 2, 2, 1, 0", 0" is a MCRMCC [4, <3, 2, 4, 3>>].

III. APPLICATION

In this section, SCRMCC [<m, <m × n >] and MCRMCC [<m, n = <n_0, n_1, n_2 … n_{m-1}>] are applied for counting the pairs of communicating tamra and ramta antenna systems in a Q of Q^+ in the following DTS[15-24].

3.1 Cycle Counting on Communicating Tamra and Ramta Antennas in Q

DTS-15a: Constructing a L [K, G] type formal language

Definition 8: In a communicating T genetic Q swarm memory constructing Environment; "t" is called a tic tamra antenna, "r" is called a tic ramta antenna, "c" is called a tic KBO constant, "x or y" is called a tic KBO variable and K = K[n] = Kip[n] = {0, 1, 2, …, n-1} is called a numerical alphabet for supporting generation of a communicating formal language L = L[K, G] .

Where, G is a formal grammar for generating formal language L from tic numerals of K.

DTS-15b: Q [K, G] formal language

Definition 9: In a communicating T genetic Q swarm memory constructing Environment: If $\underline{A}$ = {t, x, y, @, c, r, k} is a TASIM genetic alphabet and $\underline{G}$ is a TASIM genetic formal grammar, then Q[$\underline{A}$, $\underline{G}$] is a TASIM genetic formal Q swarm memory language.

DTS-16: Elements in Q [$\underline{A}$, $\underline{G}$]

Assume that

1) "$_k$t" is a ramta antenna that it has a capacity to sense, receive and transmit any tic information coded into the signal "k" while k □ L[K, G].

2) "r_k" is A ramta antenna that it has a capacity to sense, receive and transmit any tic information coded into the signal "k" while k □ L[K, G].

3) "$_k$t … r_k" is a < t: tamra, r: ramta> antenna pair in a word Q swarm memory that it has capacity to communicate with each other by sensing, receiving and transmitting tic information coded into the signal "k" while k □ L[K, G].

Communication Rule: Each of t and r antennas in the pair has a capacity to be in two different states namely ISRS and ISTS. In the initial state, tamra antenna becomes in the state of ISRS. In the next state the pair changes its state as pair wise. Tamra antenna becomes in the state of ISRS and ramta antenna becomes in the state of ISTS in the pair. A communication process takes place between the members of the pair continuously this way, until the process of communication between tamra and ramta antenna system is over.

DTS-17: KRA[n] alphabet

Consider Kip[n] as an alphabet. An alphabet obtained by changing the numeral symbols in Kip[n] by some tic symbols or pictures is called a KRA[n] alphabet. A KRA[n] alphabet is in the same equivalence class of Kip[n]. The other properties are also exactly same as Kip[n].

Example 9: $\mathcal{A}$ = {t = "(", r = ")", @, c, x} is a KRA [5] alphabet = $\mathcal{B}$ = {"(", x, @, c, ")"} TASIM alphabet. If alphabet $\mathcal{B}$ of TASIM is substituted by alphabet $\mathcal{A}$ then the formal language L obtained by this substitution on $\mathcal{A}$ is called a TASIM genetic language.

DTS-18: TA antenna system

TA = TA[n] = "$_0$t $_1$t …$_k$t…$_{n-2}$t $_{n-1}$t" construction is called a T genetic, communication partner antenna system. It is designed for communicating in formal language L [K, G] on the alphabet of K = K[n] = Kip[n] for communicating in n different channels. The tic elements of TA = TA[n] is realized by an "IDC: Image Dress Code" of 0011. Observe that the tic elements of TA = TA[n] is countable in the RC-FRCC[n].

DTS-19: RA antenna system

RA = RA[n] = "r_{n-1} r_{n-2} … r_k… r_1 r_0" KBO construction is called a T genetic, communication partner antenna system. It is designed for communicating in formal language on the alphabet of K = K[n] = Kip[n] for communicating L[K, G] in n different channels. The tic elements of RA = RA[n] is realized by an IDC of 0011. Observe that the tic elements of RA = RA[n] is countable in the RC-BRCC[n].

DTS-20: TASIM genetic Q swarm memory

1) "c" is a tic constant representation. This tic constant c can be a tic KBO of tic KBOs. It is realized by an IDC of 0010.

2) "x" or "y" is a tic variable representation. Each x or y can be a tic KBO of KBOs. Both are realized by an IDC of 0010.

3) R = R[n] = "$_0$t $_1$t …$_k$t…$_{n-2}$t $_{n-1}$t x" KBO construction is called a **rator R** controlled by controlling variable x. Where, x has a capacity to sense, receive and transmit any tic information coded into any signal "k" while k □ Kip[n].

4) "@cr_k" is a united tic that it is constructed from 3 different tics of tic @, tic c and tic r. They are realized by a common IDC = 0011. Where, @$_k$ c_k r_k = @cr_k. This construction is solely called as a c-union. A c-union uses only one leg component in this article. Where, they are appearing to share one leg together.

5) CR = CR[n] = " "@cr_k" "kip-n" = " "@cr_{n-1}" "@cr_{n-2}" … "@cr_k" … "@cr_1" "@cr_0" " KBO construction is called a **rand CR**. Where, each tic c has a capacity to sense, receive and transmit any tic information coded into any signal "k" sent by x using a signal carrier k □ K = K[n] = Kip[n] to r_k.

6) Q = Q[x, n] = "$_0$t $_1$t … $_k$t… $_{n-2}$t $_{n-1}$t x @cr_{n-1} @cr_{n-2}… @cr_k…@cr_1 @cr_0" KBO construction is a **swarm memory**. It is shortly represented in this paper by Q = P_1 Q. Observe that the pair of antennas of Q is countable in a RC-RMCC[n].

DTS-21: TASIM genetic smooth complex Q swarm memory

Q = Q[<x, y>, <n, <n x n>>] = "$_0t\ _1t$ … $_kt$… $_{n-2}t$ $_{n-1}t$ x @ "$_0t\ _1t$ … $_kt$… $_{n-2}t$ $_{n-1}t$ y @cr_{n-1} @cr_{n-2}… @cr_k…@cr_1 @cr_0" r_{n-1} @ "$_0t\ _1t$ … $_kt$… $_{n-2}t$ $_{n-1}t$ y @cr_{n-1} @cr^{n-2}… @cr_k…@cr_1 @cr_0" r_{n-2}… @ "$_0t\ _1t$ … $_kt$… $_{n-2}t$ $_{n-1}t$ y @cr_{n-1} @cr_{n-2}… @cr_k…@cr_1 @cr_0" r_k…@ "$_0t\ _1t$ … $_kt$… $_{n-2}t$ $_{n-1}t$ y @cr_{n-1} @cr_{n-2}… @cr_k…@cr_1 @cr_0" r_1 @ "$_0t\ _1t$ … $_kt$… $_{n-2}t$ $_{n-1}t$ y @cr_{n-1} @cr_{n-2}…@cr_k…@cr_1 @cr_0" r_0" KBO construction is a **smooth complex swarm memory**. It is shortly represented in this paper by Q = P_2 Q. Observe that the antennas appearing in Q is countable in the SCRMCC [n, <n × n>].

DTS-22: TASIM genetic mixed complex Q swarm memory

Q = Q[<x, y>, <m, <n_0, n_1, …, n_k, …, n_{m-2}, n_{m-1}>>] = "$_0t\ _1t$… $_kt$… $_{m-2}t$ $_{m-1}t$ x @"$_0t\ _1t$ … $_kt$… $_{<n0>-2}t$ $_{<n0>-1}t$ y @$cr_{<n0>-1}$ @$cr_{<n0>-2}$… @cr_k…@cr_1 @cr_0" r_{m-1} @"$_0t\ _1t$… $_kt$… $_{<n1>-2}t$ $_{<n1>-1}t$ y @$cr_{<n1>-1}$ @$cr_{<n1>-2}$… @cr_k…@cr_1 @cr_0"r_{m-2} … @"$_0t\ _1t$ … $_kt$… $_{<nk>-2}t$ $_{<n2>-1}t$ y @$cr_{<nk>-1}$ @$cr_{<nk>-2}$… @cr_k…@cr_1 @cr_0" r_k…@"$_0t\ _1t$ … $_kt$… $_{<nm-2>-2}t$ $_{<nm-2>-1}t$ y @$cr_{<nm-2>-1}$ @$cr_{<nm-2>-2}$… @cr_k…@cr_1 @cr_0" r_1 @"$_0t\ _1t$ … $_kt$… $_{<nm-1>-2}t$ $_{<nm-1>-1}t$ y @$cr_{<nm-1>-1}$ @$cr_{<nm-1>-2}$… @cr_k…@cr_1 @cr_0"r_0" KBO construction is a **mixed complex swarm memory**. It is shortly represented in this paper by Q = P_2 Q.

Observe that the antennas appearing in Q is countable in the MCRMCC [<m, n = < n_0, n_1,… n_k … n_{m-2}, n_{m-1}>>]. Remember that:

Q = Q[x, m] = "$_0t\ _1t$ … $_kt$…$_{m-2}t$ $_{m-1}t$ x @cr_{m-1} @cr_{m-2}… @cr_k…@cr_1 @cr_0",

Q = Q[y, n_0] = "$_0t\ _1t$… $_kt$…$_{<n0>-2}t$ $_{<n0>-1}t$ y @$cr_{<n0>-1}$ @$cr_{<n0>-2}$… @cr_k…@cr_1 @cr_0",

Q = Q[y, n_1] = "$_0t\ _1t$ … $_kt$…$_{<n1>-2}t$ $_{<n1>-1}t$ y @$cr_{<n1>-1}$ @$cr_{<n1>-2}$… @cr_k…@cr_1 @cr_0",

…

Q = Q[y, n_k] = "$_0t\ _1t$ … $_kt$…$_{<nk>-2}t$ $_{<n2>-1}t$ y @$cr_{<nk>-1}$ @$cr_{<nk>-2}$… @cr_k…@cr_1 @cr_0",

…

Q = Q[y, n_{m-2}] = "$_0t\ _1t$ … $_kt$… $_{<nm-2>-2}t$ $_{<nm-2>-1}t$ y @$cr_{<nm-2>-1}$ @$cr_{<n0>-2}$… @cr_k…@cr_1 @cr_0" and

Q = Q[y, n_{m-1}] = "$_0t\ _1t$ … $_kt$… $_{<nm-1>-2}t$ $_{<nm-1>-1}t$ y @$cr_{<nm-1>-1}$ @$cr_{<nm-1>-2}$… @cr_k…@cr_1 @cr_0". They are used as sub structures in the construction of Q = Q[<x, y>, <m, <n_0, n_1… n_k… n_{m-2}, n_{m-1}>>].

Observe also that the antennas appearing in Q is countable in the MCRMCC [<m, n = <n_0, n_1, n_2 … n_{m-1}>].

DTS-23: Examples

Example 10: In a communicating T genetic Q swarm memory constructing Environment:

1) Q = Q[x, 4] = "$_0t\ _1t\ _2t\ _3t$ x @cr_3@cr_2@cr_1@cr_0" is a swarm memory construction. Its communicating t: tamra and r: ramta antennas are counted in RC-RMCC [4] in this construction.

2) Q = Q[y, 5] = "$_0t\ _1t\ _2t\ _3t\ _4t$ y @cr_4@cr_3@cr_2@cr_1@cr_0" is a swarm memory construction. Its communicating t: tamra and r: ramta antennas are counted in RC-RMCC [5] in this construction.

3) Q = Q[y, 8] = "$_0t\ _1t\ _2t\ _3t\ _4t\ _5t\ _6t\ _7t$ y @cr_7@cr_6@cr_5 @cr_4@cr_3@cr_2@cr_1@cr_0" is a swarm memory construction. Its communicating t: tamra and r: ramta antennas are counted in RC-RMCC [8] in this construction.

4) Q = Q[x, 3] = "$_0t\ _1t\ _2t$ x @cr_2@cr_1@cr_0" is a swarm memory construction. Its communicating t: tamra and r: ramta antennas are counted in RC-RMCC [3] in this construction.

5) Q = Q[y, 2] = "$_0t\ _1t$ y @cr_1@cr_0" is a swarm memory construction. Its communicating t: tamra and r: ramta antennas are counted in RC-RMCC [2] in this construction.

DTS-24: Examples

Example 11: In a communicating T genetic Q swarm memory constructing Environment:

1) Q = Q[y, 3] = "$_0t\ _1t\ _2t$ y @cr_2@cr_1@cr_0" is a swarm memory construction. Its communicating t: tamra and r: ramta antennas are counted in RC-RMCC [3] in this construction.

2) Q = Q[<x, y>, <4, <2, 2, 2, 2>>] = "$_0t\ _1t\ _2t\ _3t$ x @"$_0t\ _1t$ y @cr_1@cr_0" r_3@"$_0t\ _1t$ y @cr_1@cr_0" r_2@"$_0t\ _1t$ y @cr_1@cr_0" r_1@"$_0t\ _1t$ y @cr_1@cr_0" r_0" is a swarm memory construction. Its communicating t: tamra and r: ramta antennas are counted in SCRMCC [4, <2, 2, 2, 2>] in this construction.

3) Q = Q[<x, y>, <3, <3, 3, 3>>] = "$_0t\ _1t\ _2t$ x @"$_0t\ _1t\ _2t$ y @cr_2@cr_1@cr_0" r_2@"$_0t\ _1t\ _2t$ y @cr_2@cr_1@cr_0" r_1@"$_0t\ _1t\ _2t$ y @cr_2@cr_1@cr_0" r_0" is a swarm memory construction. Its communicating t: tamra and r: ramta antennas are counted in SCRMCC [3, <3, 3, 3>] in this construction.

4) Q = Q[<x, y>, <4, <5, 8, 8, 3>>] ="$_0t\ _1t\ _2t\ _3t$ x @"$_0t\ _1t\ _2t\ _3t\ _4t$ y @cr_4@cr_3@cr_2@cr_1@cr_0" r_3@"$_0t\ _1t\ _2t\ _3t\ _4t\ _5t\ _6t\ _7t$ y @cr_7@cr_6@cr_5 @cr_4@cr_3@cr_2@cr_1@cr_0" r_2@"$_0t\ _1t\ _2t\ _3t\ _4t\ _5t\ _6t\ _7t$ y @cr_7@cr_6@cr_5 @cr_4@cr_3@cr_2@cr_1@cr_0" r_1@"$_0t\ _1t\ _2t$ y @cr_2@cr_1@cr_0" r_0" is a swarm memory construction. Its communicating t: tamra and r: ramta antennas are counted in MCRMCC [<4, <5, 8, 8, 3>>] in this construction.

5) Q = Q[<x, y>, <3, <2, 3, 5>>] = "$_0t\ _1t\ _2t$ x @"$_0t\ _1t$ y @cr_1@cr_0" r_2@"$_0t\ _1t\ _2t$ y @cr_2@cr_1@cr_0" r_1@"$_0t\ _1t\ _2t\ _3t\ _4t$ y @cr_4@cr_3@cr_2@cr_1@cr_0" r_0" is a swarm memory construction. Its communicating t: tamra and r: ramta antennas are counted in MCRMCC [<3, <2, 3, 5 >>] in this construction.

IV. RESULT AND SUGGESTION

The notion of cycle counting for marking the same frequencies on a pair of tamra and ramta antennas appearing in Q of Q^+ has been studied. It is found that:

(a) Q = P_1 Q with property P_1 = <C, T; K_n, x, n; 4B ∈ IDC: *> Q can use FRCC [x, n], BRCC[x, n], FBRCC[x, n] and RMCC[x, n] cycle counting systems for marking the pair of tamra and ramta antenna systems being in the communication with each other while information processing taking place in a Q of Q^+.

(b) Q = P_2 Q with property P_2 = <C, T; <K_m, K_n >, <x, y>, <m, <n_0, n_1, …, n_k, …, n_{m-2}, n_{m-1}>>; 4B ∈ IDC>Q can use SCRMCC [<x, y>, <n, <n, n, …, n>>] and MCRMCC [<x, y>, <m, <n_0, n_1, …, n_k, …, n_{m-2}, n_{m-1}>>]

cycle counting systems for marking the pair of tamra and ramta antenna systems being in communication with each other while information processing taking place in a Q of Q^+. Therefore this paper is written for reporting and introducing the new found cycle counting processes to mark proper frequencies to be used by the communicating antenna resource elements while an information processing taking place in an I@I of $I@I^+$ swarm internet "+"closure generating Q of Q^+ swarm memory "+" closure communicating in every K = [n] = Kip[n]. The author is declaring that this internet closure is a securely communicating universal internet closure.

REFERENCES

[01] F. Ünlü: CITALOG: Compact and Integrated Tasim Logic Closure, *Journal of King Abdulaziz University, Science, Vol. 2 pp 117-136, Jeddah, 1990.*

[02] F. Ünlü: FTD Grammar Graph, *International Journal of Computer Mathematics,* 2003, Vol. 80(1) pp1-9.

[03] F. Ünlü: us-Crop Based Compact Memory, *International Journal of Contemporary Mathematical Science, Volume 1, No. 5-8, pp 317-325, 2006.*

[04] F. Ünlü: A Remote Programming Technology on a Remote VDM Clustering in λ-Calculus, *International Mathematical Form, Vol. 1, No. 13-16, pp 671 - 685, 2006* .

[05] F. Ünlü: Plemvanal: A Communicating Commuting Mathematics Generator Type, *International Mathematical Form, Vol. 1, No. 13-16, pp 671 – 685, 2006* .

[06] F. Ünlü: T-genetic RCR-U Form, *INISTA 2010, ID 16, pp 1-5, Kayseri, Turkey, 2010.*

[07] F. Ünlü: Biçimsel TASIM Dilbilimi, AYSU 2010, ID 5, pp 1-5, Kayseri, 2010.

[08] F. Ünlü: A Formel Property Dependent United Business System Design and Programming, ICBME 7-9 October 2010 e-Proceeding, Yasar University, Izmir, Turkey.

[09] F. Ünlü: Bildirişimli Matematik, 9. Matematik Sempozyumu, 20-22 Ekim 2010 Karadeniz Teknik Üniversitesi, Trabzon.

[10] F. Ünlü: Q ve Q^+ Sürü Bellekli I@I Modeli Tasarımında Kullanılan T Genetik Altyapı Elamanları, *XVI. Türkiye 'de İnternet Konferansı. Bildiri No. 3, 30 Kasım-2 Aralık 2011, Ege Universitesi, İzmir.*

[11] F. Ünlü: Bildirişimli Matematiğin <T<x>, 1, n> Q Sürü Bellekli 3D I@I İnternet Sürüsü. *XVI. Türkiye'de İnternet Konferansı. Bildiri No. 4, 30 Kasım -2 Aralık 2011, Ege Universitesi, İzmir.*

[12] P. Linz, *Introduction to Formal Languages and Automata,* Fourth Edition, Jones and Bartlett Publishers, London, 2006.

[13] R. L. Causey, *Logic, Sets, and Recursion,* Second Edition, Jones and Bartlett Publishers, Inc., London, 2006.

[14] W. Lark, *LISP 1.5 Primer,* Dickenson Publishing Inc. California, 1968.

Metin ve Grafiksel Öğeleri Birleştiren Yeni bir Parola Tabanlı Kimlik Doğrulama Yöntemi

Murat AKPULAT, Kemal BIÇAKCI, Uğur ÇİL

Özet— **Günümüzde en yaygın kullanılan kimlik doğrulama yöntemi şifre (parola) tabanlı olanlardır. Son yıllarda pek çok grafiksel parola yöntemleri geliştirilmiş fakat bu yöntemler pratikte henüz klasik metin parolaların yerini alamamıştır. Bu çalışmada hem metin hem grafiksel öğeler içeren melez bir parola tabanlı kimlik doğrulama yöntemi önermekteyiz. Yaptığımız deneysel çalışma Yaz&Tıkla ismini verdiğimiz yeni yöntemin hem uzun dönem hatırlanabilirlik hem de kullanıcı memnuniyeti açısından sadece metin ve sadece grafik tabanlı parola yöntemlerine oranla daha başarılı olduğunu göstermektedir.**

Anahtar Kelimeler—**Kullanışlı Güvenlik, Grafik Şifre, Resim Şifre, Parola, Kimlik Doğrulama.**

Abstact— **Today, the most widely used authentication methods are password based. In recent years, many graphical password methods have been developed but these methods could not replace traditional text passwords, yet. In this work, we propose a hybrid method called Type&Click which incorporates both text and graphical elements. We conduct a usability study which shows that with respect to long-term memorability and user satisfaction, Type&Click is more successful as compared to only-text and only-graphical password methods.**

Keywords—**Usable Security, Graphical Password, Password, Authentication**

I. GİRİŞ

METİN tabanlı klasik parola (şifre) en iyi bilinen ve en yaygın kullanılan kimlik doğrulama yöntemidir. Kullanıcılar şifrelerini genelde kolay hatırlayabilecekleri şekilde belirlerler (doğum tarihi, memleketi, tuttuğu takımı ya da bir arkadaşının ismi gibi). Hatırlanması kolay şifreler saldırganlar için de kırılması kolay şifrelerdir. Diğer taraftan rastgele karakterlerden oluşturulmuş ve belli sayıda karakter içeren (en az 8 karakter gibi) şifreler, güçlü ve kırılması daha zor şifrelerdir. Ancak bu şekilde belirlenen şifreler, hatırlanması zor olduğu için kullanıcılar tarafından çok da tercih edilmezler. Bazı sistemler bu tür güçlü şifrelerin kullanılmasını zorunlu kılmıştır. Fakat bu durumda da kullanıcılar kurallara uygun olarak belirledikleri güçlü şifreleri bir yere not ederek kullanırlar ve bu durum ayrı bir güvenlik tehlikesi olarak karşımıza çıkar.

Yukarıda kısaca bir örnek vererek bahsettiğimiz güvenlik-kullanışlılık kısır döngüsünü kırmak tahmin edilenin ötesinde zor bir problemdir. Güvenlik sistemlerini bir bütün olarak düşünecek olursak; içinde barındırdığı süreçler, kurallar, algoritmalar, protokoller ve donanımsal faktörlerle birlikte, unutulmaması gereken bir diğer faktör de kullanıcıdır. Arka planda alınan bir dizi güvenlik önlemi, kullanıcının belirlediği tahmin edilmesi kolay bir şifreyle bütün değerini kaybedebilir. Bu noktada sistemlerin ihtiyacı güvenliğin kullanışlı olmasıdır. Önceki bir çalışmada [1] kullanışlı güvenliğin tanımı şu şekilde yapılmıştır:

"Bir (güvenlik) yazılımı (donanımı, sistemi); o yazılımı kullanması beklenilen kişilerce

- *Güvenilir ve gerekli bulunuyorsa,*
- *Yapılması gerekenler doğru bir şekilde anlaşılıyor ve güvenli bir şekilde yapılabiliyorsa,*
- *Devamlı kullanımda yeteri kadar rahat ve sorunsuz kullanılabiliyorsa,*

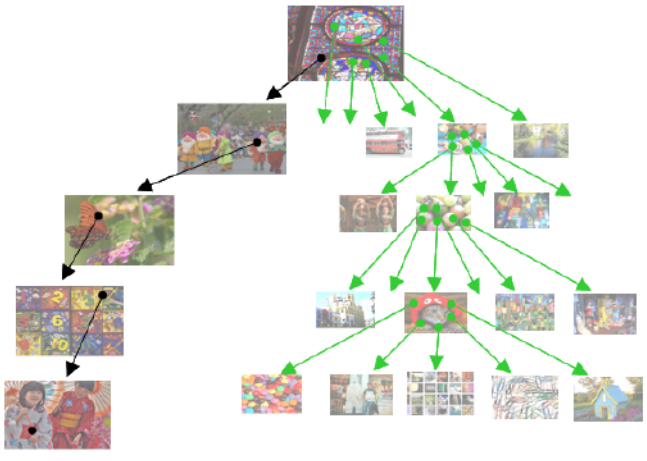
bu yazılım (donanım, sistem) Kullanışlı Güvenlik (usable security) özelliğine sahiptir."

İnsan beyninin resimleri hatırlayabilmesinin metinlere oranla daha kolay olduğunu ortaya koyan çalışmalar [2] sonrasında başlatılmış ve metin tabanlı yöntemlere alternatif sunmayı hedefleyen grafiksel yöntemler konusunu 'kullanışlı güvenlik' bağlamında incelemek gerekir. Daha açık ifadeyle, yeni yöntemlerin tercih edilmesi için metin tabanlı parola yöntemine göre belirgin kullanışlılık ve/veya güvenlik avantajlarına sahip olmaları şarttır. Fakat önceki çalışmaları incelediğimizde neredeyse tamamının yapmış oldukları deneysel değerlendirmelerde (hatırlanabilirlik, giriş süresi, vb. metrikleri kullanarak) önceki benzer grafiksel yöntemler ile karşılaştırmalarda bulunmuş oldukları görülmektedir [3]. Bu hususta bir istisna araştırmacıların PCCP sistemini [4] değerlendirirken Passpoints sisteminin yanı sıra metin tabanlı şifreler ile de yapmış oldukları karşılaştırmadır. Bizim bu çalışmamızı önceki pek çok çalışmadan ayıran birinci fark deneysel karşılaştırma için klasik metin tabanlı şifrelerin seçilmesi ve böylece daha gerçekçi ve yönlendirici sonuçların ortaya konulmasına çalışılmış olunmasıdır.

M. Akpulat, Gümüşhane Üniv., Kelkit Aydın Doğan M.Y.O., Bilgisayar Teknolojileri Bölümü, Okutman ve TOBB Ekonomi ve Teknoloji Üniversitesi, Bilgisayar Mühendisliği Bölümü, Yüksek Lisans Öğrencisi. (telefon: 90-456-3173992, faks: 90-456-3173993, e-posta: muratakpulat@gumushane.edu.tr).

K. Bıçakcı, TOBB Ekonomi ve Teknoloji Üniversitesi, Bilgisayar Mühendisliği Bölümü, Doç. Dr. (telefon: 90-312-2924262, faks: 90-312-2924180, e-posta: bicakci@etu.edu.tr).

U. Çil, TOBB Ekonomi ve Teknoloji Üniversitesi, Bilgisayar Mühendisliği Bölümü, Yüksek Lisans Öğrencisi, e-posta: ucil@etu.edu.tr.



Şekil 1. CCP ve PCCP yöntemlerinin çalışma prensibi [3] (tıklanılan noktaya bağlı olarak bir sonraki resim belirlenir).

Çalışmamızın konu literatürüne ikinci ve daha önemli bir katkısı metin ve grafiksel öğeleri birleştiren bir şifre yönteminin ilk defa deneysel olarak incelenmesi ve hem metin tabanlı hem de grafik tabanlı şifre yöntemleri ile karşılaştırılmasıdır (benzer bir melez yöntem daha önce önerilmiş, fakat deneysel olarak incelenmemiştir [5]). Bu makalede, tarafımızca geliştirilen Yaz&Tıkla (Type&Click) ismini verdiğimiz melez kimlik doğrulama yönteminin tasarım aşamaları, deney süreci ve değerlendirme sonuçları sunulmaktadır. Deney sonuçları ışığında Yaz&Tıkla yönteminin mevcut metin tabanlı parola yöntemlerine kullanışlı bir alternatif sunduğunu söyleyebiliriz.

Çalışmamızın ikinci bölümünde literatür özetine yer verilmiş ve grafik şifre sistemlerinin bazı özelliklerinden bahsedilmiştir. Bölüm 3'de karşılaştırılacak yöntemlerin teknik incelemesi yapılmıştır. Bölüm 4'de geliştirdiğimiz yöntemi karşılaştırabilmek için kullanılan deneysel metodoloji tanıtılmıştır. Bölüm 5'de deney sonrası elde edilen veriler sunulmuş ve yorumlanmıştır. Son olarak bölüm 6'da yapılan çalışmadan elde edilen sonuçlar özetlenmiştir.

II. LİTERATÜR ÖZETİ

Bilgi-tabanlı (veya parola-tabanlı) kimlik doğrulama (knowledge-based authentication) şu mantığa dayanır: Kişilerle sistem arasında gizli bir bilgi sır olarak paylaşılmaktadır ve sistem bu bilgiyi doğru olarak sağlayabilen kişinin, o kişinin kendisi olduğunu kabul ederek gerekli yetkilendirmeyi yapmaktadır. Burada bahsedilen gizli bilgi farklı şekillerde karşımıza çıkabilir. Örneğin kullanıcının ezberlediği ve biliyor olması gereken bir bilgi veya kullanıcının ezberlemesi gerekmeyen ancak gördüğünde tanıması gereken bir bilgi gibi.

Bilgi-tabanlı kimlik tanımlama yöntemleri iki başlık altında incelenebilir.

A. *Metin Tabanlı Şifre Yöntemleri*

Metin tabanlı şifreler güvenlik zaafları ve bazı kullanım problemlerine rağmen halen yaygın bir şekilde kullanılan kimlik doğrulama yöntemidir. Yapılan bir çalışma İngiltere'deki firmaların %93'ünün personel ve müşterileri için metin tabanlı şifreleme yöntemini kullandığını ve her kullanıcının ortalama 3 farklı kullanıcı adı-şifre çiftini ezberlemek zorunda olduğunu ortaya koymuştur. İnternet kullanıcılarının bir diğer problemi de güvenlik sebebiyle farklı sistemler için farklı parolalar oluşturmak zorunda olmalarıdır. Yapılan bir araştırma İnternet kullanıcılarından sadece %19'unun her sitede farklı şifre kullandığı gerçeğini göstermiştir.

Kullanıcıların birçok sitede kullandıkları farklı kullanıcı adı ve şifreleri güvenli bir şekilde saklayabilen ve ihtiyaç olduğunda sunabilen, aynı zamanda kullanıcıdan aldıkları bilgileri o site için güvenli birer şifre haline getirip kullanıcıya sunan şifre yöneticisi yazılımları kullanışlılık problemine kısmen çözüm sunan sistemlerdir. Ayrıca bazı bellenir (mnemonic) kelime hafıza teknikleri de şifre hatırlamada yardımcı olarak önerilmiştir [6].

B. *Grafik Tabanlı Şifre Yöntemleri*

Grafik şifreler, bazı grafiksel öğeler üzerinde yapılan işaretlemeleri, resimdeki herhangi bir noktayı ya da daha önce gördüğü bir resmi tekrar hatırlayabilmeyi paylaşılan gizli bilgi olarak kullanıp yetkilendirme yapabilen sistemlerdir.

"*Bir fotoğraf bin sözcüğe bedeldir*" genel kabul görmüş bir prensiptir. Yapılan bilişsel psikoloji çalışmaları insan hafızasının sözel ifadelerden çok görsel bilgileri daha kolay hatırlayabildiğini ya da tanıyabildiğini göstermiştir [2]. Grafik tabanlı sistemler kullanıcının daha kolay hatırlayabileceği görsel öğeleri kullanarak farklı bir yaklaşım getirmişlerdir.

Bazı grafik şifreleme sistemlerinde kullanıcının bir resim kümesi içinden seçtiği bazı resimleri sistem girişi sırasında tekrar tanıması beklenir. PassFaces yöntemi kullanıcıdan yüz resimlerinin olduğu bir kümeden 4 tanesini seçmesini ister. Kullanıcının şifresi bu 4 yüz resmidir ve 4 aşamada şifresini sisteme girer. Her bir aşamada 8 çeldirici resim ve 1 de kullanıcının seçtiği yüz resimlerinden bir tanesi bulunur [3].

Grafik kimlik doğrulama sistemlerinin bazılarında ise bir büyük resmin belli bir bölgesinde yapılan tıklamanın belli bir tolerans aralığında yeniden yapılması beklenir. Grafik şifreleme yöntemlerinden PassPoints bu mantıkla çalışır [3]. Sistem kullanıcıya bir resim gösterir ve kullanıcı resimde 5 farklı noktaya tıklayarak şifresini oluşturur. Kullanıcı ne zaman sisteme giriş yapacak olsa belli tolerans aralıkları dahilinde aynı resimde aynı noktalara tıklayarak sisteme giriş yapabilir.

Passpoints sistemini daha da geliştiren Cued Click Points (CCP) yönteminde ise kullanıcıya bir resim gösterilir ve bir noktayı tıklaması istenir [3]. Sistem kullanıcının tıkladığı noktaya göre farklı bir resim gösterir ve kullanıcı şifresinin ikinci elemanını bu farklı resimdeki bir noktaya tıklayarak girer. Bu şekilde tıklanılan noktaya göre gelen farklı resimlerde toplam 5 tıklama işlemiyle kullanıcı şifresini belirlemiş olur. Her bir resim bir önceki resimde tıklanılan noktaya göre seçildiği için kullanıcı resimlere tıklarken karşılaştığı resimlerden çıkarım yaparak şifresini doğru girip girmediğini kontrol edebilir. Gösterilen her bir resim kullanıcıya ipucu olur.

PCCP yöntemi, CCP ve Passpoints sistemlerinde gözlemlenen sıcak nokta problemini çözme adına önerilmiştir [4]. Sıcak noktalar, kullanıcının resim üzerinde tıklama ihtimalinin yüksek olduğu noktalardır. Tıklanması tahmin edilebilir bir nokta güvenlik açığı olarak düşünülebilir. PCCP, İkna Teknolojisinden (Persuasive Technology) yararlanmıştır. Kullanıcı bu yöntemde resim üzerinde istediği noktaya değil de sistemin kendisine sunduğu resim üzerindeki görüntü kapısı (viewport) içinden herhangi bir noktaya tıklayabilir. Ancak kullanıcı isterse görüntü kapısının tekrar oluşturulmasını isteyebilir ama yeni görüntü kapısı yine resim üzerindeki rastgele bir konumdadır. Bu sistem kullanıcıyı daha güçlü şifre belirlemeye teşvik eder (Şekil 2'de gösterilen Yaz&Tıkla yönteminde de görüntü kapısı kullanılmaktadır).

Bu makalede karşılaştırılacak PCCP ve Yaz&Tıkla yöntemlerinde görüntü kapısı kullanılacaktır. Resim 451x331 piksel çözünürlükte ve görüntü kapısı 75x75 piksel büyüklüğündedir (Şekil 2). Diğer teknik özellikler üçüncü bölümde anlatılacaktır.

C. Şifre Uzayı ve Entropi

Şifre uzayı, oluşturulması mümkün olan bütün şifrelerin kümesini oluşturur. Metin tabanlı şifrelerde 8 karakterli bir şifrenin içerisinde kullanılabilecek 26 küçük harf, 26 büyük harf, 10 rakam ve 32 özel karakter olduğunu varsayarsak, 94 farklı ASCII karakterden oluşturulabilecek şifre sayısı teorik olarak 94^8 olur. Ancak kullanıcılar kolay hatırlayabilmeleri için şifrelerinde rakam ya da özel karakteri kullanmak istemezler ya da rastgele karakterler yerine anlamlı sözcükler tercih ederler. Dolayısıyla teoride mümkün olan şifre uzayına pratikte erişilemez [7]. Benzer durum sıcak nokta probleminden ötürü grafik tabanlı şifrelerde de söz konusu olabilir [3]. Fakat PCCP yönteminde sıcak nokta probleminin ihmal edilebilir seviyelerde kaldığı gözlemlenmiştir [4].

Belirsizliğin bir ölçütü olarak tanımlanan entropi, bilgi kuramında bilginin belirsizliği anlamına gelir. Şifreler bağlamında ise, belirlenen şifrenin belirsizliği ve dolayısıyla şifrenin gücünü nicel olarak ifade eden bir ölçüttür [7]. Entropi değeri yukarıdaki örnekte yaklaşık $\log_2(94^8) = 52,4$ bittir.

III. KARŞILAŞTIRALACAK YÖNTEMLER

Bu çalışmada üç farklı kimlik doğrulama yöntemi deneysel olarak karşılaştırılmaktadır. Bu yöntemlerden birincisi metin tabanlı şifre yöntemi, ikincisi grafik tabanlı PCCP yöntemi ve üçüncüsü tarafımızca geliştirilen Yaz&Tıkla adlı melez şifre yöntemidir.

Kimlik tanıma yöntemleri arasında anlamlı bir karşılaştırma yapılabilmesi için her bir yöntem ile oluşturulacak şifrenin sağladığı güvenliğin eşit seviyede (eşit entropi değerine sahip) olması gerekir. Ayrıca kullanıcı her üç yöntemde de benzer aşamalardan geçerek şifresini oluşturmalıdır. Karşılaştırılan üç yöntemde de kullanıcılar sırasıyla,

- İsim-soyisim girip, kullanıcı adı belirler.
- Şifresini belirler.
- Belirlediği şifresini tekrar girerek şifresini doğrular.



Şekil 2. Yaz&Tıkla yöntemi şifre-giriş kullanıcı arayüzü (kullanıcı, metin şifresi ile ve görüntü kapısı içerisinde yapmış olduğu bir tıklama ile parolasını oluşturur).

Bu üç aşamayı da başarıyla gerçekleştiren kullanıcı ilgili yöntem ile kendine ait bir hesap oluşturmuş olur.

Aşağıda her alt bölümde yöntemlerin teknik özellikleri açıklanacaktır. Tüm yöntemler Java programlama dilinde masaüstü programlar olarak yazılmıştır.

A. Metin Tabanlı Şifre Yöntemi

Bu yöntem şifrenin sadece klavyeden girilen karakterler ile belirlenmesi prensibine dayanır. Kullanıcıdan şifresinde en az 14 karakter bulundurması istenmektedir. Bu tercihin sebebi 14 karakterden oluşan ve içinde herhangi bir özel karakter bulundurma zorunluluğu olmayan şifrenin entropi değerinin yaklaşık olarak 27 bit olarak tahmin edilmesidir [7] (diğer iki yöntemde de belirlenen şifreler aynı entropi değerine sahiptir).

B. PCCP

PCCP'de kullanıcı art arda gelen resimler üzerinde birer kez tıklayarak şifresini oluşturur (Şekil 1). 451x331 piksel büyüklüğündeki resim üzerinde bulunan 75x75 piksel büyüklüğündeki görüntü kapısı (viewport) içinde kalan kısımdan bir yere tıklayarak parolasının her bir bileşeni oluşturulur. Kullanıcı "Değiştir" düğmesine basarak isterse görüntü kapısının yerini değiştirebilir. Deneyde kullandığımız PCCP uygulamasında kullanıcıların 3 resim üzerinde tıklama yapması gerekmektedir. Eğer kullanıcı daha önceki adımlarda seçmiş olduğu resim ve/veya noktalardan vazgeçmek isterse "Baştan Başla" düğmesine basarak parola oluşturmaya tekrar baştan başlayabilir.

Şifre doğrulaması için kullanıcıdan bir önceki adımda oluşturduğu şifresini tekrar girmeleri istenecektir. Fakat bu sefer resimlerin üzerinde görüntü kapısı olmayacaktır. Kullanıcı şifre oluşturma aşamasında belirlediği noktalara tekrar tıklamak zorundadır. Eğer tıkladığı nokta bir önceki adımda şifresini oluştururken tıkladığı noktanın 19x19 piksellik bir tolerans aralığında değil ise karşısına şifre oluştururken kullandığı resimden farklı bir resim gelecektir. Bu durumda kullanıcının yanlış yere tıkladığını fark etmesi

beklenir. Kullanıcı isterse "Önceki Resim" düğmesine basarak bir önceki resme dönebilir ya da "Baştan Başla" düğmesine basarak şifresini doğrulamaya en baştan başlayabilir.

451x331 piksel resim boyutu, 19x19 piksel tolerans değeri ve 3 tıklama işlemiyle oluşturulan şifrenin entropi değeri aşağıdaki formülle bulunabilir.

$$[\frac{451x331}{19^2}]^3 \cong 2^{27} \quad (1)$$

Bu sonuca göre PCCP yönteminden de oluşan şifrenin entropi değeri 27 bit'tir.

C. Yaz&Tıkla Şifre Yöntemi

Tarafımızca geliştirilen bu yöntemde kullanıcının belirlediği metin tabanlı şifresine ek olarak bu şifreye bağıntılı olarak karşısına gelen bir resimde tek bir noktaya tıklaması istenir.

Kullanıcı şifresini belirleyebilmek için şifre oluşturma sayfasına gelir. Bu sayfada kullanıcının şifresinin ilk kısmını oluşturabilmesi için bir metin giriş alanı ve girilen şifreye bağlı olarak dinamik olarak değişen bir resim vardır.

Kullanıcı metin giriş kısmına en az 8 karakterlik bir şifre girer. Belirlenen bu şifreye göre sistem kullanıcıya bir resim (451x331) gösterir ve resimde görüntü kapısı sınırları (75x75) içinde olmak koşulu ile bir tek noktaya tıklanması istenir (Şekil 2). Sistem görüntü kapısının haricinde tıklanılan noktayı şifre olarak kabul etmez. Ancak PCCP' ye benzer şekilde "Değiştir" düğmesiyle kullanıcı eğer isterse bu sınırın yerini sistemin atadığı rastgele başka bir yere taşıyabilir. Kullanıcı tıklama işlemini gerçekleştirdikten sonra resmin artık tıklanılamaz olduğunu görür, artık şifrenin iki kısmı da belirlenmiştir. Ancak kullanıcı herhangi bir değişiklik yapmak istediğinde "Baştan Başla" düğmesine tıklayarak resmi tekrar aktif hale getirebilir, tıklanılan nokta ve şifrenin metin kısmında istediği değişikliği gerçekleştirebilir. Şifresini belirleyen kullanıcı, "Parolamı Kaydet" düğmesine tıklayarak belirlediği şifreyi doğrulamak üzere bir sonraki aşamaya ulaşır.

Şifre kısmına girilen her bir karakterle dinamik olarak ekranda değişen resmin sisteme her giriş yapıldığında aynı şekilde gösterilmesini sağlayan algoritma şu şekilde çalışır:

1) Kullanıcı adı ve şifrenin metin kısmı MD5 özet algoritmasından geçirilerek 128 bit veri elde edilir.
2) Verinin ilk 10 biti alınır.
3) 10 bitlik veri onluk tamsayıya dönüştürülür.
4) Bu tamsayı kullanıcıya gösterilen resmin indeks numarasıdır.

Sistem kullanıcı adının birden fazla kullanılmasına izin vermediği için kullanıcıların belirlediği şifreler aynı olsa bile görüntülenen resim farklı olur. Bu işlem aşamaları her karakter girişinde tekrarlanır.

Şifre doğrulamada kullanıcıdan belirlediği şifrenin metin ve tıklama aşamalarını doğru bir şekilde tekrarlaması istenir. Kullanıcı metin kısmına girdiği aynı şifreyle beliren aynı resimde 19x19 piksellik tolerans aralığında daha önce tıkladığı noktaya tekrar tıklar. Doğrulamada resim üzerinde görüntü kapısı yoktur.

Şifrenin metin kısmı girilirken resmin dinamik olarak değişmesi kullanıcıya hemen o anda şifre doğrulama imkânı sunar. Kullanıcı eğer şifresini girdiğinde beklediği resimle karşılaşmazsa şifresini yanlış girdiğini anlayabilir. Yani resim kullanıcı için şifrenin her karakteri için bir ipucu olur (fakat söz konusu bu geri besleme başkaları için bir ipucu teşkil etmez). Çünkü kullanıcı şifrenin her karakterini sırasıyla girdiğinde sistemin gösterdiği resim sırası hep aynıdır. Böylece kullanıcı şifrenin hangi karakterinde hata yaptığını dahi anlayabilir.

Bu yöntemle oluşacak şifrelerin entropi değerleri metin ve resim kısımlarının entropi değerleri ayrı ayrı belirlenerek bulunabilir. Sadece en az sekiz karakter bulundurma zorunluluğu olan metin kısmın entropiye katkısı yaklaşık 18 bittir [7]. Resim üzerine tek tıklamayla elde edilen entropi değeri de yaklaşık 9 bittir. Böylece toplamda bu yöntemle oluşturulan şifrelerin entropi değeri de 27 bit olarak bulunur.

IV. METODOLOJİ

İlk olarak deneysel olarak test edilecek hipotezler belirlenmiştir. Bu hipotezler;

1) Yaz&Tıkla yöntemi ile belirlenen şifreler diğer iki yöntem ile belirlenen aynı güvenlik seviyesindeki şifrelere göre uzun vadede kullanıcılar tarafından daha iyi hatırlanacaktır.
2) Kullanıcılar Yaz&Tıkla yöntemi ile oluşturulan şifreleri diğerlerine nazaran daha güvenli ve daha kullanışlı olarak algılayacaktır (bir sistemin güvenli olması kadar kullanıcılar tarafından da güvenli bulunması o sistemin pratikte uygulanabilirliği açısından çok önemlidir).

Aşağıda, belirlenen hipotezleri test etmek için tasarlanan deneyde takip edilecek metodoloji kısaca tanıtılmaktadır.

Deneysel laboratuar çalışmamız Kelkit Aydın Doğan Meslek Yüksekokulu Bilgisayar Teknolojileri bölümü öğrencilerinden 39 kişinin katılımı ile gerçekleştirilmiştir. Kullanıcıların tamamı e-posta, alış-veriş, vb. şifre gerektiren siteleri aktif olarak kullanabilmektedirler.

Deney iki aşamadan oluşmaktadır. İlk aşamada kullanıcılar 6-7'li gruplar halinde laboratuara davet edilmişler ve sistem hakkında 5 dakika süresince aşağıdaki konularda bilgilendirilmişlerdir:

1) Deneyin amacı (hangi sistemin tarafımızca geliştirildiği açıklanmamıştır).
2) Sistemin doğru sonuçlar verebilmesi için daha önce kullanmadıkları ve ezberlerinde olmayan bir şifre kullanmaları,
3) Önemli bilgilerinin bulunduğu bir e-posta hesabının yada banka hesabının şifresini belirleyeceklerini düşünerek bu sistemi kullanmaları,
4) Belirledikleri şifreleri herhangi bir yere not etmemeleri,
5) Metin ve Yaz&Tıkla yöntemlerindeki şifrelerinin metin kısımlarının benzer olmaması gereği.

Daha sonra kullanıcılar yaklaşık 10 dakika boyunca programı denemiş ve kullanımına alışmışlardır.

Tablo 1
Test edilen üç yöntem için birinci ve ikinci aşamadaki başarı oranları

	Parolayı Girme (ilk gün)		Parolayı Girme (45 gün sonra)		
	Başarılı	Düzelterek Başarılı	Başarılı	Düzelterek Başarılı	Başarısız
PCCP	36/39	3/39	7/39	17/39	15/39
	92,31%	7,69%	17,95%	43,59%	38,46%
Yaz&Tıkla	36/39	3/39	25/39	6/39	8/39
	92,31%	7,69%	64,10%	15,38%	20,51%
Metin	35/39	4/39	16/39	5/39	18/39
	89,74%	10,26%	41,03%	12,82%	46,15%

Tablo 2
Test edilen üç yöntem için ikinci aşama başarı sonuçlarının özeti

Parola Girme (45 gün sonra)	Başarılı	Başarısız	Başarı Oranı %
PCCP	24	15	61,54
Yaz&Tıkla	31	8	79,49
Metin	21	18	53,85

İlk aşamanın son adımı olarak her kullanıcıdan her üç yöntem ile de sisteme giriş yapmaları istenmiştir (Denek-İçi (Within-Subjects) metodu kullanılmıştır). Dolayısıyla her kullanıcı 3 farklı şifre oluşturmuş ve onaylamıştır. Yöntemlerin kullanılma sırası farklı kullanıcı grupları için farklı seçilmiştir. Kullanıcılara 45 gün sonra sisteme 3 yöntem ile de giriş yapmak için tekrar davet edilecekleri söylenerek ilk aşama tamamlanmıştır. İkinci aşama 45 gün sonra gerçekleştirilmiş ve kullanıcılardan ilk aşamada belirledikleri şifreler ile sisteme tekrar giriş yapmaları istenmiştir. Anket çalışması ile ikinci aşama sonlanmıştır.

V. SONUÇLAR VE DEĞERLENDİRME

Toplanan veriler ışığında ulaşılan sonuçlar aşağıda özetlenmiştir.

A. Başarı Oranları

Bu bölümde kullanıcıların yöntemleri kullanırken gösterdikleri başarı oranları sunulmuştur. Başarı oranları iki farklı durum için incelenmiştir:

1. Kullanıcının şifresini belirlerken ilk aşamada gösterdiği başarı.
2. Kullanıcının 45 gün sonra ikinci aşamada gösterdiği başarı.

Tablo 1'de PCCP ve Yaz&Tıkla yöntemlerinde başarı oranları sunulurken şu şekilde bir ayrım yapılmıştır. Kullanıcılar "Baştan Başla" ve "Önceki Resim" düğmelerine tıklamadan parolasını girebilmiş (ve ilk aşamada doğrulayabilmiş) ise "Başarılı", eğer bu düğmelere basarak parolasını girebilmiş (ve doğrulayabilmiş) ise "Düzelterek Başarılı" addedilmiştir.

Üç yöntemde de parolasını önce hatalı sonra doğru girenler yine "Düzelterek Başarılı" kategorisinde değerlendirilmiştir. Tablo 2'de Düzelterek Başarılı ve Başarılı sonuçları "Başarılı" başlığı altında birleştirilerek ikinci aşamada elde edilen sonuçlar tekrar özet bir şekilde sunulmuştur. Tablo 2'de görüleceği üzere Yaz&Tıkla yöntemi yaklaşık % 80 oranı ile diğer iki yöntemden daha fazla başarılı olmuştur. Bu başarı sonuçları ışığında birinci hipotezimizin doğru olduğuna dair bir delil elde edildiği - Yaz&Tıkla yöntemi ile oluşturulan şifrelerin kullanıcılar için daha hatırda kalır olduğu - sonucuna varabiliriz. Bu başarı oranları istatistiksel anlamlılık bağlamında incelendiğinde aralarında anlamlı bir fark olduğu görülmektedir. [$p<0.052$]. Deney esnasında yaptığımız gözlemler bizde şu fikri oluşturmuştur. Kullanıcıların PCCP yöntemindeki şifrelerinin tamamen resim üzerinden belirlemeleri grafik tabanlı şifrelere aşina olunmadığı için kullanışlılık problemi oluşturmuştur. Yaz&Tıkla yönteminde ise ilk başta metin şifre girilmesi ve sonrasında tek resimde tıklama işlemi uygulanması kullanıcıların sisteme daha kolay adapte olmasını sağlamıştır.

Tablo 3
PCCP ve Yaz&Tıkla yöntemlerinde "değiştir" düğmesinin kullanılma sayıları

	PCCP			Yaz&Tıkla
	Resim1	Resim2	Resim3	Resim1
Ortalama	14,2	9,5	8,7	11,3
Ortanca	5	7	4	7

45 gün sonra tekrar sisteme giriş yapılması esnasında kullanıcılardan birçoğunun Yaz&Tıkla yöntemini kullanırken ekranda görünen resimler yardımı ile şifrelerinin metin kısmının doğruluğunu kontrol ettikleri gözlemlenmiştir. Kullanıcının, şifresinin ilk kısmını hatırlar ve doğru resme ulaşırsa, resimde yaptığı tıklamada çok da zorlanmadığı görülmüştür. Bazı kullanıcılar Yaz&Tıkla yöntemini kullanırken şifresinin metin bölümünü belirlerken görünen resme göre metini değiştirmiş ve kendisi için kolay olabileceğini düşündüğü resme karşılık gelen metini şifrenin ilk kısmı olarak belirlemiştir. Aslında benzer durum PCCP'de

Tablo 4
Test edilen üç yöntemde kullanıcıların her bir adımda harcadıkları zaman bilgileri

Toplam süre (ortalama)	Parola Oluşturma	Parolayı Onaylama	Parolayı Girme	Parola Girme (45 gün sonra)
Yaz&Tıkla	35,9	14,1	21,4	35,5
Metin	20,3	9,6	16,0	22,4
PCCP	44,6	17,6	21,6	35,6

de vardır. Ancak kullanıcıların resimler üzerinde tıklama işlemlerini birkaç defa denemesi ve beğenmediği resmi değiştirmek için önceki resme dönüp tekrar nokta belirlemesi esnasında kimi zaman konsantrasyon kaybına ve hatalara sebep olduğu gözlemlenmiştir. Kullanıcıların görüntü kapısını tolerans aralığı olarak algılaması ve ona göre şifre doğrulama işlemleri yapması iki yöntemde de (PCCP ve Yaz&Tıkla) karşılaşılan bir diğer problemdir. Metin tabanlı yöntemde en az 14 karakterden oluşan şifreleri 45 gün sonra hatırlamak yaklaşık kullanıcıların yarısı için mümkün olmamıştır. Kullanıcıların bazılarının kısa cümlecikleri şifre olarak belirlemeleri sayesinde başarılı oldukları gözlemlenmiştir (örnek: şampiyonfenerbahçe).

Tablo 3'de PCCP ve Yaz&Tıkla yönteminde değiştir düğmesini kullanma sayıları verilmiştir. Bu sayıların resim başına ortalamada yaklaşık aynı olması güvenlik (sıcak nokta problemi) konusunda bu iki yöntemin yaklaşık aynı özellikleri gösterdikleri konusunda bir ipucu teşkil etmektedir.

B. *Zaman Bilgileri*

Tablo 4'de kullanıcıların şifre oluşturma, şifre doğrulama ve tekrar sisteme giriş yapma adımlarının her birisi için toplam harcadığı zaman bilgisi (saniye) sunulmuştur. Özetle, metin şifre yönteminde kullanıcıların daha hızlı oldukları, diğer iki yöntemde ise yaklaşık aynı seviyelerde zaman harcadıkları anlaşılmaktadır.

C. *Anket Sonuçları*

Tablo 5'de yapılan anket sonucunda elde edilen veriler sunulmuştur. Bu veriler, kullanıcıların Yaz&Tıkla yöntemini daha güvenli ve daha kullanışlı bulduklarını göstermektedir. Sonuç olarak, anket yolu ile ikinci hipotezimiz için de bir delil elde ettiğimizi söyleyebiliriz.

Tablo 5
Yapılan anket sonucunda elde edilen sonuçlar

Anket Soruları	Yaz&Tıkla	PCCP	Metin
1.soru: Hangi yöntemle şifre oluşturup kullanmayı tercih edersiniz?	26	8	5
2.soru: Şifrenizi en kolay hangi yöntemle oluşturabildiniz?	19	7	13
3.soru: Şifrenizi en kısa sürede hangi yöntemle oluşturabildiniz?	12	8	19
4.soru: Sizce hangi yöntem daha güvenlidir?	21	13	5
5.soru: Sizce hangi yöntemle oluşturulan şifreyi hatırlamak daha kolaydır?	22	6	11
6.soru: Bir banka hesabınızın şifresini belirlerken hangi yöntemi kullanırsınız?	20	13	6

VI. SONUÇ

Kullanıcıların uzun yıllardır metin tabanlı parolaları kullanmaları ve genel bir alışkanlık elde edinmeleri sebebiyle grafiksel şifre yöntemlere ani ve hızlı bir geçişin mümkün olmadığını düşünüyoruz. Bu düşünceden hareketle bu çalışmada metin ve grafiksel öğeleri birleştiren Yaz&Tıkla yöntemini önermekteyiz. Tarafımızca yönetilen ve sonuçlarını yukarıda özetle incelediğimiz laboratuar deneyi ile Yaz&Tıkla yönteminin kullanışlılık avantajlarının olabileceğine dair ipuçları elde edilmiştir. Fakat yapılan pilot çalışma ile yetinmemek gerekir. Daha geniş kapsamlı deneyler, saha çalışmaları, farklı katılımcı profilleri ile yapılan denemeler gibi ilave çalışmaların yürütülmesi tarafımızca planlanan çalışmalar arasındadır.

KAYNAKLAR

[1] Bıçakcı, K. (6-8 Mayıs 2010). Kullanışlı Güvenlik için Temel Prensipler. 4. Uluslararası Bilgi Güvenliği ve Kriptoloji Konferansı.
[2] Paivio, A., Rogers, T., Smythe, P. (1968). Why are pictures easier to recall than words? Psychonomic Science, 11, 1-2.
[3] R. Biddle, S. Chiasson, and P. van Oorschot, "Graphical passwords: Learning from the first twelve years," ACM Comp. Surv., vol. 44,2012.
[4] Chiasson, S., Stobert, E., Forget, A., Biddle, R., P.C. van Oorschot (Oct 2011). Persuasive Cued Click-Points: Design, implementation, and evaluation of a knowledge-based authentication mechanism. *IEEE Transaction on Dependable and Secure Computing (TDSC)* .
[5] P.C. van Oorschot, T. Wan. TwoStep: An Authentication Method Combining Text and Graphical Passwords. MCETECH 2009: 4th International MCETECH Conference on eTechnologies, 4-6 May 2009.
[6] Kuo, C., Romanosky, S., Cranor, L. Human selection of mnemonic phrase-based passwords. SOUPS 2006.
[7] Burr, W. E., Dodson, D. F., Polk, W. T. (April,2006). *Electronic Authentication Guideline.* Gaithersburg,MD USA: National Institute of Standards and Technology (NIST).

Covert Channels Detection using Process Mining

Amir Jalaly Bidgoly, Behrouz Tork Ladani, Ahmad Baraani Dastjerdi
Department of Computer Engineering,
Faculty of Engineering, University of Isfahan,
Isfahan, Iran

Abstract—**Covert channel is a communication channel between two processes that is neither designed nor intend for communication. Since it is very hard to detect covert channels, they are an important security challenge for current systems and may be used for illegal data transfer by malwares. There exist two main approaches for finding covert channels. First identifying potential covert channels and second detecting currently used covert channels. In this paper, two methods are proposed for covert channel detection based on process mining. Whereas most of existing methods try to identify potential covert channels, the proposed methods detect currently using ones. In both methods, first the process model is extracted using process mining and then covert channel patterns are searched in the model. In the first proposed method, both high and low processes should be available whereas in the second one only high process is required for detection. The efficiency and accuracy of the proposed methods is demonstrated by a simple but clear case study.**

Index Terms—**Covert channel, Process mining, Process model, Temporal logic.**

I. Introduction

Covert channel is a type of information leak from a higher classification process to a lower one that the communication channel used by the processes is neither designed nor intended to transfer information[1]. This characteristic of covert channels makes them very hard to detect, therefore they are often hidden from the security and design viewpoint. Covert channels are an important challenge for security of current systems since it enables malicious process to transfer top-secret information to a lower class process.

Nowadays, in almost security documents, there exist standards to overcome covert channels or reduce their risk [2][3][4]. Five base approaches exist for this purpose: Identification, Detection, Analysis, Prevention and Migration. Many methods are proposed in the literatures based on these approaches and we have reviewed some of famous ones in the related works section. However these methods suffer from two common weaknesses: First, They are not an automated and need an expert supervisor. Second, however the methods have shown their effectiveness in theory but in practice they are not so useful, because they consider a very limit or abstract system which is very far from the reality.

In this paper two novel methods using process mining are proposed for covert channel detection. *Process Mining* [6][7] is a tool for extracting information from event logs that usually presented as a process model. Process mining enables us to have a quit real model from running process, therefore in practice the performance of the proposed methods is greatly enhanced. On the other hand, unlike other existing methods which are more intended to identify potential channels, the proposed methods is looking for a way to detect currently using covert channels.

The reminder of the paper is organized as follow: in next section related works have been reviewed. Motivation and contribution of the proposed method is presented in section three. In section four, process mining is reviewed in summary. The proposed methods are described in section five, and a case study is presented in section six. Finally the paper ends with conclusion and future works in section seven.

II. Related Works

As mentioned before, there are five approaches in the field of covert channels: *Identification*, *Detection*, *Analysis*, *Prevention* and *Migration*. In covert channel identification, all potential covert channels will be identified. Identified cases may not currently used by any malware, but they are capable to be used as a communication media between malwares later. In identification, the goal is to analyze of system design and structure to eliminate and avoid possible covert channel attacks as much as possible. *Shared Resource Matrix* [7][8] and *Covert Flow Tree* [9] are two famous methods of this class.

Covert channel detection as the second approach is not to find all potential channels but just the currently using one. In most systems, identification will find many potential covert channels that are hard or even impossible to be eliminated. So in practice, detection is a better approach then identification, but, in literatures the former methods gains less interest than the later and there are not many methods for covert channels detection. [10][11][12] are some examples of these type of methods.

The third approach, covert channel analysis, helps us in

different way. In this approach, the capacity of channel will be analyzed to determine how dangerous it be if used by malwares. For example a 1 bit per second covert channel is not a big security challenge but a 1000 bits per second one could make important security problems. Most of security documents say that eliminating of all covert channels is not possible [13]. For example, DoD documents described for securing a system there must exist no more then 1 bit per second covert channel. Covert channel analysis is a tool for this mean. [14] is an example method of these approach.

Another approach in this field is covert channel prevention. This approach is trying to separate and distinct processes of a certain security class from other processes. This means a higher process could neither communicate nor be observed by lower process. *Virtual Machines* and *Sand Box* [15] are two important methods in this approach. However prevention methods are usually impractical since eliminating all communication media and the shared resource is impossible and hinders normal behavior of process.

The last approach is *Migration*. Migration methods are used when there is a covert channel that cannot be eliminated. Here the goal is to reduce the risk of channel (i.e. decrease channel capacity). Pump [16] is the famous tool for migration however these methods usually reduce system performance due to the changes in the allocation of the shared resources.

In next section weakness points of above methods are discussed and the motivation of the proposed methods is presented.

III. Motivation

Identification and detection of covert channels are distinguished between other mentioned approaches, due to the fact that for analysis, migration and prevention of covert channel, first we need to identify or detect them. This shows the importance of identification and detection. On the other point of view, in many cases, identification of a covert channel is not very helpful, because in any system that needs shared resource or communication between processes, various types of covert channels could be identified. In practice, eliminating all covert channels is possible only when two conditions could be met [13]: First, the process cannot be observed or monitored by any other process of lower class and second there is no communication media or shared resource between processes. The above assumptions are often not applicable. So identification is not an effective approach for covert channels.

Detection approach, unlike identification, is to find covert channels which are currently used by malwares. This approach has several advantages compared to identification. Detecting currently using covert channels not only enables us to eliminate them but also help to detect/remove malwares from the system.

Despite to the advantages of detection approach, it needs to analysis running processes. To analysis running processes, their specifications and documentations are required which are often not available or accessible. Even in the cases where a specification or document is provided, if the process uses a covert channel, the specification is reorganized in a way that makes it difficult or impossible to discover the covert channel. Who give a document that say "I am a covert information thief"?. It can be said that in the most cases either there is no documentation or if documentation is provided, it is different from reality (i.e. have been manipulated to mislead). Lake of specifications for running processes is a big challenge for detection approach.

Considering above, in this paper a novel method is presented for detecting of covert channels based on process mining. Process mining provides a real (or at least close to reality) model of the process. Using this method, the process are not be black box anymore, thus a detection method can be applied. In next section a brief description of process mining is given before describing the proposed methods.

IV. Process Mining

Process mining (PM) [5][6] is a tool to discover information about a process from its event logs. It can be used when no specification is available about a process or there are doubts about correctness of a given specification. There are three different classes in PM. First class involves the algorithms for extracting the process model from collected process logs [17]. The model is usually shown by a standard formalism like Petri nets. In addition process mining may be used for extracting other types of knowledge like social networks.

The second class in PM is used when the question is about the correctness of a given process model [18]. In this class, PM helps to check the matching of a provided model with recorded event logs. In addition, it helps predict or suggest next step in the running of the process. Intrusion Detection Systems (IDS) that work based on anomaly activity detection are examples of this class.

In the third class of PM, whole or a special part of the given model is improved considering event logs. This class is to enhance a property (e.g. the fitness) of the process model.

Many algorithms and useful tools are proposed for PM. Alpha [18], Genetic miner [19] are some famous algorithms and ProM [21] is one of the best tool in this regards.

V. Proposed Methods

In this section, our proposed methods are described. We have two methods for detecting covert channels based on PM called simple and advanced methods. In both, we need to collect process logs and extract the model. Since covert channels are often created via shared resources and system functions; events that are recorded for each process are events that are related to system function calls and events related to an inner state or process depend transactions are discarded. These two methods are presented in continue.

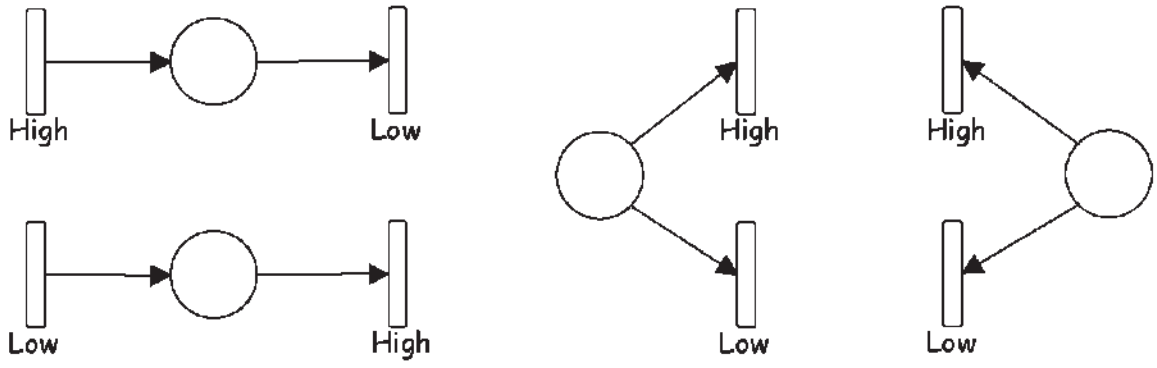


Fig. 1. Covert channel patterns in simple the method

A. Simple Method

Suppose there are two processes from different security classes in the system. The process from higher class called *High* involves access to sensitive information and the other one called *Low* does not permit to access them. A mandatory access control system checks security policies including these two processes should have no contact with each other. As mentioned before, a covert channel may allow them to have a hidden communication channel while they are explicitly prohibited from. Here the goal is to find out if there is any covert channel between *High* and *Low* or not.

If a relationship between the processes be found, it can be concluded that there is a covert channel between them because they should have no contact with each other due to the access control system. Simple method detects covert channel based on this principal. For this purpose, events in addition to the performer of each event (i.e. *High* or *Low*) are recorded and then the process model is extracted using process mining. If there is a relationship between the processes in the obtained model, the existence of covert channel can be derived.

The term "relationship between processes" should be described. Here, it is assumed that process model is presented using Petri nets. To identify relationship between processes, some patterns can be defined in Petri nets. These patterns are shown in figure (1) and include following ones:

- A token generated by *High* process enables a transaction in *low* process or vice versa.
- Events of two different processes have a shared input place.
- Events of two different processes have a shared output place.

After presenting process model by Petri net, it's required to search for above patterns. If one of the patterns is found, existence of covert channel between processes can be concluded. In section six, a case study is presented for this method. Although this method is effective and simple, but it also has some weakness points. In continue we have reviewed these weakness points and then the advanced method is introduced.

B. Advanced Method

In simple method, two conditions should be met before applying the method: First, both *High* and *Low* process or at least their recorded event logs must be available. Second, the processes should be independent. This means no relationship between them is allowed except when a covert channel exits. In some types of covert channel, above assumption are not true. For example, if an unreachable shared resource is used for creating covert channel (e.g. network resources); its event logs cannot be recorded. When *Low* process is outside of system boundary or it is a virus hidden in system files, again its event logs cannot be collected. So the extraction of the process model that includes both *High* and *Low* process is not always possible, thus the first condition is not always true. Also about the second condition, the processes may allow to have a limited and controlled connection. For example *Low* process injects itself as a virus to a trusted process. Here, the model contains some relationship stands for contact or communication between them whereas it is not clear that it is a legal or illegal data transfer. Therefore in many cases mentioned conditions are violated.

Considering the mentioned problems, advanced method is introduced. In this method is assumed that only *High* process is available thus the process model just includes and be extracted with its logs. Then this model is searched to find out if there is a covert channel or not.

In each covert channel there exist at least two signals to send 0 and 1 respectively. If these signals are created using a shared resource, a special pattern can be found in the model. This pattern is shown in figure (2). As it can be seen, three steps are required to send a signal (zero or one). First *High* process makes a change in a shared resource. We call this shared resource "high signal resource" (i.e. var_i in fig. (2)). High signal resource must be observable by *low* process so it will notice the change. After it find a change, *low* process makes a change in a so-called "low signal resource" (i.e. var_j in fig. (2)) that means it received *high* signal. Low and high signal resources can be same. After *high* process receives *low* signal via low signal resource, it goes to the third step and prepare for sending next bit. Since the process model is

obtained of event logs of system function call, it is needed to specify the shared resources in each event. These resources are the hidden system variables which are changed in system function calls. In the case study, file existence flag is the shared resource used for creating covert channel.

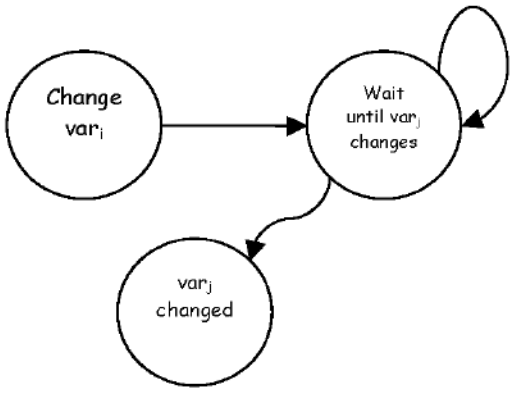


Fig. 2. Covert channel pattern in the advanced method.

In large and complex models, the given pattern may not be discovered simply. In some case given pattern is separated between irrelevant events that make it difficult to find. Hence to complete this pattern, temporal logic can be used. This not only led to a more accurate diagnosis but also makes detection process automated without need to an expert supervisor. The LTL pattern formula is shown below:

$$\exists F[change(\mathrm{var}_i, x) \; X(read(\mathrm{var}_j, \neg y) U read(\mathrm{var}_j, y))] \quad (1)$$

In above equation, var_i and var_j refer to high and low signal resources respectively. x and y are the changed state made by the processes.

VI. Case Study

In this section a simple case study is presented to clarify the efficiency of the proposed methods. The case study involves a covert channel simulation implemented by the programming language (C#). In addition, *Prom* [21] and *PromImport* [22] is used for the process mining jobs and *PDETool* [23] helps to verify the model against the given patterns.

The simulation program includes two threads as *low* and *high* processes in addition to a third one that has no role in covert channel and just makes logs noisy. The shared resource is a file management system. Four files exist in this system: *A*, *B*, *C*, and *D*. To send a signal, first *high* process creates file *A*. *Low* process monitors the file system to discover this change. If *low* detect *A* is created, it removes it from the file system. When the file is deleted, *High* notice that *low* has received the signal. This means *high* send 0 to *low*. Sending 1 is exactly in the same way but file *B* is used instead of *A*. *C* and *D* are to make logs noisy and each one of three threads may use them randomly.

After running threads, event logs are collected. These events include *CreateFile*, *DeleteFile*, and *CheckFile* for creating a file, deleting and check the existence of a file respectively. For each event, the performer of event (i.e. *High*, *low*, and *noise*) in addition to corresponding file name (i.e. *A*, *B*, *C*, and *D*) are also recorded. These data are converted to MXML format (using PromImport) as the input data for Prom. Then the process model is extracted using two different algorithms; Alpha [17] and ILP [24]. These models are shown in figure (3). The transaction of *high* process is colored in red and the transaction of *low* process is colored in blue. Applying the simple method, some relationship can be found in the models. These relationships are marked in red zone that means a covert channel is detected using the method.

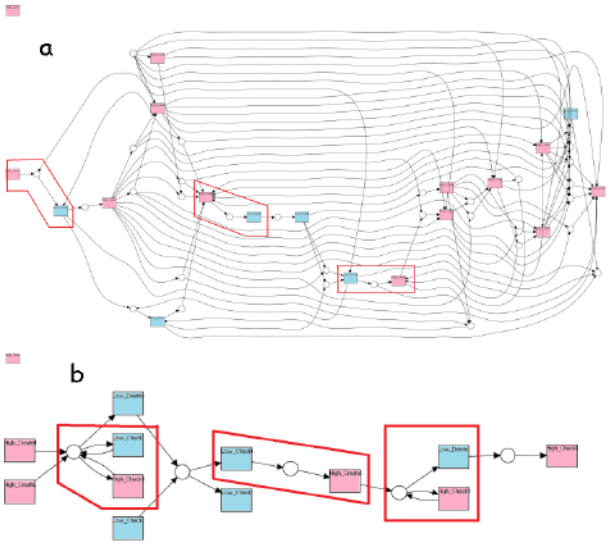


Fig. 3. The process model of case study of the simple detection method **a)** Alpha algorithm **b)** ILP algorithm

For testing the advanced method, another instance of simulation program is executed and the event logs of just *high* process are collected. As before the process model is extracted using Prom and PromImport which is shown in figure (4). Again the models are searched for given patterns. The model obtained by Alpha algorithm does not contain the pattern however the model obtained by ILP has corresponding pattern that is marked in red zone. It seems that Alpha algorithm is a primitive algorithm, thus it has some weakness that make the extracted model incomplete, whereas ILP as the more advanced algorithm discovers pattern simply. This clears the importance of used algorithm and fitness of extracted model. The models are also checked for the given LTL formula using PDETool and results confirm the existence of covert channel again.

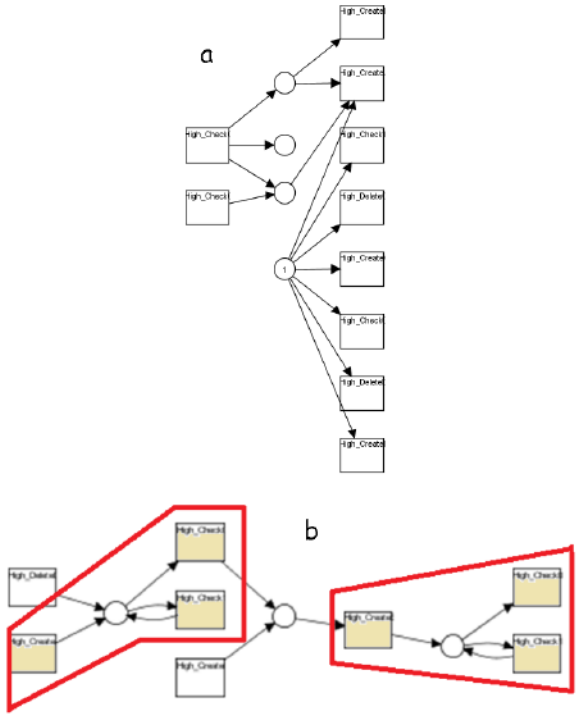


Fig. 4. The process models of the advanced detection methods **a)** Alpha algorithm **b)** ILP algorithm

For having a complete case study, a third instance of simulation is executed with no covert channel and threads using files randomly and completely independent. The goal is to check the proposed method whereas no covert channel exists. The extracted process model is shown in figure (5). As seen in this model there is neither simple nor advanced method patterns. This is a good example of efficiency and accuracy of the proposed methods.

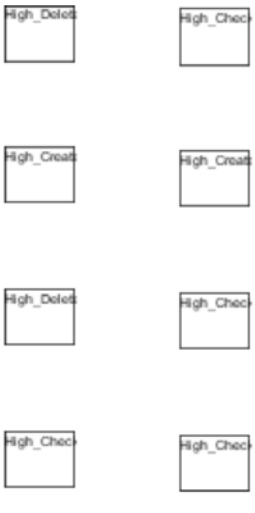


Fig. 5. The process model when no covert channel exists

VII. Conclusion and Future Works

In this paper, two methods are proposed for detecting covert channels which are based on process mining. In the proposed methods, first the event logs of processes are collected and then the process model is extracted using process mining and collected logs. In the simple detection method is assumed that both high and low processes (that intends to use covert channel) are available and should have no contact with each others. In the advanced detection method only high process and its event logs is required to detect covert channel. This method is also presented with LTL logic.

The proposed methods cannot detect time covert channels which use a sequence of events for data transfer. This could be considered in the future development. On the other hands, some other behaviors different from covert channel behaviors may create patterns discussed in this paper. In future, we should also identify and distinguished these types of behaviors.

References

[1] B. W. Lampson, "A Note on the Confinement Problem," Communications of the ACM, 16:10, pp. 613-615, October 1973.

[2] J. McHugh. Handbook for the Computer Security Certication of Trusted Systems, chapter Covert Channel Analysis, pages 4-78. US Navy, 1995.

[3] NCSC-TG-030, Covert Channel Analysis of Trusted Systems (Light Pink Book) from the United States Department of Defense (DoD) Rainbow Series publications.

[4] 5200.28-STD, Trusted Computer System Evaluation Criteria (Orange Book) from the DoD Rainbow Series publications.

[5] W. M. P. van der Aalst, and A. Weijters (2004). "Process mining: a research agenda." Computers in Industry 53(3): 231-244.

[6] Process Mining: Discovery, Conformance and Enhancement of Business Processes, Springer Verlag, Berlin (ISBN 978-3-642-19344-6).

[7] R. Kemmerer, "A Practical Approach to Identifying Storage and Timing Channels," Proceedings of the 1982 IEEE Symposium on Security and Privacy, pp. 66–73 (Apr. 1982).

[8] R. Kemmerer, "Shared Resource Matrix Methodology: An Approach to Identifying Storage and Timing Channels," ACM Transactions on Computer Systems, 1 (3), pp. 256–277 (Aug. 1983).

[9] P. Porras and R. Kemmerer, "Covert Flow Trees: A Technique for Identifying and Analyzing Covert Storage Channels," Proceedings of the 1991 IEEE Symposium on Security and Privacy, pp. 36–51 (May 1991).

[10] R. Accorsi, and C. Wonnemann (2011). Strong non-leak guarantees for workflow models, ACM.

[11] V. Berk, A. Giani, G. Cybenko, "Covert channel detection using process query systems." In: Proc. of FLOCON 2005. (Sep. 2005).

[12] V. Berk, A. Giani, G. Cybenko, "Detection of covert channel encoding in network packet delays." Technical Report TR2005-536, Department of Computer Science, Dartmouth College, Hanover, NH., USA (Aug. 2005).

[13] N. Proctor and P. Neumann. Architectural implications of covert channels. In National Computer Security Conference, pages 28 43, 1992.

[14] J. Millen, "Covert Channel Capacity," Proceedings of the 1993 IEEE Symposium on Research in Security and Privacy, pp. 60–65 (May 1993).

[15] I. Goldberg, D. Wagner, R. Thomas, and E. Brewer, "A Secure Environment for Untrusted Helper Applications: Confining the Wily Hacker," Proceedings of the 6th USENIX Security Symposium, pp. 1–13 (July 1996).

[16] M. Kang and I. Moskowitz, "A Pump for Rapid, Reliable, Secure Communication," Proceedings of the 1st ACM Conference on Computer and Communication Security, pp. 119–129 (Nov. 1993).

[17] W. van der, Aalst, A. Weijters, and L. Maruster, "Workflow Mining: Discovering Process Models from Event Logs." IEEE Transactions on Knowledge and Data Engineering, 16 (9), 1128-1142, 2004.

[18] W. van der, Aalst, H. Beer, and B. van Dongen, "Process Mining and Verification of Properties: An Approach based on Temporal Logic." In R. Meersman & Z. T. et al. (Eds.), On the Move to Meaningful Internet Systems 2005: CoopIS, DOA, and ODBASE: OTM Confederated International Conferences, CoopIS, DOA, and ODBASE 2005 (Vol. 3760, pp. 130-147). Springer-Verlag, Berlin.

[19] W. M. P. van der Aalst, , A. K. A. de Medeiros, et al. (2005). "Genetic process mining." Applications and Theory of Petri Nets 2005: 48-69, 2005.

[20] B. F. van Dongen, A. K. A. de Medeiros, et al. "The ProM framework: A new era in process mining tool support." Applications and Theory of Petri Nets 2005: 444-454, 2005.

[21] C. Günther, and W. van der Aalst "A generic import framework for process event logs," Springer, 2006.

[22] A. Khalili, A. Jalaly Bidgoly, M. Abdolahi Azgomi, "PDETool: A multi-formalism modeling tool for discrete-event systems based on SDES description." Applications and Theory of Petri Nets: 343-352, 2005.

[23] J. M. Werf, B. F. Dongen, et al., "Process Discovery Using Integer Linear Programming," Proceedings of the 29th international conference on Applications and Theory of Petri Nets. Xi'an, China, Springer-Verlag: 368-387, 2008.

İlköğretim ve Lise Öğrencilerinin Bilgi ve Bilgisayar Güvenliği Farkındalığı: Kahramanmaraş Örneği

Mehmet Tekerek,

Özet— **Bu araştırmada ilköğretim ve lise öğrencilerinin bilgi ve bilgisayar güvenliği farkındalık düzeyleri ortaya çıkarılmaya çalışılmıştır. Araştırma kapsamında Kahramanmaraş ili, il merkezi, ilçe, kasaba ve köylerinde öğrenim gören 2447 öğrenciye, geliştirilen bilgi ve bilgisayar güvenliği farkındalık ölçeği uygulanmış ve elde edilen veriler istatistik analiz programı kullanılarak değerlendirilmiştir.**

Bilgi ve bilgisayar güvenliği farkındalığı konusunda, pozitif ve negatif olarak nitelenebilecek bulgulara ulaşılmıştır. Temel olarak öğrencilerin etik konularında yeterli farkındalık düzeyine sahip oldukları gözlenirken, kurallar ve bilgi gerektiren konularda farkındalık düzeylerinin düşük olduğu gözlenmiştir. Bu da bilgi ve bilgisayar güvenliği farkındalık eğitim ve etkinliklerinin yetersiz olduğu düşüncesini ortaya çıkarmaktadır.

Anahtar Kelimeler— Bilgi ve Bilgisayar Güvenliği, Farkındalık, Bilgi Güvenliği Farkındalığı Eğitimi

Information and Computer Security Awareness of Elementary and High School Students: Sample of Kahramanmaraş City

Abstract— **In this study, the awareness levels of elementary and high school students' information and computer security were tried to reveal. A developed information and computer security scale was conducted to 2447 students from the center of Kahramanmaraş, towns, small towns and villages of Kahramanmaraş. The data were assessed by using statistical analysis program.**

About awareness of information and computer security both positive and negative findings were obtained. Basely, it was found that while students have sufficient awareness level in terms of ethical issues, they have low awareness level in terms of issues that required rules and knowledge. This situation reveals the idea that education and activities of awareness of information and computer security seem insufficient.

Index Terms— **Information and computer security, Awareness, Information security Awareness Education**

M. Tekerek, KSÜ, Bilgisayar ve Öğretim Teknolojileri Eğitimi Bölümü, 46100 Kahramanmaraş, Türkiye; (e posta: tekerek@ksu.edu.tr)

I. GİRİŞ

Bilginin, bilgi güvenliğinin ve risklerin tanımlandığı bilgi güvenliği farkındalığı, internetin cemiyet hayatında her geçen gün biraz daha etkili olduğu günümüzde önemini giderek artırmaktadır.

Bilgisayar ve haberleşme teknolojilerinde yaşanan gelişmeler ve özellikle internet'in katalizör etkisi ile insanların, çalışma, iletişim kurma ve her türlü günlük ihtiyaçlarını karşılama biçimi sürekli bir dönüşüm halindedir[5]. İnternet, birçok bilgisayar sisteminin birbirine bağlı olduğu, dünya çapında yaygın olan ve sürekli büyüyen bir iletişim ağıdır. Aynı zamanda, insanların gittikçe artan "üretilen bilgiyi saklama/ paylaşma ve ona kolayca ulaşma" istekleri sonrasında ortaya çıkmış bir teknolojidir. Bu teknoloji yardımıyla pek çok alandaki bilgiye insanlar kolay, ucuz, hızlı ve güvenli bir şekilde erişebilmektedirler[18]. Asan ve Koca'nın yaptığı araştırmanın (2006) sonuçlarına göre öğrencilerin büyük bir çoğunluğu internetin evrensel bir dijital kütüphane olduğunu, hayatı oldukça kolaylaştırdığını ve bilgiye ulaşmak için en hızlı yol olduğunu düşünmektedir.[1]

Günümüz toplumunda insanlar, teknoloji ile küçük yaşlarda tanışmakta; evde ve okulda, gerek ödevleri için gerek eğlence için bilgisayardan yoğun bir şekilde istifade etmektedir [11]. Son yıllarda yapılan araştırma sonuçları da bunu doğrulayıcı niteliktedir.

Radyo ve Televizyon Üst Kurulu'nun 17 ilde 1719 ilköğretim öğrencisinin katılımıyla yapmış olduğu araştırmada öğrencilerin çoğunun evlerinde bilgisayar olmadığını belirtirken, bilgisayarı olanların çoğunluğunun da internet bağlantısına sahip olduğu belirlenmiştir. Bilgisayar ve interneti kullanma amaçları incelendiğinde birinci sırayı oyun eğlence alırken ikinci sırayı derslerine yardımcı olması amacı almıştır[2]. 2011 yılı Nisan ayında gerçekleştirilen Hanehalkı Bilişim Teknolojileri Kullanım Araştırması sonuçlarına göre Türkiye genelinde hanelerin %42,9'u İnternet erişim imkânına sahiptir.[15].

Tüm bunların yanında yasal olmayan, şiddet ve cinsellik içeren sitelere kolay erişim, tehlikeli insanlarla iletişim, çocuk istismarı, oyunlara aşırı bağımlılık başta gelen riskler arasındadır. Uyuşturucu ve terör gibi yasal olmayan yollara destek arayanlar interneti propaganda aracı olarak kullanmaktadırlar[19]. Watson (2005) e göre de, bilgisayar başında toplumdan kendini izole eden çocukların kendilerine güvenlerinin azaldığı, depresyon ve sosyalleşme problemleri yaşadıkları görülmektedir[9]. Buna karşın, öğrencilerin birçoğu internetin sosyalleşmeyi engellediği fikrine katılmamaktadır ve sohbet ederek arkadaşlıkların kurulacağını düşünmektedir[1].

Bilgi Güvenliği farkındalığı ile ilgili alan yazını incelendiğinde; çocuk ve gençlerin bilgisayar ve internette karşılaşabilecekleri risk ve tehditlere karşı yeterli farkındalığın oluşmadığı ve bunlarla baş edebilecek önlemlere sahip olmadıkları görülmüştür.

Dunkels',n Children's Strategies on the Internet (2008) isimli çalışmasında, çocuk ve gençlerin internette karşılaştıkları tehditlere karşı bilinçsiz olarak stratejiler geliştirdikleri ama zararlarından korunmak için bunların yeterli olmadığı ortaya konulmuştur.

Çocukların ve gençlerin, gittikçe yaygınlaşan internet ve bilgisayar kullanımı sırasında elde edecekleri bilgi birikimi, gelişme ve tecrübenin yanında, karşılaşabilecekleri güvenlik tehdit ve tehlikeleri işaret edilerek alınması gerekli olan tedbirlere dikkat çekilmesi, çocuklarımızın bu ortamlarda bu tür olumsuzluklara maruz kalmamaları için kendilerinin uymaları ve ailelerinde uygulaması gereken kurallar oluşturulmalıdır [8]. Hatta çocuklarını bu risklerden korumak isteyen ebeveynler için piyasada birçok filtreleme ve kontrol araçları bulunmaktadır [14]. Çocuklar ve gençler ister internet konusunda deneyimsiz isterse birer bilgisayar kurdu olsunlar, onların büyürken geçtikleri farklı yaşlardaki ve yaşamlarının çeşitli dönemlerindeki internet kullanımını yönlendirebilmek onların cinsel bilgiler, şiddet davranışları, alkol, sigara, kumar ve sağlıksız beslenme gibi istenilmeyen alışkanlıklar edinmesini ve fiziksel zararlar görmesini engelleyecektir [12]. İnternet ve bilgisayar kullanımı tüm yönleriyle değerlendirildiğinde, eğitim sistemlerinin de bilgi iletişim teknolojilerine hızla yöneldiği günümüzde öğrencilerin bilgi ve bilgisayar güvenliği farkındalıklarının araştırılması önemli görülmüştür.

İlköğretim ve lise düzeyinde öğrenim gören öğrencilerin bilgisayar ve internet güvenliği farkındalık seviyelerinin ortaya konmasının amaçlandığı bu araştırmada ana problem cümlesini, Öğrencilerin bilgi ve bilgisayar güvenliği farkındalık düzeyleri nasıldır? Oluşturmaktadır.

Bu kapsamda aşağıdaki alt problemlere cevap aranmıştır.

Öğrencilerin bilgi güvenliği farkındalığı, cinsiyete göre değişmekte midir?

Öğrencilerin bilgi güvenliği farkındalığı, kullanım kuralı olup olmamasına göre değişmekte midir?

Öğrencilerin bilgi güvenliği farkındalığı, yaşadıkları yerleşim yerine göre değişmekte midir?

Öğrencilerin bilgi güvenliği farkındalığı, öğrenim seviyelerine göre değişmekte midir?

II. YÖNTEM

Araştırmada Kahramanmaraş bölgesinde şehir merkezi, ilçe merkezi, kasaba ve köylerde okuyan ilköğretim ve ortaöğretim öğrencilerinin bilgisayar kullanma alışkanlıkları ve bilgi güvenliği farkındalığı seviyelerini ölçmek amacıyla tarama modeli kullanılmıştır.

Tarama modelleri, geçmişte ya da halen var olan bir durumu var olduğu şekliyle betimlemeyi amaçlayan araştırma yaklaşımlarıdır. Bilinmek istenen şey vardır ve oradadır. Önemli olan onu uygun şekilde gözleyip belirleyebilmektir [19].

Araştırma sonunda elde edilen veriler istatistik analiz paket programında analiz edilerek yorumlanmıştır. Araştırmaya katılanların demografik özelliklerine ait verilerin analizinde frekans değeri kullanılmıştır. Cinsiyet değişkeni ile öğrencilerin bilgi güvenliği farkındalığı arasında ve bilgi güvenliği farkındalıklarının kullanım kuralı olup olmamasına göre anlamlı bir farklılık bulunup bulunmadığını belirlemek için bağımsız örneklem t testi uygulanmıştır. Öğrencilerin yaşadıkları yerleşim yeri değişkenine ve öğrenim seviyesi değişkenine göre bilgi güvenliği farkındalığına ilişkin görüşleri bakımından anlamlı bir farklılık olup olmadığını belirlemek için ise tek yönlü ANOVA uygulanmıştır. Anlamlılık düzeyi 0,05 olarak alınmıştır.

Örneklem

Bu çalışmanın örneklemini, Kahramanmaraş'ta öğrenim gören ilköğretim ve ortaöğretim öğrencilerinden oluşan 2449 kişi oluşturmaktadır. Araştırmaya katılan öğrenciler tesadüfî olarak belirlenmiştir. Öğrenciler anketi öğretmenleri gözetiminde doldurmuşlardır. Öğrencilerin cinsiyetleri, öğrenim seviyeleri, yaşadıkları yerleşim yerleri, Tablo 1'de sıklık ve yüzde olarak verilmiştir.

Tablo 1. Öğrencilerin Kişisel Özellikleri

	Özellik	*N*	*%*
Cinsiyet	Kız	1351	55,2
	Erkek	1098	44,8
Okul Türü	İlköğretim (1. Kademe)	694	28,3
	İlköğretim (2. Kademe)	1506	61,5
	Lise	249	10,2
Yerleşim yeri	Köy	317	12,9
	Kasaba	208	8,5
	İlçe	368	15,0
	İl merkezi	1556	63,5

Veri Toplama Aracı

Kahramanmaraş bölgesinde şehir merkezi, ilçe merkezi, kasaba ve köylerde okuyan ilköğretim ve ortaöğretim öğrencilerinin bilgisayar kullanma alışkanlıkları ve bilgi güvenliği farkındalığı seviyelerini ölçmek amacıyla araştırmacı tarafından geliştirilen "Bilgi Güvenliği Farkındalığı Ölçeği" kullanılmıştır.

Öğrencilerin anket sorularına verdiklerin cevapların aritmetik ortalama değerleri Tablo 4'te sunulmuştur. Aritmetik ortalamaların değerlendirilmesinde; "Aralık Genişliği = Dizi Genişliği (Ranj)/Grup Sayısı" formülünden faydalanarak, 4/5=0,80 olarak puan aralıkları belirlenmiştir (Tekin, 1996). Buna göre belirlenen puan aralıkları Tablo 2'de verilmiştir.

Tablo2. Ölçek puan aralıkları

Görüş	*Puan*
(4) Kesinlikle Katılıyorum	4,20- 5,00
(3) Katılıyorum	3,40- 4,19
(3) Kararsızım	2,60- 3,39
(2) Katılmıyorum	1,80- 2,59
(1) Kesinlikle Katılmıyorum	1,00- 1,79

İlgili alan yazından yararlanılarak öncelikle "Bilgi Güvenliği Farkındalığı Taslak Ölçek Formu" oluşturulmuştur. Bu taslak ölçek 35 ifade içermektedir. Taslak ölçek, geçerlik analizi için alanında uzman 5 öğretim üyesine gönderilmiş ve onların görüşleri doğrultusunda ölçeğe son şekli verilmiş ve 27 ifadeden oluşmasına karar verilmiştir. Bu şekilde oluşturulan veri toplama aracı, öğrencilerin demografik özelliklerinin belirlendiği bölüm ile bilgi güvenliği

farkındalığını ölçen bölüm olmak üzere iki bölümden oluşmaktadır. Ölçekte olumsuz anlam içeren 15 maddede tersten kodlama yapılmıştır. Ölçeğin Cronbach's alfa güvenirlik katsayısı 0,72 olarak hesaplanmıştır.

III. BULGULAR VE YORUMLAR

Araştırmanın bu bölümünde veri toplama aracı ile elde edilen bulgular ve bunlara ilişkin yorumlar bulunmaktadır

Araştırmada öğrencilerin evde interneti kullanma amaçları sorulmuş bulgular tablo 3'de sunulmuştur.

Tablo 3. Evden internete bağlanan öğrencilerin İnterneti kullanma amaçları

Amaç	*N*	*%*
Oyun Oynamak	91	14,5
Müzik Dinlemek	47	7,5
Sohbet Etmek	107	17,1
Ders Çalışmak	382	60,9
Toplam	627	100,0

Tablo 3'ten de görüleceği gibi öğrencilerin önemli bir kısmı (%60,9; N=382) internete ders çalışmak amacıyla girdiklerini ifade etmişlerdir. Bu oranın yüksek bulunması veli kontrolünden kaynaklanmış olabileceğini düşündürmüştür. Evden internete bağlanan öğrencilerin %39,1'i ise interneti oyun oynamak, müzik dinlemek, sohbet etmek gibi eğlence amaçlı kullandıklarını ifade etmeleri de yine önemli bir bulgu olarak görülmüştür.

Araştırmada öğrencilerin internet kafede interneti kullanma amaçları sorulmuş bulgular tablo 4'de sunulmuştur.

Tablo 4. İnternet kafeden internete bağlanan öğrencilerin İnterneti kullanma amaçları

Amaç	N	%
Oyun Oynamak	223	32,7
Müzik Dinlemek	57	8,3
Sohbet Etmek	95	13,9
Ders Çalışmak	308	45,1
Toplam	683	100,0

Tablo 4'ten de görüleceği gibi öğrencilerin önemli bir kısmı (%45,1; N=308) internete ders çalışmak amacıyla girdiklerini ifade etmişler bunun yanında internet kafeyi oyun oynamak amacıyla kullanan (%32,7; N=223) öğrencilerin oranı da dikkat çekicidir. Bu oranların internet kafelerde veli kontrolünün bulunmamasından kaynaklandığı düşünülmektedir. İnternete bağlanmak için internet kafeleri kullanan öğrencilerin %22,2'si ise, müzik dinlemek, sohbet etmek gibi amaçlarla kullandıklarını ifade etmişlerdir.

Araştırma kapsamında geliştirilen ölçekten elde edilen bilgi ve bilgisayar güvenliği farkındalık unsurları ile ilgili farkındalık düzeyleri, Tablo 5, Tablo 6, Tablo 7, Tablo 8 de verilmiştir.

Tablo 5. Öğrencilerin kararsız oldukları bilgi ve bilgisayar güvenliği farkındalık unsurları

Unsur	*X; SS*
Şifre gerektiren tüm işlemlerde aynı şifreyi kullanırım	(X=3,19; SS=1,40)
İnternette sohbetlerimin başkaları tarafından izlenebileceğini biliyorum	(X=3,55; SS=1,34)
Dosya indirirken veya e-posta ekleri için virüs denetlemesi yaparım	(X=3,16; SS=1,55)
Okul için önemli bir belge olduğunda, onu birden fazla yere kayıt ederim	(X=3,06; SS=1,52)
Ebeveynim ya da ben bilgisayarımdaki bilgilerin güvenli olup olmadığını kontrol ederiz	(X=3,36; SS=1,50)
Güvenlik Duvarı veya Filtreleme Yazılımı kullanıyorum	(X=3,06; SS=1,50)
Çevremdeki arkadaşlarım interneti sadece oyun ve sohbet için kullanmaktadır	(X=3,17; SS=1,32)
İnternetin güvenli bir alan olduğunu düşünüyorum, bilgilerime ve bilgisayarıma internetten zarar gelmez.	(X=2,71; SS=1,40)

Tablo 6. Öğrencilerin katılmış oldukları bilgi ve bilgisayar güvenliği farkındalık unsurları

Unsur	*X; SS*
İnternette başkalarının bilgisine izinsiz olarak erişmenin suç olduğunu biliyorum.	(X=4,30; SS=1,19)
Okulumda, okul için uygun ya da elverişli olmayan internet sitelerinden uzak tutucu programlar kullanılır.	(X=4,03; SS=1,45)
Bir web sitesinin güvenli olup olmadığını ve güvenilir bilgi verip vermediğini anlayabiliyorum.	(X=3,52; SS=1,31)
Çevrimiçi olduğum zaman birinin benim hakkımdaki bilgileri çalmasından yana kaygılarım vardır	(X=3,41; SS=1,30)

Tablo 7. Öğrencilerin katılmadıkları bilgi ve bilgisayar güvenliği farkındalık unsurları

Unsur	*X; SS*
Çevrimiçi iken tanımadığım kişi/kişiler tarafından rahatsız ediliyorum	(X=1,89; SS=1,17)
Çevrimiçi iken uygunsuz materyaller gönderiliyor.	(X=1,85; SS=1,14)
Bilgi güvenliğine ilişkin yeterli bilgiye sahibim.	(X=2,37; SS=1,23)
İnterneti müzik, program vb. gibi dosya paylaşım sitelerinden program indirmek için kullanırım.	(X=2,47; SS=1,32)
Sohbet odalarını kullanırım.	(X=2,02; SS=1,35)
Sohbet ettiğim insanların kim olduklarına ve söylediklerine inanıp inanmama konusunda tereddüt ediyorum.	(X=2,40; SS=1,50)
Bir program için ücretsiz verilen kullanma zamanı geçtiğinde ya o programı silerim ya da satın alırım.	(X=2,13; SS=1,43)
Bir programın ücretsiz kullanma zamanı geçtiğinde bir çözümünü bulup ücretsiz kullanmaya devam ederim	(X=2,04; SS=1,40)
İzinsiz müzik, video veya programların ücretsiz olarak indirilmesi yanlış değildir	(X=2,25; SS=1,30)
Başka birinin web sitesinde değişiklik yaptığında başın belaya girmez çünkü o gerçek değil	(X=2,32; SS=1,20)
İnternette önemli olan eğlencedir, gezindiğim sayfaların güvenli olup olmaması çok da önemli değildir	(X=2,10; SS=1,23)

Tablo 8. Öğrencilerin kesinlikle katılmadıkları bilgi ve bilgisayar güvenliği farkındalık unsurları

Unsur	*X; SS*
İnternetten ürün satın alırım.	(X=1,39; SS= 0,89)
Ailemin izni olmadan internetten ürün satın aldım.	(X=1,32; SS= 0,95)
Hiç tanımadığım kişilerle sohbet ederim.	(X=1,54; SS= 1,02)
Kimin söylediğinin belli olmadığını bildiğim	(X=1,47; SS= 1,04)

için İnterneti insanlarla alay etmek için kullanırım.

Araştırmada "öğrencilerin cinsiyetleri ile bilgi güvenliği farkındalığı arasında istatistiksel olarak anlamlı bir ilişki var mıdır?" sorusuna cevap aranmıştır. Örneklem grubunun büyük olması durumunda parametrik testlerin yapılabileceğinden [19] verilere bağımsız örneklem t testi yapılmasına karar verilmiştir.

Tablo 9. Cinsiyete göre bilgi güvenliği farkındalığı t testi

Cinsiyet	N	$\bar{X}$	SS	Levene Testi F	Levene Testi p	df	t	p
Kız	1351	2,67	0,38	3,8	0,05	2447	11,84	0,000
Erkek	1098	2,50	0,35					

Tablo 9 incelendiğinde kız öğrencilerin (X=2,67) bilgi güvenliği farkındalığı konusunda erkek öğrencilere (X=2,50) göre daha olumlu görüşe sahip oldukları belirlenmiştir. Bu farkın istatistiksel olarak anlamlı olup olmadığına karar vermek için p değerine bakıldığında, p değerinin anlamlılık düzeyi 0,05'ten küçük olduğu görülmektedir ($t_{(2447)}$=11,84; p=0,000).

Araştırmada öğrencilerin öğrenim seviyesi değişkenine göre bilgi güvenliği farkındalığına ilişkin görüşleri istatistiksel olarak analiz edilmek istenmiş bunun için verilere tek yönlü ANOVA uygulanmış ve sonuçlar Tablo 10'da verilmiştir.

Tablo 10. Bilgi güvenliği farkındalıklarının öğrenim seviyesine Göre Tek Yönlü ANOVA Analizi

Okul Türü	N	$\bar{X}$	SS	Karelerin Toplamı		df	F	p
İlk. 1. Kdm. İlk. 2. Kdm.	694 1506	2,53 2,6	0,37 0,38	Gruplar Arası	11,65	2	42,74	0,000
Lise	249	2,8	0,33	Grup İçi	333,41	2446		

Tablo 10 incelendiğinde lisede öğrenim gören öğrencilerin bilgi güvenliği farkındalığının diğerlerine göre daha yüksek olduğu anlaşılmaktadır (X=2,78). Öğrencilerin öğrenim seviyeleri ile bilgi güvenliği farkındalığı arasında istatistiksel olarak anlamlı bir fark olduğu görülmektedir ($F_{(2,2446)}$=42,736; p=0,000). Bu farkın hangi gruplar arasında olduğuna karar vermek için ANOVA analizinde Bonferroni analizi uygulanmış ve lisede öğrenim gören öğrenciler lehine istatistiksel olarak fark olduğu belirlenmiştir.

Araştırmada öğrencilerin yaşadıkları yerleşim yeri değişkenine göre bilgi güvenliği farkındalığına ilişkin görüşleri istatistiksel olarak analiz edilmek istenmiş bunun için verilere tek yönlü ANOVA uygulanmış ve sonuçlar Tablo 11'de verilmiştir.

Tablo 11. Bilgi güvenliği farkındalıklarının yerleşim yerine Göre Tek Yönlü ANOVA Analizi

Yerleşim yeri	N	$\bar{X}$	SS	Karelerin Toplamı		df	F	p
Köy	317	2,53	0,37	Gruplar Arası	3,87	3	9,24	0,000
Kasaba	208	2,51	0,41					
İlçe	368	2,64	0,35	Grup içi	341,19	24 45		
İl Merkezi	1556	2,61	0,37					

Tablo 11 incelendiğinde ilçe merkezinde yaşayan öğrencilerin bilgi güvenliği farkındalığının diğerlerine göre daha yüksek olduğu anlaşılmaktadır (X=2,64). Öğrencilerin yaşadıkları yerleşim yeri ile bilgi güvenliği farkındalığı görüşleri arasında istatistiksel olarak anlamlı bir fark olduğu görülmektedir ($F_{(2,2446)}$=42,736; p=0,000). Bu farkın hangi gruplar arasında olduğuna karar vermek için ANOVA analizinde Bonferroni analizi uygulanmış ve il merkezinde, ilçe merkezinde yaşayan öğrencilerin köyde ve kasabada yaşayanlara göre daha olumlu görüşe sahip oldukları belirlenmiştir.

Araştırmada "evde internete bağlanan çocuklara bilgisayar kullanımı konusunda kural konulması ile bilgi güvenliği farkındalığı arasında istatistiksel olarak anlamlı bir ilişki var mıdır?" sorusuna cevap aranmıştır. Bu amaçla verilere bağımsız örneklem t testi yapılmış ve bulgular Tablo 12'de verilmiştir.

*Tablo 12. Bilgi güvenliği farkındalıklarının kullanım kuralı olup olmamasına göre t testi**

Kural	N	$\bar{X}$	SS	Levene Testi F	Levene Testi p	df	t	p
Var	535	2,70	0,33	5,812	,016	906	0,452	0,651
Yok	373	2,71	0,38					

Tablo 12 İncelendiğinde internete bağlanma konusunda kural uygulanmayan öğrencilerin (X=2,71) bilgi güvenliği farkındalığının kural uygulanan öğrencilerin (X=2,70) görüşlerinin aritmetik ortalamaları arasında çok az bir fark olduğu belirlenmiştir. Bu farkın istatistiksel olarak anlamlı olmadığı sonucuna ulaşılmıştır ($t_{(906)}$=0,452; p=0,651).

IV. TARTIŞMA VE SONUÇLAR

Akkoyunlu'nun yaptığı bir araştırmada (2004) ilköğretim 4. – 8. sınıftan, 10 – 14 yas arasındaki 319 öğrenciye "Bilgisayar ve bisiklet arasında bir secim yapmanız gerekseydi hangisini seçerdiniz? Niçin?" sorusu yöneltilmiştir. Sonuçlara bakıldığında öğrencilerin çoğunluğu bilgisayarı tercih etmişlerdir. Öğrenciler düşüncelerini ifade ederken bilgisayar ve internet ile her şeyin yapılabileceğini, ileride seçecekleri mesleklerle ilgili olduğunu, internetten araştırma yaparak kendilerini geliştirdiklerini, haberleşme aracı olarak kullandıklarını, hem eğitici hem de eğlenceli oyunlar oynadıklarını ve derslerinde yardımcı olduğunu belirtmişlerdir. Ayrıca, bilgisayarın öğrencilerin büyük bir kısmı için internet ve oyunla özdeşleştiği sonucu çıkmıştır[3]. Information Technology Resource Management Council, (ITRMC) ise, 5.-12. sınıf öğrencilerinin %90'ının bilgisayar kullandığını belirtmiştir. Amerika Birleşik Devletlerinin ulusal bilgi güvenliği raporunda da çocuk ve gençlerin günlerinin %33 lük kısmını internet başında geçirdiklerini tespit edilmiştir.

Amerika Birleşik Devletleri ulusal bilgi güvenliği raporunda, öğrencilerin %94 ünün interneti araştırma yapmak amacıyla kullandığı ifade edilmiştir. Bu çalışmada da evden ve internet kafeden internete bağlanan öğrencilerin internete ders çalışmak amacıyla girdikleri sonucuna ulaşılmıştır. Dolayısıyla bu sonuç Amerika Birleşik Devletleri ulusal bilgi güvenliği raporundaki durumla benzer görülmüştür. Bu çalışmanın diğer bir sonucu da internet kafeden internete bağlanan öğrencilerin internet kafeyi oyun oynamak amacıyla kullanma oranının yüksek olmasıdır. İnternet kafelerde veli kontrolünün bulunmamasının bu duruma yol açabileceği düşünülmüştür.

Araştırmaya katılan öğrencilerin bilgi ve bilgisayar güvenliği konusundaki farkındalık düzeyleri konusunda aşağıdaki sonuçlara ulaşılmıştır.

Öğrenciler, güvenli şifre kullanımı, çevrimiçi güvenli iletişim, kötücül yazılım denetlemesi yapma, belge koruma, kişisel bilgisayar güvenliği, güvenlik duvarı ve filtreleme yazılımları kullanımı, çevrimiçi arkadaş edinme ve internetin güvenli bir alan olup olmadığı konularında farkındalık düzeylerinin çok düşüktür. Yine Amerika Birleşik Devletlerinin ulusal bilgi güvenliği raporunda, çok az öğretmenin temel internet kullanım becerilerini öğrettikleri görülmüştür[17]. Örneğin öğretmenlerin % 23 ü güçlü şifre oluşturma, %34 ü kişisel bilgileri internette kullanma ve %33 ü özel hayata saygı gösterme ile ilgili konularda öğrencileri bilgilendirdiğini belirtilmiştir. Türk Eğitim Sisteminde de Bilişim teknolojileri derslerinin seçmeli ve 1 saat olduğu göz önüne bu durumun oluşması beklenen bir durumdur. Öğretmenlerin çok azının bilgi güvenliği konusunun öğretimine önem verdiği göz önüne alındığında, bu çalışmada öğrencilerin güvenli şifre kullanımı, çevrimiçi güvenli iletişim, kötücül yazılım denetlemesi yapma, belge koruma, kişisel bilgisayar güvenliği gibi konularda farkındalık düzeylerinin düşük bulunması doğal görülmüştür.

İnternette başkalarının bilgisine izinsiz olarak erişmenin suç olduğu, okul içinde kullanılan internetin güvenli olduğu, web de dolaşırken güvenli web sitesini ayırt edebilme ve kendi bilgilerinin kötü niyetli kişiler tarafından kullanılabileceği konularının farkında oldukları görülmüştür. Hâlbuki ITRMC, 5-12. sınıf öğrencilerinin yarısından çoğunun internette sohbeti güvenli bulduğunu ve % 40'ının kişisel bilgilerini internette paylaştıklarını kabul ettikleri vurgulamıştır[16].

Öğrencilerin, interneti sadece bir eğlence aracı olarak görmedikleri, izinsiz müzik ve program edinmenin yanlış olduğu, başkalarına ait alanlarda izinsiz işlem yapmanın sakıncalı olduğu, orijinal olmayan yazılım kullanımının sakıncalı olduğu, dosya paylaşım sitelerinin kullanımının etik olmadığı, sohbet odaları ve tanımadığı kişilerle iletişim kurmanın güvenli olmadığı, çevrim içi uygunsuz ortamlara girmenin sakıncalı olduğu konularında orta düzeyde farkındalık düzeyine sahip oldukları saptanmıştır. Ayrıca öğrenciler, bilgi güvenliğine ilişkin yeterli bilgiye sahip olmadıklarını belirtmişlerdir.

İnternetten alışveriş yapma konusunda aileleri de dâhil olmak üzere öğrencilerin internetten alışverişi tercih etmedikleri görülmüştür. Aynı zamanda internet üzerinden bilerek yasadışı etkinlikler yapılmaması gerektiği konusunda öğrencilerin yüksek bir farkındalığa sahip oldukları belirlenmiştir.

Araştırmada kız öğrencilerin erkek öğrencilere göre bilgi güvenliği farkındalığı seviyeleri daha yüksek bulunmuştur. Bunun sebebinin bölgesel etkilerden kaynaklamış olabileceği düşünülmüştür. Bununla birlikte il ve ilçe merkezinde yaşayan öğrencilerin kasaba ve köyde yaşayan öğrencilere göre bilgi güvenliği farkındalık seviyeleri daha yüksek bulunmuştur. Öğrencilerin öğrenim düzeylerine göre bilgi güvenliği farkındalık düzeylerinin ise öğrenim seviyesi yükseldikçe arttığı belirlenmiştir. Araştırmada lisede öğrenim gören öğrencilerin bilgi güvenliği farkındalık düzeylerinin diğerlerine göre daha yüksek olduğu belirlenmiştir.

Dunkels'ınChildren'sStrategies on the Internet (2008) isimli çalışmasında da K8 düzeyindeki çocukların internet kaynaklı zararlara maruz kaldığı ve önlemlerin yetersiz olduğu vurgulanmıştır. ITRMC'de günümüz çocuklarının ailelerinden daha çok bilgisayar ve internet kullanımı bilgisine sahip olduğu ve dolayısıyla ailelerin internet kullanımıyla ilgili çocuklarına danışmanlık yapamadığını belirtmektedir[16]. ITRMC yine bu konuda öğrencilerin 1/3 ünün internet filtreleme önlemini kaldırma yeteneğine sahip olduklarını vurgulamıştır. Canbek ve Sağıroğlu'nun "Çocukların ve Gençlerin Bilgisayar ve İnternet Güvenliği" isimli çalışmasında ise, ebeveynlerin yeterli güvenlik önlemlerini almadıklarından dolayı çocuklarını internetteki tehlikelerden koruyamadıkları görülmüştür. Hâlbuki Tekerek ve Mart (2010), ailelerin bu tehlikelerin çoğundan habersiz olduklarını ve buna bağlı olarak süre sınırlaması koymak gibi basit önlemler kullandıklarını belirtmişlerdir. Bu çalışmada ise öğrencilerin internete bağlanmaları konusunda ailelerin kural uygulamalarının öğrencilerin bilgi güvenliği farkındalık düzeyleri üzerinde herhangi bir farklılık oluşturmadığı sonucuna varılmıştır.

Araştırma sonucunda, bilgi ve bilgisayar güvenliği farkındalığı konusunda, pozitif ve negatif olarak nitelenebilecek bulgulara ulaşılmıştır. Temel olarak öğrencilerin etik konularında yeterli bilinç düzeyine sahip oldukları gözlenirken, kurallar ve bilgi gerektiren konularda farkındalık düzeylerinin düşük olduğu belirlenmiştir. Bu da bilgi ve bilgisayar güvenliği farkındalık eğitim ve etkinliklerinin yetersiz kaldığı düşüncesini doğurmaktadır.

Bilgiye erişim olanaklarının internete erişimle aynı anlamda kullanıldığı gerçeği doğrulturunda eğitim kurumlarımızın öğrencilerini bilgi çağına hazırlamasının beklenmesi kaçınılmaz bir durumdur. Bu doğrultuda FATİH projesi gibi uygulamalarla bilgi iletişim teknolojilerini yoğun bir şekilde kullanmaya başlayan eğitim kurumlarının öğrencilerine bilgi güvenliği farkındalığı kazandırmak adına üzerlerine düşenler yadsınamaz bir gerçektir.

Bilişim Teknolojileri derslerinin haftada 1 saat ve seçmeli olarak okutulduğu Türk Eğitim Sistemi içerisinde öğrencilere bilgi ve bilgisayar güvenliği farkındalığının kazandırılması açısından bu çalışmanın araştırmacılara ışık tutması amaçlanmıştır.

KAYNAKLAR

[1] Asan, A. & Koca, N. "An analysis of students' attitudes towards the Internet", Conference Paper 4th *International Conference on Multimedia and Information and Communication Technologies in Education*, Spain, 2006

[2] A.Z. Akman, İlköğretim Öğrencilerinin Bilgisayar, İnternet, Televizyon Sahiplik ve Kullanım Durumları,"s. 21-24, 2006

[3] B. Akkoyunlu, "Bilgisayar mı Bisiklet mi?", Türkiye Bilişim Derneği Dergisi Sayı: 152, 2004

[4] A. Yıldırım, , H. Şimşek, "Sosyal bilimlerde nitel araştırma yöntemleri. ". Ankara: Seçkin yayıncılık, 2005

[5] D. Fallows, "The Internet and Daily Life", Pew Internet & American Life Project, Washington, D.C. ,2004.

[6] E.Dunkels ," Children's strategies on the Internet", Vol. 49, No. 2, 171–184, September 2008

[7] G. Canbek, Ş. Sağıroğlu, "Bilgisayar Güvenliği ve Casus Yazılımlar Kapsamında Kişisel Gizlilik ve Yasal Düzenlemeler" 2007.
[8] G. Canbek, Ş. Sağıroğlu, "Çocukların ve Gençlerin Bilgisayar ve İnternet Güvenliği", cilt.10, no.1 s. 33-39, 2007.
[9] J. C. Watson, "Internet addiction diagnoss and assessment: implications for counselors," *Journal of Professional Counseling Practice and Researsh*, Vol.33, No. 2, pp. 3- 29, 2005.
[10] K. Subrahmanyam , R. E Kraut., P . M. Greenfield, , E. F. Gross, , "The Impact of Home Computer Use on Children's Activities and Development", Children and Computer Technology, Vol.10, No. 2, pp. 123- 144, 2000.
[11] M. K. Shields, R. E Behrman, "Children and Computer Technology: Analysis and Recommendations", The Feature of Children Journal, Vol.10, No. 2, pp. 3- 29, 2000.
[12] N. Yalçın, "İnterneti Doğru Kullanıyor muyuz? İnternet Bağımlısı mıyız? Çocuklarımız ve Gençlerimiz Risk Altında mı? "Denizli: Pamukkale Üniversitesi: Akademik Bilişim Konferansı, 9-11 Şubat 2006
[13] P. Stock, , "The Harmful Effects on Children of Exposure to Pornography", Canadian Institute for Education on the Family, 2004.
[14] T. Yiğit, , M. Sığla, , N. Aksungur, S. Erbağ, Ü. Palaz, "Çocuklar İçin İnternet Güvenliği: Bir Ebeveyn Kontrol Aracı ", Akademik Bilişim 2007
[15] DPT, "Bilgi Toplumu İstatistikleri" 2011,pp. 13, 2011
[16] ITRMC, "Cyber Security Awareness Month Key Messages", 2006, pp.3,2011
[17] National Cyber Security Alliance, " State of U.S. Cyber Education",
http://staysafeonline.org/sites/default/files/resource_documents/Cyber%20Education%205.3.11%20PDF.pdf, 12.03.2012
[18] M. Tekerek, İ. Mart, "Behavioral Computer and Web Security Awareness for K8 Level, 4th Information Security and Cyriptology Conference Proceeding Book, pp: 254-258, 2010
[19]. N. Karasar, "Bilimsel Araştırma Yöntemi", Nobel Yayınları, 2005
[20]. H. Tekin, "Eğitimde Ölçme ve Değerlendirme", Yargı Yayınları, 1996

On Applications of Privacy-Preserving Collaborative Filtering Schemes[1]

A. Bilge, C. Kaleli, I. Yakut, H. Polat[2]

Abstract— **Privacy-preserving collaborative filtering (PPCF) has been receiving increasing attention lately. Several PPCF schemes have been proposed for performing collaborative filtering services without deeply jeopardizing data owners' privacy. The proposed methods have been investigated in terms of privacy, performance, and accuracy. For each method, it has been shown that they are secure, able to provide accurate recommendations, and their online performance is comparable. However, they have not been investigated in terms of possible challenges and problems that might occur while utilizing them in real applications.**

In this study, we scrutinize different PPCF methods in terms of usability; and discuss the challenges that might be faced while utilizing them. We first classify the PPCF schemes according to various dimensions. We then list possible challenges and/or problems that might occur while applying them in recommender systems. We finally recommend some suggestions to eliminate them at all if possible or to lower their effects. Our study can give an idea about the applicability of the proposed PPCF approaches to those users and/or companies that plan to utilize them.

Index Terms — **Application, privacy, collaborative filtering, recommendation, usability.**

I. Introduction

With increasing popularity of e-commerce, number of online vendors utilizing recommender systems has been rapidly growing. Collaborative filtering (CF) techniques are widely used by recommender systems for estimating recommendations on customers' past experiences. The idea behind CF is that if two customers share similar interests in the past, they tend to share similar preferences in the future, as well [1]. Customers get predictions about the products they plan to buy, which help them choose the right products without wasting money and time. Online vendors are able to increase their sales and profits by providing recommendations to their customers because such services help them increase number of loyal customers and recruit new ones.

Performing CF services on plain data might cause some privacy, financial, and legal concerns [2, 3]. First, data collected for CF purposes are considered confidential data. In case of bankruptcy, such data are considered valuable asset. E-commerce sites can derive useful information about their customers from the ratings they provided. Online vendors can learn how much their customers like or dislike an item; or what products they bought before or showed interest. Moreover, since they are used to increase sales and profits, disclosing them might cause financial losses. Finally, legal regulations prevent data collectors from sharing or transferring such data. Revealing them might cause legal concerns. Due to such issues, it becomes important to provide recommendations without divulging private data. Hence, various schemes have been proposed to achieve CF services while preserving data owners' confidentiality. On one hand, privacy-preserving schemes should protect private data; on the other hand, they should still be able to offer predictions with decent accuracy. Moreover, they should be comparable with the traditional methods in terms of online efficiency. But, due to conflicting nature, it is a challenge to achieve three goals simultaneously.

In addition to privacy, accuracy, and performance, usability should be another dimension of which the proposed schemes should be analyzed. Although various PPCF schemes have been proposed; and they have been analyzed in terms of privacy, accuracy, and online efficiency, they have not been scrutinized in terms of usability. In other words, there exist no studies concerning the applications of such methods. Practical applications of PPCF schemes might face with various challenges. It is critical for the success of PPCF schemes to determine the possible problems and propose related solutions to eliminate them at all or reduce their effects. In addition to investigating such methods in terms of privacy, accuracy, and performance, their usability should be analyzed, as well.

In this study, we investigate PPCF schemes in terms of challenges that might be faced while using them in recommender systems. There are various PPCF methods having different properties besides the common ones. Since different schemes might face different challenges, we first classify PPCF schemes according to some dimensions that we determined. We then study various challenges of each class of the methods. Besides conflicting goals of privacy, accuracy, and performance, we scrutinize the PPCF approaches in terms of usability. The methods might achieve the expected goals theoretically. However, applications of them in recommender systems might face with some challenges. Thus, our major intend is to unveil such problems. After determining possible challenges, we recommend some possible solutions to eliminate them at all if it is possible or reduce their effects as much as possible. Our work guides those online vendors that plan to apply PPCF schemes in their recommender systems.

[1] This work was supported by TUBITAK under Grant 108E221.
[2] Corresponding Author: Department of Computer Engineering, Anadolu University, 26470 Eskisehir, Turkey (e-mail: polath@anadolu.edu.tr)

II. Related Works

Since privacy is an important challenge for CF schemes, researchers have great intention on this subject and propose several solutions for different privacy challenges in recommender systems. We can partition those studies into two groups, first one covers the studies related protecting individuals' privacy while the second group considers data holders' privacy.

Canny [4] proposes a homomorphic encryption-based solution to protect users' privacy in a fully P2P system. Polat and Du [5] discuss privacy protection for correlation-based and singular-value decomposition (SVD)-based CF algorithms. They employ randomized perturbation techniques (RPT) to protect users' confidentiality. To achieve private recommendations with Eigentaste-based CF, Yakut and Polat [6] introduce an RPT-based solution. In addition to RPT, data obfuscation and randomized response techniques (RRT) are utilized in CF to protect users' privacy. Parameswaran and Blough [7] propose a framework for obfuscating confidential information of individuals in CF. Kaleli and Polat [8] introduce a privacy-preserving scheme based on RRT for naïve Bayesian Classifier (NBC)- based CF algorithm. The same authors also propose a solution for protection individuals privacy on a P2P network while performing NBC-based CF algorithm [9]. Lathia et al. [10] introduce a new measure to compute correlation between users while protecting their privacy. This measure is employed in P2P systems-based CF applications. Shokri et al. [11] enable users to control their private profile and they disguise their profile by partly merging the profiles with other similar users' profile.

Besides protecting individuals' privacy, data holders need to consider their privacy if they collaborate with other parties. Since users do shopping from different online vendors, data collected for CF purposes might be distributed among parties. Thus, researchers investigate solutions providing collaboration of parties while producing recommendations. Kaleli and Polat [12] introduce private protocols for parties aiming to collaborate while producing NBC-based recommendations on partitioned (horizontally or vertically) data. In the same way, Yakut and Polat [13] propose solutions for providing SVD-based referrals on partitioned data without greatly jeopardizing data holders' privacy. In addition to collaboration of two parties, data might be distributed among multiple parties. Kaleli and Polat [14] study on private protocols to enable data holders providing SOM-based recommendations on vertically distributed data. Besides horizontally and vertically distributed data configuration, data might be partitioned arbitrarily between two parties. To make possible collaboration of parties when data arbitrarily partitioned, Yakut and Polat [15, 16] introduce different solutions.

III. Classification of PPCF Schemes

As explained previously, there are various PPCF approaches proposed in the literature. It is not appropriate to discuss the challenges that each method might face. Better alternative is to group such schemes into some classes according to some dimensions and attributes. Hence, in this section, we first determine the conceivable dimensions. Then, possible attributes for each dimension are decided. We finally create classes based on them. Notice that there are various CF algorithms. Namely, there are memory- or model-based algorithms and hybrid schemes. Different approaches might apply different soft computing techniques like Bayesian classification, neural network approaches, self-organizing map (SOM) clustering, and so on. Moreover, some utilize binary ratings while others use numeric ratings (discrete or continuous). Each algorithm might have different weaknesses or disadvantages. Similarly, they might have various challenges related to their applications. Our focus here is not CF algorithms and their challenges. We want to focus on the challenges of PPCF schemes.

To better scrutinize the possible challenges introduced during applications of PPCF methods, we first determine dimensions, which can be used for classification. After investigating various PPCF schemes, we conclude the following three major dimensions for classification:

A. Data Partitioning-DP
B. Data Partitioning Configuration-DPC
C. Privacy-preserving Measure-2PM

The dimensions have different attributes that can be used for classifying various PPCF approaches. In the following, we explain each dimension and their related attributes.

A. Data Partitioning (DP)

Data collected for CF purposes might be held by different entities. Such data collected as ratings are saved in an $n \times m$ matrix, called user-item matrix **D**, where n and m represent number of users and items, respectively. The way in which data are held is called data partitioning (DP). DP is an important dimension that might affect the applicability of various PPCF schemes. Different partitioning cases may pose different challenges. In terms of DP, we determine the following attributes:

I. Central Server-based DP-1P: In some applications like client-server (the systems run by Yahoo, Amazon, etc.), collected data are held by a single vendor, referred to as central server-based DP (**1P**). The server gathers ratings from n users for m items; and then saves them in **D**. Notice that **D** is held by a single party only. The data collector or the server controls all collected data. When an active user (a) who is looking for a prediction for a target item (q) wants a prediction (p_{aq}), she communicates with the server. After estimating p_{aq}, the server returns it to a.

II. Distributed Data Partitioning-2DP: Unlike **1P** partitioning case, users' preferences might be distributed between various online vendors, referred to as distributed DP (**2DP**). Some online vendors, especially recently established companies, might have problems collecting enough ratings for CF purposes. Those companies holding scarce data may want to integrate their data for better services. In **2DP**, **D** is distributed among various number of e-commerce sites, even competing ones. When data are distributed, there are three possible cases, as follows:

a. Partitioned Data-2P: In this case, **D** is partitioned between two companies only. Thus, we call this partitioning as partitioned data or **2P**. In this scenario, a asks a prediction from one of the parties. The party estimates the predictions based on integrated data.

b. Multi-party Distributed Data Partitioning-MP: Unlike **2P**, data are distributed among multiple parties. In other words, **D** is partitioned among more than two parties. We call this data partitioning case as multi-party or **MP**. Notice that if M shows number of parties, then M is usually a small constant and $M << n$ and $M << m$. In the **MP**, one of the collaborating companies acts as a leading party that communicates with both a and other helping vendors.

c. Fully Distributed Data Partitioning-P2P: Although data are distributed in this case, each user actually acts as an involving company. This type of partitioning is common in social network applications like one-to-one (chat) communication applications. When data are distributed among n parties or users, we call this scheme as peer-to-peer (**P2P**).

As expected, abovementioned partitioning cases might pose different challenges and application issues because each scenario has its own specific properties. Therefore, we investigate application challenges of PPCF schemes after grouping them into different classes using data partitioning attributes. Fig. 1 shows these data partitioning cases. On one extreme point, data are held by a single party (**1P**), on the other extreme point; **D** is fully distributed among n users (**P2P**). Between these two extreme points, we have partitioned and multi-distributed cases (**2P** and **MP**, respectively).

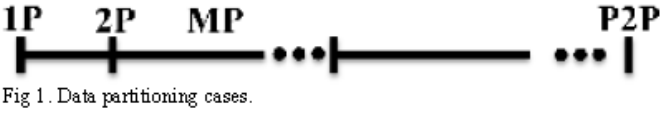


Fig 1. Data partitioning cases.

B. Data Partitioning Configuration (DPC)

Another dimension that can be used for classification is called data partitioning configuration (DPC). DPC represents how data are distributed between different online vendors. Data might be partitioned horizontally, vertically, or arbitrary. Hence, we determine the following attributes:

I. Horizontal Partitioning (HP): In horizontal partitioning, each party holds the ratings of the disjoint sets of users for the same items. Suppose that data are partitioned among C vendors, where C can be 2 (representing **2P**), $2 < C << n$ (representing **MP**), or $C = n$ (representing **P2P**). Each party c holding ratings of disjoint sets of n_c users for the same m items, where $c = 1, 2, \ldots, C$. Thus, the integrated data has the size $(n_1 + n_2 + \ldots + n_C) \times m$, while split data held by each vendor c, called $\mathbf{D}_c$, has the size $n_c \times m$.

II. Vertical Partitioning (VP): Unlike horizontal partitioning, in vertical partitioning, each party has the same users' ratings for the disjoint sets of items. Assume again that data are partitioned among C vendors, where C can be 2 (representing **2P**), $2 < C << m$ (representing **MP**), or $C = m$ (representing **P2P**). Each party c holding ratings for disjoint sets of m_c items of the same n users, where $c = 1, 2, \ldots, C$. Thus, the integrated data has the size $n \times (m_1 + m_2 + \ldots + m_C)$, while split data held by each vendor c, called $\mathbf{D}_c$, has the size $n \times m_c$.

III. Arbitrary Partitioning (AP): Arbitrary partitioning is the combination of both horizontal and vertical partitioning. Given the **D** including the ratings of n users for m items, each party holds some of the ratings in **D**. Suppose that v_{ij} represents a rating of user i for item j in **D**, then each company owns v_{ij} values for some i and j. As an example, we show AP for two parties only in Fig. 2. We assume that **D** is partitioned between two companies, c_1 and c_2. Given m products, users usually rate some of them leading to very sparse data. Hence, some of the cells are unrated in Fig. 2.

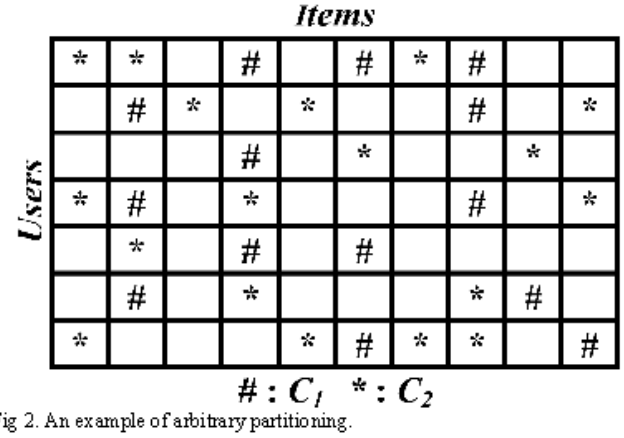


Fig 2. An example of arbitrary partitioning.

C. Privacy-preserving Measure (2PM)

In PPCF schemes, users' preferences as ratings and the rated and/or unrated items are considered confidential. For any data owner, either a customer or a company, performing CF services without divulging private data is imperative. With increasing popularity of privacy-preserving data mining, researchers have been recommended different privacy-preserving measures. Since CF can be considered as a subset of data mining, those techniques invented for preserving privacy in data mining functionalities can be applied to and have been applied to CF schemes, as well.

In traditional CF algorithms without privacy concerns, various challenges have been identified and efficient solutions have also been proposed. When privacy is a concern, offering CF services while achieving confidentiality brings some issues, too. Two major constraints that each CF scheme should satisfy are accuracy and efficiency (online performance). However, as expected, applying privacy-preserving measures might make accuracy and/or online performance worse. The reason for this phenomenon is that privacy, accuracy, and efficiency are conflicting goals. Different privacy-preserving technique might bring different issues. Although effects of privacy measures on accuracy and online performance have been investigated, there are still open questions about how such measures affect usability of PPCF schemes. Moreover, it is likely that the effects of different privacy-preserving methods cause different issues or challenges related to applications of PPCF schemes as a part of recommender systems used by various e-commerce sites. Therefore, we consider privacy-preserving methods as another dimension for grouping PPCF schemes; and scrutinize challenges of applications of PPCF schemes in terms of such methods. We determine the following techniques used as privacy-preserving methods in PPCF schemes:

I. Randomization Techniques (RT): Randomized methods have been widely used in PPCF schemes for data masking.

Randomization-based approaches are useful when we are interested in aggregate data. There are three randomization schemes applied to CF algorithms for privacy-preserving:

a. Randomized Perturbation Techniques (RPT): Random numbers, drawn from over a specified range with mean being 0 using some distribution like uniform or Gaussian, are added to confidential data. Instead of actual data items, perturbed data values are sent to data collectors. Such techniques are suitable for numeric ratings-based schemes and widely used in central server-based PPCF methods.

b. Randomized Response Techniques (RRT): When users' preferences are represented using binary ratings, RRT are utilized for data masking. According to the result of a comparison between a specified value (θ) and a random number (r), data owners decide whether to send true data or false data (exact opposite of actual ratings) to data collectors. RRT are useful in central server-based PPCF schemes. There are two variants of RRT. They are one-group scheme (**1G**) and multi-group scheme (**MG**).

1. In **1G**, all ratings are placed in a vector. Entire ratings are disguised together.
2. In **MG**, ratings are divided into groups and each group is masked independently.

c. Random Filling (RF): In addition to perturbing real ratings, it is also crucial to mask rated and/or unrated item cells. To do so, PPCF schemes also utilize random filling (**RF**) in which some uniformly randomly chosen cells are filled with some default votes or noise data.

II. Cryptographic Techniques (CT): In addition to randomized methods, cryptographic methods have been also widely used for achieving privacy in PPCF schemes. Most commonly utilized CT are given in the following:

a. Homomorphic Encryption (HE): Encryption functions with homomorphic property allow performing certain operations on encrypted data without decrypting them [17]. HE methods can be used in various systems for ensuring privacy of processed data. For example, assuming that ξ is an encryption function, K is a public key, and x and y are private data values, HE property allows an addition operation to be conducted based on the encrypted data without decrypting them, as follows: $\xi_K(x) \times \xi_K(y) = \xi_K(x + y)$. HE methods happen to be secure schemes. However, they have efficiency and implementation problems.

b. 1-out-n Oblivious Transfer Protocol (OT): OT refers to a protocol, where at the beginning of the protocol one party, Bob has n inputs $X_1, \ldots, X_n$ and at the end of the protocol the other party, Alice, learns one of the inputs X_i for some $1 \leq i \leq n$ of her choice, without learning anything about the other inputs and without allowing Bob to learn anything about i.

c. Secure Multi-party Computation (SMC): SMC enable two or more parties to evaluate a specified function of their inputs collaboratively without disclosing their inputs to each other. When multiple companies want to perform some computations jointly while keeping their private data secret, they might decide to use SMC protocols.

III. Data Obfuscation (DO): Basic idea behind DO methods is to substitute private data values with some other data whose disclosure does not violate privacy constraint. DO techniques used in PPCF schemes substitute real ratings with predefined values or their neighbors in the metric space. Berkovsky et al. [18] list three general policies for obfuscating the ratings in the user profiles in CF systems for accomplishing confidentiality. *Default obfuscation* of real rating votes, v_{ij} values, means that substituting the real ratings in the user profile with a fixed predefined value. *Uniform random obfuscation* allows substituting the real ratings in the user profile with random values chosen uniformly in the range of ratings in the dataset. Finally, in *bell-curved random obfuscation*, real ratings in the user profile are substituted with values chosen using a bell-curve distribution reflecting the distribution of ratings in the data set. Paremeswaran and Blough [7] propose to use *Nearest Neighbor Data Substitution* (NeNDS) approach to CF systems for protecting privacy. NeNDS substitutes individual data elements with one of their neighbors in the metric space.

IV. Others: There are some other techniques used in PPCF schemes as privacy-preserving measures. Anonymity and k-anonymity are among such methods. They are not widely used like randomization and cryptographic techniques. Anonymity prevents data collectors from learning the origin or the owner of the ratings. k-anonymity demands that every tuple in the data table released be indistinguishably related to no fewer than k respondents.

In Fig. 3, we show the dimensions we determined, which can be used to classify PPCF schemes. Also, we display the related attributes for each dimension. The figure shows the big picture of PPCF schemes in terms of various aspects.

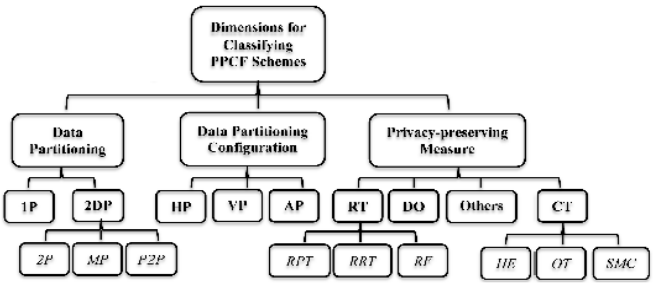


Fig 3. Dimensions and their related attributes for classifying PPCF schemes.

IV. Applications of PPCF Schemes: Challenges

In theory, theory and practice are the same; but in practice, they never are[3]. Although everything is clearly depicted and organized during design stages of any system, unexpected problems might occur due to avoidable and/or inevitable challenges. We describe such challenges in the following.

A. Data Losses during Communication

CF is designed to automate the "word-of-mouth" habit in web environment and hence, all PPCF applications run over

[3] Albert Einstein.

such applications; e.g., typically web browsers. Users of PPCF applications interact with the system through an unreliable packet-switched network infrastructure, which is vulnerable to packet losses during transmission. Since PPCF is an interactive and online process, users require quick and accurate responses to their queries. If any query or part of preference data is lost on the way through, the server might not be able to produce a recommendation. Even worse, after successful transmission of preference data and query, produced recommendation might not be delivered to the client side. Both can reduce credibility of PPCF systems and lead customers to refrain from using such systems. Similar problem can be observed in distributed PPCF schemes. Notice that the collaborating parties exchange data during off-line and online stages. Although data losses during off-line computations can be overcome due to unrestricted requirements, data losses during online process might hinder the quality of predictions. When some of the data required for estimating recommendations get lost during online phase, accuracy losses are expected because smaller amount of data is used for generating predictions reducing the gains due to collaboration.

B. *User Interface Design*

According to Stone et al. [19], "good user interface design encourages an easy, natural, and engaging interaction between a user and a system, and it allows users to carry out their required tasks." However, PPCF schemes increase the visual design and algorithmic complexities. Without privacy-preserving measures, it is easy to create a user-friendly interface. Privacy concerns make it difficult for designers to design intelligible interfaces. Moreover, e-commerce sites must serve prediction services based on the privately collected data by means of web sites having a clear visual design.

C. *Unconscious Users*

One goal of PPCF systems is to protect individual privacy. However, the term "privacy" is getting interest through developments in the information systems and most of the average users of such systems are unaware of this phenomenon. Privacy, in the context of PPCF systems, includes both hiding true preferences and rated items. Such aspects are controlled via different parameters and selecting their values optimally due to personal requirements is vital because privacy protection and accuracy of recommendations are inversely correlated. If users are unconscious of those aspects and/or uninformed on how to choose privacy parameters optimally, all effort might become void for designing PPCF applications.

Cranor et al. [20] carried out a survey on the Internet users concluding that privacy concerns differs from one user to another. There are PPCF algorithms, which are sensitive to users' different privacy characteristics [21, 22]. To realize such schemes, PPCF web designers must consider various privacy concern levels of the Internet users. One of the application challenge of PPCF is that designed web site should serve from unconscious users to sophisticated users with all concerning about privacy in different levels. For those users living in developed countries, preserving privacy is vital. Customers are aware of their privacy and situations causing privacy violations. They act in such a way so that their privacy is not jeopardized. However, those users living in developing countries are not that aware of their privacy. Confidentiality might not be a big concern for them. Thus, they might hesitate to use PPCF schemes.

D. *Overheads due to Cryptographic Techniques*

Cryptographic techniques such as HE and OT protocol are effectively utilized in PPCF schemes. Due to their computational complexity, such techniques are heavily placed in off-line phase. However, there are also schemes offering them in online transactions [15]. To respond for user prediction request in decent time, such cryptographic overheads are cumbersome.

Although some works are performed off-line in PPCF applications, in essence, it is an online process; and like all online applications, the bottleneck of PPCF is time constrained. However, while encryption schemes provide a secure and privacy-preserving framework, they lead much computation complexity. Such side effects of encryption schemes must be overcome to make PPCF systems operate online and respond within reasonable amount of time.

E. *Practical Problems due to Encryptions*

To overcome privacy challenges, it is inevitable employing HE schemes. However, HE has no natural way of encrypting and decrypting floating point numbers and negative integers. In CF algorithms, similarities between users are operated and they are from the range [-1, 1]. When data are distributed, the parties perform sub-computations with their private data to use them in online recommendation process [14]. To protect their privacy, they encrypt those interim results, which are generally floating point numbers. Besides distributed data-based CF schemes, some solutions for protecting individuals' privacy in central server-based CF systems employ HE solutions. Thus, encryption of floating point numbers and negative integers are practical challenges that might be overcome for PPCF schemes.

F. *Synonymy*

In distributed data-based PPCF schemes, especially in HDD-based schemes, it is assumed that all collaborating parties own the same item sets. In other words, they provide predictions for the same products. However, different names might refer to the same item. Different parties might use different names for representing the same items leading synonymy problem.

V. SMOOTHING CHALLENGES: PROPOSED SOLUTIONS

Described challenges on deploying PPCF systems might be eliminated at all or their effects can be lowered by means of some application level measures. We suggest some procedures to handle referred problems on applications of PPCF schemes.

To reduce packet losses during communications between client applications and the server, or between multiple parties, secure and bandwidth allocated channels might be used and such applications need to be run over TCP to guarantee packet transmissions. In addition to TCP's 3-way handshaking reliable packet transfer protocol, also application level implementations can be deployed to assure successful data exchange and inform users and the server on this. Therefore,

an extra module responsible for reliable data transmission issues can be very useful to avoid such inconveniences.

To smooth above-mentioned user design challenges, first of all, rather than entering numerical privacy-adjusting parameters from keyboard, the system should offer user privacy level selection bar as in Fig. 3. Similar bar is utilized in Jester recommender system [23] to collect continuous ratings from users. Visuality facilitates user comprehension about privacy, enhances the user comfort and simplifies the use of interface. Moreover, if user clicks *no privacy* region, system ought to warn user as "you are publicly saving your rating information." Touch screen technologies also contributes visuality and can be considered in use for additional private information collection frameworks. Alternatively, privacy menu can be used by users for selecting the required level of privacy. For generation of such menu, one classification is realized by Aïmeur et al [24]. Considering different levels of concerns, they classify users into four classes: no privacy, soft privacy, hard privacy, and full privacy. Similar classification and labels can be given for particular value of privacy parameters. Finally, PPCF applications must provide a user-friendly GUI to make users feel comfortable on using such systems offering easy-to-use interactive interfaces to adjust level of privacy. Also, a detailed but easy to follow "Help" section must be made available to inform users about the aspects of their individual privacy and how to tune parameters of them.

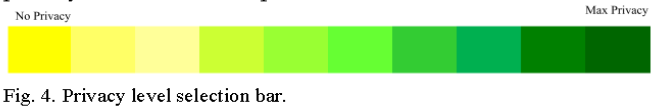


Fig. 4. Privacy level selection bar.

To handle overhead costs due to cryptographic methods, parallel computation techniques can be used. E-commerce parties can apply parallel and concurrent computation techniques to improve online time. If the selected cryptographic method is not parallelizable satisfactorily, parallelizable algorithms can be preferred. For instance, Kamara and Raykova [25] propose a parallel HE algorithm. Moreover, application-oriented hardware design can be another alternative. If the cryptographic tools must be used in online and parallel computation is unavailable or insufficient, then application-oriented hardware may be a solution. Also, rapidly evolving hardware, software, and information technologies may produce a solution to smooth such problem. Finally, some preprocessing schemes and model-based approaches must be followed to lower their side effects on online performance and accuracy. Extensive experiments must be performed periodically before and during publication of PPCF schemes. Also they must be updated occasionally according to experimental findings and latest improvements in scientific research area.

Encrypting floating point numbers and negative integers is not a challenge only for PPCF schemes. It is a general privacy-preserving data mining problem. Thus, researchers introduce solutions for practical challenges of utilizing HE. Pathak and Raj [26] study computing eigenvectors from distributed data without jeopardizing data holders' privacy. Since eigenvalue computation requires working with floating numbers and negative integers, the authors propose practical solutions for encrypting such values. To encrypt floating point numbers, they propose to floor this numbers by a fixed constant that is power of two for efficient arithmetic. After decryption, they divide the results with the same constant to get the actual result. In PPCF schemes, the same approach can be employed as a solution introduced by the authors to encrypt positive floating point numbers. To encrypt negative floating numbers, we can shift the interval of the numbers into a positive range after we can use the solution. In the case of encrypting negative integers using an HE, Pathak and Raj [26] represent negative numbers in binary two's complement system. It is possible to perform arithmetic operations such as addition, subtraction, and multiplication using two's complements numbers. In PPCF schemes, the proposed solution overcomes challenges caused by encryption of negative integers. In another study, Pathak et al. [27] utilize a similar solution to encrypt floating point numbers.

Collaborating parties make sure that they share or use the same item names for the same products before they start providing recommendations collaboratively to resolve synonymy problems. In order to offer predictions for the same items, the parties must use the same IDs or names referring for the same products. Similar case is true for the user IDs. Collaborating companies also utilize the same IDs representing for the same users. Hence, before they start collaborative work, they should agree on user and item IDs and/or names referring for the same entities.

VI. Conclusions and Future Work

Although there are various studies describing how to offer predictions with privacy, they fail to explain possible challenges that might occur while implementing the proposed solutions in real life applications. Therefore, in this paper, we first determined possible attributes and dimensions with which the proposed privacy-preserving collaborative filtering schemes can be classified. We then classified such schemes in terms of data partitioning, partitioning configuration, and utilized privacy-preserving measures. We also investigated them in terms of the challenges and problems that they might face with while utilizing them in real applications. We finally suggested some solutions and approaches to remove such challenges at all or reduce their effects.

Similar application issues might occur during implementation of such methods. After intensive user requirement analyses, more issues can be determined. More work should be conducted to suggest possible solutions to overcome such practical challenges.

References

[1] M. Grcar, "User profiling: Collaborative filtering," in *7th International Multiconference Information Society IS 2004* Slovenia, 2004, pp. 75–78.

[2] OECD, "Guidelines on the Protection of Privacy and Transborder Flows of Personal Data," 2005.

[3] OECD, "Guidelines for Consumer Protection in the Context of Electronic Commerce," 2000.

[4] J. Canny, "Collaborative Filtering with Privacy," in *Proceedings of the 2002 IEEE Symposium on Security and Privacy*, Oakland, California, USA, 2002, pp. 45-57.

[5] H. Polat and W. Du, "Privacy-Preserving Collaborative Filtering," *International Journal of Electronic Commerce,* vol. 9, pp. 9-35, 2005.

[6] I. Yakut and H. Polat, "Privacy-Preserving Eigentaste-Based Collaborative Filtering Advances in Information and Computer Security." vol. 4752, A. Miyaji, H. Kikuchi, and K. Rannenberg, Eds., ed: Springer Berlin / Heidelberg, 2007, pp. 169-184.

[7] R. Parameswaran and D. M. Blough, "Privacy Preserving Collaborative Filtering Using Data Obfuscation," in *Proceedings of the 2007 IEEE International Conference on Granular Computing*, Silicon Walley, CA, USA, 2007, pp. 380-386.

[8] C. Kaleli and H. Polat, "Providing Private Recommendations Using Naïve Bayesian Classifier," in *Advances in Intelligent Web Mastering*, vol. 43, K. Wegrzyn-Wolska and P. Szczepaniak, Eds., ed: Springer Berlin / Heidelberg, 2007, pp. 168-173.

[9] C. Kaleli and H. Polat, "P2P collaborative filtering with privacy," *Turkish Journal of Electric Electrical Engineering and Computer Sciences,* vol. 8, pp. 101-116, 2010.

[10] N. Lathia, S. Hailes, and L. Capra, "Private distributed collaborative filtering using estimated concordance measures," in *Proceedings of the 2007 ACM conference on Recommender systems*, Minneapolis, MN, USA, 2007, pp. 1-8.

[11] R. Shokri, P. Pedarsani, G. Theodorakopoulos, and J.-P. Hubaux, "Preserving privacy in collaborative filtering through distributed aggregation of offline profiles," presented at the Proceedings of the third ACM conference on Recommender systems, New York, New York, USA, 2009.

[12] C. Kaleli and H. Polat, "Providing Naïve Bayesian Classifier-Based Private Recommendations on Partitioned Data," in *Knowledge Discovery in Databases: PKDD 2007*. vol. 4702, J. Kok, J. Koronacki, R. Lopez de Mantaras, S. Matwin, D. Mladenic, and A. Skowron, Eds., ed: Springer Berlin / Heidelberg, 2007, pp. 515-522.

[13] I. Yakut and H. Polat, "Privacy-preserving SVD-based collaborative filtering on partitioned data," *Int. J. Information Technology & Decision Making,* vol. 9, pp. 473–502, 2010.

[14] C. Kaleli and H. Polat, "SOM-based recommendations with privacy on multi-party vertically distributed data," *Journal of Operational Research Society,* 2011.

[15] I. Yakut and H. Polat, "Arbitrarily distributed data-based recommendations with privacy," *Data & Knowledge Engineering,* vol. 72, pp. 239-256, 2012.

[16] I. Yakut and H. Polat, "Privacy-preserving hybrid collaborative filtering on cross distributed data," *Knowledge and Information Systems,* vol. 30, pp. 405-433, 2012.

[17] P. Paillier, "Public-key cryptosystems based on composite degree residuosity classes," in *Proceedings of the 17th international conference on Theory and application of cryptographic techniques,* Prague, Czech Republic, 1999, pp. 223-238.

[18] S. Berkovsky, Y. Eytani, T. Kuflik, and F. Ricci, "Privacy-Enhanced Collaborative Filtering," in *Workshop on Privacy-Enhanced Personalization, at the International Conference on User Modeling*, Edinburgh, UK, 2005, pp. 75-83.

[19] D. Stone, C. Jarret, M. Woodroffe, and S. Minocha, *User Interface Design and Evaluation*: Morgan Kaufmann 2005.

[20] L. F. Cranor, J. Reagle, and M. S. Ackerman, "Beyond Concern: Understanding Net Users' Attitudes About Online Privacy," AT&T Labs-Research1999.

[21] H. Polat and W. Du, "Effects of inconsistently masked data using RPT on CF with privacy," in *Proceedings of the 2007 ACM symposium on Applied computing*, Seoul, Korea, 2007, pp. 649-653.

[22] I. Yakut and H. Polat, "Achieving Private SVD-based Recommendations on Inconsistently Masked Data," in *Achieving Private SVD-based Recommendations on Inconsistently Masked Data*, 2007.

[23] K. Goldberg, T. Roeder, D. Gupta, and C. Perkins, "Eigentaste: A Constant Time Collaborative Filtering Algorithm," *Inf. Retr.*, vol. 4, pp. 133-151, 2001.

[24] E. Aimeur, G. Brassard, J. M. Fernandez, and F. S. M. Onana, "Alambic: a privacy-preserving recommender system for electronic commerce," *International Journal of Information Security,* vol. 7, pp. 307-334, 2008.

[25] S. Kamara and M. Raykova, "Parallel Homomorphic Encryption," Microsoft Research2011.

[26] M. Pathak and B. Raj, "Privacy preserving protocols for eigenvector computation," presented at the Proceedings of the international ECML/PKDD conference on Privacy and security issues in data mining and machine learning, Barcelona, Spain, 2011.

[27] M. Pathak, S. Rane, S. Wei, and B. Raj, "Privacy preserving probabilistic inference with Hidden Markov Models," in *Acoustics, Speech and Signal Processing (ICASSP), 2011 IEEE International Conference on*, 2011, pp. 5868-5871.

Kablosuz Algılayıcı Ağlarda Güvenli Ortam Erişim Protokolleri

Feyza YILDIRIM OKAY, Suat ÖZDEMİR
Gazi Üniversitesi, Mühendislik Fakültesi, Bilgisayar Mühendisliği Bölümü, Maltepe, Ankara, 06570
feyzaokay@gazi.edu.tr, suatozdemir@gazi.edu.tr

***Özet*—Kablosuz algılayıcı ağlar (KAA) son zamanlarda geliştirilen ve araştırmacıların üzerinde durduğu konulardan biridir. Çok geniş bir kullanım alanı olan kablosuz algılayıcı ağlar, askeri, sağlık, kimyasal, çevresel, endüstri ortamlarında kullanılabilmekle beraber, saptama, iz sürme, gözlemleme gibi işlevleri yapabilmektedirler. Kötücül kişiler, sınırlı güç tüketimi olan algılayıcıların oluşturduğu KAA'ların güvenliğini, ortam erişim kontrol protokollerindeki açıklardan faydalanarak tehdit etmektedir. Özellikle, farklı saldırı yöntemleriyle saldırganlar ağın yaşam ömrünü kısaltmaktadır. Bu makalede KAA'lardaki ortam erişim protokolleri üzerine gerçekleştirilen saldırılar ve bu saldırılara karşı geliştirilen protokoller özetlenmiş ve karşılaştırılmıştır.**

***Anahtar Kelimeler*—KAA; MAC; güvenlik; ağ ömrü**

***Abstract*—Wireless Sensor Networks (WSN) are one of the recent hot research areas that attracts researchers. WSNs have a wide range of application areas that include military, chemical, environmental and industrial applications. Due to their unattended nature malicious users attack WSNs by exploiting the weaknesses in medium access protocols. Especially, using different kind of attacks, attackers attempt to reduce the network lifetime. This paper summarizes the important attacks against the medium access control protocols of WSNs. The existing solutions to these attacks are also investigated and a comparison of these solutions is provided.**

***Key Words*—WSN; MAC; security; network lifetime**

I. GİRİŞ

Kablosuz algılayıcı ağlar (KAA), genel olarak çok sayıda algılayıcı düğümden oluşmaktadır. Bu düğümlerin sayısı KAA'nın kullanılacağı uygulamaya göre değişmektedir. Her bir düğüm oldukça sınırlı bir işleme yeteneğine ve hafızaya sahiptir [1]. Düşük enerjili akıllı algılayıcı düğümler, bir veya birden çok algılayıcı, işlemci, hafıza, güç kaynağı, radyo ve çalıştırıcı ile donatılmaktadır. Batarya, algılayıcı düğümlerdeki ana güç kaynağıdır. Düğümlerin dağılacağı ortamın uygun olmasına göre ikinci güç kaynağı olarak güneş panelleri konulabilmektedir [2]. Genellikle KAA'lar fiziksel veya çevresel durumları görüntüleyen sistemlerdir. Kablosuz algılayıcılar birçok farklı uygulamada kullanılabilmektedir. Bunlar; çevresel görüntüleme, ortam görüntüleme, askeri operasyonlar, bilimsel araştırmalar, oluşabilecek felaketleri tahmin etme ve ortaya çıkarma, tıbbi görüntüleme ve yapısal sağlık görüntülemeleridir [3,4]. Algılayıcı düğümler oldukça düşük enerjili ve değiştirilmesi çoğu zaman mümkün olmayan bataryalara sahiptirler. İşlem ve iletişim kaynakları da oldukça kısıtlı olup, sınırlı bir ömürleri vardır [1]. Bu nedenle kablosuz algılayıcı ağlarda yapılan çalışmalar daha çok algılayıcı düğümlerin yaşam sürelerini uzatmaya yöneliktir.

Ortam erişim katmanı, iki düğüm arasındaki iletimden sorumlu olup görevi düğümlerin paylaşımlı bir kanal üzerinden ne zaman ve nasıl iletim yapacağını belirlemektedir [5]. Ortam erişim kontrolü (MAC) protokolleri ile ağın yaşam süresi uzatılmakta ve enerji tüketimi azaltılarak enerjinin daha etkin kullanılması sağlanmaktadır. Ayrıca, adaptasyon ve ölçeklenebilirlik ile araştırmacılar algılayıcı ağların yaşam sürelerini uzatmaya çalışmaktadırlar [6,7]. Diğer taraftan MAC protokollerinin hareketlilik (mobilite) desteği olması dikkat edilmesi gereken diğer bir konudur. KAA'ların çoğu zaman askeri ve görev kritik alanlarda kullanıldığını da düşünürsek güvenlik MAC protokolleri için oldukça önem arz etmektedir.

Bu çalışmada literatürde KAA'lar için geliştirilmiş olan önemli MAC protokolleri araştırılmış ve özetlenmiştir. İncelenen MAC protokolleri özellikle güvenlik açısından ele alınmıştır. KAA'ların güvenliği üzerine yapılan araştırmalar incelenmiş, sonrasında MAC protokolleri ile KAA'ların güvenliğinin nasıl sağlanabileceği konusundaki çalışmalar özetlenerek bir karşılaştırma verilmiştir. Ayrıca, ele alınan bu MAC protokollerinin etkin oldukları saldırı türleri ve özellikleri belirtilmiştir.

Makalenin geri kalan kısmı şu şekilde düzenlenmiştir: II. bölümde KAA'larda güvenlikten bahsedilmiştir. III. bölümde MAC protokolleri tasarımı hakkında bilgi verilmiş ve IV. Bölümde literatür çalışması ile güvenli MAC protokolleri arasında karşılaştırmalar yapılıp, avantaj ve dezavantajları belirtilmiştir. V. bölümde ise incelenen MAC protokolleri üzerinden sonuç ve çıkarımlar yapılıp, geleceğe yönelik araştırılabilir konular üzerinde durulmuştur.

II. KAA GÜVENLİK

Düşman hatlarının ya da sınır bölgelerinin gözetlenmesi gibi hassas KAA uygulamalarında, algılayıcı düğümlerden baz istasyonuna gizli veri aktarımını sağlayan güvenlik protokolleri kullanılmalıdır. Ancak, KAA'ların düşük hafıza kapasitesi, sınırlı güç kaynağı, kısıtlı hesaplama yeteneği bulunması güçlü koruma sağlamasını zorlaştırmaktadır. Düğümler arasındaki yüksek hata oranı,

ara sıra kapanmalar yaşanması, ani iletişim girişimlerini kapsayan sürekli değişim gösteren topolojileri nedeniyle KAA'larda güvenliği sağlamak oldukça zordur. Ayrıca, algılayıcıların fiziksel olarak güvenlikleri sağlanamadığından, algılayıcı düğümleri kötücül kişiler tarafından ele geçirilebilmekte ya da yeniden programlanabilmektedir. Bu tip algılayıcı düğümler "ele geçirilmiş düğümler" (compromised nodes) olarak tanımlanır. Algılayıcı düğümler bir görevi tamamlamak için birbirleriyle etkileşim halinde ve koordine bir şekilde çalışırlar. Bir düğümün düşmanlar tarafından ele geçirilmesi ağ yapısındaki düğümler arasındaki koordinasyonu bozmaktadır [1]. Bu nedenle güvenliği sağlamak ve bu zorluklarla başa çıkmak için daha sınırlı bir kablosuz algılayıcı güvenlik protokollerinin oluşturulması gerekmektedir [8].

Şifreleme ve doğrulama işlemleri bir sistemi, kulak misafiri olma veya diğer saldırı türlerine karşı daha güvenli hale getirmektedir. Şifreleme veriyi düşmanlara karşı güvenli halde tutarken, doğrulama ise sistemi sahte verilerden korumaktadır [9]. Geleneksel ağlarla kıyaslandığında, KAA'lar düğümler arasındaki bazı işlemsel kısıtlar ve ağın yaşam ömrü için önemli olan enerjiyi korumak adına çok daha karmaşık bir yapı göstermektedir [10]. Diffie-Hellman anahtar değişimi veya RSA imzalama gibi açık anahtarlama kriptografileri limitli hafıza, hesaplamalar ve güç gibi nedenlerden dolayı KAA'larda çok fazla tercih edilmemektedir. Simetrik kriptografi ve özet fonksiyonları ise açık anahtar algoritmalarından daha hızlı ve daha çok işlemsel etkinliğe sahiptirler. Dolayısıyla KAA'lardaki güvenlik araştırmalarında ve geliştirilen güvenlik şemalarında çoğunlukla simetrik anahtar kriptografisi kullanılmaktadır. Simetrik şifrelemedeki temel problemlerden birisi, paylaşılan anahtarın düğümler arasında nasıl dağıtılacağıdır. Diğeri ise, dağıtılan bu anahtarın iletim sırasında gizliliğinin korunmasıdır. Düşman saldırısında bu anahtar ele geçirilmemelidir. Bu nedenle anahtar yönetimi ve anahtar dağıtımı KAA'lardaki güvenliğin korunmasındaki temel gereksinimlerdendir [11].

[32] nolu çalışmada güvenlik açığına sebep olan hizmet engelleme saldırına ortam erişim kontrol protokolleri üzerinden saldırı türüne uygun şekilde çözümler gerçekleştirilmiştir. Ayrıca düşmanlar tarafından ele geçirilen, imha edilen ya da kötücül düğümler sürekli mesaj yollayarak çevrelerindeki düğümlerin enerjisinin tüketimine sebep olabilmektedir. Bu tip saldırılara karşı etkin çözümler sunulmuştur. Düşman düğümlerin hareketli oldukları da varsayılarak düğümlerin bulundukları bölge karantinaya alınmakta ve komşu düğümlerin sadece kimlik doğrulama mesajları göndermeleri sağlanmaktadır.

A. KAA'LARDA GÜVENLİK GEREKSİNİMLERİ

Genel olarak bahsedildiği gibi, güvenlik KAA'ların en önemli sorunlarından biri sayılmaktadır. Bu bölümde KAA'larda ne tür güvenlik gereksinimlerine ihtiyaç olduğunu açıklanmaktadır. Gereksinimlerin çoğu geleneksel kablolu ve kablosuz ağlar için ortak olmasına rağmen bu bölümde KAA'lar açısından güvenlik ön planda tutulmuştur [12].

1) Veri Gizliliği

Veri gizliliği KAA'larda, veriye yetkisiz kişilerin erişiminin engellenmesini garanti altına almaktır ve hassas KAA uygulamalarındaki en önemli gereksinimden biridir. Algılayıcı ağdaki bir düğüm çevreden okuduğu verileri komşu düğümlere sızdırmamasının sağlaması gerekir [13,14]. KAA'ların uygulama alanlarından biri olan askeri uygulamalarda düğümler çok hassas veriler depolayabilmektedir. Ayrıca diğer birçok uygulamalarda düğümler anahtar dağılımı gibi çok hassas olan bu verileri kablosuz kanal üzerinden diğer algılayıcı düğümlerine aktarmak zorundadırlar. Aktarılan bu verilerin kötücül düğümlere karşı gizliliğinin sağlanması gerekmektedir. Çünkü kötücül düğümler bu verilerden yararlanarak ağın performansını düşürebilirler. Bu nedenlerle KAA'larda veri aktarımı için güvenli bir iletişim kanalı oluşturulması çok önemlidir. Hassas olan bu verileri gizli tutabilmek için verinin gizli bir anahtarla şifrelenmesi gerekmektedir.

2) Veri Bütünlüğü

Veri gizliliği bir verinin kötücül düğümler tarafından ele geçirilmesi önleyebilirken, içeriğinin değiştirilmesini önleyemez. Veri bütünlüğü verinin yetkisiz kişiler tarafından değiştirilmemesini garanti etmektedir. Bir kötücül düğüm mesajları bozarak ağın düzgün çalışmasına engel olabilir. Dahası, doğrudan doğruya bir kötücül düğüm olmadan da mesajlar aktarım esnasında da bozulabilir. Bu nedenle veri bütünlüğü için MAC ya da dairesel kodları (cyclic codes) kullanmak zorunludur.

3) Kimlik Doğrulama

KAA'lar ortak kablosuz ortamı kullandığından, kötücül düğümlerden gelen mesajları veya yanıltma paketlerini bulmak için, kimlik doğrulama mekanizmalarına ihtiyaç vardır. kimlik doğrulama metotları bir düğümün iletişim halinde olduğu düğümün kimliğini doğrulayabilmesini sağlamaktadır. Kötücül düğümler, kimlik doğrulamanın olmadığı durumlarda, başka bir düğüm gibi yaparak hassas bilgilere ulaşabilirler. Eğer sadece iki düğüm arasında veri iletişimi yapılıyorsa kimlik doğrulama gizli anahtar kriptografisi ile yapılabilir. Alıcı ve verici düğüm ortak bir gizli anahtar paylaşımı yaparak tüm mesajların doğrulama kodunu hesaplayabilir. Ancak buradaki problem ise gizli anahtarın alıcı ve verici düğümler arasında nasıl dağıtılacağıdır.

Yayımlama (broadcast) türü iletişimde kaynak doğrulama için daha kompleks çözümlere ihtiyaç vardır. Perrig et. al. µTESLA [14] adlı güvenli yayımlama protokolünde gizli anahtarların açıklanmasını geciktirerek gizli anahtar kriptografisi ile yayımlama türü iletişimde kaynak doğrulamayı başarmıştır. µTESLA her bir düğüme özel olarak gönderilmiş "özetlenmiş anahtar zincirlerine" (hashed key chains) bağlıdır. Ancak her bir düğüme anahtar zincirlerinin güvenli olarak gönderilmesi bir sorundur.

4) Erişilebilirlik

Erişilebilirlik KAA'ların hizmet devamlılığını hizmet engelleme (denial of service/DoS) saldırıları sırasında da devam ettirebilmesidir. DoS saldırıları KAA'daki tüm katmanlarda olabilir ve düğüm etkisiz hale getirilebilir. DoS

yükü düğümün bataryasını beklenenden daha çabuk bitirebilir. Erişilebilirlik KAA'larda genelde algılayıcı düğüm artıklığı ile sağlanmaktadır.

III. ORTAM ERİŞİM KONROL PROTOKOLLERİ TASARIMI

MAC protokollerinin ağın yapısına, alt üst katmanların gereksinimlerine ya da parçaların yeteneklerine göre farklı fonksiyonlar gerçekleştirmeleri beklenir. Çerçeveleme, ortam erişimi, güvenilirlik, akış kontrolü ve hata kontrolü MAC protokollerinin genel olarak ağ üzerinde sağlaması gereken özelliklerdir [15].

KAA'ların sınırlı bir güç kaynağı, hafıza kapasitesi, işleme yeteneği bulunmasından dolayı kablosuz algılayıcı ağlar için bir ortam erişim kontrol protokolü tasarlamak oldukça zordur. Sürekli değişen topolojiye sahip olmaları ağ yapısında dinamizm oluşturmaktadır. Tasarlanan MAC protokollerinin düğümlerdeki bu değişimlere adaptasyonları sağlanmalıdır [16]. Ayrıca bu protokollerin askeri, sağlık, çevresel ve kimyasal alanlar başta olmak üzere çok farklı alanlarda kullanılabilir olması hepsini kapsayan ortak bir ortam erişim kontrolünün tasarlanmasını oldukça zorlaştırmaktadır [17].

İyi bir MAC protokolünde olması gereken başlıca özellikler şu şekildedir [6,7,18]. Düğümler için ağın yaşam ömrü çok önemlidir. Bu nedenle, KAA'larda MAC protokolleri için öncelikle enerji etkinliği sağlanmalıdır. Diğer önemli husus da ölçeklenebilirliktir. Ağ genişliği, düğümün yoğunluğu ve topolojileri değişebilir. Ağ yapısına yeni bir düğüm eklendiğinde ağ üzerindeki etkileşimde ya da tüm ağın topolojisinde değişmeler meydana gelebilmektedir. İyi bir MAC protokolünün bu tip değişimlere karşı uyumlu olması gerekmektedir. MAC protokolleri için diğer önemli hususlar ise tarafsızlık, gecikme, iş çıkarma (throughput) yetenekleri ve bant genişliği kullanımıdır. Gecikme, iş çıkarma yeteneği veya tarafsızlık durumları yapılan uygulamaya göre değişebilmektedir. Gecikmede çevreden alınan bilgiler, çıkış düğümüne uygun harekete geçmesi için haber vermektedir. Tarafsızlıkta ise sınırlı bant genişliği olduğu durumlarda çıkış düğümü, tüm düğümlerden adil bir şekilde bilgi almaktadır. Geleneksel ağ yapıları için bunlar birinci dereceden önem arz ederler. Ancak KAA'da ise bunlar ikinci dereceden önemlidirler. KAA için en önemli konu ağın ve düğümlerin yaşam süreleridir.

Yapılan son çalışmalarda MAC protokollerinin güvenlik özelliği üzerinde de durulmuştur. Kötücül kişiler ağlar üzerindeki düğümleri ele geçirerek veya ağlardaki MAC protokollerinin açıklarından yararlanarak KAA'lar için tehdit oluşturulabilmektedir. Çünkü KAA'lar oldukça hassas bilgiler taşımaktadırlar [19]. Alana dağıtımı yapılan düğümler her zaman kurallara uygun düğümler olmayabilmektedir. Bazen düşmanlar tarafından kötücül bir düğüm yeni bir düğüm olarak tanıtılabilmektedir. Bu kötücül yeni düğümleri günümüzdeki kablosuz ağlar güvenlik teknolojisi ile kurallara uygun olan düğümlerden ayırt etmek oldukça güçtür. Bu nedenle kötücül düğümler, diğer normal olan düğümler tarafından kurallara uygun düğümler olarak kabul edilecektir. Kötücül düğümlerin bu şekilde kablosuz ağlara katılımını engellemek için erişim kontrolü ile kablosuz düğümlerin dağıtımlarının kontrol edilmesi gerekmektedir [31]. Ayrıca, KAA'larda kullanılacak olan MAC protokolleri bu ağların kendilerine has özellikleri ve "ele geçirilmiş algılayıcılar" göz önüne alınarak tasarlanmış olmalıdır. Yapılan çalışmalar farklı türdeki saldırılardan korunmayı amaçlamaktadır. Saldırı türlerinden biri olan hizmet engelleme saldırıları, farklı şekillerde olabilmektedir. Uyumayı engelleme, çakışma atakları, tüketme atakları ve karıştırıcı ataklar başlıca üzerinde durulan hizmet engelleme saldırılarıdır [20]. Örneğin uyumayı engelleme saldırıları, düğümü uyanık tutmaya çalışarak daha fazla güç harcanmasına neden olur. Herhangi bir güvenlik mekanizmasında algılayıcı düğümler veri almadan ve güvenlik özelliklerini kontrol etmeden önce uyanık olmalıdır. Güvenlik mekanizması olmadan, anti-düğümlerden biri sahte bir başlangıç yayınlayabilir. Alıcı gerçek ile sahte olanı ayırt edemezse, anti-düğümden aldığı sahte başlangıç ile veriyi alır ve işler. Bu şekilde veri iletimi devam eder ve alıcı saldırgan tarafından devamlı uyanık tutulur. Bu durumda ise düğümün bataryası çok hızlı bir şekilde tükenir [21].

Hizmet engelleme saldırıları MAC'lerde kullanılan protokollere, açıklarından faydalanarak iletişimi kesme, düğümlerin yaşam ömürlerini kısaltma gibi ağ güvenliğini tehdit edici zararlar vermektedir. Bozma türünde (jamming) ve ortam erişimlerinde hizmet engelleme türünde saldırılar yapılabilmektedir. Bozma türünde yapılan saldırılar kanala yayılan eş frekanstaki bir dalga sonucu fiziksel katmanlara ve ortam erişim katmanlarına zarar vermektedir. Ayrıca, erişim kurallarına aykırı bir şekilde çok sayıda paket göndererek ortam erişimin protokolüne zarar vermektedir [17,22,23].

IV. GÜVENLİ ORTAM ERİŞİM PROTOKOLLERİ

MAC protokollerinin algılayıcı ağlar üzerinde geniş bir kullanım alanı vardır. Algılayıcı ağlar üzerindeki farklı MAC protokollerinin bir özelliği sağlamak için diğer özelliklerden ödün vermeleri gerekebilmektedir.

Güvenlik konusu KAA'lar için önemli olup güvenliğe dayalı çalışılan ortam erişim protokolleri şu şekildedir. [17] nolu çalışmada farklı DoS saldırıları tespit edilip, saldırı türüne en uygun çözümü üretebilecek bir AR-MAC protokolü tasarımı yapılmıştır. Bu protokol, KAA'lardaki hizmet engelleme saldırı türlerinden olan sürekli saldırgan, aldatıcı saldırgan, reaktif saldırgan, rastgele saldırgan ve periyodik küme saldırganlarını birbirinden ayırarak, saldırı türüne göre en uygun çözümü üretmektedir. Simülasyon sonuçlarına göre, saldırıların etkinliği önemli ölçüde azalırken, düğümlerin yaşam sürelerinde de artışlar meydana gelmiştir. Çalışmada AR-MAC protokolü, S-MAC [7] protokolüyle kıyaslanarak protokolün performans analizi yapılmıştır. AR-MAC protokolünde, düğümlerin yaşam sürelerinin uzun olması sebebiyle, engellenen paket oranı S-MAC ile kıyaslandığında daha düşük olmaktadır. AR-MAC protokolünde dinleme süresinin ile paket gönderme oranları azalmaktadır. Düşük görev döngüsü ile yaşam ömürleri uzayan düğümlerin toplam engellenen paket oranları düşmektedir.

Sınır ağlarının KAA'lardaki güvenliğini sağlaması üzerine yapılan bir araştırmada, MAC'lere dayalı çok

katmanlı algılayıcılar (MLP) [4] kullanılmıştır. DoS saldırılarını çakışma saldırıları, adaletsizlik saldırıları ve tüketme saldırıları olarak incelemiştir. Şekil 1'de yapısı gösterilen bu çok katmanlı algılayıcılar KAA'lara karşı olası herhangi bir saldırıda değişen parametreler ve varyasyonlar göstererek güvenlik sağlamaktadırlar. Düğümler için oldukça kritik olan bu parametler, çakışma oranı (R_C), paket isteği oranı (R_T) ve paket bekleme süresidir (T_w). Şüpheli bir durum anında parametler olağandışı bir şekilde değişmeye başlamakta ve MLP bu değişimlere göre saldırıyı tespit etmektedir. Sonrasında protokol, düğümün fiziksel ve MAC katmanlarını kapatarak, güvenli hale getirmeye çalışmaktadır. Bu sayede güç tasarrufu sağlanarak, ağın ömrü uzamış olmaktadır. Yapılan çalışmalar aynı zamanda düğüm üzerinde saldırı olmadığı halde aktivasyonunda normal şartlar altında bir artış meydana geldiğinde, MLP'lerin yanlış alarm verebileceğini ve düğümün kapatılmasına sebep olabileceğini de göstermektedir. Yanlış alarmlar sonucu ağ üzerindeki katmanlar kendilerini kapatarak ve bu nedenle gereksiz yere enerji harcayarak ağın etkinliğini azaltmaktadır. MLP'ye dayalı MAC protokolü ile farklı saldırı türlerinde ağın yaşam süresi değişmektedir. Bu nedenle uygulanacak benzetim göre bir enerji modeli oluşturulmalıdır.

FSMAC [24] protokolü CSMA/CA [25] protokolünün üzerine sızma tespit ve sızma savunma modülleri eklenerek oluşturulmuş yeni bir güvenli MAC protokolüdür. CSMA/CA protokolü daha çok ortak kanalın daha etkin ve adaletli bir şekilde nasıl kullanılacağını belirlemek için tasarlanmıştır. Ancak DoS saldırılarına karşı kırılgan bir yapı göstermektedir. Geliştirilen FSMAC ile her bir düğüm kendi kendini savunabilmektedir. Merkezi bir kontrol bulunmamaktadır. Her iki modül de dağıtık bir yapıdadır. Bu protokolün belirlenmesi için öncelikli olarak KAA'lar üzerindeki hizmet engelleme saldırıları çakışma atakları, haksızlık atakları ve tüketme atakları olmak üzere üç farklı sınıfa ayrılmıştır. Göstergeler olarak RTS varış oranı, ortalama bekleme süresi ve çakışma oranları tanımlanmıştır. Çünkü tüketme saldırılarında yüksek sayıda paket alınırken, haksızlık ve çakışma saldırılarında ortalama bekleme süresi uzamaktadır. Ayrıca, çakışma saldırılarında çakışmalar oldukça sık yer almaktadır. Bu nedenle gösterge olarak bu değerler ölçülüp, güvenli MAC protokolü tasarlanmıştır.

Sonuç olarak, FSMAC protokolü ile herhangi bir yanlış alarm olmadan tüm sızmalar tespit edilebilmektedir. Hizmet engelleme saldırılarına dayalı başarısız veri transferleri %25 oranında azaltılmıştır. Böylece başarısız iletişimden dolayı enerjinin boşa harcanması azaltılarak yarı yarıya enerji korunmuştur. [24].

Adrian Perrig ve arkadaşlarının önerdiği SPINS protokolü [14], SNEP ve µTESLA adlı iki güvenli yapı bloğundan oluşmaktadır. SNEP, her bir mesaja sadece 8 baytlık ek yük ile düşük iletişim ek yükü sağlamaktadır. Ayrıca, anlamsal güvenlik ile şifreli mesajın içeriğine kulak misafiri olmayı önlemektedir. Veri kimlik doğrulama (MAC) ile verilerin yollayıcıdan gönderildiği durumlarda alıcı tarafından alındığını garanti eder. MAC'lerde bulunan sayaç değerleri ile tekrarlama mesajları engellenir. Böylece tekrarlama saldırılarına karşı da bir korunma sağlanmış olur. Ayrıca, eğer bir mesaj doğru bir şekilde doğrulanmışsa, kullanıcı bir önceki mesajı aldıktan sonra gönderici tarafından yollandığını bilmektedir. Bu da zayıf da olsa tazelik sağlamaktadır. Diğer bir güvenli yapı bloğu olan µTESLA protokolünde ise, standart TESLA'nın algılayıcı ağlar üzerindeki bazı zorluklarına çözümler üretilmiştir. Son zamanlarda önerilen TESLA doğrulanmış yayın yapmak için geliştirilen bir protokoldür. µTESLA protokolü ile ilk olarak başlangıç paketindeki sayısal imzalamanın çok maliyetli olmasından dolayı simetrik anahtarlama kullanılmıştır. Her bir paket için bir anahtar bildirmek, alım ve gönderim için çok enerji gerektirdiği için her devirde bir kere anahtar bildirilmiştir. Son olarak ise, tek yönlü anahtar zinciri oluşturmak çok maliyetli olduğundan, µTESLA ile doğrulanan yollayıcı sayısı kısıtlanmıştır.

TinySec [19], KAA'larda güvenliği sağlamak amacıyla tasarlanmış bir link katmanı protokolüdür. Tamamlanmamış SNEP'in yerine tasarlanan bu protokol, erişim kontrolü, mesaj bütünlüğü ve gizliliğini sağlamaktadır. IEEE 802.11 [26] ve GSM'lerdeki güvenlik açıkları düşünülerek oluşturulmuştur. Klasik güvenlik protokollerinde güvenlikli hale getirmek için 16-32 bayt ek yük oluşmaktadır. Ancak KAA'ları düşündüğümüzde küçük hafızası, zayıf işlemcisi, kısıtlı enerjisi ve 30 bayt paketleriyle ek yük oluşturmak istenilen bir durum olmamaktadır. TinySec, çeşitli donanımlara ve radyo platformlarına uyumlu olacak şekilde tasarlanmıştır. TinySec güvenliği sağlamak için ortak bir anahtar kullanır. TinySec'in 36 düğümü üzerinde yapılan çalışma ile bu link katmanı protokolünün uygun ve etkin olduğu saptanmıştır. Ayrıca %10'dan az bir enerji, gecikme ve bant genişliği ek yükü eklemektedir [27].

TinySec'de iki farklı işlem modu bulunmaktadır. Bunlar TinySec-AE (authenticated encryption) ve TinySec-Auth. (authentication only)'dir. TinySec-AE modunda TinySec veri yükünü şifreler ve paketleri MAC (message authentication code) doğrular. TinySec-Auth. modunda ise TinySec bütün paketi MAC ile doğrular. Veri yükü ise şifrelenmez. TinySec'in en önemli özelliklerinden biri de kullanım kolaylığı ve şeffaflığıdır [9].

TinySec düşük enerji tüketimi ve hafıza kullanımı sağlarken, güvenlik konusunda istenen performansı gösterememektedir. Ayrıca, düğüm yakalama saldırılarına karşı koruma girişiminde de bulunmamaktadır. Güvenli bir iletişim için gerekli olan gizlilik, doğrulama ve mesaj tekrarlama korumasını sağlarken aynı zamanda düşük enerji tüketimi yapamamaktadır [28].

SenSec [29], TinySec'e benzeyen bir link katmanı protokolüdür. TinySec iki farklı modda çalışırken, SenSec tek bir modda çalışmaktadır. TinySec-AE modu ile benzer olan şifrelemeli doğrulama modunda çalışır. SenSec ile güvenliği artırıcı ve enerji tüketimini azaltıcı bazı iyileştirmeler yapılmıştır. Ayrıca hesaplama ve MAC (mesaj doğrulama kodu) için gerekli olan maliyet azaltılmıştır. Çoklu-anahtarlamalı mekanizma ile tüm ağ yapısı farklı saldırı türlerine karşı dayanıklı hale gelmiştir. SenSec'deki bu anahtarlama mekanizması düğüm yakalama saldırılarına karşı kısmi esneklik sağlamaktadır. Kullandığı Skipjack-X blok şifresi ile SenSec, Skipjack blok şifresini kullanan TinySec'e göre tüketme saldırıları karşı daha

esnek yapı göstermektedir. Ayrıca, kaba kuvvet saldırılarına karşı da güçlü bir koruma mekanizması bulunmaktadır.

MiniSec [28] güvenli bir ağ katmanı protokolüdür. ZigBee [30] gibi yüksek güvenlik seviyesi sağlarken, TinySec'den daha düşük enerji tüketmektedir. Blok şifreleme modu olarak OCB (offset codebook) modunu kullanmaktadır [9].

MiniSec'de iki farklı işlem modu bulunmaktadır. Bunlar, tek yönlü paket yayını yapan MiniSec-U ve geniş paket yayını yapan MiniSec-B'dir [9]. İki işlem modu da blok şifreleme modu olarak OCB modunu kullanmaktadır. Ayrıca anlamsal güvenliği sağlamaktadır. MiniSec-B işlem modunda ayrıca tekrarlama saldırılarına karşı da korunma sağlanmaktadır [29]. Ayrıca, herhangi bir iletim ekyükü de oluşmamaktadır [19].

TE_2S [21], çapraz-katmanlı güvenli bir yaklaşımla MAC protokol güvenliğini sağlar. KAA'ları uyumayı engelleme gibi saldırılara karşı korumak için tasarlanmıştır. İki katmanlı güvenli iletim protokolü önerilmiştir. Birinci katmanda oturum anahtar anlaşması yapılırken, ikinci katmanda veri iletimi yapılmaktadır. MAC protokolüne entegresinde herhangi bir ekstra paket kullanılmamaktadır. Bu protokol ile kimlik doğrulama süreci önemli ölçüde azaltmaktadır. Böylece gücü tüketen saldırıların etkisi de azalmaktadır. Enerji analizine bakıldığında etkinlik sağlandığı gözlemlenmiştir. Ayrıca, tekrarlama ve sahtecilik saldırılarına karşı da enerji etkin bir şekilde karşı koyabilmektedir.

V. SONUÇ VE ÖNERİLER

KAA'ların fiziksel özelliklerinden dolayı MAC protokolleri tasarlanırken üzerinde durulan başlıca konulardan biri enerji etkinliğini sağlamaktır. Enerji etkinliği sağlanarak ağın ömrü uzatılmaktadır. Ancak bazı durumlarda enerji etkinliğini sağlamak gecikme ve maliyet artışı, güvenlik sorunları gibi istenmeyen durumlara neden olmaktadır. Literatürde bu problemleri önlemeye çalışan MAC protokolleri bulunmaktadır.

Yakın zamanda yapılan çalışmaların enerji etkinliği üzerine değil, özellikle güvenlik üzerinde de durulduğu gözlemlenmiştir. Bu protokollerde saldırı etkinliği düşürülerek, güvenli bir veri iletişimi gerçekleştirilmeye çalışılmıştır. Böylece, ağın yaşam süresini de artırmak hedeflenmiştir. Bu çalışmanın bir özeti olarak Tablo I'de farklı MAC protokollerinin hangi saldırı türlerinde etkin oldukları ve ne gibi özellikler gösterdikleri bilgileri yer almaktadır.

ARMAC protokolü hizmet engelleme saldırılarılarına karşı etkinlik sağlamakla beraber, farklı hizmet saldırılarına göre saldırı türünü belirleyerek bir güvenlik geliştirmektedir. MLP'ye dayalı MAC protokolü ve FSMAC protokolü de hizmet engelleme saldırılarına karşı etkinlik sağlamaktadırlar. MLP'ye dayalı MAC protokolünde herhangi bir saldırı durumunda değişen parametrelere göre fiziksel ve MAC katmanlarını kapatarak güvenlik sağlanırken, FSMAC protokolünde her bir düğüm kendi kendini korumaktadır. Bu durum dağıtık bir yapı göstermesinden kaynaklanmaktadır.

TABLO I
GÜVENLİ ORTAM ERİŞİM PROTOKOLLERİ

PROTOKOLLER	ETKİLİ OLDUĞU SALDIRI TÜRÜ	ÖZELLİKLERİ
ARMAC	DoS Saldırısı	Farklı hizmet saldırılarında, saldırı türünü belirleyerek güvenliği sağlamaktadır. Herhangi bir ek donanıma ihtiyaç duymaz.
MLP'ye Dayalı MAC	DoS Saldırısı	Herhangi bir saldırı anında değişen parametreleri izleyerek, düğüm üzerindeki fiziksel ve MAC katmanlarını kapatarak güvenliği sağlar.
FSMAC	DoS Saldırısı	Merkezi bir kontrol yapısı bulunmayıp, dağıtık yapı gösterir. Her bir düğüm kendi kendini savunabilmektedir.
SPINS	Tekrarlama Saldırısı Gizlice Dinleme Saldırısı	Anlamsal güvenlik ile kulak misafiri olmayı engeller. Gizlilik, bütünlük ve tazelik (freshness) özelliklerini sağlar.
TinySec	Tekrarlama Saldırısı	Kullanım kolaylığı ve şeffaflık sağlar. Ayrıca erişim kontrolü, mesaj bütünlüğü ve gizliliği sağlar.
SenSec	Kaba Kuvvet Saldırısı Tekrarlama Saldırısı	Çoklu anahtarlama mekanizması ile farklı saldırı türlerine dayanıklıdır.
MiniSec	Tekrarlama Saldırısı	Anlamsal güvenlik sağlamaktadır. Ayrıca herhangi bir iletim ek yükü oluşturmaz.
TE_2S	Tekrarlama Saldırısı Sahtecilik Saldırısı Güç Tüketme Saldırısı Uyumayı Engelleme Saldırısı	Herhangi bir ek paket kullanılamaz. Kimlik doğrulama sürecini azaltarak güç tüketme saldırılarının etkilerini azaltır.

SPINS protokolü, tekrarlama ve gizlice dinleme saldırılarına karşı etkilidir. Kulak misafiri olmayı engellerken, ver gizliliği, bütünlüğü ve tazelik sağlamaktadır. TinySec protokolü tekrarlama saldırılarına karşı bir etkinlik sağlayıp veri bütünlüğü ve gizliliği sağlamaktadır. SenSec, TinySec'e benzer bir protokol olup TinySec'e ek olarak maliyet ve mesaj doğrulama kodu maliyetleri azaltılmıştır. Ayrıca, çoklu anahtarlama mekanizması ile farklı saldırı türlerine karşı bir koruma sağlamaktadır. MiniSec protokolü, anlamsal güvenlik sağlamaktadır. Ayrıca TinySec'den düşük enerji tüketimi sağlamaktadır. Son olarak TE_2S protokolü tekrarlama, sahtecilik, güç tüketme ve uyuma saldırıları gibi birçok saldırı türüne karşı enerji etkinliği sağlamaktadır. Bu bilgilere ek olarak enerji etkinliği ve mobilite (hareketlilik) sağlamaya yönelik MAC protokollerine sayfa sınırlaması nedeniyle değinilmemiştir. Makalenin genişletilmiş versiyonunda bu konulara da değinilecektir.

Bu çalışmada elde edilen sonuçlar göstermiştir ki güvenli MAC protokolleri konusunda yapılan çalışmalar çoğunlukla benzetim ortamı üzerinde yapılmaktadır. Bu protokollerin gerçek ortam üzerindeki etkinlikleri denenmemiş ve sadece benzetim performansı gerçek ortamlarda da benzer şekilde gerçekleştirebilecekleri varsayılmıştır. Diğer KAA alanlarında yapılan çalışmalarda görüldüğü üzere, gerçek ortamlarda hesaba katılmayan bazı faktörler olabilmekte ve sonuçlar çok farklılık gösterebilmektedir. Dolayısıyla gerçek ortamlarda çalışılarak geliştirilecek protokoller bu protokollerin asıl çalışma performanslarını gösterecektir.

KAYNAKLAR

[1] S. Misra, A. Vaish, "Reputation-based role assignment for role-based access control in wireless sensor Networks," Computer Communications 34 (2011) pp. 281–294

[2] J. Yick, B. Mukherjee, D. Ghosal, "Wireless sensor network survey," Computer Networks 52 (2008) pp. 2292–2330

[3] E. Sabbah, K. D. ,Kang, "Guide to Wireless Sensor Network: Security in Wireless Sensor Network," Chapter 19, pp. 489-490

[4] R. V. Kulkarni, G. K. Venayagamoorth, "Neural Network Based Secure Media Access Control Protocol for Wireless Sensor Network" Proceedings of International Joint Conference on Neural Networks, Atlanta, Georgia, USA, June 2009 pp.14-19

[5] C. Cano, B. Bellalta, A. Sfairopoulou, M. Oliver, "Low energy operation in WSNs: A survey of preamble sampling MAC protocols," Computer Networks, 55 (2011) pp. 3351-3363

[6] I. Demirkol, C. Ersoy, F. Alagoz, "Mac protocols for wireless sensor networks: a survey," IEEE Communications Magazine, 44 4 (2006), pp. 115–121.

[7] W. Ye, J. Heidemann, D. Estrin, "An Energy-Efficient MAC Protocol for Wireless Sensor Networks," IEEE INFOCOM, New York, Vol. 2, (June 2002) pp. 1567-1576

[8] H. S. Ng, M. L. Sim, C. M. Tan, "Security issues of wireless sensornetworks in healthcare applications," BT Technology Journal, 24 2 (2006), pp. 138–144.

[9] N. Sultana, T. Ahmed, S. Hossain, "Study of a new link layer Security scheme in a wireless sensor network," AIUB Journal of Science and Engineering (AJSE), Vol. 10, No. 1, August 2011

[10] X. Chen, K. Makki, K. Yen, N. Pissinou, "Sensor network Security: A survey," IEEE Communications Surveys & Tutorials, 11(2), Second Quarter 2009, pp. 52–73,

[11] J. Rehana, "Security of Wireless Sensor Network," TKK T-110.5190 Seminar on Internetworking, 2009

[12] M. Megdadi, S. Özdemir, İ. Güler, "Kablosuz Algılayıcı Ağlarında Güvenlik: Sorunlar ve Çözümler", Bilişim Teknolojileri Dergisi, Cilt: 1, Sayı: 1, Ocak 2008

[13] D.W. Carman, P.S. Krus, B.J. Matt, "Constraints and approaches for distributed sensor network security," Technical Report 00-010, NAI Labs, Network Associates, Inc., Glenwood, MD, 2000.

[14] A. Perrig, R. Szewczyk, V. Wen, D. Culler, J. D. Tygar "SPINS: Security Protocols for Sensor Networks," Wireless Networks 8 (2002) 521-534

[15] J.F. Kurose, K.W. Ross "Computer Networking: A Top-Down Approach Featuring the Internet," (third ed.), Addison Wesley (2005).

[16] S.Ray, I. Demirkol, W. Heinzelman, "ADV-MAC: Analysis and optimization of energy efficiency through data advertisements for wireless sensor Networks," Ad Hoc Networks 9 (2011) pp. 876-892

[17] M. Çakıroğlu, A. T. Özcerit,. "Kablosuz Algılayıcı Ağlarda Hizmet Engelleme Saldırılarına Dayanıklı Ortam Erişim Protokolü Tasarımı," J. Fac. Eng. Arch. Gazi Univ.,Vol 22, No 4, (2007) pp. 697-707,

[18] W. Ye, J. Heidemann, D. Estrin, "Medium Access Control with Coordinated, Adaptive Sleeping for Wireless Sensor Networks," IEEE/ACM Transactions on Networking, 12 3 (2004), pp. 493–506.

[19] D. Boyle, Thomas Newe "Securing Wireless Sensor Networks: Security Architectures," Journal of Networks, Vol. 3, No. 1, January 2008

[20] P. M. Pawar, R. H. Nielsen, N. R. Prasad, S. Ohmori, R. Prasad, "Behavioural Modelling of WSN MAC Layer Security Attacks: A Sequential UML Approach,"; Journal of Cyber Security and Mobility, (2012) pp. 65–82

[21] C. T. Hsueh, C. Y. Wen, Y. C. Ouyang, "A Secure scheme for power exhausting attacks in wireless sensor Networks," Ubiquitous and Future Networks (ICUFN), 2011 Third International Conference on, , Volume: Issue: , 15-June 2011, pp. 258 - 263

[22] Y. Wei, P. Hartel, J. Den Hertog, P.Havinga, "Link layer Jamming Attacks on S-MAC," Proceeedings of the Second European Workshop on Sensor Network, İstanbul, Türkiye, 2005, pp. 217 – 225,

[23] Y. Wei, L. Lodewijk, V. Hoesel, J. Doumen, P. Hartel, P.Havinga, "Energy-Efficient Link-Layer Jamming Attacks against Wireless Sensor Network MAC Protocols", SANS'05, Virginia, USA, Kasım 2005

[24] Q. Ren, Q. Liang, "Fuzzy Logic-Optimized Secure Media Access Control (FSMAC) Protocol for Wireless Sensor Networks," CIHSPS 2005 - IEEE Iutemational Conference on Computational Intelligence for Homeland Security and Personal Safety Orlando, FL, USA, 2005

[25] L. Kleinrock, F.A. Tobagi, Packet switching in radio channels: Part I-Carrier sense multiple-access modes and their throughput-delay characteristics, IEEE Transactions on Communications 23 (12) (1975) pp. 1400–1416.

[26] IEEE Standard 802.11: Wireless LAN MediumAccessControl (MAC) and Physical Layer (PHY) Specifications, 1999

[27] C. Karlof, N. Sastry, D.Wagner, "TinySec: A Link Layer Securty Architecture for Wireless Sensor Networks," In Second ACM Conference on Embedded Networked Sensor Systems, SenSys 2004, (2004)

[28] M. Luk, G. Mezzour, A. Perrig, V. Gligor, "MiniSec: Secure Sensor Network Communication architecture,",In Proc. of the 6th Int'l Conf. on Information Processinng in Sensor Networks, ACM Press, (2007), pp. 479-488

[29] I. Krontıris, T. Dımıtrıou, H.Soroush, M. Salajeghe "WSN Link-layer Security Frameworks," Athens Information Technology, Greece

[30] ZigBee Alliance. Zigbee specication. Technical Report Document 053474r06, Version 1.0, ZigBee Alliance, June 2005

[31] Y. Zhou, Y. Zhang, Y. Fang "Access control in wireless sensor networks," Ad Hoc Networks 5 (2007), pp. 3–13

[32] G. F. Türker, İ. Tarımer "Türkiye'de Kablosuz Algılayıcı Ağlar ile Yapılan Teknolojik Uygulamalar Üzerine Bir İnceleme," Muğla Üniversitesi, Elektronik ve Bilgisayar Eğitimi Bölümü, Muğla

Anonymous RFID Authentication Protocol Without a Trusted Party

Mehmet Sabır KİRAZ, Muhammed Ali BİNGÖL,
Süleyman KARDAŞ, Fatih BİRİNCİ

Abstract—**Anonymous authentication is a technique enabling users to prove that they have privilege without disclosing real identities. This type of authentication can be useful especially in scenarios where it is sufficient to ensure the server that the claiming parties are indeed registered. Many existing anonymous authentication protocols assume absolute trust to the back-end server in which all private keys are stored. This trust may result in serious security and privacy issues in case of private key leakage from the server.**

In this paper, we propose forward secure anonymous and mutual RFID authentication protocols where trust to the server-side is not needed. That is to say, even the private keys are obtained from the corrupted tags or the server owners of these tags cannot be traced from the past authentication actions. In fact, anonymity of the users will continue even the private keys of their tags are compromised. Our schemes are based on the threshold cryptosystems which provide security and simplicity. We assume all computations can be carried out with limited resources such as RFID tags.

Index Terms—**RFID, Authentication, Anonymity, Threshold cryptosystem**

I. Introduction

Radio Frequency IDentification (RFID) is a means for identifying objects via a radio signal, and enables automated data gathering in a variety of applications. A typical RFID system is setup by a set of readers, a number of RFID tags and a back-end server. In general sense, an RFID tag is known as a small integrated circuit with a unique identifier which transmits data over the air in response to interrogation by an RFID reader [1]. A smart tag, on the other hand, has on-board processors that are typically capable of performing cryptographic operations. These smart RFID cards are being deployed in a range of applications, including electronic tickets, access control, public transportation payment cards, and novel forms of credit cards, and they are likely to be carried by most of the people as a means of identification, e.g. as a national ID card or electronic passport. Some recent works show that public-key cryptosystems can be deployed in RFID systems [2]–[4]. Our interest here is in smart RFID tags with public-key cryptosystem, and in particular we focus on the means of authentication used to access tag-specific information stored in a back-end server.

This work has been partially funded by COGSA (Multimedia Security Systems) project.

M.S. Kiraz, M. A. Bingöl, S. Kardaş, and F. Birinci are with TUBİTAK BİLGEM UEKAE (National Research Institute of Electronics and Cryptology), Gebze 41470 Kocaeli/Turkey e-mail: {m.kiraz, muhammedalib, skardas, fatih}@uekae.tubitak.gov.tr

There exists some applications (e.g., electronic tickets, public transportation, e-voting, reusable payment and cash system etc.) where it is only necessary and sufficient to verify whether a tag is a legitimate one without determining its identity. In these examples, people may prefer to register only once (e.g., after some payment or being a member) and would like to keep their anonymity and privacy when they use these applications. Nonetheless, most of existing approaches consider a back-end server as trusted entity and assumed to be physically secure and not attackable. However, the security of server-side cannot be guaranteed for some real-life applications. A variety of security and privacy threats to RFID authentication protocols have been widely studied, including, cloning tag, eavesdropping, replay attacks, denial of service (DoS) attacks, tracking, and traceability. Also, it is usually assumed that back-end server maintains all private information about tags, assigned keys, etc. In addition to these security and privacy threats, an adversary that has compromised a server could impersonate a valid tag using knowledge of the tags internal state. In this paper, we introduce this practical threat, namely Untrusted Server Side Attack (Big brother attack). In fact, a person, who is responsible for operating the server, may be interested in detailed user profiles (e.g., for later misuse). Hence, this malicious officer can link the users with their authentication information like authentication time, location. Therefore, if the contents of a server are revealed or controlled by an attacker, then such an attack could be used to cause cloning the tag, impersonating or tracing the users which is the case for most of the conventional RFID protocols.

Motivated by this need, we consider anonymous RFID based authentication protocol. In these protocols, even if an adversary corrupts the reader as well as the back-end server, she is not be able to trace any tags in the system but can authenticate them.

Our contributions. In this paper, we propose an anonymous RFID authentication protocol without using a trusted third party. To the best of our knowledge, this is the first paper that addresses and tries to provide a solution to the problem of server side corruption. We show the security of our protocol against what we called 'Big-brother attack' in which the server-side is corrupted or controlled by a malicious administrator. In this way, no malicious party from the server side has sufficient information for computing the private content of the tags and tracing them. We prevent those attacks by using threshold cryptosystems between the server and the tags. Our protocol also achieves forward and backward secrecies. Namely, although the private keys of tags are obtained this

will give no advantage to trace neither in the past nor in the future.

Organization of the paper. After giving brief preliminaries about threshold homomorphic cryptosystems, we present our first unilateral anonymous authentication scheme for RFID in Section III. In Section IV, we propose our mutual anonymous authentication scheme. We prove its security in Section IV-A and finally we conclude our paper in Section V.

II. Related Work

There are many RFID authentication protocols available. For more information, we refer interested readers to the excellent resource maintained by Avoine [5] and survey papers [6], [7]. Instead, we only focus on anonymous RFID authentication protocols.

In [8], the authors focus on anonymous credential systems where they propose a generic anonymous payment system including anonymous authentication for RFID-powered public transport tickets. An alternative approach to anonymous RFID-based payment has been proposed in [9]. In [10], the authors present an implementation of an anonymous credential system on Java Cards.

In [11], the authors propose three anonymous RFID authentication protocols (a 2-pass authentication protocol and two 1-pass authentication protocols). The authors claim that the last protocol is "optimistic" the cost is minimal when the adversary is passive.

In [7], the authors present an authentication protocol and a search protocol for RFID tags. Their authentication protocol provides security and privacy requirements without the need of a persistent central database. they also address the disadvantages having a secure central database and suggested solutions for overcoming them. Finally, they introduce a new problem of performing secure search for RFID tags.

In [12], the authors extend the universally composable (UC) framework for RFID authentication protocols. Informally speaking, the security of UC protocols is maintained under general composition with arbitrary other protocols running concurrently, and therefore such protocols are easily plugged into more complex protocols in a modular fashion without requiring a new security analysis. In addition to the availability, anonymity, and authenticity, in this paper, the authors address the forward-security issues for this UC framework in the presence of key compromise. They propose new protocols which satisfy forward-secure anonymity, authenticity, and availability requirements in the UC model. The article [13] recently proposed a universally composable security framework especially for RFID applications. They adopt RFID setup, communication, and concurrency assumptions in a model that guarantees strong security, privacy, and availability properties. Unlike [12], they do not consider security issues in the presence of key-compromise and tag corruption.

[14] proposes mutual authentication protocols for RFID systems. Some significant characteristics of the protocols are forward security, tag anonymity, location privacy, low complexity on the back-end server, and scalability. The authors claim that their protocols offer the most enhanced security features in RFID mutual authentication protocols with respect to user privacy. They also show that forward security and tag anonymity are guaranteed.

The authors in [15] proposed an anonymous RFID authentication protocol that preserves the security and privacy properties, and achieves better scalability compared with other contemporary approaches. However, [16] shows that this protocol some of the claimed security properties (especial untraceability) are not fulfilled. In this attack, an adversary can manipulate the messages between a tag and a reader during the protocol runs and can successfully trace the tag. The authors in [16] also improves the flawed protocol to satisfy all the claimed security and efficiency properties.

In [17], the authors propose an anonymous authentication scheme that allows RFID tags to authenticate to readers without disclosing any other information that allows tags to be traced. Their protocol provides anonymity and untraceability of tags against readers, tag authentication and availability.

We note that none of the above work considers the case of a malicious back-end server.

III. Warm up: Our First Protocol for Anonymous and Unilateral Authentication

A. Threshold cryptosystems

Our protocols for RFID authentication are based on threshold cryptosystems [18]. For the completeness of the paper, we give a brief description of threshold cryptsystems below.

We denote $E(m,r)$ the encryption of message m using randomness r with a semantically secure public key encryption scheme. In a (t,n)-threshold cryptosystem there are n parties, each of them holds a share of the overall secret key. In the set up phase a public key is generated which is available for all n parties to encrypt messages. If at least t parties cooperate, any encryption can be successfully decrypted, whereas any collusion of less than t parties cannot get any information about the plaintext.

The most widely used threshold cryptosystems are (based on) ElGamal or Paillier [19], [20]. Threshold ElGamal has the drawback of only allowing decryption of values belonging to a relatively small set, for which it is feasible to compute discrete logs. On the other hand, Paillier does not have this problem and allows decryption of encrypted values in an arbitrarily large set (e.g., 1024-bit integers). However, the distributed key generation protocol for threshold Paillier is very expensive compared to that for threshold ElGamal. Our both protocols are applicable to any threshold cryptosystem. Without loss of generality, in our protocols, we use the popular threshold ElGamal homomorphic encryption as an instance.

Denote x_i^P for a value x which belongs to a party P with an index i. Let q be a prime number of binary size of n where n is a security parameter. G_q forms a group of order q generated by $g \in G_q$. Let $f(x) = a_{t-1}x^{t-1} + \ldots + a_0$ be a polynomial of degree t where the coefficients are $a_i \in G_q$. The value $a_0 = f(0)$ is the overall secret key which is computed during the setup phase and unknown to everybody. We denote (x^P, y^P) as public and secret key pair of the party P respectively where y^P is computed as $y^P = f(x^P)$.

a) Threshold Decryption.: Given a ciphertext in the (t,n)-threshold cryptosystem and t decryption shares of t parties based on their respective shares of the secret key everyone can simply recover the plaintext by using a reconstruction algorithm. More formally, on ciphertext c, at least t parties broadcast $c_i = D_{sk_i}(c)$, where sk_i denotes the secret key share for the i-th party at this stage. Later, everyone can perform $m = R(c_1,\ldots,c_t)$ where $c = E(m)$, where R denotes the public reconstruction algorithm. Let us illustrate for the decryption and reconstruction algorithm using $(2,n)$-threshold ElGamal as an instance. The domain parameter of the threshold scheme is (G_q, g). There are two parties in our protocol, the server S and the i-th tag T_i. Each party has a unique secret key shares (x,y) which is computed from a secret curve $y = f(x) = a_1x + a_0$ where a_0 is the private key and $h = g^{a_0}$ is the corresponding public key. Given a message m, the encrypted message pair is computed as $(C = (g^r, h^r m))$ where $r \in_R \{0,1\}^\ell$. The server computes its decryption share as $\sigma_S = g^{ry^S \frac{x^T}{x^T - x^S}}$ and the tag computes its decryption share as $\sigma_T = g^{ry^T \frac{x^S}{x^S - x^T}}$. Finally, the original message could be recovered by computing $m' = \frac{h^r m}{\sigma_S \sigma_T}$.

B. Our protocol

We are now going to present our first protocol which satisfies anonymous and mutual authentication. This protocol is interesting since the overhead for the server can be significantly decreased. Namely, the server can pre-compute a large set of encryptions before running the protocol, in this way the protocol can be more efficient.

Note that the system uses $(2,n)$-threshold cryptosystems therefore two parties the server and a tag can decrypt encryptions in order to pass the authentication. Our protocol involves the following entities.

C. Entities

The protocol can be implemented using any threshold cryptosystem. For ease understanding, we are going to illustrate our protocol with threshold ElGamal encryption. In this system, each party stores only one unique decryption shares $(x, y = f(x))$, which is computed and distributed by an issuer.

1) **Server** S: The server stores its own key share (x^S, y^S).
2) **Tag** i: Each tag is attached to a single object. A tag i has enough volatile for computation and non-volatile memory for storing its own share (x^i, y^i) and public share of server (x^S). Tags can compute modular exponentiation and inversion and can generate random nonces.
3) **Issuer** $\mathcal{I}$: Issuer generates a prime number q of binary size of n (n is a security parameter and should be large enough) that uniquely specifies a group G_q of order q. It also generates a generator g which is element of G_q. Moreover, $\mathcal{I}$ sets up a secret polynomial degree of 1 $(f(x) := a_1x + a_0)$ where the coefficients are elements of G_q and $a_0 = f(0)$ is the actual secret key. Lastly, $\mathcal{I}$ generates unique secret shares and sets up each entity with unique share in a secret channel.

The protocol steps are described as follows. The protocol is also sketched in Figure 1.

Step 1. The i-th tag picks a random value $r^i \in_R \{0,1\}^\ell$ and sends it to the server where ℓ is a security parameter.

Step 2. The server also picks a random value $r_S \in_R \{0,1\}^\ell$ and computes an ElGamal encryption of $m = r_S||r^i$. Note that because of using semantically secure randomized encryption scheme any two ciphertexts of a message m are completely different. To encrypt the message m, she first picks a random nonce $r \in \mathbb{Z}_q$. Then the encryption pair is computed $(C = (h^r m, g^r))$. She also computes the decryption share $\sigma = g^{ry^S}$. The server sends C and σ to the i-th tag.

Step 3. Upon receiving the message σ, C, the tag first completes the decryption share of the server as $\sigma_s = \sigma^{\frac{x^i}{x^i - x^S}}$. Then, it computes its decryption share as $\sigma_i = g^{ry^i \frac{x^S}{x^S - x^i}}$. Finally, it recovers the original message as $\widehat{r}^S||r'^i = \frac{h^r m}{\sigma_S \sigma_i}$. If the $\widehat{r}^i$ is equal to the original random value r^i, it sends $\widehat{r}^S$. Otherwise, it sends a random value $\widehat{r} \in_R \{0,1\}^\ell$.

Step 4. The server verifies whether the received value $\widehat{r}$ is equal to the value r_S she generated at Step 1.

In the next section, we will slightly adapt this protocol to be able to satisfy anonymous and secure mutual authentication. This protocol will be interesting since the overhead for the server can be significantly decreased. Namely, the server can pre-compute a large set of encryptions before running the protocol, in this way the protocol can be more efficient.

D. Adding/Removing a Tag

Whenever $\mathcal{I}$ wants to add a newly generated tag i to the system, he first picks a random x^i and computes y^i value from the curve $y = a_1x + a_0$. Then, (x^i, y^i) and public key share of the server x^S are attached to tag T_i. In order to revoke a tag from the system, the issuer simply generates another secret curve and re-compute the share of the each tag and the reader.

IV. Our Second Protocol for Anonymous and Mutual Authentication

We are now ready to present our second anonymous protocol in which the server can revoke at most $t-1$ tags. In this system, the server has $t-1$ different secret shares $((x_1^S, y_1^S), \ldots, (x_{t-1}^S, y_{t-1}^S))$ whereas each tag i has only one unique secret share (x^i, y^i). This protocol is based on (t,n) threshold cryptosystem. The protocol steps, which are also sketched in Figure 2, are described as follows.

Step 1. The i-th tag picks a random value $r^i \in R\{0,1\}^\ell$ and sends it to the server.

Step 2. The server also picks a random nonce $r^S \in_R \{0,1\}^\ell$ and computes an ElGamal encryption of $m = r^S||r^i$. To encrypt the message m, she first picks a random nonce $r \in \mathbb{Z}_q$. Then the pair of encryptions are computed $(C = (h^r m, g^r))$. She also computes its decryption shares $\sigma_i = g^{ry_i^S} \forall i = 1,\ldots,t-1$. The server sends C and the decryption shares along with

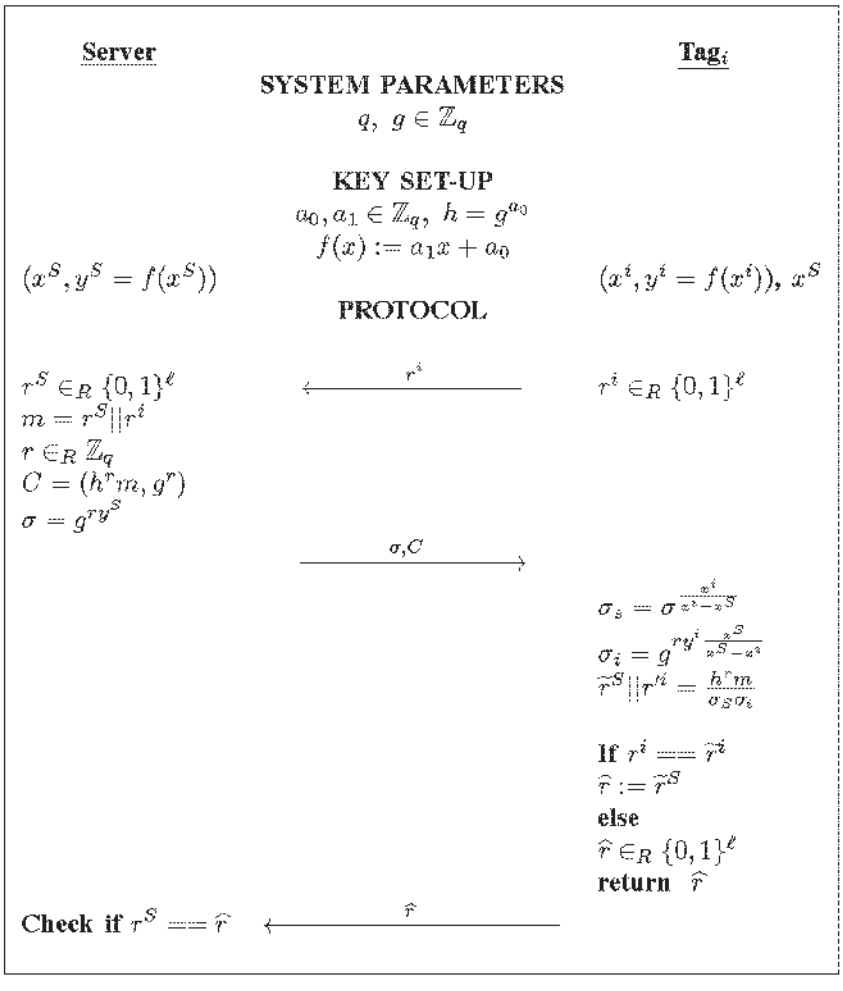


Fig. 1. Our anonymous mutual authentication protocol based on (2,n) threshold cryptosystem.

its public shares $((\sigma_1, x_1^S), \ldots, (\sigma_{t-1}, x_{t-1}^S))$ to the tag i.

Step 3. Upon receiving the message $((\sigma_1, x_1^S), \ldots, (\sigma_{t-1}, x_{t-1}^S), C)$, the tag first completes the decryption shares of the server as $\sigma_S = \prod_{j=0}^{t-1} \sigma_j^{\frac{x^i}{x^i - x_j^S}}$. Then, it computes its decryption share as $\sigma_i = g^{ry^i \prod_{j=1}^{t-1} \frac{x_j^S}{x_j^S - x^i}}$. Finally, it recovers the original message as $\widetilde{r}^S || \widetilde{r}^i = \frac{h^r m}{\sigma_S \sigma_i}$. If the $\widetilde{r}^i$ is equal to the original random value r^i, it sends $\widetilde{r}^S$. Otherwise, it sends a random value $\widehat{r} \in_R \{0,1\}^\ell$.

Step 4. The server verifies whether the received value $\widetilde{r}^S$ is equal to the value r_S she generated at Step 1.

A. Security & Complexity Analysis

For the security analysis, we are going to show that this protocol fulfills the privacy and security requirements for RFID authentication.

Theorem IV.1. *Our first protocol depicted in Figure 1 achieves anonymous authentication even the server is fully corrupted.*

Proof: (Sketch) Assume that an adversary compromises the server and has access to all the private information. The adversary has two choices for an attack.

(i) In the first case, she behaves like a semi-honest party, i.e., follows the protocol properly but try to identify the tag. In that case, at Step 1 of the protocol, the adversary cannot obtain any information about the tag since r^i is completely random. At Step 2, the adversary computes the decryption shares properly and sends them to the tag. At Step 3, the adversary receives only $\widehat{r}$ which gives only the information that the tag is one of the member in the database.

(ii) Now, the adversary does not behaves like a malicious party. Assume that she access to all the private values of the tags from the server. Similar to the previous attacks, the adversary cannot obtain any information about the tag since r^i is completely random. However, at Step 2, the adversary computes the decryption shares with one of the secret shares of the tags in the system and sends them to the tag. At Step 3, the adversary receives only $\widehat{r}$ which is random because the tag could not extract his r^i, and hence the tag sends random bits. The adversary still could not distinguish this tag from others and therefore cannot identify it. ∎

Corollary IV.2. *Our protocol depicted in Figure 1 achieves both forward and backward secrecies without any assumption.*

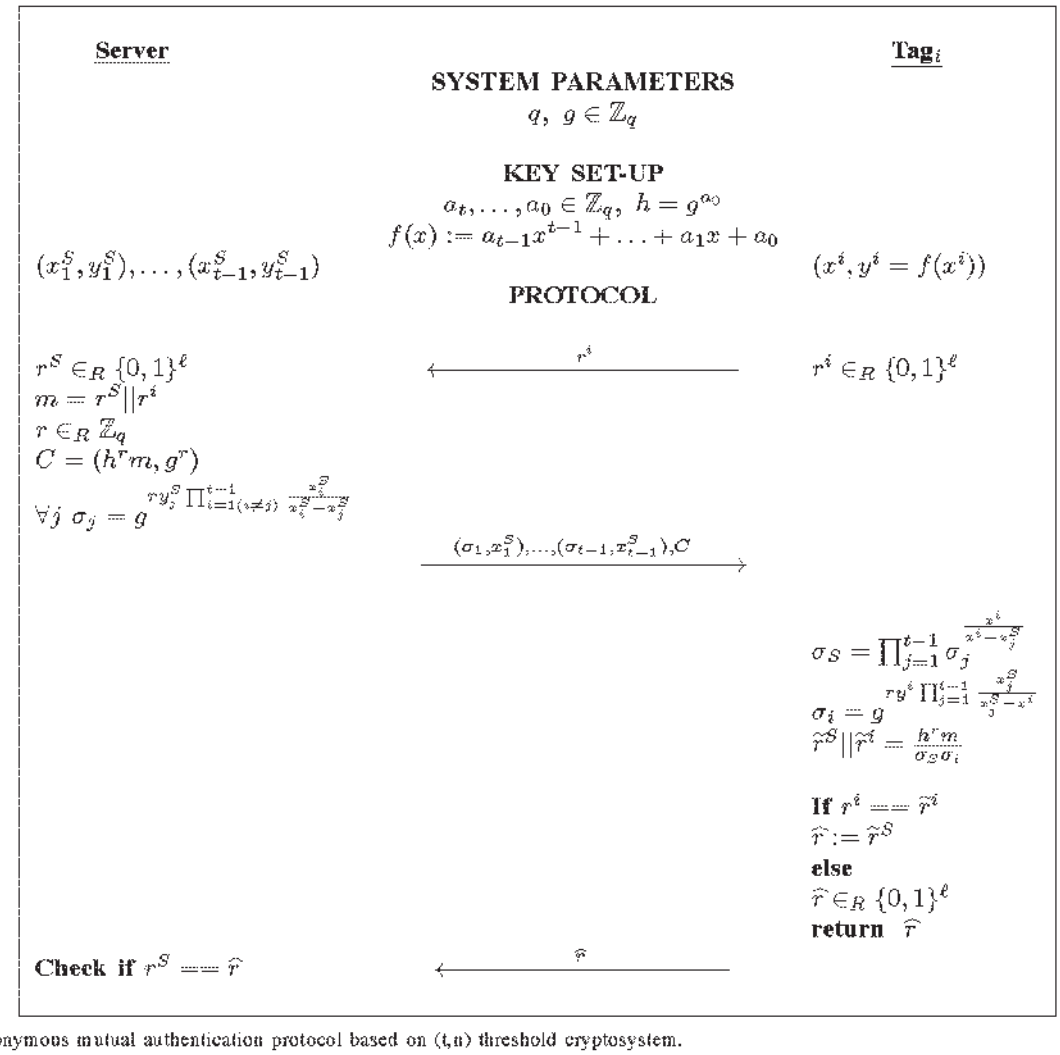


Fig. 2. Our anonymous mutual authentication protocol based on (t,n) threshold cryptosystem.

Proof: (Sketch) Since the protocol achieves secure and anonymous authentication against even Big Brother attack (Theorem IV.1), the adversary is not able to distinguish a tag from others at any time line. Therefore, our protocol achieves both forward and backward secrecies. ■

Unlinkability of tags. The term 'unlinkability' means that an attacker cannot distinguish tags based on their communications. In other words, the protocol messages generated by the tags should not leak any information to an adversary for identification or traceability. Since only the random numbers (which is independent of the secret keys) are sent at the first and the third steps of our protocol, no information about the tag identity is revealed. At the second step, the encryptions $C, (\sigma_i, x_i^S)$ for $i = 1, \ldots, t-1$ are sent by the server which is common for all the tags. Therefore, no attacker can be able to link this message to a tag.

Complexity analysis. Unlike previous protocols, although our protocols use public key operations it is completely secure against server side attacks described above. Still, in total there are only three exponentiations, three inversion and only one multiplication for a tag. At the tag side, two inversions ($\frac{x^i}{x^i - x^S}$, $\frac{x^S}{x^S - x^i}$) can be done off-line and can be stored on its memory beforehand. At he server side, only three exponentiations and one multiplication are performed. We highlight that all the encryptions and partial decryption done by the server can be pre-computed off-line. Note that adding a new tag does not change the complexity of the overall system. Namely, a new user will only get a new share of the secret key, and will do the same computations as other tags. This does not incur any additional complexity to the server.

V. Conclusion

In this paper, we have discussed and proposed a new anonymous and mutual RFID authentication protocol. Our protocol enables RFID tags to authenticate to readers without disclosing any information that allows the identification or tracking of tags even to malicious readers. First, we introduced our first anonymous RFID protocol to give a warm-up which is based $(2, n)$-threshold homomorphic encryption. This protocol does not provide tag revocation. We then proposed our second protocol based on (t, n)-threshold homomorphic encryption which allows tag revocations up to t tags. We highlight that the protocol is still secure even if the server side is

corrupted. However, our current solution does not capture removing an tag which is an interesting open problem for future research. Finally, we show that our protocol satisfies the security requirements like anonymity, privacy, authentication and unlinkability.

REFERENCES

[1] K. Finkenzeller, *RFID Handbook: Fundamentals and Applications in Contactless Smart Cards and Identification*, 2nd ed. New York, NY, USA: John Wiley & Sons, Inc., 2003.

[2] L. Batina, J. Guajardo, T. Kerins, N. Mentens, P. Tuyls, and I. Verbauwhede, "Public-Key Cryptography for RFID-Tags," in *International Workshop on Pervasive Computing and Communication Security – PerSec 2007*, IEEE. New York City, New York, USA: IEEE Computer Society, March 2007, pp. 217–222.

[3] M. McLoone and M. J. B. Robshaw, "Public key cryptography and rfid tags," in *Topics in Cryptology - CT-RSA 2007, The Cryptographers' Track at the RSA Conference 2007*, San Francisco, CA, USA, 2007, pp. 372–384.

[4] Y. Yao, J. Huang, S. Khanna, A. Shelat, B. H. Calhoun, J. Lach, and D. Evans, "A Sub-0.5V Lattice-Based Public-Key Encryption Scheme for RFID Platforms in 130nm CMOS," in *Workshop on RFID Security – RFIDSec Asia'11*, ser. Cryptology and Information Security, vol. 6. Wuxi, China: IOS Press, April 2011, pp. 96–113.

[5] G. Avoine, "Rfid security & privacy lounge," http://www.avoine.net/rfid, 2012.

[6] A. Juels, "Rfid security and privacy: A research survey," *JOURNAL OF SELECTED AREAS IN COMMUNICATION (J-SAC)*, vol. 24, no. 2, pp. 381–395, 2006.

[7] A. S. T. Melanie R. Rieback and, Bruno Crispo and, "The evolution of rfid security," *IEEE Pervasive Computing*, vol. 5, no. 1, pp. 62–69, 2006.

[8] T. S. Heydt-benjamin, H. jin Chae, B. Defend, and K. Fu, "K.: Privacy for public transportation," in *In: Proceedings of Privacy Enhancing Technologies workshop (PET*, 2006.

[9] E.-O. Blass, A. Kurmus, R. Molva, and T. Strufe, "Psp: private and secure payment with rfid," in *Proceedings of the 8th ACM workshop on Privacy in the electronic society*. ACM, 2009, pp. 51–60.

[10] P. Bichsel, J. Camenisch, T. Groß, and V. Shoup, "Anonymous credentials on a standard java card," in *Proceedings of the 16th ACM conference on Computer and communications security*, ser. CCS '09. ACM, 2009, pp. 600–610.

[11] C. Chatmon, T. van Le, and M. Burmester, "Secure anonymous rfid authentication protocols," no. Technical Report TR-060112, pp. 1–10, 2006.

[12] T. V. Le, M. Burmester, and B. de Medeiros, "Universally composable and forward-secure rfid authentication and authenticated key exchange," in *Proceedings of the 2nd ACM symposium on Information, computer and communications security*, ser. ASIACCS '07. ACM, 2007, pp. 242–252.

[13] M. Burmester, T. V. Le, B. D. Medeiros, and G. Tsudik, "Universally composable rfid identification and authentication protocols," *ACM Trans. Inf. Syst. Secur.*, vol. 12, 2009.

[14] A. Sadighian and R. Jalili, "Afmap: Anonymous forward-secure mutual authentication protocols for rfid systems," *Emerging Security Information, Systems, and Technologies, The International Conference on, SECURWARE'09*, pp. 31–36, 2009.

[15] M. Burmester, B. de Medeiros, and R. Motta, "Robust, anonymous rfid authentication with constant key-lookup," in *Proceedings of the 2008 ACM symposium on Information, computer and communications security*, ser. ASIACCS '08. New York, NY, USA: ACM, 2008, pp. 283–291.

[16] B. Liang, Y. Li, C. Ma, T. Li, and R. Deng, "On the untraceability of anonymous rfid authentication protocol with constant key-lookup," in *Proceedings of the 5th International Conference on Information Systems Security*, ser. ICISS '09. Springer-Verlag, 2009, pp. 71–85.

[17] F. Armknecht, L. Chen, A.-R. Sadeghi, and C. Wachsmann, "Anonymous authentication for rfid systems," in *Workshop on RFID Security (RFIDSec)*, ser. LNCS, vol. 6370. Springer, 2010, pp. 158–175.

[18] *Threshold Cryptosystems*, ser. Lecture Notes in Computer Science, vol. 435. Springer, 1990.

[19] T. E. Gamal, "A public key cryptosystem and a signature scheme based on discrete logarithms," in *Proceedings of CRYPTO 84 on Advances in cryptology*. Springer-Verlag New York, Inc., 1985, pp. 10–18.

[20] P. Paillier, "Public-key cryptosystems based on composite degree residuosity classes," in *Advances in Cryptology - EUROCRYPT '99, International Conference on the Theory and Application of Cryptographic Techniques*, ser. Lecture Notes in Computer Science. Springer, 1999, pp. 223–238.

Recommender System Based on Group Trust

Somayeh Naghshbandi, Behrouz Tork Ladani

Abstract— **The rapid growth of world wide web has brought about a new issue named, "Information overload ", a state in which we won't be able to take decision, choose or update our information on a special subject due to huge amount of information. Recommender systems have been proposed as an effective solution to solve this problem. The recommender systems which use trust of users within social networks, can offer more personal recommendations compared to traditional recommender systems like collaborative filtering, but still remain problems like data sparsity, scalability and low coverage.**

This article presents a new way for making recommendation based on group-based trust. In group-based trust, the groups, themselves, are the mediator and developer of trust. Because of belonging to the same group, the users will have some degree of trust to other members of the group and due to the relationship of his group with other groups; they can trust to other members of groups and use their recommendations. Our results show that when the combination of trust and similarity in groups is used for recommendation, the coverage increases without reducing precision.

Index Terms— **recommender system, trust, group**

I. Introduction

With the increasing amount of information on the web, a need for some tools to help users get their required information increases. Recommender systems have been proposed as an effective solution to solve this problem. Generally in a recommender system, there exists a set of users and items. The purpose of recommender system is picked out the few items that might be of interest for the specific user.

Two main algorithmic techniques have been used to make recommendations are content-based and collaborative filtering methods. Content-based approaches try to suggest items that are similar to the ones that user liked in the past. They operate by comparing descriptions of content of items and the user's preferences. One of the biggest problem of content-based is that it needs that items can be parsed by machines. The collaborative filtering (CF) recommends to the active users the items that users with similar preferences liked in past.

S. N. is with the Department of Computer Engineering, University of Isfahan, Isfahan, Iran, e-mail: somayeh.naghshbandi@yahoo.com.

B. T. L is with the Department of Computer Engineering, University of Isfahan, Isfahan, Iran, e-mail: ladani@eng.ui.ac.ir.

The traditional recommender systems suppose that the users are independent and identically distributed. They ignore social relationships or relationships among users [1]. With the advent of online social networks, the trust-based approach to recommendation has emerged. This approach assumes a trust network among users and makes recommendations based on the ratings of the users that are directly or indirectly trusted by user. These methods utilize the inferred implicit or observed explicit trust information to further improve traditional recommender systems.

The main advantage of the methods based on trust is that the items are recommended to the users who are interested by the users of the same situation or interests, instead of setting the base of recommendation on the similarity of users or items which has so far been the user's favorites [2].

In internet, social networks or other environments in which a large number of users grow every day, the trust-based recommender systems face severe problems regarding efficiency and gathering information. Many of the capabilities of social networks are not also taken into account in these methods like the fact that the users within one group are interested in enjoying the recommendations of other members because of similarity with the members or in fact, trusting to the group's members.

In Oxford dictionary the word "group" is defined as, "A number of users either working with each other or have the same beliefs". Since each group has one main goal or common characteristics, the general characteristics of the group can be used while recommending.

In this article to improve recommender system performance, we use of group-based trust [3]. In this model, trust is considered as a collective and shared feature of all group members. This way, the trust between individuals can be realized by membership in their groups.

With recommender system based on group trust, we can use of recommendations of our group memberships that have similarity in beliefs with us, trust to persons that my group trust them and trust to persons with whom we never have been familiar. Such a model helps in creation of trust between different groups easily with less communication and calculation overhead.

The rest of the paper is organized as follows: Section 2 reviews some related work. In section 3 we propose our novel method. We describe the real life data sets used in our experiments in section 4. In section 5, our experimental results are discussed, and section 6 concludes the paper with a summary.

II. RELATED WORK

In this section, we review two major approaches for recommender systems, collaborative filtering and trust-based recommender system and then we present a definition of trust especially group-based trust.

A. Collaborative filtering

One of the most commonly-used and successfully-deployed recommendation approaches is collaborative filtering. There are two types of collaborative filtering approaches, namely, memory-based and model-based approaches. Memory-based methods mainly focus to find the similar users or items for recommendations. User-based approaches [4] predict the ratings of active users based on the ratings of similar users found, while item-based approaches [5] predict the ratings of active users based on the computed information of items similar to those chosen by the active user.

In contrast to the memory-based approaches, the model-based approach constructs a model of users' interests, instead of recording all user ratings, so that ratings could be predicted via the model instead of directly manipulating the original rating database as the memory-based approaches.

However, Recommender Systems based on CF have some important weaknesses. The cold start problem [6] refers to the situation when a user enters the system and has expressed no ratings so that the RS cannot find the similar users and, because of the sparsity of the input data, the CF algorithm is often not able to predict the degree of similarity between two users.

B. Trust-based recommender system

The recommender systems based on the trust of users within social network, can offer more personal recommendations compared to collaborative filtering systems [7]. Trust-based recommender systems usually get their information through a web of trust in which indicates how much users trust each other.

In [6] a trust-based collaborative filtering system for recommender systems has been presented. In this method, the process of collaborative filtering is measured by the users' creditability gained by propagation of trust. A test on a large number of users has shown that this method can increase the number of predicted rates without decreasing the accuracy.

In [8] a system has been presented for trust-based collaborative filtering recommender system for semantic web. It uses the web of trust to make recommendations.

These methods are not applicable to a large data sets as the rate of similarity and the degree of trust of other users has to be calculated for each user. To remove these problems, the group-based trust model has been used in this study.

C. Group-based trust

In group-based trust model [3], the role and significance of groups in determining and management of the rates of trust has been emphasized. Users and groups can act as mediators, generalizing trust and transferor of trust to users to whom they have never had any contact with. On the other hand the rate of users' dependency to groups called the degree of user's membership in group, affects the rate of transferred trust and group membership and is used as a criterion for judging on a user's probable behavior and the manner of trust. GTrust model establishes acceptable levels of trust among people with little acquaintance by mediating groups and users with the help of the concept of membership degree. In this model, group is used as mediator and trust-generalizing. For instance two members of one group, who have had no relationship with each other, can have a degree of trust to each other because of membership in one group or two members in two different groups can have a degree of trust to each other because of the trust of their groups to each other.

In recommender system based on group-based trust, groups are formed based on users' interests. Then the presented model has been presented based on weighted metagraph. Metagraph is a mathematical tool by the help of which a directed relationship between two collections of elements can be defined. A metagraph contains all characteristics of a simple graph. As it can be seen in fig.1, each edge in a metagraph is a well-formed pair of two collections.

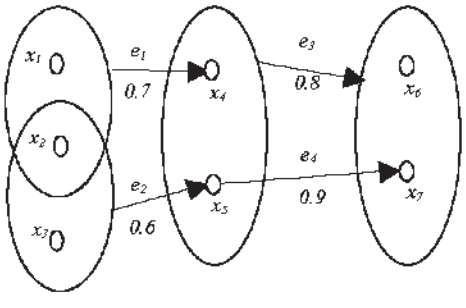


Fig. 1. An Example of MetaGraph

In weighted metagraph, numerical labels are added to the edges. Each label assigns a weight to the edge. The purpose is to add calculative ability to the metagraph. This weight shows the relationship between two nodes. In our model, nodes represent users or group of users. The values of the edges are gained by the average of similarity between the rates of the users and the rate of trust among them. In fuzzy metagraph, each node in the group has a fuzzy factor. This factor represents the degree of the node's membership in the group it belongs. The degree of membership of each user in each group is gained based on two factors: The amount of similarity between the rates users assigned to the items and the rates of memberships of group assigned to the items as well as the rate of trust of the group to the user.

Group propagation can be used as a tool for trust development. That means that if user 1 has a degree of trust to user 2 and the same is true for user 2 to user 3, then the user 1 will have a degree of trust to user 3.

III. OUR MODEL

Our model includes four steps. In first step, users are placed in K different groups based on the rates they have assigned to different items. In second step, users' membership in groups they belong and relation between groups are determined. In third step, we propagate trust by using groups and in fourth step, the recommend system predicate the ratings based on the relation between users. This model has two input data sets: rating dataset in which all the ratings expressed by

users on items are represented and trust dataset which rating expressed by users to each other are represented.

The pseudocode of our model is presented in Fig. 2.

```
Step1 : group formation
Input : rating[n*m] , k          Output : group[n*k]

1: group[n*k] = kmeansClustering(rating[n*m] , k),

Step2 : find userMembership, groupRelation
Input : rating[n*m] , dirTrust[n*n] , groups[n*k]
Output : membership[n*k] , groupRelation[k*k]

for i = 0:n     // find user membership
   for all k that groups[i,k]=1
     simMem[i, k] = Pearson (i,k);
     trustMem[i, k] =
     #dirTrust(i) − #dirDisTrust(i)/#posEdges(k) − #negEdges(k)
     membership[i, k] =simMem[i, k] + trustMem[i, k]/2
   end
end
for i=0:k     // find group relation
   for j=0:k
     simRel[i , j ] = Pearson(i, j) ;
   trustRel[i,j] = posEdges(i , j) − negeEdges(i , j)/|i| * |j| − |i ∩ j|
    groupRel[i , j ] = simRel[i , j] + trustRel[i , j] / 2;
   end
end

Step3 : Propagation Input : membership[n*k] , groupRel[k*k]
Output : userRel[n*n]

groupRel [k*k] = tidalTrustPropagation(groupRel [k*k]);
for i=0:n
   for j= 0:n
      If (dirTrust [i , j ] != 0
        simTrust[i , j ] = dirTrust[i , j ] *Perason(i , j);
      else
        simTrust[i , j ]=0;
   end
end
for i=0:k
  for j=0:k
    If(groupRelation[i , j]>0)
       for all users u_i∈ i && u_j∈ j
        userRel(u_i, u_j) = f(userMem(u_i, G_i) * userMem(u_j, G_j)
                          * groupRel(G_i, G_j), dirRel(u_i, u_j))
       end
       userRel[i,u]=userRel[i,u] / userRelNo[i,u];
    end
  end
end

Step4 : predict rate
Input : userRel[n*n] , rating[n*m] Output : predictRate[n*m]

for all users like a && item like i
   for all neighbors of a like u that
     (rating [u , i ] !=0 && userRel [a,u] > threshold)
     p_a,i = Σ userRel(a,u) * rate(u,i)/Σ userRel(a,u)
   end
end
```

Fig. 2. The pseudocode of our model

In first step, users are placed in K different groups based on the rates they have assigned to different items. It ensures that users who are similar will place in same groups. Nevertheless, it is possible that users place in more than one group.

We employ the K-means algorithm for user clustering and group formation because it is effective and efficient [9]. First, the algorithm randomly selects K users as the initial cluster centroids. Then, the algorithm finds the distance between every point(user rating) and cluster centroids. The assignment operation assigns each user to the cluster with the maximum similarity. It repeats until until the clustering result is stable. We adopt the Pearson correlation coefficient method to calculate the similarity between users and clusters. The Pearson Correlation Coefficient is the most effective and most applicable equation used for estimating similarity.

$$\mathrm{Sim}_{u,g} = \frac{\sum_{i=1}^{m}(r_{u,i}-\overline{r_u})(r_{g,i}-\overline{r_g})}{\sqrt{\sum_{i=1}^{m}(r_{u,i}-\overline{r_u})^2 \sum_{i=1}^{m}(r_{g,i}-\overline{r_g})^2}} \quad (1)$$

In equation (2), $r_{g,i}$ and $r_{u,i}$ are indicating the rate group g and user u have assigned to item i respectively. In order to gain the ratings that a group has assigned to different items, the average of the rates given to items by the group- member users are used. Also $\overline{r_g}$ indicates the average of rates the group g has assigned to all items.

When the clustering result is stable, users place in K clusters.

In the next step, the model determines the degree of users' membership in group and finds the relation between different groups. This includes the following three stages.

In the first stage, the similarity of each user with the groups to which he belongs is gained based on (1).

In the next stage, the value of trust of each group to the members inside the group is gained. For this purpose, the number of the users of the same group with the user who trust the user is gained. The trust membership is gained based on (2).

$$trustMem[i,k] =$$

$$\#dirTrust(i) - \#dirDisTrust(i)/\#posEdges(k) - \#negEdges(k) \quad (2)$$

In (3) $\#dirTrust(i)$ is the number of the users of the same group with the user who trust the user and $\#dirDisTrust(i)$ is the number of the users of the same group with the user who distrust the user. $\#posEdges(k)$ is the number of positive edges in the group k and $\#negEdges(k)$ is the number of negative edges in the group k.

By averaging of two values of simMem(u,g) and trustMem(u,g), the degree of user membership in the group g is determined.

For finding the relation between group i and j, we use two factors. First, we find the similarity between two groups by Pearson Correlation Coefficient. To determine the degree of trust from i to j, we use (3).

$$trustRelation[i,j] = posEdges(i,j) - negEdges(i,j)/|i| * |j| - |i \cap j| \quad (3)$$

In this equation $\mathrm{posEdges}(i,j)$ indicates number of users of group i who trust to members of group j. $\mathrm{negEdges}(i,j)$ indicates number of users of group i who distrust to members of group j. $|i|$ indicates the number of members of group i by averaging of this two factors, the relation between two groups is determined.

In third step, we spread relation between users by using groups. In this model, we propagate trust between groups instead of users. Because of the number of users are less than groups, this model is in general computationally much more efficient.

In this article, the method of TidalTrust [10] is used for trust propagation. TidalTrust is gained through (4). $t_{i,j}$ indicates the value of trust from user i to user j and $adj(i)$ indicates users that user i has a trust more than maximum to them.

$$t_{i,s} = \frac{\sum_{j \in adj(i) | t_{i,j} \geq max} t_{i,j} t_{j,s}}{\sum_{j \in adj(i) | t_{i,j} \geq max} t_{i,j}} \quad (4)$$

After propagation of trust between groups, we spread relation between users by using relation between groups. The relation between two users is gained by (5).

$$userRel(u_i, u_j) = f(userMem(u_i, G_i) * userMem(u_j, G_j) * groupRel(G_i, G_j), dirRel(u_i, u_j)) \quad (5)$$

In (4) $dirRel(u_i, u_j)$is gained by the following equation

$$dirRel(u_i, u_j) = dirTrust(u_i, u_j) * userSim(u_i, u_j) \quad (6)$$

$dirTrust(u_i, u_j)$ shows the trust information that user u_i inserted about user u_j. It has a value between -1 and 1. If user u_i doesn't have any idea about user u_j then, the value of $dirTrust(u_i, u_j)$ would be zero and as a result, the value of $dirRel(u_i, u_j)$ would be zero too.

We can use different function for f in (5). Some possible functions are maximum and minimum and average or give different weight to inputs. Of course the sum of the weights has to be 1.

Since some of the users are members of different groups, it is necessary that (5) is gained based on membership in different groups and at the end the average of the results is gained.

When the rate of users' weighting to each other is determined, the stage of recommendation is beginning. In this stage, the values of rates are gained based on weighting average on the basis of group-based trust .As it is shown in (7):

$$p_{a,i} = \frac{\sum_{u=1}^{k} w_{a,u} \times r_{u,i}}{\sum_{u=1}^{k} w_{a,u}} \quad (7)$$

In (7), $w_{a,u}$ presents the value of relation between user a and user u. $r_{u,i}$ means that the value that user u rated item i.

IV. Experiments

This section reports our experimental results on a real life data set comparing Group-Based Trust against state of the art methods for trust based and item based recommendation. We implemented Group-Based Trust as well as the MoleTrust based recommendation proposed by Massa [11] and TidalTrust proposed by Golbeck. We also implemented standard User based Collaborative Filtering fundamental similarity based recommendation method.

A. Dataset

In this section we briefly introduce the data set we use in our experiments. We used the version of the Epinions dataset published by the authors of [11]. The dataset contains 49,290 users who rated a total of 139,738 different items at least once and 487,181 issued trust statements.

Each user has on average 7.12 expressed ratings and 9.88 direct neighbors. The social relations in Epinions are directed. The distribution of the number of ratings per user follows a power law. The items in Epinions are from different categories such as cameras, dvd players, music.

B. Experimental setup

We perform 2-fold cross validation in our experiments. In each fold we have 50% of data as the training set and the remaining 50% as the test data.

We use the Root Mean Squared Error (RMSE) to measure the error in recommendation:

$$RMSE = \sqrt{\frac{\sum_{i=1}^{n}(r_{u,i} - p_{u,i})^2}{n}} \quad (8)$$

Where n is number of all pairs (u, i) in the test data. $r_{u,i}$ is the rate of user u assigned to item i and $p_{u,i}$ is the predicted rate of user u to item i. A small value of RMSE indicates more precise recommendation.

We define a *coverage* metric to measure the percentage of pairs of <user,item> for which we can predict a rating.

To combine *RMSE* and coverage into a single evaluation metric, we compute the *FMeasure* [12]. For this purpose, we have to convert *RMSE* into a precision metric in the range of [0,1]. So we define *precision* as follows:

$$Precision = 1 - \frac{RMSE}{4} \quad (9)$$

In this equation, 4 is the maximum possible error since the values of ratings are in the range [1,5].

$$FMeasure = \frac{2 * precision * coverage}{precision + coverage} \quad (10)$$

In our experiments, we compare the results for different methods. Following is the description of labels we use to denote each of these algorithms:

TTR. This is refers to TidalTrust.

MTR. This is refers to MoleTrust.

CF. This refers to collaborative filtering.

GTR. This refers to Group-based Trust(our model).

We examine our model with different distance threshold. Distance threshold means max depth for propagation of trust. MTR3 and MTR5 as well as GTR3 and GTR5 refer to 3 max distances and 5 max distances respectively.

C. Experimental results

In this subsection, we present the results of our experiments, first for cold-start users and then for all users.

Fig. 3 shows the chart comparing the results of different methods according to each of three evaluation measures separately for cold start users.

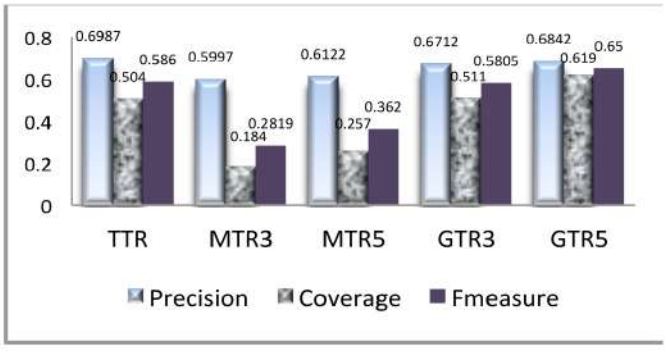


Fig. 3. Comparison of Coverage and Precision together with F-Measure for different methods on cold start users.

As shown in Fig. 3, *GroupBasedTrust* has lower error than all the other methods except for *TTR*. But *TTR* has lower coverage (0.504%) and as a result GTR5 has a better Fmeasure than all the other methods.

The comparison between *GTR5* and *GTR3* shows that increasing the distance threshold reduces the error and respectively increases the coverage and F-Measure.

Of course the precision and coverage of MTR is worth than all the others methods.

Fig. 4 shows the chart comparing the results of different methods according to each of three evaluation measures separately for cold friendship users. In this article we refer to users with less than 5 friends as cold friendship users.

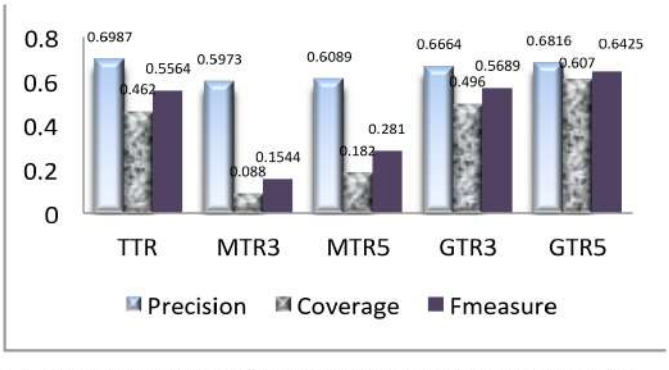


Fig. 4. Comparison of Coverage and Precision together with F-Measure for different methods on cold friendship users.

As shown in Fig. 4, *GroupBasedTrust* has a better Fmeasure than all the other methods. The coverage of *GroupBasedTrust* is significantly better than the other. The best coverage among the other one is 0.42 for *TTR*. Notice that the error of *TTR* is very close to *GroupBasedTrust*, but *GroupBasedTrust* clearly has a better coverage.

It shows when we do not have enough information especially when users have little relation with the other one, our model outperforms all other methods according of coverage.

Table 1 shows the F-Measure for all users. The columns show distance threshold. As table 1 show, the GTR5 has a better F-Measure than the other entire one. It should be noted that all methods perform significantly better over all users since there is less information available for cold start users and cold friendship users. GTR5 outperforms all other methods in terms of F-Measure, although the gain for all users is less than the gain for cold start users.

TABLE 1: Comparison of F-Measure for different methods with different distance threshold for all users

	GTR	TTR	MTR	CF
1	0.3176	0.634	0.1976	0.1838
2	0.5382	0.634	0.4662	0.1838
3	0.6193	0.634	0.586	0.1838
4	0.6488	0.634	0.6223	0.1838
5	0.6566	0.634	0.6315	0.1838

V. CONCLUSION

The need for recommender systems is increasing every day. Despite powerful search engines and sites for discussions and talk, our questions still remain unanswered or we are given answers not conforming to our demands. That's because they are answers given by people who have no common characteristics with us. In this case the significance of social networks in which we can enjoy our friends' recommendations is more tangible.

In this study, the group-based trust in social networks was used for recommendation. Users are seen as individuals with interests in the same line with the groups to which they belong. We performed an evaluation on the Epinions dataset, demonstrating that recommender system based Group Trust outperforms both collaborative filtering method and tidal trust and mole trust methods specially in terms of coverage.

ACKNOWLEDGMENT

Thanks for the support of Research Institute for ICT, Tehran, Iran.

REFERENCES

[1] W. Hill, L. Stead, M. Rosenstein, and G. Furnas, "Recommending and Evaluating Choices in a Virtual Community of Use". *Proc. Human Factors in Computing Systems*, 1995.

[2] G. K. Hummel, B.V. Berg, J. Berlanga, Hend José Janssen, R.Nadolski, "Combining social-based and information-based approaches for personalised recommendation on sequencing learning activities ", *International Journal Learning Technology*, Vol. 3, No. 2, pp.152-168, 2007

[3] M.Ezhei ," GTrust: A group based trust model", *MSC thesis*, Esfahan university, 2009.

[4] R. Jin, J. Y. Chai, and L. Si. "An automatic weighting scheme for collaborative filtering". *In Proceeding of the 27th annual*

international ACM SIGIR conference on Research and development in information retrieval, pp. 337– 344, New York, NY, USA, 2004.

[5] M. Deshpande and G.Karypis."Item-based top-n recommendation". *ACM Transactions on Information Systems*, vol. 22, no. 1, pp. 143–177, 2004.

[6] P. Massa and P. Avesani. "Trust-aware collaborative filtering for recommender systems". *In Proc.CoopIS/DOA/ODBASE*, pp. 492–508, 2004.

[7] P. Victor, C. Cornelis, M. De Cock, A. Teredesai, "Trust- and Distrust-Based Recommendations for Controversial Reviews," *IEEE intelligent Systems*, 2011.

[8] P. Bedi, H. Kaur, and S. Marwaha. "Trust base recommender system for semantic web". *In Proc. International Joint Conferences on Artificial Intelligence*, pp.2677–2682, 2007.

[9] C. Manning, P. Raghavan, and H. Schutze, "Introduction to Information Retrieval". Cambridge University Press, 2008.

[10] J. Golbeck, "Generating Predictive Movie Ratings from Trust in Social Networks". *In Proceedings of the 4th International Conference on Trust Management*, pp. 93-104 , 2006.

[11] P. Massa and P. Avesani. "Trust-aware recommender systems". In ACM Recommender Systems Conference), USA, 2007.

[12] M. Jamali and M. Ester, "TrustWalker: A Random Walk Model for Combining Trust-based and Item-based Recommendation," *in the 15th SIGKDD conference (KDD'09)*, Paris, France, 2009.

Elektronik Seçim: Norveç'in İnternet Üzerinden Oylama Sistemi ve Kriptografik Altyapısı

Mehmet Sabır KİRAZ, Fatih BİRİNCİ, Uğur Kaşif BOYACI

***Özet*—Bu çalışmada internet tabanlı elektronik seçimi uygulayan iki ülkenin seçim protokolü anlatılacaktır: internet üzerinden e-Seçim'i ülke çapında ilk defa uygulayan ülke Estonya ve ikinci uygulayan ülke Norveç. Yazıda ayrıca genel olarak internet tabanlı elektronik seçimlerin güvenliğini analiz edeceğiz ve elektronik seçimler ile ilgili özgün bir risk analizi sunacağız. Sonuç bölümünde ise Türkiye için bazı tavsiyelerde bulunacağız.**

***Anahtar Kelimeler*—Elektronik seçim, Eşik şifreleme sistemleri, Homomorfik şifreleme**

***Abstract*—In this work, we present the Internet-based electronic voting protocols of two countries: Estonia, the first country that used internet based voting and Norway, the second country that used internet based voting for the local elections at the end of 2011. We discuss the security of an Internet based voting scheme in general and give a detailed risk analysis. We conclude this paper by giving some recommendations for Turkey.**

***Keywords*—Electronic voting, Threshold cryptosystems, Homomorphic encryption**

I. Elektronik Seçim ve Kriptografi Kullanımı

Oy verme ve/veya oy saymanın elektronik olarak yapıldığı seçimlere elektronik seçim ya da kısaca e-Seçim denir. Elektronik seçim sistemi bilgi güvenliğinden insan psikolojisine, kriptolojiden hukuka kadar birçok konuda çözüm gerektiren sorunlar barındırır [1], [2], [3], [4]. Kriptografi açısından birbirleri ile neredeyse zıt farklı isterler aranmaktadır. [1], [5]'de elektronik seçim sistemlerinin sağlaması beklenen güvenlik özellikleri hakkında detaylı bilgi bulabilirsiniz. Farklı güvenlik beklentileri, farklı ödünleşimler ve farklı kriptografik teknikler sayesinde çok farklı elektronik seçim mekanizmaları tasarlamak, hatta kağıt tabanlı seçimlerde sağlanmayan bazı özellikleri sağlayan sistemler bulmak mümkündür. [6], [7], [8], [9].

Bu yazıda internet üzerinden yapılan iki e-Seçim sistemi (i-Seçim) incelenecek, e-Seçim ile ilgili kapsamlı ve özgün bir risk analizi sunulacaktır.

A. İnternet tabanlı seçim sistemleri (i-Seçim)

İ-seçim sayesinde oyumuzu seçim zamanı süresince istediğimiz saatte, sıra beklemeden, istediğimiz yerden hatta yurtdışından kullanabiliriz. Sandık başına gelmesi çok müşkül engelli seçmenlerin oy kullanabilmeleri sağlanabilir. Diğer yandan, kullanıcılar alışkanlık kazandıkça seçim otoritelerinin yükü azalacak, oylar çok daha hızlı ve zahmetsiz sayılacak ve seçim maliyetleri tahminen çok düşecektir. [10] Bu yazımızda Estonya ve Norveç'in i-Seçim uygulamalarını inceleyeceğiz. Kullanılan kriptografik yöntemler kısaca anlatılacak ve sistemlerin analizleri verilecektir.

Bu çalışma kısmen Akıllı Kart Tabanlı Elektronik Kimlik Doğrulama Sistemi ve TC Kimlik Kartı Geliştirme Projesi tarafından desteklenmiştir.

M. S. Kiraz, F. Birinci ve U. K. Boyacı TÜBİTAK BİLGEM Ulusal Elektronik ve Kriptoloji Araştırma Enstitüsü'nde çalışmaktadır, e-posta: {m.kiraz, ukasif, fatih}@uekae.tubitak.gov.tr

II. Estonya'da İ-seçim

Estonya, nitelikli imza fonksiyonu içeren akıll vatandaşlık kartının mecburi olduğu ilk ülkedir ve kamu hizmetlerinin neredeyse tamamı internet üzerinden verilmektedir [11].

Estonya, 2005 yerel seçimleri ile birlikte internet yoluyla ülke çapında vatandaşlarına oy kullandıran ilk ülke oldu. 2011 genel seçimlerine kadar i-seçmen katılımcıların oranı ülke genelindeki her yeni seçimde artarak %2'lerden %24'lere vardı [12]. Estonya seçim protokolünün ana adımları aşağıda verilmiştir.

A. Estonya i-seçim sistemleri adımları

1) Seçmen, kurumsal bir e-seçim sitesine girer ve elektronik kimlik kartı vasıtasıyla kimliğini doğrulatır. İstemci uygulamasını siteden indirir.
2) İstemci uygulaması, seçmeni Oy Yönlendirme Sunucusu'na (OYS) bağlar.
3) OYS, kimlik doğrulamasının ardından seçmene aday listesini gönderir.
4) Seçmen, listeden bir aday seçer. İstemci uygulaması, OYS'nin açık anahtarını kullanarak seçmenin oyunu şifreler.
5) Seçmen, imza özel anahtarını kullanarak şifreli zarfı imzalar ve OYS'ye yollar.
6) OYS, seçmenin oyunu Oy Depolama Sunucusu'na (ODS) gönderir.
7) ODS, Açık Anahtar Altyapısı (AAA) sistemi ile iletişim kurar ve seçmen kimliğini doğrulatır. Oyu veritabanına kaydeder ve OYS'ye onay gönderir.
8) OYS, istemciye (seçmene) oyun başarılı olduğunu gösteren onay bilgisini gönderir.
9) Oy kullanma süresi bitiminde ODS oyları sıralar ve mükerrer oyları veya klasik yolla oy kullanan i-seçmenlerin oylarını iptal eder.

10) ODS, farklı kesimlerden gelen gözetmenlerin izlediği bir prosedürle oyların üzerindeki elektronik imzayı kaldırır.
11) ODS personeli, tüm şifreli oyları çevrimdışı bir kanaldan Oy Sayım Sunucusu'na (OSS) taşır.
12) OSS asimetrik şifreleme özel anahtarı daha önceden farklı yetkililere dağıtılmıştır. Özel anahtar eşik sır paylaşımı yoluyla tekrar oluşturulur. OSS, şifreli oyların şifresini çözer.
13) OSS yetkilileri açılan oyların sayımını yapar ve seçim sonucu üretir.
14) Sistemde anlık bilgi kayıtları tutulmaktadır. Kayıt bilgileri gözetmenler tarafından incelenerek güvenlik ihlalleri tespit edilir.

III. Norveç'te 2011'de Uygulanan İ-seçİm sİstemİ

Birçok kritere göre dünyanın en gelişmiş ülkelerinden biri olan 4,9 milyon nüfuslu Norveç'in nüfusun %95'i internet kullanmaktadır. Dolayısıyla i-Seçim'e en hazır ülkelerden biri olduğu söylenebilir. Yine de Avusturya gibi gelişmiş bir ülkede yaşanan olumsuz tecrübeler, Norveç hükümetini daha temkimli davranmaya yöneltmiştir.

A. Avusturya Deneyimi, Norveç e-Seçim Hazırlıkları

Avusturya'da sistemin kriptografik bazı detaylarının topluma açıklanmamasından dolayı medyada az sayıda kişi tarafından dile gettirilen fakat çok ses getiren eleştiriler yer almış ve halkın e-Seçim'e güveni azalmıştır. Avusturya hükümeti bunun üzerine sistem kaynak kodunu gönüllü katılımcı uzmanlardan oluşan bir gruba kısmen açmışsa da, toplumda oluşan güven eksikliğini gidereməmiş ve akabinde e-Seçim projelerini rafa kaldırmak zorunda kalmıştır. Avusturya Federal Anayasa Mahkemesi 2009 yılında yapılan bir pilot uygulamanın sonuçlarını geçersiz saymıştır [13]. Avusturya deneyimi e-Seçim'in benimsenmesinde açıklık ve şeffaflığın payını göstermesi açısından önemli bir örnek olmuştur.

Norveç Yerel Yönetimler ve Bölgesel Kalkınma Bakanlığı (KRD), e-Seçim'in uygulanabilirliği açısından halkın beklentilerinin önemli bir rol oynayacağının bilinciyle, 2004 ortasında bir çalışma komitesi atamıştır. Komite dört alt çalışma grubundan oluşmuştur: 1. e-Seçim teknikleri, 2. Ekonomik ve idari hususlar, 3. e-Seçim ve demokrasi 4. Hukuki durum. Bu çalışma gruplarının yanı sıra komite, genel toplantılar düzenlenmiş ve bulgularını hükümete sunmuştur [14]. 2009 yılında Norveç hükümeti, 2011 yerel seçimleri için elektronik seçim pilot projesini uluslararası bir ihale prosedürüyle başlatmıştır. 2017'deki milletvekili seçimlerinde uygulanacak i-seçimlere kadar milli açık anahtar altyapısı ve ulusal elektronik kimlik kartının hazır olacağı öngörülmüştür.

Norveç hükümetinin internet üzerinden elektronik oylamaya yönelmesinin en temel nedenleri şunlardır:

- Sayım sürecini hızlandırmak. Tüm seçmenler elektronik oylama yoluyla oyunu kullanırsa, sayma işlemi potansiyel olarak sandık kapanışından kısa süre sonra sonuçlandırılabilir.
- Yenilik sayesinde katılım oranını artırmak. Özellikle genç seçmenlerde katılım oranının hissedilir oranda yükseleceği tahmin edilmektedir.
- Engelli vatandaşların daha rahat oy kullanmalarını sağlamak. Özellikle görme engelli vatandaşların sesli ekran okuyucular aracılığıyla başkalarının yardımı olmadan oy kullanabilmesi sağlanabilir.
- Elektronik seçimlerin orta vadede maliyet-etkinliğinden faydalanmak. i-Seçimlerin kurulum maliyeti nedeniyle kısa vadede olmasa da uzun vadede diğer seçim sistemlerine göre daha az zaman ve para gerektireceği kestirilmektedir.

B. Norveç sistemi

Norveç'in seçim mimarisi genel olarak Estonya seçim sistemi ile benzerlik taşımaktadır [15]. Estonya seçim sistemi ile en temel fark Norveç i-Seçim sisteminin açık ve şeffaf olmasıdır. Norveç hükümeti sistemin kriptografik mimarisi ve kaynak kodu dahil teknik konularla ilgili birçok belgeyi detaylarıyla yayınlamıştır. Norveç sisteminin kriptografik protokolü, İspanyol elektronik seçim şirketi Scytl tarafından tasarlanmış fakat ulusal ve uluslararası uzman danışmanlar tarafından pek çok değişikliğe uğramıştır. Scytl şirketi standart seçim çerçevesi ve iki farklı kanal mekanizması önermiştir. Önerilen standart seçim çerçevesi genel olarak bilinen standart kriptografik protokol ve mekanizmalarından oluşmaktadır [16].

Norveç sistemi iki önemli tehdit türüne karşı önlem almıştır:

- Seçmen bilgisayarlarına yönelik kötü amaçlı yazılım (malware), kurban saldırganlar ağı (botnet), palıkçılık (phishing) gibi tehditler,
- Zorlama (coercing) ve oy satma

Norveç sisteminin Estonya sisteminden bir diğer önemli farkı, seçmen bilgisayarındaki tehditlerin engellenmesi için internetin dışında, farklı ve bağımsız iletişim kanallarının kullanılmasıdır. Seçim öncesi ve seçim sonrası kullanılan bu iletişim kanallarına posta servisi ve kısa mesaj servisi (SMS) örnek gösterilebilir.

Norveç seçimlerinde de Estonya'da olduğu gibi, i-Seçim yoluyla seçmenler istedikleri kadar oy kullanabilmekte fakat varsa klasik seçim sistemi ile kulanılan oy, yoksa i-Seçim ile kullanılan en son oy sayılmaktadır.

i-Seçim sistemlerinde oy verme aşamasında homomorfik şifreleme yapılmakla birlikte, oy sayımı için genelde aşağıdaki iki yöntemden biri tercih edilir:

- Şifreli oyların hepsi çarpıldıktan sonra, ortaya çıkan şifre bir çeşit eşik sır paylaşımı yoluyla çözülür. Homomorfik şifrelemenin özelliği nedeniyle şifresi çözülen mesaj oy toplamlarıdır. Bu yöntem, basit ve küçük seçimler için uygulanabilir olmakla birlikte büyük ölçekli seçimlerde verimi tartışmalıdır.

- Karıştırıcı ağlar kullanılarak oylar anonimleştirilir, sonrasında şifreli oylar (eşik sır paylaşımı yoluyla) tek tek deşifre edilir. Oylar yetkili gözetmenler huzurunda toplanır [1].

Norveç seçimlerinde güvenlik seviyesi ve verimliliğinden dolayı homomorfik sistemler yerine, karıştırıcı ağlar tercih edilmiştir.

1) Zorlama ve Oy Satma: Evden oy kullanılabildiği için maalesef kriptografik yöntemler, zorlamayla oy kullanımını doğrudan engelleyemektedir fakat zorlama altında oyunu kullanan seçmen daha sonra internet üzerinden ya da klasik seçim yoluyla oyunu tekrar kullanabilir. Zorlamaya karşı alınan önlemler aynı zamanda oy satmayı da bir ölçüde engellemektedir. Bunun yanında, aşağıda bahsedileceği gibi, kanunlar bu tarz eylemleri yasadışı sayacak şekilde değiştirilmiştir.

C. Norveç: i-Seçim için değişikliğe uğrayan yasalar

Bir ülkede elektronik seçim ülke yasalarının müsaade ettiği çerçevede uygulanabilir. Norveç Anayasası'nda ve seçim ile ilgili birçok yasada ülkede elektronik seçim yapılabilmesi için düzenlemeye gidilmiştir. Anayasada yer alan elektronik seçimi ilgilendiren temel direktifler aşağıdaki gibidir:

- Oylama sonuçlarını bozmak veya değiştirmek yasadışıdır.
- Seçmeni oy vermeye zorlamaya veya zorla istediği birine oy verdirmek yasadışıdır.
- Oy satmak ve oy satın almak yasadışıdır.
- Oy sayımına etki edebilecek her türlü davranışta bulunmak yasaktır.

Bunun yanında aşağıdaki hukuksal metinlerde düzenlemeler yapılmıştır: Seçim Mevzuatı, Elektronik İmza Mevzuatı, Gizliliğin Korunması hakkında Mevzuat, Elektronik İdare Yönetmeliği, Özgür ve Gizli Seçme Hakkı ve İlkeleri, Eşit Seçme Hakkı İlkesi, Evrensel Seçme Hakkı İlkesi, Seçim Uygulama Yönergesi, Ceza kanunu. Ayrıca, yapılan değişikliklerin İnsan Hakları Avrupa Sözleşmesi'ne uygunlugu incelenmiştir.

D. Norveç: i-Seçim akışı

Çift zarf yöntemini kullanan i-Seçim sistemi şu adımlardan oluşmaktadır:

1) Seçimlerden önce seçmenlerin adreslerine adayların isimlerini ve doğrulama kodlarını içeren bir posta ulaşır.
2) Seçmen oy kullanmak için seçim merkezinin web sayfasına bağlanır ve bilgisayarına seçim uygulamasını indirir.
3) Seçmen, seçim uygulamasını kullanarak ulusal kimlik kartı ile oy sunucusuna kimliğini doğrulatır.
4) Seçim uygulaması güvenli bir kanal üzerinden parti ve adayların listesini alır. Bu liste, aynı bölgedeki tüm seçmenler için aynıdır ve şifreli değildir.
5) Seçim uygulaması partileri rasgele bir şekilde (karışık olarak) görüntüler.
6) Seçmen oy vermek istediği partiyi seçer ve bir sonraki adıma geçer. Seçmen için boş oy seçeneği de mevcuttur.
7) Seçilen parti için aday listesi gösterilir ve seçmenlerin istediği adaylara oy vermesi sağlanır. Seçmene karar verdiği oya ait bir özet sunulur. Seçmen yaptığı seçimden memnun ise "İleri" butonunu tıklar. Yapılan seçime ait metin, oy sayım sunucusunun açık anahtarı ile şifrelenir.
8) Seçmen, imzalama özel anahtarı ile oyunu imzalar. Şifreli imzalı oy, elektronik sandığa gönderilir.
9) Oy kullanıldıktan sonra seçmenin cep telefonuna bir doğrulama kodu gönderilir: "Siz, [seçmen adı], [gün-ay-yıl] tarihinde saat [GMT+1]'te bir oy kullandınız. Onay kodunuz [kod]'dur".
10) Seçmen cep telefonuna gelen doğrulama kodunu posta yoluyla evine gelen kodla eşleştirerek kullandığı oyun başarılı bir şekilde kullanılıp kullanılmadığını kontrol edebilir. Seçmen SMS ile gelen bu mesajla posta yoluyla gelen mesajlardan farklı olduğu durumlarda, "Oy sandığı bulunamadı" gibi mesajlarda veya oy vermediği halde mesaj geldiği durumlarda itiraz eder. Bu durumda seçmen tekrar oy kullanır, ya da klasik şekilde oy verir.

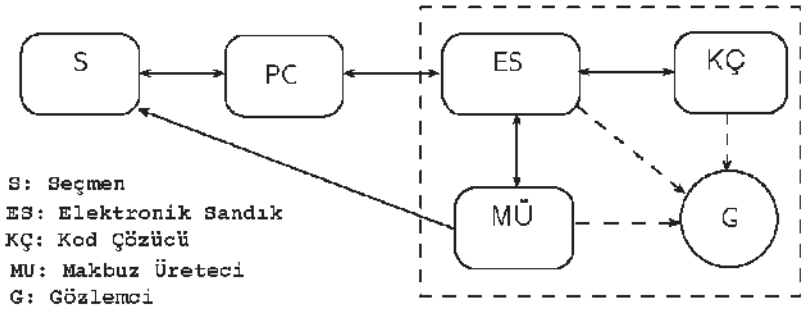
E. Oy kullanma protokolü

Uzaylar ve protokol katılımcıları: k_{max} toplam aday sayısını göstermek üzere, aday listesini $O = \{1, 2, 3, \ldots, k_{max}\}$ ile ifade edelim. $(v_1, \ldots, v_k)$ ise bir seçmenin oy verdiği adaylar olsun, öyle ki $v_i \in O$ $(k < k_{max})$.

- C Kodlama uzayı,
- F Fonksiyon uzayı,
- S Seçmen uzayı,
- PC Kişisel bilgisayar seçim uygulaması,
- ES Elektronik sandık,
- MÜ Makbuz Üreteci ,
- KÇ Kod Çözücüsü,
- SBP Sıfır bilgi protokolünü göstersin.

G, g elemanı tarafından üretilen (asal) q mertebeli bir çarpımsal grup olsun. C olarak ifade edilsin. S G'den C'ye (seçmene posta yoluyla gönderilen doğrulama kodlarının uzayı) giden sanki rassal fonksiyon uzayı F olsun. $f \in F$ bire-bir kodlama fonksiyonu, d buna ait kod çözme fonksiyonu olarak tanımlansın.

Anahtar üretimi: Anahtarların güvenli bir otorite (örneğin, Yüksek Seçim Kurulu) tarafından üretildiğini varsayılım . Bu anahtarlar eşik sır paylaşımı kriptografik yapı taşı kullanılarak üretilir [18]. Seçimden önce otorite tarafından a_1, a_2 ve a_3 parametreleri, $a_1 + a_2 = a_3 \pmod q$ olacak şekilde seçilir. a_1, a_2 ve a_3 anahtarları sırasıyla D, ES ve MÜ'ye dağıtılır. Açık anahtarlar ise şu şekilde hesaplanır: $y_1 = g^{a_1}, y_2 = g^{a_2}$ ve $y_3 = g^{a_3}$. Seçmen, oyunu bu açık anahtarları kullanarak şifreler ve ES'ye gönderir. ES ve MÜ özel anahtarları a_2 ve a_3'ü kullanır



Şekil 1. Norveç Protokolü iletişim kanalı [17]

ve çıkan sonucu D'ye gönderir. D ise özel anahtarı a_1'i kullanarak oyları sayar. Burada ES, MÜ ve D fiziksel ve organizasyonel olarak farklı olmak zorundadır, aksi takdirde farklı servisler olarak algılanmazlar. Bunun yanında, ES, MÜ, D ve gözetmenler arasındaki iletişim için güvenli bir kanal olması gerekmektedir. Bu amaçla standart internet güvenlik protokolleri, örneğin TLS veya IPSEC, kullanılabilir.

Makbuz üretimi: Makbuzlar seçimden önce şu şekilde oluşturulur: Her seçmen için $s_i \in_R \{0,\ldots,q\}$ ve $d \in_R F$ seçilir öyle ki $f : x \longmapsto x^{s_i}$ ve $r : O \longmapsto C$. f ve d fonksiyonlarının bileşke fonksiyonu $r(v) = d((f(v))^{s_i})$ olarak hesaplanır. Seçimden önce, $\{(v, r(v)) \,|v \in O\}$ ikilisi yani makbuz seçmene posta yoluyla gönderilir.

Protokol adımları:

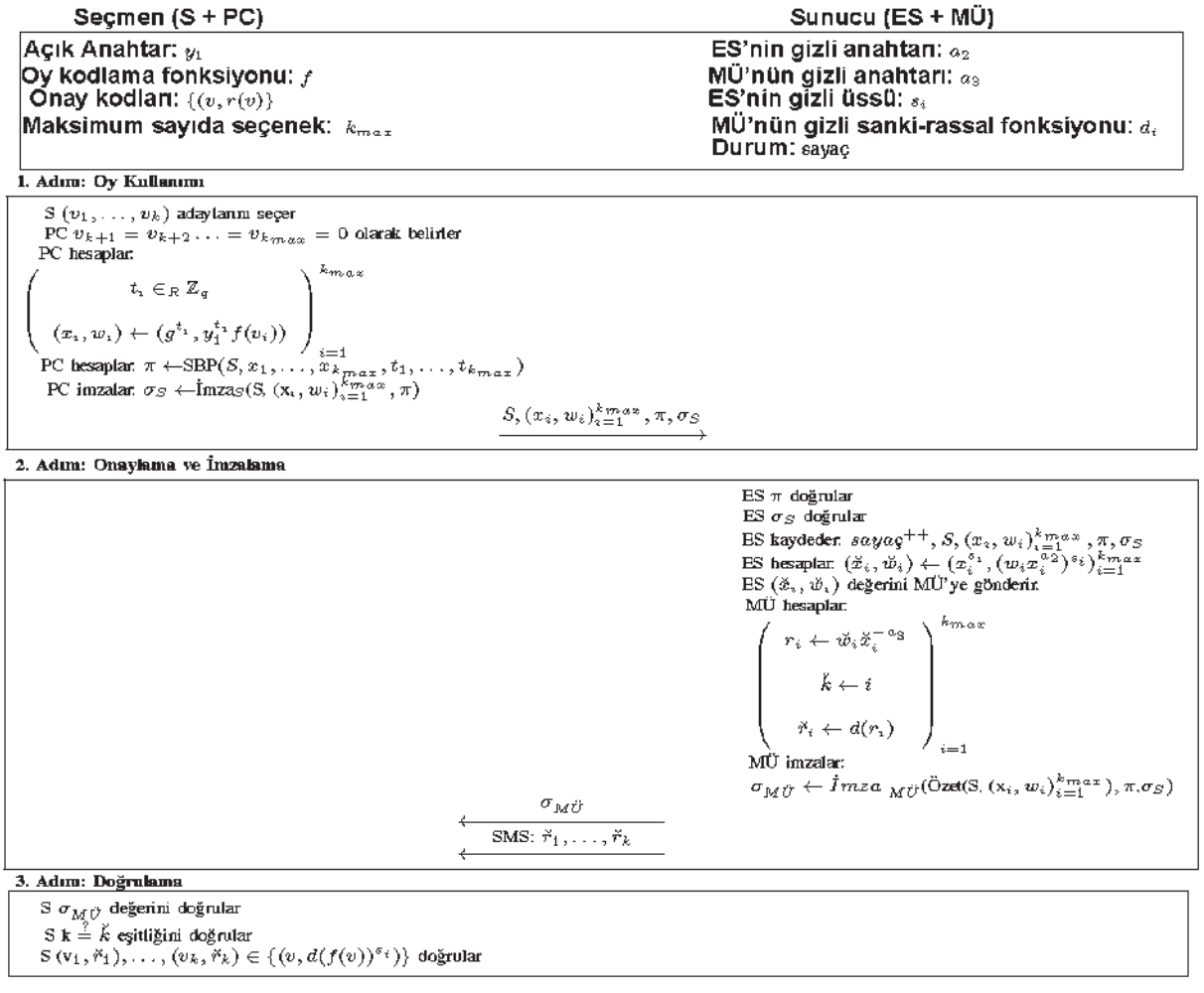
1) **Oy kullanımı**: Seçmen oylama esnasında O aday listesinden $(v_1,\ldots,v_k)$ seçeneklerine karar verir. PC, seçmenin yaptığı k seçiminden arta kalan adaylar için $v_{k+1} = v_{k+2} = \ldots = v_{k_{max}} = 0$ olarak belirler. Daha sonra PC her adayı $t_i \in_R \mathbb{Z}$, $(x_i, w_i) \leftarrow (g^{t_i}, y_1^{t_i} f(v_i))$ $\forall i = 1,\ldots,k_{max}$ homomorfik şifreler. PC yaptıklarının doğruluğunu ispatlamak için $\pi \leftarrow \text{SBP}(S, x_1,\ldots,x_{k_{max}}, t_1,\ldots,t_{k_{max}})$ sıfır bilgi protokol değerini hesaplar. Seçmen $\sigma_S \leftarrow \text{İmza}_S(S, (x_i, w_i)_{i=1}^{k_{max}}, \pi)$ imzaladıktan sonra ES'ye $S, (x_i, w_i)_{i=1}^{k_{max}}, \pi, \sigma_S$ bilgilerini gönderir.
2) **Onaylama ve İmzalama:** ES, ilk olarak π'yi ve σ_S'yi doğrular. Daha sonra $sayaç^{++}, S, (x_i, w_i)_{i=1}^{k_{max}}, \pi, \sigma_S$ bilgilerini kaydeder, $(\breve{x}_i, \breve{w}_i) \leftarrow (x_i^{s_i}, (w_i x_i^{a_2})^{s_i})_{i=1}^{k_{max}}$ şeklinde hesaplar ve MÜ'ye gönderir.
MÜ $\forall i = 1,\ldots,k_{max}$ için şu hesapları yapar: $r_i \leftarrow \breve{w}_i \breve{x}_i^{-a_3}$, $\breve{k} \leftarrow i$, $\breve{r}_i \leftarrow d(r_i)$. Daha sonra $\sigma_{MÜ} \leftarrow \text{İmza}_{MÜ}(\text{Özet}(S, (x_i, w_i)_{i=1}^{k_{max}})), \pi, \sigma_S$ imzasını oluşturur ve PC'ye gönderir. C uzayından $SMS = \breve{r}_1,\ldots,\breve{r}_k$ makbuzunu üretir ve seçmene SMS yoluyla gönderir.
3) **Doğrulama:** Seçmen öncelikle $\sigma_{MÜ}$ değerini doğrular. $k \stackrel{?}{=} \breve{k}$ eşitliğini kontrol eder, eşit değilse oylama esnasında bir problem olduğu kabul edilir. SMS yoluyla gönderilen $(v_1, \breve{r}_1),\ldots,(v_k, \breve{r}_k)$ makbuzu ile posta yoluyla gelen $\{(v, d(f(v))^{s_i})\}$ makbuzunu karşılaştırır. Eğer farklı ise seçmenin oyu kötü amaçlı yazılım tarafından değiştirilmiş veya iletim esnasında bozulmuş olabilir.

F. Oy sayma protokolü

1) **Gözetmen listeyi alır:** i-Seçmen listesi Li şu şekilde oluşturulur: En yüksek $sayaç$ değeri seçilir, $S, (x_i, w_i)_{i=1}^{k_{max}}, \pi, \sigma_S$. $(x, w) \leftarrow \prod_{i=1}^{k_{max}} (x_i, w_i)$. Daha sonra $L \leftarrow L+$ ekle(x, w). Bütün i-seçmen listesi gözetmene gönderilir.
2) **Şifre çözülür ve oylar sayılır:** Gözetmen listenin doğruluğunu onaylar. $|L| = n$ olsun. D, $\forall i \in \{1,\ldots,n\}$ ve $s_i \in_R \mathbb{Z}_q$ değerleri için $(x_i', w_i') \leftarrow (x_{\prod(i)} g^{s_i}, w_{\prod(i)} y_1^{s_i})$ hesaplar. Sonrasında $\mu_i \leftarrow w_i'(x_i')^{-a_1}$ hesaplar. $\pi_i \leftarrow$ SBP sıfır bilgi protokolunu kontrol eder ve şifre çözülür. En sonunda da $\forall i = 1,\ldots,n$ değerleri için $\pi' \leftarrow$ SBP Karıştırıcı işlemi yapılarak oylar karıştırılır. D, yapılan işlemleri gözetmene ispatlar. Oylar ϕ kod çözme fonksiyonu olmak üzere $\phi(\mu_1),\ldots,\phi(\mu_n)$ şeklinde ortaya çıkar.

IV. Norveç Seçim Protokolünün Bütünlüğü

Bir protokolün bütün olup olmadığının kontrolü dürüst modelde incelenir [18], yani bütün katılımcıların dürüst olduğu durumda protokolün doğru işlemi yaptığı kontrol edilir. Bu seçim protokolünde her dürüst katılımcı için şifreli oy doğru bir şekilde açılır. Seçmenin doğruladığı makbuz kodu hariç protokolün diğer kısımları bütündür. Seçmene gönderilen $(v_i, \breve{r}_i)$ (öyle ki, $\breve{r}_i = d(r_i)$) makbuz kodunun aynı olmasını gösterelim:



Şekil 2. Oy kullanma protokolü.

$$\begin{aligned} r_i &= \breve{w}_i \breve{x}_i^{-a_3} \\ &= w_i^{s_i} \breve{x}_i^{a_2 s_i} \breve{x}_i^{-a_3 s_i} \\ &= w_i^{s_i} \breve{x}_i^{(a_2 - a_3) s_i} \\ &= w_i^{s_i} x_i^{-a_1 s_i} \\ &= (w_i x_i^{-a_1})^{s_i} \\ &= (f(v))^{s_i} \end{aligned}$$

Böylece, eşik sır paylaşımı kriptografik yapıtaşı özelliğinden dolayı a_1, a_2 ve a_3 özel anahtarları kullanılarak $r_i = (f(v))^{s_i}$ değerinin sağlandığını ve bu sayede makbuz üretimi sürecinde gönderilen doğrulama kodlarının $\{v, r_i(v) | v \in O\}$ doğruluğunu göstermiş olduk.

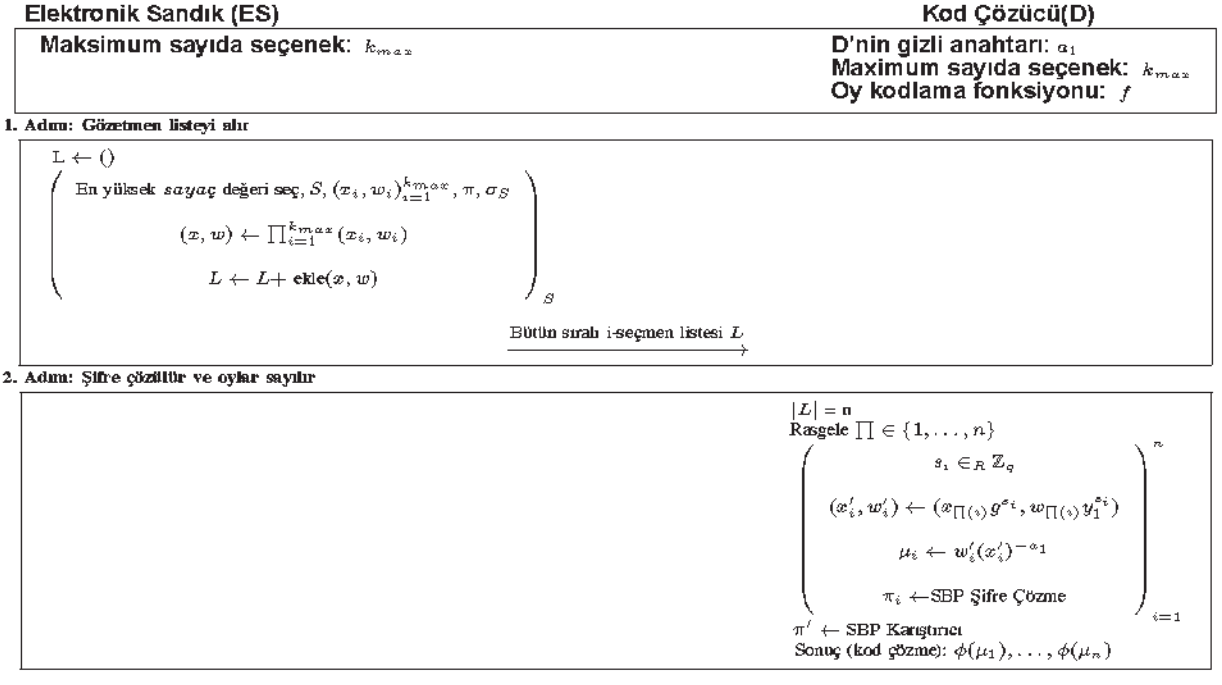
V. Norveç I-Seçim Protokolü Güvenlik Analizi

Bu bölümde Norveç e-seçim sistemine yönelik özgün bir güvenlik analizi verilecektir. Mahremiyet ile ilgili baz potansiyel problemler için [19]'ye bakınız.

A. SMS saldırıları ve güvenlik problemleri

Estonya sisteminde mobil kimlik doğrulama için bir prosedür vardır fakat Norveç sisteminde SMS saldırıları, ayrı olarak ele alınmayı gerektiren ciddi bir açıklık kaynağı olarak göze çarpmaktadır. SMS göndermek için kullanıcı etkileşimi gerekli olmadığından bu tür saldırıları engellemek çok kolay görünmemektedir. SMS saldırılarından bazıları aşağıda listelenmiştir:

- SMS servis sağlayıcısının güvenlik duvarının olmaması
- SMS mesajlarını filtreleyen bir mekanizmanın eklenmemiş olması
- Bir mesajın orijinal biçiminde hedef telefona ulaşıp ulaşmadığının belirsiz olması (Standart SMS, kriptografik bütünlük korumadan yoksundur.)
- Cep telefonu operatörlerinin gönderilecek mesajları engellemesi



Şekil 3. Oy sayma protokolü.

- SMS servisinin güvenilir bir hizmet olmaması, (Mesajlar gecikebilir ya da hiç ulaşmayabilir.)
- Hizmet engelleme (DoS) saldırıları
- Telefona özgü SMS sorunları (Örneğin bazı telefonlara gelen özel formatlı mesajlar telefonun SMS servis hizmetini bozabilir ve telefonu hizmet dışı bıraktırılabilir [20]).
- Yeni nesil akıllı telefonların SMS virüslerine karşı daha savunmasız olması [20]'da Nokia, iPhone ve Android platformları için çok sayıda yeni SMS virüsleri rapor edilmiştir.
- Truva Atı benzeri programlar sayesinde cep telefonlarından istenmeyen e-posta/mesajlar gönderilmesi.
- Kötü niyetli kişiler cep telefon numaralarını bir veritabanına kaydedebilir ve seçim zamanı mesaj bu telefonlara gereksiz mesaj yağdırabilir.

VI. Estonya ve Norveç İ-seçim sistemlerinin karşılaştırılması

Norveç e-Seçim sisteminin Estonya sistemine göre daha güvenli olduğu düşülmektedir. Norveç sisteminde, kötü niyetli seçmen bilgisayarlarına karşı önlemler geliştirilmiştir ve gözetim sistemi daha iyi organize edilmiştir.

- Seçmenin oyundan emin olması: Estonya sisteminde seçmen sadece oyunun "Oy Depolama Sunucusu"'da depolanmış olup olmadığını bilir. Diğer yandan, Norveç sisteminde seçmen oyunun kime verildiğini bilir.
- Seçmen bilgisayarına ynelik tehditler: Estonya sisteminde savunmasız seçmen bilgisayarına karşı seçmen oyunu korumak için bir mekanizma geliştirilmemiştir. Norveç sisteminde bulunan iki farklı kanal mekanizması seçmen bilgisayarına yönelik saldırılara karşı kullanılır. Hatta bilgisayar, seçmen oyunu bozmaya kalkışsa dahi seçmen gelen makbuz sayesinde oyunun değiştirildiğini anlayabilir.
- Verilen oy işlemleri için karıştırıcı ağlar yöntemi kullanma [1]: Daha verimli ve sağlam olması için Norveç sisteminde karıştırıcı ağlar kullanılmaktadır.
- Mobil kimlik doğrulama sistemi: Norveç sisteminde mobil kimlik doğrulama uygulaması yoktur. Ancak, Estonya sisteminde seçmen mobil kimliği ile kayıt olabilir.
- Matbaa: Seçim öncesi ve sonrası olan iletişimlerde, seçim öncesinde her bir seçmenin adresine yazılı bir kod gönderileceğini belirtmiştir. Seçim otoritesi her vatandaşa bu kodu göndermek zorundadır. Bu yüzden baskı hacmi büyük olacaktır. Matbaalarda çalışanları bu kodları çalabilir ve seçmen mahremiyetini ihlal edebilir. Kötü niyetli kişiler, matbaanın bilgisayar altyapısını hack'leyerek kodları ele geçirebilir.

Bilinen bazı potansiyel açıklıklara rağmen, ne Estonya'da yapılan birçok seçimde ne de Norveç 2011 seçimlerinde i-Seçim ile ilgili herhangi bir güvenlik ihlali vakası ihbar edilmemiştir.

VII. E-SEÇIM SISTEMLERİNİN AÇIK KAYNAK KODLU OLMASININ ÖNEMİ

Seçmenlerin seçim sistemine olan güvenlerini arttırmak için kullanılabilecek bir yöntem, sistemin tüm detaylarını ve kaynak kodlarını yayınlamaktır. Norveç bu yolu tercih etmiştir. Diğer yandan, seçim sisteminin detaylarının açıklanmasının getireceği avantaj ve dezavantajların çok iyi incelenmesi gerekmektedir.

Açık kaynak kodlu sistemlerin detaylarını bir çok kişinin incelediği ve açıklıkların uzmanlar tarafından tespit edilerek sistemin iyileştirilebileceği ve nihai sistemin çok az açık içereceği, bu nedenle seçmenlerin sisteme daha çok güven duyacağı düşünülür.

Sistemin açık kaynak kodlu olmasının en büyük dezavantajı, kötü niyetli kişilerin ve bilgisayar korsanlarının da sistemin detaylarına ve kaynak kodlarına erişebilecek olmasıdır. Bu kişiler buldukları zayıflıkları topluma açıklamayıp saldırı yapabilme amacıyla kullanmak isteyeceklerdir.

Açık kaynak kodlu olmayan sistemlerde bile istemci (seçmen) tarafında çalışan yazılımlar saldırganlar tarafından kaynak koda dönüştürülebilir. Kaynak kodun derlenmeden önce perdelenmesi (obfuscation) bu işi sadece biraz zorlaştıracaktır. e-Seçim sürecinin uzun olduğu düşünüldüğünde (Norveç'te bu süreç üç ay sürmektedir) perdeleme işleminin getireceği yarar tartışılabilir. Dolayısıyla, sistemin açık kaynak kodlu olması daha çok sunucu güvenliğini ilgilendirmektedir. Sistemin açık kaynak kodlu olması sonucunda saldırganlar sunucu tarafındaki detaylara ve kodlara da sahip olacaklardır [21].

Bir sonraki bölümde internet tabanlı sistemler için yapılan tehdit analizlerini incelemeye çalışacağız.

VIII. İ-SEÇİM TEHDİT ANALİZİ

Tehdit analizinde saldırganın e-Seçim sistemine gizlilik, bütünlük, erişim denetimi ve kullanılabilirlik yönlerinden yapabileceği saldırılar incelenecektir [20], [22]. Bu saldırıların yapılabilmesi için saldırganın sahip olması gereken bilgi düzeyi ve kaynak miktarı da dikkate alınmalıdır. Bu tehditlerin önlenmesi için alınabilecek önlemler konusunda fikir verilmeye çalışılacaktır. Farklı uzmanlar i-Seçim'in başlangıçta %5'lik kısmında uygulanmasını veya öncelikle yurtdışındaki seçmenlerin kullanabilmesini tavsiye etmişlerdir. Bu yolla zorlama gibi engellenmesi güç problemlerin çözülmesinden önce, kullanılabirlik analizi, ölçeklenebilirlik gibi konularda sahadan geribesleme alınabilir.

Tehdit analizi tablolarındaki sütunlar hakkında kısa bilgi aşağıda verilmiştir.

1) Tehdit: Güvenliği etkileyebilecek olay ve durumlardır. Seçim sistemine yapılabilecek bazı saldırılar basit tekniklerle çok nitelikli olmayan saldırganlar tarafından gerçekleştirilebilirken, bazılarını yapmak için bilgi birikimi, kaynak gereksinimi veya seçim sistemindeki cihazlara erişim gerekebilecektir. Kaynak gereksinimi içerden ve dışarıdan olmak üzere iki sınıfa ayrılır. İçeriden olan kaynaklar, seçim sistemindeki cihazlara veya iç ağa belirli seviyede erişimi olan kişi veya gruplardır. İnternet tabanlı seçim için tehdit kaynağı aşağıda verilmiştir:
   - Sistem içi tehdit kaynakları: i. Seçmen: Seçim sistemine sınırlı erişim imkanları vardır. Her bir seçmen, kayıt olmak, oy vermek ve seçim sonrası doğrulama amaçları için seçim sistemi ile etkileşim içinde olacaktır. ii. Seçim Görevlisi: Seçim sistemine ve verilerine kullanıcı düzeyinde erişim imkanları vardır. Fakat sistem operatörleri gibi yönetimsel hakları yoktur. iii. Sistem Yöneticisi: Seçim sisteminde yönetimsel düzeyde erişim imkanları vardır ve sistemin düzgün işlemesinden ve hata durumunda müdahale edilmesinden sorumlulardır. iv. Diğerleri: 1. Seçim sisteminin üreticileri, geliştiricileri 2. Sistemin entegrasyonunu yapanlar 3. Destek/Bakım elemanları 4. Doğrulama kodlarının üretildiği yerler(matbaa veya cep telefonu operatörleri)
   - Sistem dışı tehdit kaynakları: i. Kötü niyetli kişiler: Seçim sisteminin zayıf yönlerinden yararlanmak isteyen kişilerdir. ii. Kötü niyetli gruplar: Bu saldırılar hacking, organize suç veya terör faaliyeti için biraraya gelmiş olabilir. Kötü niyetli kişilerden iş gücü ve teknik kaynak miktarı açısından daha güçlülerdir.
2) Tehdit Sonucu: Saldırının sisteme, yapılan seçime ve/veya seçmenlere vereceği zararlar.
3) Tehdit Seviyesi: Tehdidin gerçekleşmesi durumunda oluşacak etkinin büyüklüğü.
4) Alınabilecek Güvenlik Önlemleri: Saldırıları önleme ya da etkisini azaltmak için alınabilecek önlemler.

A. Kriptografik yönüyle tehdit analizi

Bu bölümde kriptografik hizmetler açısından genel bir tehdit analizi yapılacaktır, detaylar için Şekil 4 bakınız.

B. e-Seçim'in bilgisayar ve ağ güvenliği yönüyle olası tehdit analizi

Bu bölümde yer alan tehditler, genellikle seçmen tarafına (verilen oya ya da mahremiyete) yönelik ciddi tehditlerdir, detaylar için Şekil 5 bakınız..

C. İletişim kanalları yönüyle olası tehdit analizi

Bu bölümde, alternatif kanalların güvenlik sorunundan kaynaklanan tehditler de yer almaktadır, detaylar için Şekil 6 bakınız.

Kriptografik yönüyle tehdit analizi				
	Tehdit	Tehdit Sonucu	Tehdit Seviyesi	Alınabilecek Güvenlik Önlemi
1	Erişim Denetimi, Kimlik ve Kaynak Doğruluğunun Düzgün Yapılmaması	Kayıtlı olmayan kişilerin oy vermesi, Kayıtlı seçmenlerin yerine oy verme, Oyların değiştirilmesi, Birden fazla oy verme	Yüksek	Parola tabanlı erişim denetimi, Sayısal imza, Güçlü kriptografik kimlik doğrulama yöntemleri
2	Seçmenlerin kime oy verdiğinin ortaya çıkması	Oy gizliliğinin ihlali, Oyların değiştirilmesi, Ara sonuçların öğrenilmesi, Zorlama	Yüksek	Ağ katmanında Şifreleme, Uygulama katmanında Şifreleme (uçtan uca şifreleme)
3	Oyların Bütünlüğünün Sağlanması	Oyların değiştirilmesi	Yüksek	Mesaj Doğulama Kodu Kullanımı, Sayısal İmza
4	İmzalı ve Şifreli Oyların Ele Geçmesi	Anahtar uzunluklarına bağlı olarak oy gizliliğinin ihlali, Saldırganın seçim sonrasında (örn, yıllar boyu kriptanalizle) belirli seçmenlerin kime oy verdiğini ortaya çıkarması	Orta	Anahtarların yeterince uzun olması veya anahtar uzunluğundan bağımsız olarak güvenlik sağlanması [1], Anahtarların korunması, Sistemdeki şifreli verilere eşik sır paylaşımı ile erişilmesi
5	Seçim Sisteminin Özel Anahtarının Korunamaması	Oy gizliliğinin ihlali, Ara sonuçların öğrenilmesi, Zorlama, Servis Dışı Bırakma	Yüksek	Basit Erişim Denetimi, Sır Paylaşımı
6	İmzasız ve Şifreli Oyların Ele Geçmesi	Anahtar ortaya çıkmadığı takdirde tehdit oluşturmamaktadır	Düşük	-
7	Oyların Anonimliğinin Sağlanamaması	Oy gizliliğinin ihlali, Zorlama, Ara sonuçların öğrenilmesi	Yüksek	Şifreleme/ Deşifreleme, Karıştırıcı Ağlar, Homomorfik Sayım
8	Denetlemenin Güvenilir Olmaması	Oy gizliliğinin ihlali, Oyların değiştirilmesi, Zorlama, Birden fazla oy verme	Yüksek	Standart Kayıt (Log), Değiştirilemez, Kayıt (immutable log), Standart Makbuz, Bireysel Doğrulanabilirlik, (seçmenin niyeti oya doğru şekilde yansıdı), Bireysel Doğrulanabilirlik, (oylar doğru sayıldı), Evrensel Doğrulanabilirlik

Şekil 4. Kriptografik yönüyle tehdit analizi

D. Sunucu güvenliği

i-Seçim sistemlerinde Oy Sayım Sunucusu, Oy Yönlendirme Sunucusu, Oy Depolama Sunucusu ve benzeri sunucular bulunmaktadır. Bu sunucuların güvenliği genel anlamda bu başlık altında incelenecektir, detaylar için Şekil 7 bakınız.

IX. Sonuç ve Ülkemiz için Ön Değerlendirmeler

Bu yazıda Estonya (internet kanalıyla elektronik seçimi ilk uygulayan ülke) ile Norveç i-seçim sistemlerini inceledik. Bahsi geçen ülkelerdeki göreceli başarıda, pek çok faktörün etkili olduğu görülmektedir. Kullanıcı profili özellikle internet okur-yazarlığı oranı, internet ve cep telefonu erişim ağının yaygınlığı, seçim sistemine duyulan güven bu etmenlerin başlıcalarıdır. Elektronik seçim sistemi hakkında topluma genel bilgiler sağlamak ve güvenilir bir otoritenin bu sistemi resmi olarak nitelikli hale getirmesi toplumda güven duyulmasını artıracaktır. e-Seçim projesinin analiz edilebilirliği çok önemlidir, Avusturya e-seçim projesinin rafa kaldırılması buna güzel bir karşı örnektir.

Diğer yandan, i-Seçim'in seçmen demokratik katılımına ne kadar tesir ettiği tartışılır. Örneğin i-seçmen oranı artsa da, Estonya seçimlerinde hissedilir bir seçmen artışı olmamıştır. Diğer yandan özellikle genç seçmenlerde oy verme şekli değişmektedir. Ülkemizde, özellikle e-kimlik kartının yaygınlaştırılmaya başladığı şu günlerde, demografik yapının genç ağırlıklı olduğu da göz önüne alınırsa, muhtemel bir e-seçim uygulamasında i-seçmen oranı azımsanmayacak oranda çıkabilir. Üstelik Türkiye'de elektronik okur-yazarlık konusunda potansiyel olarak büyük gelişmelerin devam edeceği öngörülmektedir. (Okullara tablet PC

e-Seçim'in bilgisayar ve ağ güvenliği yönüyle olası tehdit analizi				
	Tehdit	Tehdit Sonucu	Tehdit Seviyesi	Alınabilecek Güvenlik Önlemi
1	Seçmen bilgisayarındaki kötü amaçlı kodların (örneğin, Truva atı) seçmenin oyunu öğrenmesi, silmesi değiştirmesi veya seçmen yerine oy vermesi	Oy gizliliğinin ihlali, Oyların değiştirilmesi, Seçmenin haberi dışında oy kullanma, Oy verememe, Sunucuya saldırı amaçlı kullanım	Yüksek	Seçmen bilgisayarından tehdit gelmeyeceğinin garanti edilmesi farklı ve bağımsız iletişim kanallar kullanılması (örn., posta, SMS), Virüs, Truva atı, Casus yazılımlara karşı kullanılan programlarını güncel olması; Seçmenin bilgisayar başında bulunduğunun kanıtlanması (Kart, Parola, PIN, Parmak izi kullanımı vb.)
2	Seçmenin başka siteye yönlendirilmesi	Oy gizliliğinin ihlali , Oyların değiştirilmesi, Oy verememe	Yüksek	Virüs, Truva atı, Casus yazılımlar, vs. güncel olmalıdır.Seçmenler yapılabilecek saldırılar konusunda bilgilendirilmelidir.
3	Zorlama	Oyların değiştirilmesi	Yüksek	Seçmenlerin seçim sonuna kadar oylarını değiştirmesine müsaade edilebilir. Seçmen fiziksel olarak oy sandığına ulaşamayacağı bir noktadan i-Seçim bitmesine yakın kullandığında cebine mesaj gelir. Mesaj geldiğinde ne zaman oy kullandığı bilinecektir. Seçim sonrası tekrar oy kullanamayacağına ve fiziksel olarak da oy sandığına gidemeyeceğine göre oy satışı veya zorlama gerçeklenebilir.
4	Aile bireyleri evinden oy kullanırken baskı altında kalabilirler (Bu probleme literatürde Aile Oylaması denilir).	Seçmenlerin kendi inisiyatifleri doğrultusunda oy kullanamaması	Yüksek	Aile oylamasını uzaktan seçim uygulandığı müddetçe engellemek pek mümkün değildir.
5	Oy Satma	Seçim sonucunun değiştirilmesi	Yüksek	Seçmenlerin seçim sonuna kadar oylarını değiştirmesine müsaade edilebilir.
6	Seçmen doğru olduğu halde bazı işlemlerin yanlış gerçekleştiğini iddia edebilir (örn. SMS kontrolü)	Seçime olan güvenin azalması	Düşük (kişisel olursa), Orta (büyük grup olursa)	Bunu iddia eden kişilerin klasik seçime yönlendirilmesi, Kötü niyetli bir seçmen kasten telefonuna yanlış kod gönderildiğini iddia ederse, onun yanlış veya yalan söylediğini doğrulayan anlık bir mekanizma yoktur. Bir grup insan bu senaryoyu kasıtlı olarak uygularsa bu durum vatandaşlar arasında güvensizlik oluşturabilecektir. Bu teknik bir saldırı değildir fakat vatandaşlar arasında yanlış kanı doğurabileceğinden önemlidir.

Şekil 5. e-Seçim'in bilgisayar ve ağ güvenliği yönüyle olası tehdit analizi

dağıtılması, cep operatörlerinin akıllı telefon kampanyaları vb.) Ülkemizde engellilerin seçim sandığına ulaşma imkanları da bahsi geçen ülkelere kıyasla yeterli olduğu söylenemez. i-Seçimin engelli vatandaşların seçime katılıma katkısı farklı olacaktır. Bu ve benzer nedenlerle, yakın ya da orta vadede, ülkemizde e-Seçim'in gerekliliği tartışılmaya başlanacaktır. Çeşitli e-Seçim teknikleri şimdiden bazı bilim kurumlarında teorik olarak araştırılmaya başlanmıştır. Ne var ki, e-Seçim uygulamasına geçilmeden önce detaylı bir fayda-maliyet analizi yapılmalı ve öngörü ve kestirimler yapabilmek adına bazı temel sorular hakkında bilgi toplanması gereklidir.

- Mevcut sistemin olası sorunları ve riskleri
- Kullanılacak yeni teknolojinin faydaları
- e-Seçim teknolojisinden beklenen hedefler
- Kullanılacak e-Seçim sisteminin belirlenmesi: i-Seçim, elektronik oy kayıt sistemleri (örneğin DRE), görsel e-Seçim sistemleri (örneğin "Prêt à Voter") ya da ülkemize has özgün tasarım kullanılabilir.
- Yeni teknoloji kullanımı ile beraber olası yeni problemler ve yeni riskler
- Kullanılacak yeni teknoloji ve seçim sürecinin

İletişim kanalları yönüyle olası tehdit analizi				
	Tehdit	Tehdit Sonucu	Tehdit Seviyesi	Alınabilecek Güvenlik Önlemi
1	İnternet ortamının güvensizliği nedeniyle seçmen bilgisayarı ve sunucu arasındaki iletişimin içeriğinin öğrenilmesi, değiştirilmesi, engellenmesi	Oy kullanılamaması, Oy gizliliğinin ihlali, Oyların değiştirilmesi, Seçimin sonucunun değiştirilmesi	Yüksek	Bknz. Bölüm 6.1 Kriptogafik yönüyle tehdit analizi, Bknz. 6.2 Bilgisayar ve ağ güvenliği yönleriyle tehdit analizi
2	Posta sisteminin zaafiyetlerinden dolayı postanın seçmenin eline geçmemesi (postanın dağıtılmaması, başkası tarafından kasıtlı olarak alınması) veya seçmenden habersiz içeriğinin öğrenilmesi	Seçmen güvenli ve güvenilir bir şekilde oy verdiğini doğrulayamaz	Düşük	Posta yanlışlıklarına sık rastlanılması seçmenler arasında huzursuzluk doğurabilir. Bunun yanında sistemin doğru çalışıp çalışmadığının anlaşılması için bütün seçmenlerin bu doğrulamayı yapmasına gerek yoktur. Belirli oranda seçmenin bu doğrulamayı yapması yeterlidir.
3	Kötü niyetli kişiler cep telefonu altyapısına veya bireysel cep telefonuna saldırı yaparak servis vermesini/almasını engelleyebilir. (Servis dışı bırakma, SMS virüsleri, SMS enjeksiyon gibi farklı saldırı türleri olabilmektedir.)	Seçmen güvenli ve güvenilir bir şekilde oy verdiğini doğrulayamaz	Orta	Bu tür saldırılar seçmenin farkına varabileceği türlerdendir. Seçmen herhangi bir saldırı altında kaldığını hissederse tereddüt etmeden klasik seçimde oyunu kullanabilir.

Şekil 6. İletişim kanalları yönüyle olası tehdit analizi

demokrasi bilinci ve kurumların şeffaflığına etkileri
- Yeni teknoloji ile ilgili donanım, yazılım ve altyapı için gerekli iletişim, ulaşım, personel, danışmanlar, bakım ve güncellemeler ilgili tüm masraf kestirimleri
- Yeni teknolojinin uygulanması için detaylı bir zaman çizelgesi
- Kullanılacak sisteme bağlı olarak gerekli hukuki altyapının hazır olması adına gerekli düzenlemeler
- Uygulanan yeni teknoloji başarısız olursa ilgili maliyet tahmini
- Sistemi işletenlerin ve seçmenlerin sistem çalışması hakkında eğitim ve bilgilendirilmesi için gerekli planlamanın yapılması

Yukarıda saydığımız genel hususların yanı sıra, e-Seçim sistemi tasarlarken e-güvenlik açısından yapılacak çalışmaların aşağıdaki ilkeler çerçevesinde olması beklenir:
- Sistemin güvenlik gerekleri kesin olarak belirlenmelidir [2].
- Biçimsel (formel)analiz ve sistemin güvenilirliğinin ispatı uzman ulusal ve uluslararası yetkililer veya danışmanlar tarafından yapılmalıdır.
- Tehditler yapılandırılmalıdır ve sınıflandırılmadır.
- Tehdit önleme stratejileri geliştirilmelidir.
- Muhtemel hata işleme, yönetme ve kurtarma senaryoları çıkarılmalıdır.
- Sosyo-teknik sistem analizi geliştirilmelidir.
- Küçük ölçekli prototip seçimlerle (birçok ülkede saygın bir üniversitenin bilgisayar bölümü ilk pilot bölge seçilir) ara tasarımlar denenmeli, geri beslemeler ışığında olası güvenlik açıkları kapatıacak ve kullanıcı kolaylığını artırıcak değişikliklerle sistem geliştirilmelidir.

Elektronik seçimin birçok avantajının olmasına rağmen hala problemlerinin olduğu görülmektedir. Ancak zaman içerisinde edinilen bilgi birikimi ve tecrübe ile beraber bu problemler azaltılabilmiştir. Estonya'da 2005, 2007 ve 2009 yılında başarılı uygulaması Norveç hükümeti için bir ilham kaynağı olmuş bu başarıyı kendi ülkelerinde de uygulamak istemişlerdir. ABD yurtdışındaki vatandaşlarının oy kullanabilmesi için bir çalışma yürütmektedir [23]. İngiltere, ABD, Belçika, Estonya ve Norveç başta olmak üzere gelişmiş ülkeler

e-Seçim'in sunucu güvenliği yönüyle olası tehdit analizi				
	Tehdit	Tehdit Sonucu	Tehdit Seviyesi	Alınabilecek Güvenlik Önlemi
1	Kullanılmış oy pusulalarının bazı kısımlarına yetkili personel tarafından erişilmesi (okuma, silme veya değiştirme).	Oy gizliliğinin ihlali, Oyların değiştirilmesi, Seçimin sonucunun değiştirilmesi	Yüksek	Bknz. Resim-18, Bölüm 6.1 e-Seçim'in kriptografik yönüyle olası tehdit analizi (Örneğin, Kimlik Doğrulama, Oyların Bütünlüğünün Sağlanması Deşifrelemede Oyların Anonimletirilmesi)
2	Kullanılmış oy pusulalarının bazı kısımlarına yetkisiz personel tarafından eriilir (okuma, silme veya değitirme).	Oy gizliliğinin ihlali, Oyların değitirilmesi, Seçimin sonucunun değitirilmesi	Düşük	Eriim denetiminde ve kimlik doğrulamada güçlü kriptografik yapılar kullanılması (Bknz. Tablo-18, Bölüm 6.1 Kriptogafik Yönden Tehdit Analizi)
3	Yetkisiz personelin sunuculara uzaktan erierek kullanılmış oy pusulalarını okuması, silmesi veya değitirmesi.	Oy gizliliğinin ihlali, Oyların değitirilmesi, Seçimin sonucunun değitirilmesi	Düşük	Sunuculara uzaktan eriimin zorunlu olduğu durumlarda güçlü eriim denetim ve kimlik doğrulama mekanizmalarının kullanımı
4	Sunuculardaki kötü amaçlı kodların (örneğin, Truva atı, Casus Yazılım) seçmenin oyunu öğrenmesi, silmesi veya değitirmesi	Oy gizliliğinin ihlali, Oyların değitirilmesi, Seçimin sonucunun değitirilmesi	Orta	Virüs, Truva Atı, casus yazılımlar, vs. programları güvenilir ve güncel olmalıdır.
5	Sunucu yazılımındaki hatalar nedeniyle seçmen oylarının yanlış kaydedilmesi	Seçim sonucunun seçmenlerin niyetini yansıtmaması	Orta	Yazılımın geliştirilmesinde endüstri standartlarına uyum, Sistemin ve yazılımı sertifikasyonun yapılması, Kaynak kodların açıklanması
6	Seçmenlerin yanlış bir sunucuya yönlendirilmesi (Örneğin, Phishing yoluyla)	Oy gizliliğinin ihlali, Oyların değiştirilmesi, Oy verememe	Yüksek	Seçmenlerin saldırı yöntemleri konusunda bilgilendirilmesi, Kriptografik yöntemlerle sunucunun taklit edilmesinin önüne geçilmesi.
7	DNS sistemine yapılan bir saldırı sonucunda seçmenlerin yanlış sunucuya yönlendirilmesi	Oy gizliliğinin ihlali, Seçmenlerin oy kullanamaması, Oyların değiştirilmesi	Düşük	DNS güvenlik önlemleri alınmalıdır. Kriptografik yöntemlerle sunucunun taklit edilmesinin önüne geçilmesi. Siber saldırılar için acil müdahale ekibinin bulundurulması
8	Sunuculara yönelik servis dışı bırakma saldırısında bulunulması	İ-seçimde oy kullanmanın engellenmesi, İ-seçimin sabote edilmesi	Orta	Birden Fazla Seçim Kanalı, Kiosk (DRE) kullanımı, Siber saldırılar için acil müdahale ekibinin bulundurulması
9	Sunucuların normal seçim trafiğini kaldırabilecek altyapıda olmaması	Seçmenlerin i-Seçim'de oy kullanılamaması	Düşük	Planlamanın iyi yapılması, Sistemin sertifikasyonunun yapılması
10	Doğal afetler veya acil durumlar	Seçmenlerin i-Seçim'de oy kullanılamaması	Düşük	Seçimin tekrarlanması veya Seçmenlerin klasik seçime yönlendirilmesi

11	Başarısızlıklar veya istemci uygulamasının kalitesi sorunları	Seçmenlerin oy kullanamaması	Orta	Tekrar oy kullanabilme imkanı verilmesi
12	Oy Yönlendirme Sunucusuna servis dışı bırakma saldırısı da düzenlenebilir.	Seçmenlerin oy kullanamaması	Orta	Sunucuların yedeklemesi, Siber saldırılar için acil müdahale ekibinin bulundurulması.
13	Açık Anahtar Altyapısı ile Oy Depolama Sunucusu arasında da bir saldırı gerçekleşebilir.	Seçmenlerin oy kullanamaması	Orta	Sunucuların yedeklemesi, Siber saldırılar için acil müdahale ekibinin bulundurulması
14	Oy Yönlendirme Sunucusu ve Oy Sayım Sunucusu aynı anda saldırı altında olması	Oy gizliliğinin ihlali	Orta	Her ne durumda olursa olsun Oy Yönlendirme Sunucusu ve Oy Sayım Sunucusu birlikte işbirliği yapamayacağının prosedürel yöntemlerle garanti altına alınması gerekmektedir. Bu sunucular bağımsız merkezlerin sorumluluğun altında olması gerekmektedir.
15	Oy Sayım Sunucusuna içeriden gelen saldırılar (dışarıya bağlantısı olmadığından dışarıdan saldırı beklenmemektedir)	Oyların değiştirilmesi, Seçimin sonucunun değiştirilmesi	Düşük	Oy Sayım Sunucusu diğer sunuculara nispeten en güvenli sistemdir, çünkü hatta bağlı değildir. Bu yüzden sadece içeriden tehdit gelebilir. Bunların engellenmesi için de Eşik Sır Paylaşımı kriptografik yöntemleri kullanılabilir. Ayrıca bu işlemler gözetmenler tarafından yapılmalıdır. Bireysel ve evrensel doğrulanabilir yöntemleriyle ve sunucuda kötü niyetli kod olmadığı anlaşılabilir.

Şekil 7. e-Seçim'in sunucu güvenliği yöntiyle olası tehdit analizi

elektronik seçim uygulamadan önce geniş yelpazeli konsorsiyumlar oluşturmuştur. [24], [25], [26], [15] Ülkemizde de geniş çaplı bir konsorsiyum e-seçimin teknik özelliklerinden sosyo-ekonomik etkilerine, yapılması gereken hukuki değişikliklerden maliyet analizine kadar değişik yönlerden tartışmalı ve geniş anlamda bir rapor hazırlamalıdır. Konsorsiyum bulguları ve bilimsel toplantılar ışığında ülkemiz için bir yol haritası çıkarılmalıdır.

KAYNAKLAR

[1] Fatih Birinci and Mehmet Sabır Kiraz, "Elektronik Seçim: İleri Düzey Kriptografinin Yapı Taşları ve Uygulamaları", Available online at http://www.uekae.tubitak.gov.tr/dergi, BİLGEM Dergisi, Sayı 5, 84–101, 2011.

[2] Mehmet Sabır Kiraz, Fatih Birinci, and Umut Uludağ, "Elektronik Seçim: Yöntemler, Uygulamalar, Kriptoloji Altyapısı ve Ülkemizdeki Geleceği", Available online at http://www.uekae.tubitak.gov.tr/dergi, BİLGEM Dergisi, Sayı 4, 76–87, 2011.

[3] "Electronic Voting and Electronic Counting of Votes- A Status Report", Available at http://www.eca.gov.au/reports/electronic_voting.pdf, 2012.

[4] Sokratis Katsikas Lilian Mitrou, Dimitris Gritzalis and Gerald Quirchmayr, "Electronic Voting: Constitutional and Legal Requirements, and Their Technical Implications. The Role of Trust, Participation and Identity in the Propensity to e- and i-vote", Electronic Voting 2010: 65-78. Advances in Information Security, Volume 7, Part I, 2010.

[5] O. Çetinkaya, "Verifiability and Receipt-freeness in Cryptographic Voting Systems", PhD Thesis, Department of Cryptography, Institute of Applied Mathematics, Middle East Technical University, Ankara, Turkey, 2007.

[6] "Punchscan", Available at http://www.punchscan.org/, 2012.

[7] "Scantegrity", Available at http://scantegrity.org/, 2012.

[8] "Prêt à Voter", Available at http://www.pretavoter.com/, 2012.

[9] Ronald L. Rivest, "The ThreeBallot Voting System", Available at http://people.csail.mit.edu/rivest/Rivest-TheThreeBallotVotingSystem.pdf, 2012.

[10] Act, "Uniformed and Overseas Citizens Absentee Voting", Available at http://www.fvap.gov/reference/laws/uocava.html, 2012.

[11] Indrajit Basu, "Estonia Becomes E-stonia", Available at http://www.govtech.com/e-government/Estonia-Becomes-E-stonia.html, 2008.

[12] "Statistics about Internet Voting in Estonia", Available at http://www.vvk.ee/voting-methods-in-estonia/engindex/statistics/, 2008.

[13] "E-Voting Pilot in Austria Cancelled by Constitutional Court", Available at http://www.wu.ac.at/evoting/en/news, 2012.

[14] "E-Vote 2011- Pilot Project in Norway", Available at http://www.regjeringen.no/en/dep/krd/prosjekter/e-vote-2011-project.html?id=597658, 2012.

[15] Ministry of Local Government and Regional Development, "The report: Electronic voting - challenges and opportunities", Available at http://www.regjeringen.no/en/dep/krd/prosjekter/e-valg-2011-prosjektet/omprosjektet/Forprosjektrapport-2006.html?id=604417, 2006.

[16] Uğur Kaşif Boyacı, "Günümüzde Kriptoloji", Available online at www.uekae.tubitak.gov.tr/dergi, BİLGEM Dergisi, Sayı 1, 34–43, 2009.

[17] Mehmet Sabir Kiraz, Süleyman Kardas, Muhammed Ali Bingöl, and Fatih Birinci, "An improved internet voting protocol", *IACR Cryptology ePrint Archive*, 2011.

[18] Berry Schoenmakers, "Lecture Notes. Part 1 Cryptographic Protocols.", Available online at http://www.win.tue.nl/ berry/2WC13/LectureNotes.pdf, 2012.

[19] Véronique Cortier and Cyrille Wiedling, "A formal analysis of the Norwegian e-voting protocol", in *Proceedings of the 1st International Conference on Principles of Security and Trust*

(POST'12). Mar. 2012, Lecture Notes in Computer Science, Springer, To appear.

[20] Collin Mulliner and Charlie Miller, "Injecting SMS messages into smart phones for security analysis", WOOT'09 Proceedings of the 3rd USENIX conference on Offensive Technologies. USENIX Association, Berkeley, USA, 2009.

[21] Arne Ansper, Sven Heiberg, Helger Lipmaa, Tom André Øverland, and Filip van Laenen, "Security and Trust for the Norwegian E-voting Pilot Project E-valg 2011", vol. 5838, pp. 207–222, Springer-Verlag.

[22] "A Threat Analysis on UOCAVA Voting Systems", Available at http://www.nist.gov/itl/vote/upload/uocava-threatanalysis-final.pdf, 2012.

[23] Act, "Uniformed and Overseas Citizens Absentee Voting", Available at http://www.fvap.gov/reference/laws/uocava.html, 2012.

[24] "Workshop on UOCAVA Voting Systems", Available at http://www.nist.gov/itl/csd/ct/uocava-2010-workshop-agenda.cfm, 2012.

[25] D. Wagner D. Rubin Jefferson, B. A. Simons, "A security analysis of the Secure Electronic Registration and Voting Experiment (SERVE)", Available at http://www.servesecurityreport.org, 2004.

[26] UCL KUL ULg UA et UG) Consortium of Belgian universities (ULB, VUB, "BeVoting study of electronic voting systems Part 1 and 2", Available online at http://www.epractice.eu/en/library/281715, 2008.

Dr. Mehmet Sabır Kiraz Orta Doğu Teknik Üniversitesi Matematik Bölümü'nden (ODTÜ) 2000 yılında mezun oldu. Haziran 2000 - Ekim 2002 yılları arasında Pamukbank ve Yapı Kredi Bankası bilgi işlem bölümlerinde çalıştı. 2003 yılında yüksek lisans derecesini Almanya'da Max-Planck Enstitüsü Bilgisayar Bilimleri Bölümü'nden aldı. Doktorasını 2008 yılında Hollanda'da Eindhoven Teknik Üniversitesi Matematik ve Bilgisayar Bilimleri Bölümü'nden aldı. 2008-2010 yılları arasında Amsterdam'da TOMTOM ve Eindhoven'da PHILIPS Research şirketlerinde çalıştı. 2010 yılından itibaren TÜBİTAK BİLGEM Ulusal Elektronik ve Kriptoloji Araştırma Enstitüsü'nde araştırmacı olarak çalışmaktadır. İlgi alanları Kriptoloji, Kriptografik Protokoller, Mahremiyet, Anahtar Yönetimi, Güvenli Fonksiyonel Hesaplamalar, Elektronik Seçim, RFID.

Fatih Birinci ODTÜ Matematik Bölümü'nden 1995 yılında mezun oldu. 1998 yılında ODTÜ Matematik Bölümü'nden, 2002 yılında Gebze Yüksek Teknoloji Enstitüsü Bilgisayar Mühendisliği Bölümü'nden Yüksek Lisans derecesi aldı. TÜBİTAK BİLGEM Ulusal Elektronik ve Kriptoloji Araştırma Enstitüsü'nde toplam 12 yıldır çalşmaktadır. İlgi alanları Kriptoloji, Kriptografik Protokoller, Dizi Şifreleme, Anahtar Yönetimi, Formal Analiz, Elektronik Seçim.

Uğur Kaşif Boyacı ODTÜ Matematik Eğitim ve Matematik Lisans (Çift Anadal Programı) bölümlerinden 1994 yılında mezun oldu. 2003 yılında Yıldız Teknik Üniversitesi Matematik Mühendisliği'nden Yüksek Lisans derecesi aldı. 1999 yılından itibaren TÜBİTAK BİLGEM Ulusal Elektronik ve Kriptoloji Araştırma Enstitüsü'nde araştırmacı olarak çalışmaktadır. İlgi alanları Kriptoloji, Kriptografik Protokoller, Açık Anahtar Altyapısı, Anahtar Yönetimi, Yapay Sinir Ağları.

Compressed Data Public Key Cryptosystems with DLP Over Extension Fields

M. Ashraf and B. B. Kırlar

***Abstract*—In recent years, Public Key Cryptosystems (PKCs) are converging to gain high security with reduced bandwidth for data transmission. The goal of these PKCs is to face the challenges imposed by availability of faster processors for cryptanalysis and higher data transmission rates. For this purpose new PKCs are proposed which include LUC-PKC, GH-PKC, XTR-PKC and Torus based cryptography. In these systems, the cryptographic operations are carried out in subfield whereas security of extension field is ensured. The discrete logarithm problem in extension field is relatively hard when compared with subfield. In this paper we survey these PKCs by giving the underlying mathematical concepts with key group operations, relevant details of PKC, and then achieved goals in these systems. We also indicate the vulnerability of such systems to SPA attacks, wherever, applicable.**

***Index Terms*—Public Key Cryptosystems, Discrete Logarithm Problem, extension fields, LFSR, characteristic sequence, trace function, Torus Based Cryptography.**

I. Introduction

CRYPTOSYSTEMS based on intractability of discrete logarithm was first time realized by Diffie and Hellman in 1976 [1]. In their work, they showed that two parties $\mathcal{A}$ and $\mathcal{B}$ can communicate securely over an unsecured channel. For example, let $G =< g >$ be a multiplicative of large prime order and $2 < a, b < \#G$, $\mathcal{A}$ computes g^a and $\mathcal{B}$ computes g^b. They exchange these messages over unsecured channel and compute $(g^b)^a$ and $(g^a)^b$ respectively to acquire a common key g^{ab}. In this case the intractability of Discrete Logarithm Problem (DLP) that is the computation of a given g^a depends upon the large group order. On the other hand, if group order is large then number of bits to represent group element is also large. Therefore, larger transmission bandwidth is required which reduces communication efficiency.

Over the last few years, efforts were made to improve efficiency of Public Key Cryptosystems (PKCs) in terms of compact representation and increased security. These improvements resulted in form of LUC-PKC [3], GH-PKC [4], XTR-PKC [7] and Torus based cryptography [12]. In these systems, group operations are carried out in intermediate or prime subfields (i.e; $\mathbb{F}_{p^k}$, $k \mid r$ or $\mathbb{F}_p$) whereas, security of extension field (i.e; $\mathbb{F}_{p^r}$, where $r = 2, 3$ and 6 for LUC-PKC, GH-PKC and XTR-PKC, respectively) is ensured. Hence, high security is achieved with operands of lesser number of bits. In contrast, for Diffie-Hellman PKC both group operations and DLP are in prime field $\mathbb{F}_p$.

Manuscript received March 11, 2012.

Muhammad Ashraf is with the Institute of Applied Mathematics, METU, Ankara, Turkey, e-mail: ashraf6061@gmail.com

Barış Bülent Kırlar is with the Department of Mathematics, Süleyman Demirel University, Isparta, Turkey, e-mail: bariskirlar@sdu.edu.tr

Smith and Lennon introduced PKC based on Lucas functions in [2], which was further refined by Smith and Skinner in [3]. They used a subgroup of order $p + 1 \in \mathbb{F}_{p^2}$ and employed Lucas functions to perform group operation over prime subfield $\mathbb{F}_p$ thus achieving security of $\mathbb{F}_{p^2}$ for cryptographic protocols. Thereby, they compressed the operands by a factor of 2. The GH-PKC was proposed by Gong and Harn in 1999 [4]. They used 3rd order recurrence relation for Linear Feedback Shift Register (LFSR) using characteristic polynomial of degree three. This characteristic polynomial being irreducible cubic over $\mathbb{F}_p$ splits in $\mathbb{F}_{p^3}$ to ensure that roots belong to $\mathbb{F}_{p^3}$ and hence DLP in $\mathbb{F}_{p^3}$. The output sequence of LFSR is computed over $\mathbb{F}_p$ and elements are represented by $\log p$ bits. Hence, a compressed representation with DLP over $\mathbb{F}_{p^3}$. Moreover, GH-PKC employs a subgroup of order p^2+p+1 of $\mathbb{F}^*_{p^3}$ to construct cryptographic protocols. After GH-PKC, Lenstra and Verheul proposed XTR system [7] based on trace computation for cryptographic protocols. They observed that a cubic polynomial of the form;

$$f(x) = x^3 - \mathrm{Tr}(\alpha)x^2 + \mathrm{Tr}(\alpha)^p x - 1 \in \mathbb{F}_{p^2}[x],$$

splits in $\mathbb{F}_{p^6}$, where $\alpha \in \mathbb{F}_{p^6}$ and $\mathrm{Tr}(\alpha) = \alpha+\alpha^{p^2}+\alpha^{p^4} \in \mathbb{F}_{p^2}$. They proved that the elements α of $\mathbb{F}_{p^6}$ with trace in $\mathbb{F}_{p^2}$ forms a subgroup of order $p^2 - p + 1$. They also showed that powers of these elements α^n for $n \in \mathbb{Z}$ also belong to this subgroup. Thus, trace computation is carried out in $\mathbb{F}_{p^2}$ resulting into compression by a factor of 3. Some improvements in XTR were also proposed in [10] and [11] but the underlying concept does not change. We will survey only concepts and main areas for highlighting concepts.

Rubin and Silverberg [12] proposed Torus based Public Key Cryptography in 2003. They observed that cryptographic operation in extension field $\mathbb{F}_{p^n}$ are basically carried out in subgroup of $\mathbb{F}^*_{p^n}$ which is equivalent to scalar restriction $(\mathrm{Res}_{\mathbb{F}_{p^n}/\mathbb{F}_p})$ of the group. This restriction decomposes as a product of algebraic tori $\mathbb{T}_r$ for $r|n$. To enjoy full security of $\mathbb{F}^*_{p^n}$ the torus must be of the form $\mathbb{T}_n(\mathbb{F}_p) \cong G_{p,n} \subseteq \mathbb{F}^*_{p^n}$. $\varphi(n)$ is the dimension of torus over $\mathbb{F}_p$, where φ is Eulers totient function. This implies compression of $n/\varphi(n)$ is achieved. The cryptographic protocols can be carried out by computing compression map $\rho : G_{p,n} \to \mathbb{F}_p^{\varphi(n)}$ and decompression map $\psi : \mathbb{F}_p^{\varphi(n)} \to G_{p,n}$ such that $\rho \circ \psi = 1$.

This paper is organized as follows, in section 2, LUC-PKC and its relevant details are discussed. In section 3, GH-PKC or cubic field systems are presented. In section 4 XTR-PKC and related details are given. In section 5, we discuss the torus based cryptosystem and finally in section 6, we conclude the paper. Being a survey paper, relevant papers and authors are frequently referred.

II. LUC-Public Key Cryptosystem

LUC-PKC is a Public Key Cryptosystem based on the properties of Lucas functions. This system was introduced by Smith and Lennon in 1993 [2] as an alternate PKC to Diffie-Hellman and RSA cryptographic protocols. In this PKC, a second order linear recurrence relation is used to construct Diffie-Hellman key exchange protocol and RSA type cryptosystem. Later on it was further refined by Smith and Skinner [3] in 1994, by presenting cryptosystem and digital signature schemes. We will discuss salient underlying arithmetic operations and their adaptation to Diffie-Hellman's key exchange protocol.

Linear Recurrence of Higher Order [2]. Let $\ell, a_i \in \mathbb{Z}$, for $0 < i < m$, then the sequence of integers $\hat{S}_n = \{s_\ell\}$ defined by:

$$s_n = \sum_{i=1}^{m} a_i f_{n-i} = a_1 f_{n-1} + a_2 f_{n-2} + \cdots + a_m f_{n-m},$$

which is called an mth order linear recurrence relation. In this relation next term is computed through linear relation of previous m terms. For example, the second order linear recurrence can be given by,

$$f_n = A f_{n-1} - B f_{n-2}, \text{ with } \gcd(A, B) = 1, \qquad (1)$$

with given f_0 and f_1. The generating function $G(x)$ corresponding to equation (1), is as follows:

$$G(x) = x^2 - Ax + B. \qquad (2)$$

The procedure to derive generating function can be found in [13]. Let α_1 and α_2 be two roots of equation (2), then the sum $(\alpha_1+\alpha_2)$ and product $(\alpha_1 \cdot \alpha_2)$ of these roots is of special attention. If $g_1, g_2 \in \mathbb{Z}$ then following relation was proved in [2]:

$$A(g_1\alpha_1^{n-1}+g_2\alpha_2^{n-1}) - B(g_1\alpha_1^{n-2}+g_2\alpha_2^{n-2}) = g_1\alpha_1^n+g_2\alpha_2^n.$$

This implies any sequence $\hat{S}_n$ generated by equation (1), is of the form $g_1\alpha_1^n+g_2\alpha_2^n$ with $s_0 = 2$ and $s_1 = g_1\alpha_1+g_2\alpha_2$. For LUC-PKC, following solutions to $G(x)$ are of special attention as interesting relations can be defined for applications in this PKC. These solutions are given below:

$$\gamma_n = \frac{\alpha_1^n - \alpha_2^n}{\alpha_1 - \alpha_2},$$
$$\lambda_n = \alpha_1^n + \alpha_2^n,$$

with $\gamma_0 = 0, \gamma_1 = 1$ and $\lambda_0 = 2, \lambda_1 = g_1$. Note that γ_n and λ_n depends only on the integers g_1 and g_2 and the terms $\gamma_n(g_1, g_2)$ and $\lambda_n(g_1, g_2)$ are called *Lucas Functions* of g_1 and g_2.

Some Interesting Relations [2]. Let $A = \alpha_1 + \alpha_2$, $B = \alpha_1\alpha_2$ and discriminant of $G(x)$,

$$\Delta = A^2 - 4B = (\alpha_1 - \alpha_2)^2$$

be given, then following relations hold:

- $\lambda_{2n} = \lambda_n^2 - 2B^n$.
- $\lambda_{2n-1} = \lambda_n\lambda_{n-1} - AB^{n-1}$.
- $\lambda_{2n+1} = A\lambda_n^2 - B\lambda_n\lambda_{n-1} - AB^n$.
- $\lambda_n^2 = \Delta\gamma_n^2 + 4B^n$.
- $2\lambda_{n+m} = \lambda_n\lambda_m + \Delta\gamma_n\gamma_m$.
- $2B\lambda_{n-m} = \lambda_n\lambda_m - \Delta\gamma_n\gamma_m$.

Now, if second order generating function is $\bar{G}(x) = x^2 - \lambda_k(A, B)x + B^k$, then $\lambda_k(A, B) = \alpha_1^k + \alpha_2^k$. Similarly, we have

$$\lambda_n(\lambda_k(A, B), b^k) = (\alpha_1^k)^n + (\alpha_2^k)^n = \lambda_{nk}(A, B).$$

It shows a clear generalization of the rule for composition of powers, with subscript of a Lucas function playing the role of a power.

Diffie-Hellman Key Exchange and Lucas Functions. The Diffie-Hellman type key exchange protocol can be established by using Lucas functions. Let $\mathcal{A}$ and $\mathcal{B}$ want to agree on a common key $\mathcal{K}$. Also let $m, n \in \mathbb{Z}$ and $g \in \mathbb{F}_p$ a primitive element, where p is a large prime. Then $\mathcal{A}$ and $\mathcal{B}$ can do the following independently to agree on a common key $\mathcal{K}$.

- $\mathcal{A}$ computes g^m and sends to $\mathcal{B}$.
- $\mathcal{B}$ computes g^n and sends to $\mathcal{A}$
- $\mathcal{A}$ and $\mathcal{B}$ computes $\mathcal{K} = (g^n)^m = (g^m)^n = g^{nm}$.

Similarly, for Lucas functions Diffie-Hellman key exchange is carried out as follows:

- $\mathcal{A}$ computes $\lambda_m(A, B)$ and sends to $\mathcal{B}$.
- $\mathcal{B}$ computes $\lambda_n(A, B)$ and sends to $\mathcal{A}$
- $\mathcal{A}$ and $\mathcal{B}$ computes $\mathcal{K} = \lambda_m(\lambda_n(A, B)) = \lambda_n(\lambda_m(A, B)) = \lambda_{mn}(A, B)$.

Achieved Goals. Following main goals are achieved in LUC cryptosystem:

- Data transmission in prime field $\mathbb{F}_p$ and DLP lie in extension field $\mathbb{F}_{p^2}$.
- A compression factor of 2 is achieved.
- Adaptation to cryptographic protocols using Lucas functions.

III. GH-Public Key Cryptosystem

Gong and Harn proposed new public key cryptosystem in [4]. They used characteristic sequence of an LFSR to construct DLP over $\mathbb{F}_{p^s}$ while computations are carried out in prime field $\mathbb{F}_p$, with p, prime. In this section we will give the basic details of this cryptosystem and Diffie-Hellman key exchange, based on this concept as an example.

Definition : LFSR Sequence. Let $f(x)$ be a polynomial given by,

$$f(x) = \sum_{i=0}^{n} c_i x^i, \; c_i \in \mathbb{F}_p \text{ and } c_n = 1.$$

and $\hat{s}$ be a sequence over $\mathbb{F}_p$ such that;

$$\hat{s} = \{s_i\} = s_0, s_1, s_2, \ldots; \text{ with } s_i \in \mathbb{F}_p.$$

The $\hat{s}$ is called an LFSR sequence of order n generated by $f(x)$ if it satisfies the following linear recursive relation:

$$s_{k+n} = \sum_{i=0}^{n-1} c_i s_{k+i}, \; k = 0, 1, \ldots$$

The states $s_0, s_1, \ldots, s_{n-1}$ are called an *initial states* of the sequence $\hat{s}$ generated by $f(x)$.

Characteristic Sequence and Trace Representation. If $f(x)$ is an irreducible polynomial over $\mathbb{F}_p$, and let α be a root of

$f(x)$ in extension field $\mathbb{F}_{p^r}$, then the trace function is defined as

$$\mathrm{Tr}(\alpha) = \alpha + \alpha^p + \alpha^{p^2} + \cdots + \alpha^{p^{r-1}}.$$

In the extension field $\mathbb{F}_{p^3}$ the i-th term of $\hat{s}$ for some $\beta \in \mathbb{F}_p$ can be given as:

$$s_i = \mathrm{Tr}(\beta\alpha^i),\ i = 0, 1, 2 \ldots$$

If $\beta = 1$ then sequence $\hat{s}$ is called characteristic sequence of $f(x)$.

Lemma 1 [13]. If $f(x) \in \mathbb{F}_p[x]$ is irreducible over $\mathbb{F}_p$ and $\hat{s}$ as defined above is generated by $f(x)$, then

$$per(\hat{s}) = per(f) = ord(\alpha),$$

where $\alpha \in \mathbb{F}_{p^r}$ such that $f(\alpha) = 0$. Here, period of f and order of α are denoted by $per(f)$ and $ord(\alpha)$, respectively.

Third Order Characteristic Equation of GH-PKC. Let $\hat{s}$ be characteristic sequence generated by irreducible polynomial $f(x) = x^3 - ax^2 + bx - 1$ with $a, b \in \mathbb{F}_p$ and $f(x) \in \mathbb{F}_p[x]$. Let the initial states of $\hat{s}$ be $s_0 = 3, s_1 = a$, and $s_2 = a^2 - 2b$ then following holds:

Lemma 2 [4]. If $per(f)$ dividing by $p^2 + p + 1$ is equal to $per(\hat{s})$, then for some $k \in \mathbb{Z}$, s_k can be determined as follows:

$$s_k = \mathrm{Tr}(\alpha^k),\ k = 0, 1, \ldots,$$

where $\alpha \in \mathbb{F}_{p^3}$ is a root of $f(x)$.

Reciprocal Sequence. Let $f(x) = x^3 - ax^2 + bx - 1$ be the characteristic equation with associated characteristic sequence $s_k = s_k(a, b)$ or $s_k(f)$, then the reciprocal polynomial $f^{-1}(x)$ of $f(x)$ is defined as:

$$f^{-1}(x) = x^3 - bx^2 + ax - 1,$$

and the associated reciprocal sequence is $s_{-k}(a, b) = s_k(b, a)$.

Lemma 3 [4]. Let $f(x) = x^3 - ax^2 + bx - 1$ be an irreducible polynomial over $\mathbb{F}_p$, $\hat{s}$ be its characteristic sequence and $\alpha \in \mathbb{F}_{p^3}$ be the root of $f(x)$. Then following holds:

- For all integers e and r,

$$s_e(s_r(a, b), s_{-r}(a, b)) = s_{er}(a, b)$$

- For all integers n and m
  i) $s_{2n} = s_n^2 - 2s_{-n}$,
  ii) $s_n s_m - s_{n-m} s_{-m} = s_{n+m} - s_{n-2m}$.
- If $\gcd(k, per(\hat{s})) = 1$, then α^{kp^i}, $i = 0, 1, 2$ are three roots of $g(x) = x^3 - s_k x^2 + s_{-k} x - 1 \in \mathbb{F}_{p^3}$. The proofs can be found in [4].

Formulae to Compute (s_k) [4]. Let $k = \sum_{i=0}^{\ell} k_\ell 2^{\ell - i}$, $k_i \in \{-1, 0, 1\}$ be the binary representation of k, $T_0 = k_0 \neq 0$, and $T_j = k_j + 2T_{j-1}$, $1 \geq j \geq \ell$. If three terms of the $\hat{s}$ $(s_{T_{j-1}-1}, s_{T_{j-1}}, s_{T_{j-1}+1})$ are known then the next three terms $(s_{T_j-1}, s_{T_j}, s_{T_j+1})$ can be computed as follows:

If $k_j = 0$

$$\begin{aligned} s_{T_j-1} &= s_{T_{j-1}} s_{T_{j-1}-1} - b s_{-T_{j-1}} + s_{-(T_{j-1}+1)}; \\ s_{T_j} &= s_{T_{j-1}}^2 - 2 s_{-T_{j-1}}; \\ s_{T_j+1} &= s_{T_{j-1}} s_{T_{j-1}+1} - a s_{-T_{j-1}} + s_{-(T_{j-1}-1)}. \end{aligned}$$

If $k_j = 1$

$$\begin{aligned} s_{T_j-1} &= s_{T_{j-1}}^2 - 2 s_{-T_{j-1}}; \\ s_{T_j} &= s_{T_{j-1}} s_{T_{j-1}+1} - a s_{-T_{j-1}} + s_{-(T_{j-1}-1)}; \\ s_{T_j+1} &= s_{T_{j-1}+1}^2 - 2 s_{-(T_{j-1}-1)}. \end{aligned}$$

If $k_j = -1$

$$\begin{aligned} s_{T_j-1} &= s_{T_{j-1}-1}^2 - 2 s_{-(T_{j-1}-1)}; \\ s_{T_j} &= s_{T_{j-1}} s_{T_{j-1}+1} - a s_{-T_{j-1}} + s_{-(T_{j-1}-1)}; \\ s_{T_j+1} &= s_{T_{j-1}+1}^2 - 2 s_{-(T_{j-1}+1)}. \end{aligned}$$

The initial conditions are $s_0 = 3$, $s_1 = a$, $s_2 = a^2 - 2b$, $s_{-1} = b$, and $s_{-2} = b^2 - 2a$. The algorithm for above formulae can be found in [5]. Moreover, an algorithmic improvement in computational complexity for GH-PKC was also proposed in [6], but the basic concept does not change.

GH-PKC based Diffie-Hellman Key Exchange Scheme. Following key distribution scheme is just as an example for adaptation to cryptographic protocols:

- ***System Public parameters.*** A prime p, $f(x) = x^3 - ax^2 + bx - 1$ an irreducible polynomial over $\mathbb{F}_p$ with order $q = p^2 + p + 1$.
- $\mathcal{A}$ selects $a, 0 < a < q$ such that $\gcd(a, q) = 1$ as private key and computes public key (s_a, s_{-a}) and sends this key to $\mathcal{B}$.
- $\mathcal{B}$ selects $b, 0 < b < q$ such that $\gcd(b, q) = 1$ as private key and computes public key (s_b, s_{-b}) and sends this key to $\mathcal{A}$.
- $\mathcal{A}$ computes:

$$\mathcal{K} = (s_{ab}, s_{-ab}) = (s_a(s_b, s_{-b}), s_{-a}(s_b, s_{-b})).$$

- $\mathcal{B}$ computes:

$$\mathcal{K} = (s_{ab}, s_{-ab}) = (s_b(s_a, s_{-a}), s_{-b}(s_a, s_{-a})).$$

In this way both $\mathcal{A}$ and $\mathcal{B}$ compute common key $\mathcal{K} = (s_{ab}, s_{-ab})$.

Remark: ***Resistance to SPA attacks.*** Additionally, we observe that the operations while computing $k_j = 0$ and $k_j = 1$ are almost identical. This makes the algorithm resistant against Simple Power Analysis (SPA) attacks. In SPA attacks some environmental parameters (electrical power spectrum, timing analysis etc.) are analyzed to extract secret information of the cryptosystem.

Achieved Goals. In GH-PKC following gaols are achieved:

- Compact representation of operands over $\mathbb{F}_p$. A compression ratio by a factor of 3/2 is achieved [9].
- LFSR based computation of cryptographic protocols.
- Resistant to SPA based side channel attacks by employing identical computation as indicated above.
- Adaptation of the concept for public key cryptosystems such as Diffie-Hellman key distribution scheme, RSA type PKC, and digital signature scheme etc.

IV. XTR-Public Key Cryptosystem

XTR is an acronym for 'ECSTR' which means Efficient and Compact Subgroup Trace Representation. XTR-PKC was

proposed by Lenstra and Verheul in [7]. In this system, the computations are performed in an intermediate subfield of the form $\mathbb{F}_{p^2}$ rather than a prime field of the form $\mathbb{F}_p$. The security level benefits from the harder DLP defined over the extension field F_{p^6}. The subgroup of $\mathbb{F}^*_{p^6}$ is selected so that the irreducible cubic polynomial $f \in \mathbb{F}_{p^2}[x]$ can be fixed in the form $f(x) = x^3 - \mathrm{Tr}(\alpha)x^2 + \mathrm{Tr}(\alpha)^p x - 1$, where $f(\alpha) = 0$.

XTR Subgroup and Underlying Arithmetic. Let $\alpha \in \mathbb{F}_{p^6}$, then the conjugates of α over $\mathbb{F}_{p^2}$ are α, α^{p^2}, and α^{p^4}. The trace of α over $\mathbb{F}_{p^2}$ and the norm of α over $\mathbb{F}_{p^2}$ are as follows:

$$\mathrm{Tr}(\alpha) = \alpha + \alpha^{p^2} + \alpha^{p^4},$$

and

$$\mathrm{Norm}(\alpha) = \alpha \cdot \alpha^{p^2} \cdot \alpha^{p^4} = \alpha^{1+p^2+p^4}. \quad (3)$$

Note that,

$$x^n - 1 = \prod_{d|n} \Phi_d(x), \text{ so } |\mathbb{F}_{p^n}| = \prod_{d|n} \Phi_d(p).$$

where $\Phi_d(x)$ is d-th cyclotomic polynomial. So we have,

$$\begin{aligned} |\mathbb{F}_{p^6}| &= p^6 - 1 \\ &= (p^2 - p + 1)(p^2 + p + 1)(p + 1)(p - 1) \\ &= \Phi_6(p)\Phi_3(p)\Phi_2(p)\Phi_1(p). \end{aligned}$$

Therefore, an element of $\mathbb{F}_{p^6}$ of order dividing $p^2 - p + 1$ does not lie in any proper subfield of $\mathbb{F}^*_{p^6}$. Now we select $\alpha \in \mathbb{F}_{p^6}$ such that $ord(\alpha) > 3$ dividing $p^2 - p + 1$. This implies $p^2 \equiv p - 1 \pmod{p^2 - p + 1}$ and $p^4 \equiv -p \pmod{p^2 - p + 1}$. After selecting such subgroup the conjugates of $\alpha \in \mathbb{F}_{p^6}$ over $\mathbb{F}_{p^2}$ becomes α, $\alpha^{p-1} = \alpha^{p^2}$, and $\alpha^{-p} = \alpha^{p^4}$. In the light of above properties, equation (3) becomes

$$\mathrm{Norm}(\alpha) = \alpha^{1+p^2+p^4} = \alpha^{1+p-1-p} = 1.$$

After this development $f(x) \in \mathbb{F}_{p^2}[x]$ has the following representation with the roots α, α^{p-1}, $\alpha^{-p} \in \mathbb{F}_{p^6}$:

$$\begin{aligned} f(x) &= (x - \alpha)(x - \alpha^{p-1})(x - \alpha^{-p}) \\ &= x^3 - \mathrm{Tr}(\alpha)x^2 + \mathrm{Tr}(\alpha)^p x + (-1)^3 \mathrm{Norm}(\alpha) \\ &= x^3 - \mathrm{Tr}(\alpha)x^2 + \mathrm{Tr}(\alpha)^p x - 1. \end{aligned}$$

In this case, $f(x)$ is actually minimal polynomial of $\alpha \in \mathbb{F}_{p^6}$ over $\mathbb{F}_{p^2}$. Therefore, any power of α^k for $k \in \mathbb{Z}$, and its conjugates are the roots of $f(x)$ [13]. So, we can replace $\mathrm{Tr}(\alpha)$ with $\mathrm{Tr}(\alpha^k)$ and $f(x)$ still remains minimal polynomial as defined above. Therefore, we compute $\mathrm{Tr}(\alpha^k) \in \mathbb{F}_{p^2}$ instead of computing $\alpha^k \in \mathbb{F}_{p^6}$. As a result, the number of bits of group operands for exponentiation is reduced by a factor of 3.

Definitions and Notations. Some definitions and notations are given below for subsequent use.

- Let $c \in \mathbb{F}_{p^2}$ and $f(c, x) \in \mathbb{F}_{p^2}[x]$, then

$$f(c, x) = x^3 - cx^2 + c^p x - 1.$$

- Let $\tau(c, n) = \mathrm{Tr}(\alpha^n)$ in shorthand we use $\tau(c, n) = c_n$.
- Let $S_n(c) = (c_{n-1}, c_n, c_{n+1}) \in \mathbb{F}_{p^2} \times \mathbb{F}_{p^2} \times \mathbb{F}_{p^2}$.

Fundamentals for XTR Computational Algorithm [7]. We annotate the fundamental results being applied in XTR-PKC. The detailed information is provided in [7].

i). $c_{-n} = c_{np} = c_n^p$, for $n \in \mathbb{Z}$ and $c_n \in \mathbb{F}_{p^2}$.
ii). $c_{u+v} = c_u.c_v - c_v^p.c_{u-v} + c_{u-2v}$, for $u, v \in \mathbb{Z}$.
iii). $c_{2u} = c_u^2 - 2c_u^p$.
iv). $c_{u+2} = c.c_{u+1} - c^p.c_u + c_{u-1}$.
v). $c_{2u-1} = c_{u-1}.c_u - c^p.c_u^p + c_{u+1}^p$.
vi). $c_{2u+1} = c_{u+1}.c_u - c.c_u^p + c_{u-1}^p$.

XTR Algorithm for Computation of $S_u(c)$ given u and c.

- If $u = 0$, then $S_0(c) = (c^p, 3, c)$.
- If $u = 1$, then $S_1(c) = (3, c, c^2 - 2c^p)$.
- If $u = 2$, then use $c_{u+2} = c.c_{u+1} - c^p.c_u + c_{u-1}$, and $S_1(c)$ to compute c_3 and thereby $S_2(c)$.
- For $u > 2$ to compute $S_u(c)$ define $\hat{S}_i(c) = S_{2i+1}(c)$ and let $\hat{m} = u$. If m if even, then $\hat{m} = \hat{m} - 1$. Let $\hat{m} = 2m + 1$, also $k = 1$ and compute $\hat{S}_k(c) = S_3(c)$. Let $m = \sum_{j=0}^{r} m_j 2^j$ with $m_j \in \{0, 1\}$ and $m_r = 1$. For $j = r - 1, r - 2, \ldots, 0$ do the following:
  - If $m_j = 0$, then use $\hat{S}_k(c) = (c_{2k}, c_{2k+1}, c_{2k+2})$ to compute $\hat{S}_{2k}(c) = (c_{4k}, c_{4k+1}, c_{4k+2})$ and replace k by $2k$.
  - If $m_j = 1$, then use $\hat{S}_k(c) = (c_{2k}, c_{2k+1}, c_{2k+2})$ to compute $\hat{S}_{2k+1}(c) = (c_{4k+2}, c_{4k+3}, c_{4k+4})$ and replace k by $2k + 1$.

Now $2k + 1 = m$ and $S_{\hat{m}}(c) = \hat{S}_m(c)$. If u is even, then use $S_{\hat{m}}(c) = (c_{\hat{m}-1}, c_{\hat{m}}, c_{\hat{m}+1})$ to compute $S_{\hat{m}+1}(c) = (c_{\hat{m}}, c_{\hat{m}+1}, c_{\hat{m}+2})$ and replace $\hat{m}$ by $\hat{m} + 1$. As a result $S_u(c) = S_{\hat{m}}(c)$.

Algorithm to Compute $\mathrm{Tr}(\alpha)$

1. Apply XTR algorithm for $u = p + 1$ and random $c \in \mathbb{F}_{p^2} \backslash \mathbb{F}_p$ to compute c_{p+1}.
2. If $c_{p+1} \in \mathbb{F}_p$ then return to Step 1.
3. Apply XTR algorithm for $u = (p^2 - p + 1)/q$ and c to compute $d = c_{(p^2-p+1)/q}$, where q is order of α.
4. If $d = 3$, then return to step 1.
5. Let $\mathrm{Tr}(\alpha) = d$.

XTR based Diffie-Hellman (DH) Key Exchange Scheme [7]. The XTR-DH key exchange protocol is given to serve as an example for cryptographic adaptation of the XTR concept. Let $\mathcal{A}$ wants to exchange a key $\mathcal{K}$ with $\mathcal{B}$. The public parameters are $p, q, \mathrm{Tr}(\alpha)$, where q is the order subgroup of $\mathbb{F}_{p^6}$. Following is the protocol:

- $\mathcal{A}$ selects at random $a \in \mathbb{Z}, 1 < a < q - 2$, and compute $S_a(\mathrm{Tr}(\alpha)) = (\mathrm{Tr}(\alpha^{a-1}), \mathrm{Tr}(\alpha^a), \mathrm{Tr}(\alpha^{a+1}))$ and sends $\mathrm{Tr}(\alpha^a) \in \mathbb{F}_{p^2}$ to $\mathcal{B}$.
- $\mathcal{B}$ selects at random $b \in \mathbb{Z}, 1 < b < q - 2$, and compute $S_b(\mathrm{Tr}(\alpha)) = (\mathrm{Tr}(\alpha^{b-1}), \mathrm{Tr}(\alpha^b), \mathrm{Tr}(\alpha^{b+1}))$ and sends $\mathrm{Tr}(\alpha^b) \in \mathbb{F}_{p^2}$ to $\mathcal{A}$.
- $\mathcal{A}$ receives $\mathrm{Tr}(\alpha^b)$ from $\mathcal{B}$ and computes $S_a(\mathrm{Tr}(\alpha^b)) = (\mathrm{Tr}(\alpha^{(a-1)b}), \mathrm{Tr}(\alpha^{ab}), \mathrm{Tr}(\alpha^{(a+1)b}))$ and subsequently determines $\mathcal{K} = \mathrm{Tr}(\alpha^{ab})$.
- $\mathcal{B}$ receives $\mathrm{Tr}(\alpha^a)$ from $\mathcal{A}$ and computes $S_b(\mathrm{Tr}(\alpha^a)) = (\mathrm{Tr}(\alpha^{(b-1)a}), \mathrm{Tr}(\alpha^{ab}), \mathrm{Tr}(\alpha^{(b+1)a}))$ and subsequently determines $\mathcal{K} = \mathrm{Tr}(\alpha^{ab})$.

Achieved Goals. The XTR cryptosystem achieves following main goals:

- Compact representation of operands over $\mathbb{F}_{p^2}$ and compression is achieved by a factor of 3.

- The advantage of DLP in extension field $\mathbb{F}_{p^6}$ is ensured.
- It is also resistant to SPA attacks in a similar fashion as mentioned in GH-PKC section.
- Trace based computation of group operations by means of symmetric polynomials. Therefore, only $\varphi(n)$ elements are required to represent an element of $\mathbb{F}_{p^n}$ in $\mathbb{F}_{p^r}$ such that $r < n$, $r|n$.
- Adaptation tor cryptographic protocols such as Diffie-Hellman key exchange, encryption/decryption and digital signature scheme etc.

V. Torus Based Cryptosystems

Torus based public key cryptosystem is yet another system that enjoys the extension field security and carry out group operations in prime or intermediate subfields. This system was proposed by Rubin and Silverberg in [12]. This system is an improvement over LUC-PKC [2], and GH-PKC [4], where as, its performance is comparable with XTR-PKC [7].

Algebraic Tori. An algebraic torus T over $\mathbb{F}_p$ is an algebraic group defined over $\mathbb{F}_p$ which of that defined on some extension field is isomorphic to $(\mathbb{G}_m)^d$, where $\mathbb{G}_m$ is the multiplicative group and d is dimension of T. For every n, an algebraic torus T_n can be defined with the property that $T_n(\mathbb{F}_p)$ consists of the elements α in $\mathbb{F}_{p^n}^*$ such that $\mathrm{Norm}(\alpha) = 1$ over $\mathbb{F}_{p^r}^*$ with $r|n$.

Definitions.

- ***Algebraic Variety.*** An algebraic variety is an object which can be defined in a purely algebraic way, starting from polynomials or more generally from finitely generated algebras over fields. The variety structure allows to express all elements and operations in terms of polynomials.
- ***Weil Restriction.*** The Weil restriction (also known as Restriction of scalars) is a functor which, for any finite extension of fields $\mathbb{F}_{p^n}/\mathbb{F}_p$ and any algebraic variety X over $\mathbb{F}_{p^n}$, produces another variety $\mathrm{Res}_{\mathbb{F}_{p^n}/\mathbb{F}_p}X$, defined over $\mathbb{F}_p$. This means Weil restriction decomposes a multiplicative group $\mathrm{Res}_{\mathbb{F}_{p^n}/\mathbb{F}_p}G_m$ as a product of algebraic tori, one for each divisor of n.

Fundamental Arithmetic for Torus Based Cryptography. As defined above the $\mathrm{Res}_{\mathbb{F}_{p^n}/\mathbb{F}_p}\mathbb{G}_m$ is a torus. As per the property of Weil restriction of scalars gives an isomorphism:

$$(\mathrm{Res}_{\mathbb{F}_{p^n}/\mathbb{F}_p}\mathbb{G}_m)(\mathbb{F}_p) \cong \mathbb{G}_m(\mathbb{F}_{p^n}) = \mathbb{F}_{p^n}^*,$$

and Norm map for $\mathbb{F}_p \subset \mathbb{F}_{p^r} \subset \mathbb{F}_{p^n}$:

$$\mathrm{Res}_{\mathbb{F}_{p^n}/\mathbb{F}_p}\mathbb{G}_m \xrightarrow{N_{\mathbb{F}_{p^n}/\mathbb{F}_{p^r}}} \mathrm{Res}_{\mathbb{F}_{p^r}/\mathbb{F}_p}\mathbb{G}_m.$$

For $\mathbb{F}_p$ points we have:

$$T_n(\mathbb{F}_p) \cong \{\alpha \in \mathbb{F}_{p^n}^* : N_{\mathbb{F}_{p^n}/\mathbb{F}_{p^r}}(\alpha) = 1\},$$

whenever $\mathbb{F}_p \subset \mathbb{F}_{p^r} \subset \mathbb{F}_{p^n}$. The dimension of T_n is $\varphi(n)$. $T_n(\mathbb{F}_p)$ is a cyclic subgroup $\mathbb{G}_{p,n} \subseteq \mathbb{F}_{p^n}^*$ of order $\Phi_n(p)$, where Φ_n is the n-th cyclotomic polynomial. This implies that the security of cryptosystems based on the group T_n is that of $\mathbb{F}_{p^n}^*$.

Lemma 4, [12].

i). $T_n(\mathbb{F}_p) \cong \mathbb{G}_{p,n}$.

ii). $\#T_n(\mathbb{F}_p) = \Phi_n(p)$.

iii). If $\alpha \in T_n(\mathbb{F}_p)$ is an element of prime order not dividing n, then α does not lie in any proper subfield of $\mathbb{F}_{p^n}/F_p$.

Definitions

- *Rationality of Tori [12]:* Let T be an algebraic torus over $\mathbb{F}_p$ of dimension d. Then T is rational if and only if there is a birational map $\rho : T \to \mathbb{A}^d$ defined over $\mathbb{F}_p$.
- *Rational Parametrization of T [12]:* There are *Zariski* open subsets $W \subset T$ and $U \subset \mathbb{A}^d$, and rational functions $\rho_1, \ldots, \rho_d \in \mathbb{F}_p[x_1, \ldots, x_t]$ and $\psi_1, \ldots, \psi_t \in \mathbb{F}_p[y_1, \ldots, y_d]$ such that $\rho : W \to U$ and $\psi : U \to W$ are inverse isomorphisms. Such a map is a rational parametrization of T.

In this way a compact representation of the group $T(\mathbb{F}_p)$ by means of rational parametrization of torus T is obtained. Thus every element of $W(\mathbb{F}_p) \subset T(\mathbb{F}_p)$ is represented by d coordinates in $\mathbb{F}_q$.

Rational parametrization of T_2. To build a better understanding of rational parametrization for T_2 we proceed as follows. Let $\mathrm{char}(\mathbb{F}_p) \neq 2$ and $\mathbb{F}_{p^2} = \mathbb{F}_p(\gamma) : \gamma \in \mathbb{F}_{p^2}^*$ with $\omega = \gamma^2 \in \mathbb{F}_p^*$. Since $\gamma^p = -\gamma$, this implies

$$\begin{aligned} G_{p,2} &= \{a + b\gamma : a, b \in \mathbb{F}_p \text{ and } (a+b\gamma)^{p+1} = 1\}, \\ &= \{a + b\gamma : a, b \in \mathbb{F}_p \text{ and } (a^2 - \omega b^2) = 1\}. \end{aligned}$$

Define maps,

$$\rho : G_{p,2} - \{\pm 1\} \to \mathbb{F}_p^* \quad : \rho(c + d\gamma) = \frac{1+c}{d}$$

and

$$\psi : \mathbb{F}_p^* \to G_{p,2} \quad : \psi(a) = \frac{a+\gamma}{a-\gamma}.$$

Now $\psi(a) \cdot \psi(b) = \psi\left(\frac{ab+d}{a+b}\right)$. Therefore, all operations are carried out in $\mathbb{F}_p$ directly and multiplication in T_2 has been translated into the map $(a, b) \mapsto \frac{ab+d}{a+b}$ from $(\mathbb{F}_p^*)^2$ to $\mathbb{F}_p^*$.

Adaptation to Cryptographic Protocols [12]. As a demonstration, we provide analogous Diffie-Hellman key exchange protocol based on the concept of torus based cryptography.

- ***Pre-computations.*** The following are the pre-computations for Torus Based Cryptography:
  - Choose a prime power q and an integer n such that the torus T_n over $\mathbb{F}_q$ has an explicit parametrization, and a prime $\ell|\Phi_n(q)$.
  - Let $m = \varphi(n)$.
  - Fix birational map, $\rho : T_n(\mathbb{F}_q) \to \mathbb{F}_{q^m}$ and its inverse ψ such that $\rho \circ \psi = 1$.
  - Choose $\alpha \in T_n$ of order ℓ and let $g = \rho(\alpha) \in \mathbb{F}_{q^m}$.
  - The public is n, q, ρ, ψ, ℓ and either g or $\alpha = \psi(g)$.
- ***Key agreement scheme.***
  1. $\mathcal{A}$ chooses a random integer a in the range $1 \leq a \leq \ell - 1$ and computes $P_{\mathcal{A}} := \rho(\alpha^a) \in \mathbb{F}_{q^m}$ and send it to $\mathcal{B}$.
  2. $\mathcal{B}$ chooses a random integer b in the range $1 \leq b \leq \ell - 1$ and computes $P_{\mathcal{B}} := \rho(\alpha^b) \in \mathbb{F}_{q^m}$ and send it to $\mathcal{A}$.
  3. $\mathcal{A}$ computes $\rho(\psi(P_{\mathcal{B}})^a) \in \mathbb{F}_{q^m}$.
  4. $\mathcal{B}$ computes $\rho(\psi(P_{\mathcal{A}})^b) \in \mathbb{F}_{q^m}$.

Why it works? Since $\rho \circ \psi$ is the identity, we have $\rho(\psi(P_B)^a) = \rho(\alpha^{ab}) = \rho(\psi(P_A)^b)$.

Achieved Goals. Following are the main goals achieved by Torus based Cryptography:

- Data compression by rational parametrization of a torus.
- Representation of group elements of extension field $\mathbb{F}_{p^n}$ by only $\varphi(n)$ elements of $\mathbb{F}_p$.
- Torus based compression works where trace based representation has limitations [12].
- Multiplication is used as group operation instead of exponentiation. Therefore novel methods to speed up group operations are not required. This allows full functionality of group structure for variety of applications.
- The countermeasures against SPA is an open problem in this case.

VI. Conclusions

In this paper we surveyed LUC-PKC, GH-PKC, XTR-PKC and Torus based cryptosystems by going through underlying mathematical concepts and their adaptation to public key cryptosystems. These cryptosystems compress data by representing group elements in subfield of an extension field in such a way that DLP lies in extension field. In LUC-PKC, GH-PKC, and XTR-PKC novel methods for faster group operations are required, where as, in torus based cryptography conventional methods for multiplication can be employed. The group operations are carried out in prime or intermediate subfields whereas DLP lies in extension fields. As a summary, the LUC-PKC exploits Lucas functions in such a way that group operands lie in prime subfield $\mathbb{F}_p$ and DLP has to be solved in extension field $\mathbb{F}_{p^2}$. The GH-PKC carry out group operations in prime subfield and DLP in $\mathbb{F}_{p^3}$. The characteristic sequence of an LFSR is exploited for cryptographic protocol. The XTR-PKC carry out group operations in intermediate subfield $\mathbb{F}_{p^2}$ and DLP in $\mathbb{F}_{p^6}$. The trace function is used for data compression and cryptographic protocols are based on properties of trace function and symmetric polynomials over finite fields. The torus based cryptography employs rational parameterization of algebraic torus for cryptographic protocols. We also pointed out for the first time that the algorithm for computing k-th term of LFSR sequence in GH-PKC has additional characteristic to lure away simple power analysis attacks.

Acknowledgment

We would like to express my sincere gratitude to the anonymous referees for their valuable comments, to Professor Ersan Akyıldız for his diligent guidance and encouragement.

References

[1] W. Diffie, M.E. Hellman. New directions in cryptography, IEEE Trans. on Information Theory 22, 1976, 644-654.
[2] P. Smith, and M. Lennon. LUC: A new public key system, Proceedings of the 9th IFIP Symp. - IFIP/Sec 1993, 103-117.
[3] P. Smith, C. Skinner. A public-key cryptosystem and a digital signature system based on the Lucas function analogue to discrete logarithms, Advances in Cryptology - Asiacrypt 1994, Lect. Notes in Comp. Sci. 917, Springer, Berlin, 1995, 357-364.
[4] G. Gong, L. Harn. Public-key cryptosystems based on cubic finite field extensions, IEEE trans on Information Theory 45, 1999, 2601-2605.
[5] G. Gong, L. Harn, and Huapeng Wu. The GH Public-key cryptosystem, SAC 2001, Lect. Notes in Comp. Sci. 2259, Springer, 2001, 284-300.
[6] G. Gong, A. Hassan, H. Wu, and A. Youssef. An Efficient Algorithm for Exponentiation in DH Key Exchange and DSA in Cubic Extension Fields, Research report at Faculty of Math., University of Waterloo, 2002.
[7] A. K. Lenstra, E. R. Verheul. The XTR public key system, Advances in Cryptology - CRYPTO 2000, Lect. Notes in Comp. Sci. 1880, Springer, Berlin, 2000, 1-19.
[8] A. K. Lenstra, E. R. Verheul. An overview of the XTR public key system, Publickey cryptography and computational number theory (Warsaw, 2000), de Gruyter, Berlin, 2001, 151-180.
[9] W. Bosma, J. Hutton, E. R. Verheul. Looking beyond XTR, Advances in Cryptology - Asiacrypt 2002, Lect. Notes in Comp. Sci. 2501, Springer, Berlin, 2002, 46-63.
[10] M. Stam and A. Lenstra. Speeding up XTR, Advances in Cryptology - ASIACRYPT 2001, Lect. Notes in Comp. Sci. 2248, Springer, 2001, 125-143.
[11] M. Shirase, D. Han, Y. Hibin, H. Kim, and T. Takagi. A more compact representation of XTR cryptosystem. IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences, E91-A:2843-2850, 2008.
[12] K. Rubin and A. Silverberg. Torus-based cryptography, Advances in Cryptology - CRYPTO 2003, Lecture Notes in Computer Science, 2729:349-365, 2003.
[13] R. Lidl and H. Niederreiter. Finite Fields, Addison-Wesley Publishing Company, 1983.

Optimal Control Formulation of Query Model for Authentication Systems

Ferruh Özbudak, Ali D. Sezer and Üstün Yıldırım

***Abstract*—We give a stochastic optimal control representation of the N step adaptive attack on an authentication system using an authentication oracle described in [Safavi-Naini, Wild, IEEE Transactions on Information Theory, 54(6) (2008), 2426-2436]. The key quantity of interest in this attack is the maximum probability of a successful attack. We represent this quantity as the value function of an optimal control problem and derive the dynamic programming equation that this function satisfies. The same paper cited above proves that randomized queries in such an attack have the same probability of success as that of a deterministic attack. We rederive this fact using our control representation.**

***Index Terms*—Authentication system, query model, optimal control.**

I. Introduction

SUPPOSE that there are two parties called sender and receiver. The sender is to use an authentication algorithm to authenticate itself to the receiver. The authentication system consists of the set of keys K, the set of source states S (the actual text to be transmitted), the set of messages M, the authentication function $\text{Auth} : K \times S \to M$ and the verification function $\text{Ver} : K \times M \to \{0, 1\}$. The assumptions on these are as follows:

1) $\text{Ver}(e, \text{Auth}(e, s)) = 1$ for all $(e, s) \in K \times S$,
2) $\text{Ver}(e, m) = 1$ if and only if there is a source $s \in K$ such that $m = \text{Auth}(e, s)$,
3) $\text{Auth}(e, \cdot)$ is an injective function from S to M for all $e \in K$,
4) K, M and S are finite.

The authentication system works as follows. The sender and receiver chooses a random key E that takes values in K; only the sender and the reciever are assumed to know the key. If the sender is to transmit the source code k_0, it uses the authentication function $\text{Auth} : K \times S \to M$ to compute the authenticated message $m_0 = \text{Auth}(E, k_0)$ and sends this message to the receiver. The receiver, on the other hand, upon receiving a message $m_0' \in M$ checks whether $\text{Ver}(E, m_0')$ is equal to 1 to verify whether m_0' is a message authenticated using the key E.

Ferruh Özbudak is with the Institute of Applied Mathematics and Department of Mathematics, Middle East Technical University, 06800, Ankara, Turkey. Email:ozbudak@metu.edu.tr

Ali D. Sezer is with the Institute of Applied Mathematics and Department of Mathematics, Middle East Technical University, 06800, Ankara, Turkey. Email:devin@metu.edu.tr

Üstün Yıldırım is with the Institute of Applied Mathematics and Department of Mathematics, Middle East Technical University, 06800, Ankara, Turkey. Email:yildirim.ustun@gmail.com

Manuscript received March 1, 2012; revised April 14, 2012.

II. An N step attack using an authentication oracle

The paper [2] considers the following problem about this setup. Suppose that there is an attacker who has the capacity to have any source authenticated with key E, which is the key that has been fixed by the sender and the receiver and which is assumed to be known only by them. In [2] this capacity of the attacker is modeled using the concept of an "oracle." The attacker's having a message authenticated with the key E is referred to as "querying the authentication oracle;" we will also be using this terminology. The attack takes place as follows: the attacker chooses a source string s_1 and has it authenticated with key E; the result is the authenticated message $m_1 = \text{Auth}(s_1, E)$. Having observed m_1, the attacker chooses the source s_2 and has this authenticated and observes the response $m_2 = \text{Auth}(s_2, E)$. This sequence of operations continues until the attacker has had a total of $N - 1$ sources authenticated and has observed the corresponding authenticated messages. In the Nth step the attacker sends a message m to the sender that has to be different from m_1, m_2,..., m_{N-1}. The goal of the attacker is to choose $(s_1, s_2, ..., s_{N-1}, m)$ so that the probability of $\text{Ver}(E, m) = 1$ is greatest.

A. Deterministic Queries

The sequence of source messages s_1, s_2,... s_{N-1} that the attacker gets authenticated are called "queries." Let us first consider the case when the attacker chooses s_i deterministically as a function of his first $i - 1$ queries and their results. Under this assumption, the only randomness in the problem arises from the randomness of the key E. Therefore, the sample space is merely $\Omega = K$ itself; because K is finite one can use the power set $\mathcal{F} = 2^K$ as the σ algebra and we will do so. P is a probability distribution on K, it is the distribution of the random key E. P is the sole probability measure in this formulation.

First define an expanded control problem with a general initial point. To motivate the definition we will describe a generalized attack associated with the expanded control problem. In the generalized attack, *before the attack begins* the attacker is assumed to have a collection $X_0 \in (S \times M)^l$ of source and authenticated message pairs. The attacker then queries the autentication oracle taking into account the results X_0 he has before the attack began. The source string message pairs he has at the end of the $k - 1^{st}$ step of his attack is

$$X_k = (X_{k-1}, (s_k, \text{Auth}(s_k, E)).$$

Note that if $X_{k-1} \in (S \times M)^l$ then $X_k \in (S \times M)^{l+1}$. Define the following filtration on $(\Omega, \mathscr{F})$:

$$\mathscr{F}_i \doteq \sigma(X_i).$$

$\mathscr{F}_i$ represents the information available to the attacker at step i of the attack. The control s_i of the attacker (the source code he chooses to send to the oracle at step i of his attack) is assumed to be $\mathscr{F}_i$ measurable. This means that the attacker makes use of all of the information available to him before step i to decide his next query.

Remark 1. Note that $\mathscr{F}_i \subset \mathscr{F} = 2^K$. Therefore, it is merely a collection of subsets of K. Being a finite σ algebra, it is defined by its atoms.

For $X = ((m_1, s_1), (m_2, s_2), ..., (m_k, s_k))$ let P_X denote P conditioned on the set

$$\{e : e \in E,\ \mathrm{Auth}(e, s_i) = m_i, i = 1, 2, ..., k\}.$$

In particular, if X is the empty sequence, $P_X = P$.

Define

$$V(X_0, N) \doteq \max_{s_1, s_2, ..., s_{N-1}, M_N} P_{X_{N-1}}(\ \mathrm{Ver}(M_N, E) = 1), \tag{1}$$

The value of our original problem is

$$V(\emptyset, N). \tag{2}$$

Now, by definition a $\sigma(X_{k-1})$ random variable s_k can be represented as $f_k(X_k)$ where f_k is a deterministic function from $(S \times M)^{k+l-1}$ to S, where l is the dimension of X_0. Thus we can write (1) as

$$V(X_0, N) \doteq \max_{f_1, f_2, ..., f_N} P_{X_0}(\ \mathrm{Ver}(M_N, E) = 1),$$

where $f_i : (S \times M)^{l+i-1} \to S$ for $i < N$ and $f_N : (S \times M)^{l+N-1} \to M$.

For any $X_0 \in (S \times M)^l$ and an attack strategy defined by

$$\begin{aligned} g_1 &: (S \times M)^l \to S, \\ g_2 &: (S \times M)^{l+1} \to S, \\ &\vdots \\ g_k &: (S \times M)^{l+k-1} \to S, \\ g_{k+1} &(S \times M)^{l+k} \to M \end{aligned}$$

define

$$V(X_0, k, g_1^{k+1}) = P_{X_k}(\ \mathrm{Ver}(g_{k+1}(X_k), E) = 1).$$

This is the probability that an attack using the strategy g_1^{k+1} is succesful. Note that

$$V(X_0, N) = \max_{g_1^N} V(X_0, N, g_1^N) \tag{3}$$

In (2), condition on the outcome M_1

$$V(\emptyset, N) = \max_{f_1, f_2, f_3, ..., f_n} \mathbb{E}[P(\ \mathrm{Ver}(M_N, E) = 1 |\ \mathrm{Auth}(q_1, E))]$$

By [1, Exercise 1.14, page 230] the conditional probability on the right side of this display is $V((q_1,\ \mathrm{Auth}(q_1, E)), N - 1, f_2^N)$. This is less than or equal to $V(\{(q_1,\ \mathrm{Auth}(q_1, E))\}, N - 1)$ by (3), which gives

$$V(\emptyset, N) \le \max_{f_1} \mathbb{E}[V(\{(q_1,\ \mathrm{Auth}(q_1, E))\}, N - 1)].$$

On the other hand, if $f_2, f_3, ..., f_n$ are set to be the optimizers in the definition of $V(\{(s_1, m_1)\}, N - 1)$ for an arbitrary pair (s_1, m_1) we get

$$V(\emptyset, N) \ge \max_{f_1} \mathbb{E}[V(\{(q_1,\ \mathrm{Auth}(q_1, E))\}, N - 1)].$$

These yield the dynamic programming equation for the present problem:

$$V(X, N) = \max_{f_1} \mathbb{E}[V(X \cup \{(q_1,\ \mathrm{Auth}(q_1, E))\}, N - 1)].$$

B. Random queries

In this section we show that randomizing queries does not improve the optimal probability of success. There is no harm in assuming that the members of M and S are real numbers. Let O_M and O_S be the family of probability distributions on $\mathbb{R}$ that puts all of the probability mass on M and S respectively.

We are interested in an attack that will last N steps. The first $N - 1$ steps will be random authentication queries.

We use the following sample space to model this attack:

$$\Omega = K \times [0, 1]^N$$

The K part of Ω is the set of all keys and $[0, 1]^N$ correspond to the randomness in the first $N - 1$ queries and the spoof attack. Let $U_i : \Omega \to [0, 1]$,

$$U_i(e, (x_1, x_2, x_3, ..., x_n)) = x_i,$$

be the uniformly distributed random variable used in the ith query (or the spoof attack if $i = N$). Note that these numbers are iid uniform and they are completely independent of the key, the authentication scheme and everything else.

Q_1 is a variable taking values in O_S. Q_1 is a distribution and its inverse is well defined. Define $S_1 = Q_1^{-1}(U_1)$. Under P, S_1 is a random variable taking values in S and has distribution Q_1. Define

$$M_1 = \ \mathrm{Auth}(S_1, E)$$

For $i > 1$,

$$\mathscr{F}_{i-1} = \sigma(M_1, S_1, M_2, S_2, ..., M_{i-1}, S_{i-1}),$$

Q_i is an $\mathscr{F}_{i-1}$ measurable function taking values in O_M. Define

$$S_i = Q_i^{-1}(U_i), \quad M_i = \ \mathrm{Auth}(S_i, E). \tag{4}$$

Finally, Q_N is an $\mathscr{F}_{N-1}$ measurable random variable taking values in O_M. Define

$$M_N = O_M^{-1}(U_N).$$

Our control problem is

$$\sup_{Q_1^N} P(\ \mathrm{Ver}(M_N, E) = 1).$$

Now write this as

$$\sup_{Q_1^N} \mathbb{E}[P(\ \mathrm{Ver}(M_N, E) = 1 | \mathscr{F}_0)].$$

Now note that conditioned on $\mathscr{F}_0$, U_i are constants and Q_i in (4) determines S_i as a deterministic function of $(S_1, M_1, S_2, M_2, ..., S_{i-1}, M_{i-1})$. Therefore, for each Q_1^N

$$P(\ \mathrm{Ver}(M_N, E) = 1 | \mathscr{F}_0) \leq V_N$$

It follows that

$$\sup_{U_1^N} \mathbb{E}[P(\ \mathrm{Ver}(M_N, E) = 1 | \mathscr{F}_0)] \leq V_N.$$

The reverse inequality is trivial because every deterministic control is also a random control.

Acknowledgment

Ferruh Özbudak and Ali Devin Sezer were partially supported by TUBITAK under the Grant No. TBAG-109T672.

References

[1] Richard Durrett, *Probability: theory and examples*, second ed., Duxbury Press, Belmont, CA, 1996.
[2] R. Safavi-Naini and P.R. Wild, *Information theoretic bounds on authentication systems in query model*, Information Theory, IEEE Transactions on **54** (2008), no. 6, 2426–2436.

On the use of continued fractions for mutual authentication

Amadou Moctar Kane

Abstract—**The purpose of this paper is to present an improvement of the Needham-Schroder public key protocol. This new protocol will use partial quotients issue from the continued fraction expansion of some irrational numbers to secure the authentication between two principals. We introduce a new approach in the use of pseudo-random numbers, because besides using these numbers to provide uniqueness and timeliness guarantees, we use them to ensure that nobody can guess the identity of the sender. We also keep this new protocol secure against the Lowe attack, without taking the solution suggested by Lowe. This protocol remains fast although we compute some partial quotients during the authentication process.**

Index Terms— **Authentication, continued fraction, cryptography, Needham-Schroeder protocol.**

I. Introduction

The alarming increase in victims of impersonation and the need to secure emerging tools as cloud computing imply the necessity to improve existing authentication protocols. As defined by Menezes et al [11]: entity authentication is the process whereby one party is assured (through acquisition of corroborative evidence) of the identity of a second party involved in a protocol, and that the second has actually participated (i.e., is active at, or immediately prior to, the time the evidence is acquired).

In this paper, it is this definition that we will adopt.

There exits several authentication protocols including: Kerberos [16], Needham-Schroeder [12], Wide Mouthed Frog [3], Woo-Lam [18]. Some protocols are based on others such as Kerberos which is based on Needham-Schroeder.

The Needham-Schroeder protocol has two variants, the first one is based on symmetric cryptography and the second one is based on public key cryptography.

In this paper, we will focus, on the version based on the public key cryptography.

This protocol has been widely studied [5] since 1978 but the greatest improvement was made in 1995, when Lowe [10] proved that this protocol was sensitive to the impersonate attack. The improved version Needham-Schroeder-Lowe seems to be strong until now and currently most studies, on this protocol are oriented on the security proof.

The improvement of the Needham-Schroeder protocol introduced in this paper will be partly based on the fact that the continued fraction expansion of an irrational number is unique.

Also, it will be based on the difficulty of retrieving an irrational number from the sole knowledge of a part of its continued fraction expansion.

Continued Fractions: An expression of the form

$$\alpha = a_0 + \cfrac{b_0}{a_1 + \cfrac{b_1}{a_2 + \cfrac{b_2}{\ddots}}}$$

is called a generalized continued fraction. Typically, the numbers $\mathbf{a_1}, \mathbf{b_1}, \ldots$ may be real or complex and the expansion may be finite or infinite.

We will avoid the use of the continued fraction expansions involving $\mathbf{b_i} = \mathbf{1}$ for most i's. However, in order to simplify our explanation we will use in some cases the classical continued fraction expansion, namely $b_i = \mathbf{1}$ for any i:

$$\alpha = a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \cfrac{1}{\ddots}}}$$

$$\alpha := a_0, a_1, a_2 \ldots$$

In this paper we denote by Γ the combined sets of algebraic irrationals of degree greater than 2 and transcendental numbers. Our algorithm, will use the irrational numbers which are in Γ, but we will avoid the use of transcendental numbers having a predictable continued fraction expansion (some examples of irrational numbers with a given predictable continued fraction expansion are presented in [1],[8]).

To calculate the classical continued fraction expansion of a number α, write down the integer part of α. Subtract this integer part from α. If the difference is equal to 0, stop; otherwise find the reciprocal of the difference and repeat. The procedure will halt if and only if α is rational.

We can enumerate some continued fractions properties:

I. The continued fraction expansion of a number is finite if and only if the number is rational.
II. The continued fraction expansion of an irrational number is unique.
III. Any positive quadratic irrational number α has a continued fraction which is periodic from some point onward, namely a sequence of integers repeat. (Lagrange Theorem)
IV. The knowledge of the continued fraction expansions of α and β cannot determine simply those of $\alpha + \beta$, or $\alpha\beta$.

Continued fractions were widely studied by C. Olds [13] and O. Perron [14], but cryptographic views are not explored by

Manuscript received March 11, 2012.
Amadou Moctar Kane is with the *Département de Mathématiques et de Statistiques, Université Laval, Québec G1V 0A6 Canada (e-mail :* amadou-moctar.kane.1@ulaval.ca).

number theory specialists except in some areas like RSA cryptanalysis.

In addition to the RSA cryptosystem, continued fractions are used to build a stream cipher [6] or to set up a e-cash scheme [7].

This paper is organized as follows: In section 2 we will propose and demonstrate some results concerning continued fractions; in section 3, we will introduce the Needham-Schroeder protocol. In section 4 we present our new protocol, and before the conclusion, we will compare the two algorithms.

II. PRELIMINARIES

The Result 1 and the Result 2 have already been presented in [6, 7]. The Result 2 will exhibit an example of irrational number which we can use in our protocol. And the result 1 shows that the intruder will not succeed if he tries to impersonate the principal in the last attack of *section IV.E*.

Notation

In this paper we shall use the notation $E(X;Y)$ to denote the result of encrypting message plaintext X with key K.

Notation

In this design, we have three principals the first entity Alice (A), the second entity Bob (B), the Intruder (I) and the server (trusted third party) (AS). PK_A will be the public key of Alice, PK_B will be the public key of B, and PK_I will be I's public key. In the same manner SK_A will be A's private key, SK_B will be B's private key and I's private key will be SK_I. The notation I(A) denotes the principal I acting in the role of A.

A message may have several components and message components will be separated by commas. Thus $E(\{N_a, A\}: PK_B)$ denotes that the message components are a nonce N_a and a principal identifier A and this message is encrypted by the key PK_B.

Notation

Let $\alpha \epsilon \Gamma$ such that $a_1, \ldots, a_m, \ldots, a_{m+n}, \ldots$ is the continued fraction expansion of α; m and n are two integers such that $m > 1, n \geq 1$. We denote by δ the vector made with the n partial quotients following the m first partials quotients in the continued fraction expansion.

Result 1. It is not possible to find α out of the knowledge of δ.

Proof. Let $\alpha \epsilon \Gamma$. We suppose that we know a given part $a_{m+1}, \ldots, a_{m+n}$ of α's continued fraction expansion. Can we find α with the knowledge of these n partial quotients?

The answer is negative, because there exists an infinite number of irrationals with these same partial quotients.

For instance we can exhibit infinitely many irrational numbers α_ρ which are different from α and which have the property that $a_{m+1}, .., a_{m+n}$ appears as a sequence of n consecutive partial quotients. As a matter of fact, when θ is an irrational number, it suffices to consider any sequence of m integers $(r_1, r_2, \ldots, r_m)$ and to define α_ρ to be

$$\alpha_\rho = r_1 + \cfrac{1}{\ddots_{r_m} + \cfrac{\ddots_1}{a_{m+1} + \cfrac{1}{\ddots_{a_{m+n-1}} + \cfrac{\ddots_1}{a_{m+n} + \frac{1}{\theta}}}}}$$

Result 2. For an integer r such that $r \geq 3$ and a real algebraic number A ($A > 1$), the number $\sqrt[r]{\log_e(A)}$ is transcendental.

Proof .Assume that A is a real algebraic number such that $A > 1$, then $\log_e(A)$ is transcendental number by Corollary 3.6 of [2].

If we suppose that $X = \sqrt[r]{\log_e(A)}$ is an algebraic number, then X^r is a algebraic number, which is absurd because $X^r = \log_e(A)$ and $\log_e(A)$ is transcendental.

Remark

The irrational number $\sqrt[r]{\log_e(A)}$ used in this paper is not a standard which we impose. It is an example which we choose in order to illustrate our scheme.

Remark

Due to the rounding errors, the use of continued fractions must obey some rules. For example Alice and Bob must agree on their multiple precision library, on the rounding error, on the software used and on the architecture.

III. THE NEEDHAM-SCHROEDER PROTOCOL

A. The Needham-Schroeder Protocol

As defined in [12], the public key protocol consists on the following seven steps:

Step 1: A→ AS

The exchange opens with A consulting the authentication server to find B's public Key.

Step 2: AS responds with: $E(\{PK_B, B\}: SK_{AS})$.

Where SK_{AS} is the authentication server's secret key, PK_B is B's public key and B is B's identity.

Step 3: A sends to B the following $E(\{N_a, A\}: PK_B)$.

This step is for the communication with B to be initiated. This message, which can only be understood by B indicates that someone purporting to be A wishes to establish communication with B. B decrypts the message with his private key and then finds the nonce N_a chosen by A.

Step 4 & 5: B finds A's public key (PK_a) with steps similar to 1 & 2.

Step 6: At this point B return the nonce Na, along with a new nonce N_b, to A, encrypted with A's public key ($E(\{N_a, N_b\}: PK_A)$).

Step 7: At the end, A returns the nonce N_b to B, encrypted with B's public key.

The protocol can be described as follows:

1. A →AS : A, B;
2. AS → A : $E(\{PK_B, B\}: SK_{AS})$;
3. A → B : $E(\{N_a, A\}: PK_B)$;
4. B → AS : B, A;
5. AS → B : $E(\{PK_A, A\}: SK_{AS})$;
6. B → A : $E(\{N_a, N_b\}: PK_A)$;
7. A →B : $E(\{N_b\}: PK_B)$.

B. The Needham-Schroeder-Lowe Protocol

In [10], Lowe shows that an attack on the protocol allows an intruder I to impersonate another agent A to set up a false session with B. In this attack, we can ignore the interaction with the server because this does not have a real influence on

this attack. The attack involves two simultaneous runs of the protocol: in run 1, A establishes a valid session with I; and in run 2, I impersonates A to establish a fake session with B.

In step 1.3, A starts to establish a normal session with I, sending him a nonce N_a.

In step 2.3, the intruder impersonates A to try to establish a false session with B, sending it the nonce N_a obtained in the previous message.

B responds in the message 2.6 by selecting a new nonce N_b, and trying to return it along with N_a, to A. The intruder therefore forwards the message to A in the step 1.6.
A decrypts the message to obtain N_b, and returns this to I in message 1.7.

I can then decrypt this message to obtain N_b which he returns to B in message 2.7. Hence B believes that A has correctly established a session with him.

This attack can be described as follows:

1.3 A →I : $E(\{N_a, A\}: PK_I)$;
2.3 I(A) → B: $E(\{N_a, A\}: PK_B)$;
2.6 B →I(A) : $E(\{N_a, N_b\}: PK_A)$;
1.6 I → A $E(\{N_a, N_b\}: PK_A)$;
1.7 A → I $E(\{N_b\}: PK_I)$;
2.7 I(A) → B $E(\{N_b\}: PK_B)$.

In the same paper Lowe showed that it is easy to change the protocol so as to prevent the attack; for this purpose he included the responder's identity in message 6 of the protocol.

Hence, the step 2.6 of the attack would become $E(\{B, N_a, N_b\}: PK_A)$ and the intruder cannot successfully replay this message in the step 1.6.

IV. Our Contribution

The improvement proposed here is based on the work of Lowe, since we have solved the previous attack without his solution described above.
As for the Needham-Schroeder algorithm we suppose that communications are carried on an insecure channel.
We denote by $FC(X, Y)$ the first ten partial quotients issue from the continued fraction expansion of the irrational number X and where Y is a vector of ten b_i 's (we recall that the b_i 's are used during the computation of the generalized continued fraction).
We denote by $FC'(X, Y)$ the nine partial quotients following the first one in the continued fraction expansion of X (the first partial quotient is ignored in the authentication protocol).
We denote by Y_A, Y_B, or Y_I the vectors used in the computation of the generalized continued fraction as described in the introductory paragraph.
Y_A is computed as follows:

- We apply the hash function SHA1 on A's public key and we obtain $\text{sha1}(PK_A)$.
- We divide the string obtain in the previous step in ten part, and we obtain $Y_A = (b_1, b_2, \ldots, b_{10})$.

Y_B is computed like Y_A but we apply the hash function on B's public key instead of A ($\text{sha1}(PK_B)$).
Y_I is obtained in the same manner as we apply the hash function on I's public key ($\text{sha1}(PK_I)$).
We denote by $Y_u Y_v$ the concatenation of Y_u and Y_v, for example, if $Y_u = (a_1, \ldots, a_{10})$ and $Y_v = (b_1, \ldots, b_{10})$ then $Y_u Y_v = (a_1 b_1, \ldots, a_{10} b_{10})$.
The vector $Y_u Y_v$ will be used in the computation of the partial quotients if the sender of the nonce is u and the receiver is v. For example, if the sender of the nonce is A and the receiver is B, then B will use the vector $Y_A Y_B$ to compute the partial quotients.

A. The new protocol

The new protocol is conducted in accordance with the following steps:
Step 1:
A chooses randomly a nonce N_a, encrypt it with B's public key (PK_B) and sends it to B.
Step 2:
B calculates the first 10 partial quotients $FC(\sqrt[3]{\log_e N_a}; Y_A Y_B)$, ignores the first partial quotient, composes a message with the 9 remaining partial quotients $(FC'(\sqrt[3]{\log_e N_a}; Y_A Y_B))$, adds a nonce N_b (chosen randomly) encrypts the message with the public key of A and sends it to A.
Step 3:
A computes $FC'(\sqrt[3]{\log_e N_a}; Y_A Y_B)$ and verifies that the nine partial quotients received from B are correct. If these partial quotients are correct, A computes the first 10 partial quotients $FC(\sqrt[3]{\log_e N_b}; Y_B Y_A)$, ignores the first partial quotient and sends the 9 remaining in a message encrypted with B's public key.
The new protocol can be described as follows:
B →A :" Hi I am B";
A → B : $E(\{N_a\}: PK_B)$;
B → A : $E(\{FC'(\sqrt[3]{\log_e N_a}; Y_A Y_B), N_b\}: PK_A)$;
A →B : $E(\{FC'(\sqrt[3]{\log_e N_b}; Y_B Y_A)\}: PK_B)$.
Remark:

I. We suppose that we are in the case of an identity-based cryptosystem in which KC issues a private key to a registering user and uses the user's identity as his public key.
II. The status of the key (revoked or not) will depend on the security given by identity-based cryptosystem.
III. The first partial quotient is ignored because it does not change regardless the chosen b_i.
IV. We use the third root of log because it corresponds to the example exhibited in result 2.
V. We conjecture that the distribution of partial quotients in the continued fraction expansion is indistinguishable by all polynomial-time statistical tests from the uniform distribution of integers in the interval $[S; P]$. S and P will be determined by the value of b_i's (see [6]).

B. Attack using Lowe's method.

Alice wants to talk to the intruder I, hence she chooses N_a and sends $(\{N_a\})$ encrypted with I's public key.

Step 2:
We recall that I (A) is the attacker who tries to impersonate A. I (A) decrypts the message received from A with its private key and transfers to B N_a encrypted with the public key of B.
Step 3:
B computes $(FC(\sqrt[3]{\log_e N_a}, Y_A Y_B))$, chooses a nonce N_b and sends $\{FC'(\sqrt[3]{\log_e N_a}, Y_A Y_B)), N_b\}$ to A after having encrypted it with A's public key (PK_A).
Step 4:
I (A) cannot decrypt the message encrypted with the public key of A, then he transfers the message to A.
Step 5:
To check if $FC(\sqrt[3]{\log_e N_a}, Y_A Y_B))$ is correct, A computes $FC'(\sqrt[3]{\log_e N_a}, Y_A Y_I))$ since the nonce N_a was sent to I. The $FC'(\sqrt[3]{\log_e N_a}, Y_A Y_I))$ will not match with $FC'(\sqrt[3]{\log_e N_a}, Y_A Y_B))$ since the first one was calculated with Y_I and the second one was computed with Y_B.
A can then conclude that an attack is underway.
Summary:

1.3 A →I : $E(\{N_a\}: PK_I)$

2.3 I(A) → B: $E(\{N_a\}: PK_B)$

2.6 B →I(A): $E(\{FC'(\sqrt[3]{\log_e(N_a)}, Y_A Y_B)), N_b\}: PK_A)$

1.6 I → A: $E(\{FC'(\sqrt[3]{\log_e(N_a)}, Y_A Y_B)), N_b\}: PK_A)$

1.7 A computes and verifies if $FC'\left(\sqrt[3]{\log_e(N_a)}; Y_A Y_I\right) \neq FC'\left(\sqrt[3]{\log_e(N_a)}; Y_A Y_B\right)$.

Remark

The usefulness of continued fractions is noticeable at this level because without continued fractions the Lowe attack would be effective on this algorithm.

C. *Example of the new Authentication Protocol*

Before sending any message Alice and Bob will calculate the following elements in order to speed up the authentication protocol.
Let's suppose that Alice's public key is: PK_A =12345678910111213, then we apply the hash function SHA1 on that string and we obtain SHA1(PK_A)= A3 BF AE 33 E7 3F 0C A318 0D 8B FA 5C AB EA 4E F1 39 C3 6D (in hexadecimal).
The vector Y_A used in the computation of the generalized continued fraction will be Y_A=(b_{1A}=A3BF=41919, b_{2A}=AE33=44595, b_{3A}= E73F=59199, b_{4A}=0CA3=3235, b_{5A}=180D=6157, b_{6A}=8BFA=35834, b_{7A}=5CAB=23723, b_{8A}=EA4E=59982, b_{9A}=F139=61753, b_{10A}=C36D= 50029).
Let's suppose that Bob's public key is: PK_B = 9876543210, then we obtain after applying the hash function SHA1 on the public key,SHA1(PK_B)= 9C D6 56 16 96 00 15 7E C1 72 31 DC F0 61 3C 94 93 2E FC DC.
The vector Y_B used in the calculation of the generalized continued fraction will be Y_B= (b_{1B}=9CD6=40150, b_{2B}=5616=22038, b_{3B}= 9600=38400, b_{4B}= 157E=5502, b_{5B}= C172=49522, b_{6B}=31DC=12764, b_{7B}= F061=61537,b_{8B}=3C94=15508, b_{9B}= 932E=37678, b_{10B}=FCDC=64732).
The intruder public key will be: PK_I= 76543210123, hence SHA1(PK_I)= E0 68 09 F6 BB 62 9F 10 F8 48 A0 9A A5 3F E1 5C 0E D3 A5 2D.
The vector Y_I used in calculation of the generalized continued fraction will be Y_I= (b_{1I}=E068=57448, b_{2I}=09F6=2550, b_{3I}=BB62=47970, b_{4I}=9F10=40720, b_{5I}=F848=63560, b_{6I}=A09A=41114, b_{7I}= A53F=42303, b_{8I}=E15C=57692, b_{9I}= 0ED3=3795, b_{10I}=A52D=42285).

The choice of the vector Y_A, Y_B, or Y_I used in the computation of the generalized continued fraction will depend on the origin of the challenge. For example, if Bob has to respond to a challenge sent by Alice, then the vector used will be $Y_A Y_B$, if Alice sends a challenge to the intruder, then the vector used will be $Y_A Y_I$, and if the intruder sends a challenge to Bob the vector used by Bob will be $Y_I Y_B$. Below, in table I, we present the example of the new protocol.

TABLE I
EXAMPLE OF THE NEW AUTHENTICATION PROTOCOL

Alice	*Intruder*	*Bob*
Chooses randomly N_a, N_a=456576890 and Sends $E(N_a : PK_B)$	Sees $E(N_a : PK_B)$	Receives $E(N_a : PK_B)$
		Decrypts $E(N_a : PK_B)$ with SK_B
Computes $FC((\sqrt[3]{\log_e(N_a)}, Y_A Y_B$ = (a_1=2, a_2=4106694278, a_3=11096573017, a_4=285849649, a_5=455761744, a_6=3431553022, a_7=2199137734, a_8=8018839091, a_9=4822767116, a_{10}=4987704341).		Computes $FC((\sqrt[3]{\log_e(N_a)}, Y_A Y_B))$ = (a_1=2, a_2=4106694278, a_3=11096573017, a_4=285849649, a_5=455761744, a_6=3431553022, a_7=2199137734, a_8=8018839091, a_9=4822767116, a_{10}=4987704341).
Receives E(a_2,a_3,a_4,a_5,a_6,a_7,a_8,a_9,a_{10}, N_b: PK_A).	Sees E(a_2,a_3,a_4,a_5,a_6,a_7,a_8,a_9,a_{10}, N_b: PK_A)	Chooses randomly N_b, N_b=4567387 and sends E(a_2,a_3,a_4,a_5,a_6,a_7,a_8,a_9,a_{10}, N_b: PK_A)
Decrypts with SK_A E(a_2,a_3,a_4,a_5,a_6,a_7,a_8,a_9,a_{10}, N_b: PK_A). Verifies that a_2,..,a_{10} are correctly calculated.		$FC(\sqrt[3]{\log_e(N_b)}, Y_B Y_A)$ = (c_1=2, c_2=2981639062, c_3=9232230473, c_4=578035971, c_5=9394835548, c_6=6724620718, c_7=15782459451, c_8=2048625312, c_9=3728834053, c_{10}=7375783858)
Computes $FC(\sqrt[3]{\log_e(N_b)}, Y_B Y_A)$ = (c_1=2, c_2=2981639062,	Sees E(c_2,c_3,c_4,c_5,c_6,c_7,c_8,c_9,c_{10}; PK_B).	Receives E(c_2,c_3,c_4,c_5,c_6,c_7,c_8,c_9,c_{10}; PK_B).

c_3=9232230473, c_4=578035971, c_5=9394835548, c_6=6724620718, c_7=15782459451, c_8=2048625312, c_9=3728834053, c_{10}=7375783858) and sends $E(c_2,c_3,c_4,c_5,c_6,c_7,c_8,c_9,c_{10}; PK_B)$.		
		Decrypts $E(c_2,c_3,c_4,c_5,c_6,c_7,c_8,c_9,c_{10}; PK_B)$ with SK_B. Verifies that $c_2,..,c_{10}$ are correctly calculated.

D. Example of the Lowe's attack in the new protocol

This attack is detailed below, in table II.

TABLE II
EXAMPLE OF THE LOWE'S ATTACK IN THE NEW PROTOCOL

Alice	*Intruder*	*Bob*
Chooses randomly N_a, N_a=456576890 and Sends $E(N_a : PK_I)$	Receives $E(N_a : PK_I)$	
	Decrypts $E(N_a : PK_I)$ with SK_I and sends $E(N_a : PK_B)$ to Bob	Decrypts $E(N_a : PK_B)$ with SK_B
Computes $FC(\sqrt[3]{\log_e(N_a)}, Y_A Y_I)$ = (a'_1=2, a'_2=4106666894, a'_3= 5059764476, a'_4=309131866, a'_5=481976420, a'_6=3404891394, a'_7=3070712358, a'_8=4494633197, a'_9=30367444710, a'_{10}=3998170756).		Computes $FC(\sqrt[3]{\log_e(N_a)}, Y_A Y_B)$ (a_1=2, a_2=4106694278, a_3=11096573017, a_4=285849649, a_5=455761744, a_6=3431553022, a_7=2199137734, a_8=8018839091, a_9=4822767116, a_{10}=4987704341).
Receives $E(a_2,a_3,a_4,a_5,a_6,a_7,a_8,a_9,a_{10}, N_b: PK_A)$.	Receives $E(a_2,a_3,a_4,a_5,a_6,a_7,a_8,a_9,a_{10}, N_b: PK_A)$ and transfers it to Alice	Chooses randomly N_b, N_b=4567387 and sends $E(a_2,a_3,a_4,a_5,a_6,a_7,a_8,a_9,a_{10}, N_b: PK_A)$
Decrypts with SK_A $E(a_2,a_3,a_4,a_5,a_6,a_7,a_8,a_9,a_{10}, N_b: PK_A)$. Verifies if $a_2=a'_2,..,a_{10}=a'_{10}$ and then concludes that someone is trying to impersonate her.		

E. Example of attack (using the lack of identity)

This attack is detailed below, in table III.

TABLE III
EXAMPLE OF ATTACK (USING THE LACK OF IDENTITY)

Alice	*Intruder*	*Bob*
	Sends to Alice (Hi I am Bob).	
Chooses randomly N_a, N_a=456576890 and Sends $E(N_a : PK_B)$	Receives $E(N_a : PK_B)$.	
	Transfers $E(N_a : PK_B)$ to Bob saying (I am Intruder).	Decrypts $E(N_a : PK_B)$ with SK_B.
Computes $FC(\sqrt[3]{\log_e(N_a)}, Y_A Y_B)$ = (a'_1=2, a'_2=4106694278, a'_3=11096573017, a'_4=285849649, a'_5=455761744, a'_6=3431553022, a'_7=2199137734, a'_8=8018839091, a'_9=4822767116, a'_{10}=4987704341).		Computes $FC(\sqrt[3]{\log_e(N_a)}, Y_I Y_B)$ = (a_1=2, a_2=234855306, a_3=4078278518, a_4=3802145145, a_5=4630995005, a_6=24219050134, a_7=20475451123, a_8=3813152404, a_9=286637470, a_{10}=6468778119).
Receives $E(a_2,a_3,a_4,a_5,a_6,a_7,a_8,a_9,a_{10}, N_b: PK_A)$.	Decrypts $E(a_2,a_3,a_4,a_5,a_6,a_7,a_8,a_9,a_{10}, N_b: PK_I)$ and transfers to Alice $E(a_2,a_3,a_4,a_5,a_6,a_7,a_8,a_9,a_{10}, N_b; PK_A)$	Chooses randomly N_b, N_b=4567387 and sends $E(a_2,a_3,a_4,a_5,a_6,a_7,a_8,a_9,a_{10}, N_b: PK_I)$
Decrypts with SK_A $E(a_2,a_3,a_4,a_5,a_6,a_7,a_8,a_9,a_{10}, N_b: PK_A)$. Verifies if $a_2=a'_2,..,a_{10}=a'_{10}$ then concludes that someone is trying to impersonate her.		

Remark:
In this last exchange, the intruder is not able to find the correct $a'_2,..,a'_{10}$ because he cannot find N_a (by Result 1) and he is not able to guess $a'_2,..,a'_{10}$ in the sole knowledge of $a_2,..,a_{10}$.

F. Others attacks

Replay, Interleaving, and Reflection attack

The nonces play an essential role in this algorithm, they are chosen randomly ($\in_R$), and they change with each message since the principal chooses a new nonce at each exchange. Thus, it is impossible to have a replay, an interleaving or a reflection attacks. We can add that the calculations of the partial quotients are based on the sender and the receiver of the challenge, which is a kind of a signature.

The forced delay attack

This attack does not have a real influence on this algorithm because there is no timestamp, so the behaviour of the principals will be the same even if someone intercepts the message and relays it later.

Remark

We recommend the use of the generalized continued fraction instead of the classical continued fraction; because the classical continued fraction produces a several partial quotients with only one digit [9], while the partial quotients obtained from some generalized continued fraction seems to be indistinguishable by all polynomial-time statistical tests from the uniform distribution of integers [6].

V. Comparison with Needham-Schroeder-Lowe

A. Comparison

The Needham-Schroeder-Lowe protocol used nonces where we use continued fraction expansions and nonces, so it is clear that our algorithm is more expensive in terms of computation time, however we strongly believe that our scheme is more secure than the algorithm of Needham-Schroeder-Lowe. Our protocol increases the level of security with the introduction of continued fraction and if we consider that the calculation are done in two phases, the preparation phase can reduce the time needed for the authentication itself.

Similarly in the Needham-Schroeder-Lowe protocol, if the intruder sees one of the two nonces (N_a or N_b), it is risky to use this part of secret in the symmetric encryption key while in our protocol the properties of continued fractions allow to use this nonce without any detrimental effect on the security of the symmetric encryption. We recall that the knowledge of the continued fraction expansions of α and β cannot determine simply those of $\alpha + \beta$, or $\alpha\beta$ which imply that N_aN_b can be used as seed for the symmetric encryption as defined in [6]. Hence, we can add that this protocol introduced some aspects of the zero knowledge system in this algorithm, because seeing the partial quotients cannot give any idea of the composition of the nonce (see TABLE III (Example of attack using the lack of identity) & Result 1).

We have greatly simplified the Needham-Schroder-Lowe protocol, because in addition to the number of steps which we have reduced, we also removed the identities of the principals in messages. It is a great progress to remove the identity of the principal in the protocol because if the secret key of the principal A fell into the wrong hands, the attacker could use this key to impersonate A, while in the new protocol, the intruder will not be able to identify the other principal.

Let's suppose that the Intruder I has the secret key of A and he intercepts these following messages ($E(N_a: PK_B)$;
$E\ (\{FC'(\sqrt[3]{log_e N_a}; Y_AY_B), N_b\}: PK_A)$;
$E\ (\{FC'(\sqrt[3]{log_e N_b}; Y_BY_A)\}: PK_B)$.

He will not be able to decrypt ($E(N_a : PK_B)$ and $E(\{FC'(\sqrt[3]{log_e N_b}; Y_BY_A)\}: PK_B)$. He will be able to decrypt $E\ (\{FC'(\sqrt[3]{log_e N_a}; Y_AY_B), N_b\}: PK_A)$ with SK_A, however he cannot know who is the recipient of the message in order to continue the authentication.

B. Efficiency analysis

Let $b_T = \max(b_i)\ \forall\ b_i \in (Y_AY_B \cup Y_BY_A \cup Y_AY_I \cup Y_IY_A \cup Y_BY_I \cup Y_IY_B)$ and $t_1 = \max(log_2(\sqrt[3]{\log_e N_a}), log_2(\sqrt[3]{\log_e N_b}))$ we evaluate the cost of calculating a partial quotient to be $O(\delta^{1+\epsilon})$ where $\delta = \max(log_2(t_1), log_2(b_T))$ and $\epsilon \in]0,1[$.Hence, we can conclude that the time needed for computing partial quotients is low.

VI. Conclusion

In this paper, we presented a mutual authentication protocol which introduces the use of continued fractions in authentication schemes. We also improve the Needham-Schroeder-Lowe protocol by eliminating the identity of the principal in the authentication messages.

The rounding errors presents in the computation of the partial quotients could be an advantage, since the absence of agreement on the rounding errors between the principal and the intruder will increase the probability of failure of any attack.

It could be interesting to see in the future, which properties of continued fractions may help to reduce the cost of partial quotients calculations.

Due the computer limitation, the use of irrational numbers can be theoretical, but as proved in [6], we can use an approximation of irrational numbers.

References

[1] Beeler M., Gosper R.W., and Schroeppel, R. Hakmen, "MIT Artificial intelligence memo 239", Feb. 29, 1972.
[2] E.B. Burger and R. Tubbs, "Making transcendence transparent: An intuitive approach to classical transcendental number theory", Springer-Verlag, 2004.
[3] Michael Burrows, Martin Abadi, and Roger Needham, "A log_eic of authentication" Technical Report 39, Digital Systems Research Center, 1989.
[4] John Clark and Jeremy Jacob, "A survey of authentication protocol literature", 1997.
[5] D. E. Denning and G. M. Sacco. Timestamps in key distribution protocols. *Communication of the ACM*, 24(8):533-536, August 1981.
[6] Amadou Moctar Kane, "On the use of Continued Fractions for Stream Ciphers" In Proceedings of Security and Management 2009, Las Vegas, USA.
[7] AmadouMoctar Kane, "On the use of continued fractions for electronic cash" in International Journal of Computer Science and Security Vol: 4 Issue: 1 Pages: 136-148, (2010).
[8] Donald E. Knuth, "The art of computer programming Volume 2: Seminumerical algorithms (3rd Edition)", Addison-Wesley, 1997.
[9] P. Levy, "Sur les lois de probabilité dont dépendent les quotients complets et incomplets d'une fraction Continue", Bull. Soc. Math. 57 (1929) 178-194.
[10] G. Lowe, "Breaking and Fixing the Needham-Schroeder Public-Key Protocol using FDR", in: Proc. TACAS'96, Springer LNCS 1055, 1996, pp. 147–166.

[11] A.J. Menezes, P.C. van Oorschot, and S.A. Vanstone, "*Handbook of applied cryptography*", CRC Press Series on Discrete Mathematics and its Applications., CRC Press, Boca Raton, FL, 1997.
[12] R. Needham, M. Schroeder, "Using Encryption for Authentication in Large Networks of Computers", Comm. ACM 21 (12) (1978) 993–999.
[13] C. D. Olds, "Continued Fractions", Random House, 1963.
[14] Oskar Perron, "Die Lehre Von Den Kettenbrüchen", 3rd ed. (1954).
[15] Bruce Schneier, "Applied cryptography (2nd ed.): protocols, algorithms, and source code in C", John Wiley & Sons, Inc., (1995).
[16] J. G. Steiner, B. C. Neuman, and J. I. Schiller, Kerberos: An authentication service for open network systems. In *Proceedings of the Winter 1988 Usenix Conference*, pages 191-201, (1988).
[17] Michael J. Wiener, "Cryptanalysis of short RSA secret exponents", IEEE Transactions on Information Theory, 36, 553-558, 1990.
[18] Thomas Y.C. Woo, Simon S. Lam, "Authentication for Distributed Systems," *Computer*, vol. 25, no. 1, pp. 39-52, (1992).

Formalization of Blind Signature using the Inductive Method

N. S. Miramirkhani and R. Jalili

Abstract— **Verification of a security protocol can be done using model checking or theorem proving approach. Unlike model checking, theorem proving methods can prove security properties of a protocol under an unlimited number of agents participating in the protocol and interleaving an infinite number of protocol sessions. But these methods usually suffer from not being completely automatic. However, the Inductive Method is a pure theorem proving approach that has been successful in analyzing many classic to real world protocols such as SET. This method has been evolved and extended during years to be able to verify more complicated protocols such as e-commerce, smart cards, non-repudiation and multicast based protocols. Blind signature is an advanced cryptographic primitive vastly used in protocols with a major concern on anonymity such as e-voting protocols. Using the great potential of the Inductive Method in formalizing new concepts, we have extended the Inductive Method to make it support modeling this concept. Moreover, we have proved that our model meets the desired requirements and preserves the properties of already defined elements of the Inductive Method.**

Index Terms— **Formal Verification, Inductive Method, Blind Signature, Theorem Proving**

I. Introduction

THE two main approaches to the formal verification of systems and especially security protocols, are based on model checking and theorem proving . These two approaches originate from the two different insights into the proofs in a formal system. Each formal system has a syntactic and semantic structure and a deduction system.

In general, a model checking problem is a problem of verifying that a formula Φ holds in a model M: $M \models \Phi$, where M represents the protocol model and is usually finite, and Φ is the desired security property expressed in a temporal logic. Model checking techniques are based on the exhaustive state traversal of the model, and are often automatic and always terminate. The model in these techniques is often restricted to a finite state transition system, but generally the problem of model checking is not limited to finite transition systems.

This work was supported in part by Amnafzar Gostar Sharif Co.

N. S. Miramirkhani is a Senior Penetration Tester at Consulting Group of Amnafzar Gostar Sharif Co, Tehran, Iran. (e-mail: miramirkhani@amnafzar.com).

R. Jalili is an Associate Professor in the Department of Computer Engineering at Sharif University of Technology, Tehran, Iran. (e-mail: jalili@sharif.edu).

A theorem proving problem, on the other hand, is a problem of checking the validity of a formula Φ, that is, Φ must hold in every model. The logic is often much more expressive than propositional temporal logic often used in model checking, and the properties over infinite domains can be easily expressed. A theorem proving problem is solved by finding a proof of the formula (which is then called a theorem) in a proof system. Since most of the formal systems are undecidable, theorem proving tools are not automatic and they usually need the interaction of an expert user.

The Inductive Method is one of the notable works in the verification of systems relying on theorem proving. This method supported by the interactive theorem prover Isabelle/HOL is used to verify the security properties of different classic [3], [4] and real world protocols such as SET [12]-[14]. Its main underlying idea is that simple mathematical induction suffices to model security protocols and reason about their goals.

During the last decade, this method has been evolved and extended in different ways to be able to deal with different security protocols and more advanced goals. Since blind signature is an advanced cryptographic concept which is used in different security protocols such as e-voting protocols to preserve privacy of agents, we have found the opportunity of extending the Inductive Method to support this concept. Moreover, we prove a series of theorems which show that our model meet the desired requirements and expected behaviors and preserves the properties of already defined components of the Inductive Method.

Our idea in this paper is to briefly review the extensions to the Inductive Method and to motivate our augmentation of the Inductive Method with a blinding signature extension. Then we will have a review on the key concepts of the method used in the following sections. After that, we will see our contributions in the extension of the inductive method towards supporting formalization of the blind signature schema. We will also prove that our model is compatible with the threat model and already defined concepts of the method.

Isabelle/HOL is a free interactive theorem prover released under the revised BSD license. Proofs of this study are mechanized by Isabelle/HOL, but for the sake of simplicity, theorems, lemmas and definitions are presented in a simplified syntax.

II. RELATED WORK

The foundations of the Inductive Method are due to Paulson [1]. He applied the method to some classical protocols such as Needham-Schroeder, Otway-Rees and Yahalom [3], [4]. Since then, the inductive method has been extended in various aspects in order to be able to model other security protocols.

The method was first extended with the treatment of timestamps which allows modeling and verifying security properties of timestamp-based protocols such as the BAN Kerberos, Kerberos IV and V [5]-[7].

Later a third event to model message reception was introduced. Since the event of message reception [8] is not forced to occur, this models a network that is entirely controlled by an active Spy who can intercept certain messages and prevent their delivery. Moreover, the reception event allows the formalization of any agent's knowledge [9]. Introducing message reception provided a more realistic formalization of security goals and a higher level of formal expressiveness. Using this concept, protocol model for BAN Kerberos, Kerberos IV and V was updated and expressed in a simpler form.

By formalizing smartcards and their interactions with card owners, e-commerce protocols such as Shoup-Rubin could be verified [10].

After that, the threat model of the inductive model was changed to support formalization of accountability protocols like Zhou-Gollmann's non-repudiation protocol and Abadi's certified e-mail protocol [11]. Finally, by maturing this method, the e-commerce protocol SET was verified [12]-[14].

Recently, another extension to the Inductive Method has been introduced that makes it enable to reason about the multicast-based security protocols.

The above researches confirm the great potential of the inductive method to formalizing new concepts. As blind signature is an advanced cryptographic primitives vastly used in protocols with a major concern on anonymity, we decided to provide its formalization in the Inductive Method.

III. INDUCTIVE METHOD

The Inductive Method is a pure theorem proving method which uses simple mathematical induction to model security protocols and reason about their goals. A key concept here is the trace, a list of network events occurring while an unbounded population of agents is running a protocol.

Traces are defined inductively and so is the set of all traces admissible under a specific protocol. This set represents the formal protocol model. Proofs can be carried out by induction on a generic trace of the model, with mechanical support offered by the theorem prover Isabelle [2]. They establish trace properties representing goals of the underlying protocol.

In the following subsections, we will review briefly some key concepts of the method used in our model or theorems:

A. The Structure of Cryptographic Keys

The free type *key* is introduced to formally represent all types of cryptographic keys. The function *invkey* is defined over the set of keys and leaves a key unaltered in case it is symmetric; otherwise, it turns the key into its corresponding asymmetric half.

In the asymmetric-cryptography setting, each agent is endowed with the asymmetric key pair public and private keys. These keys are correspondingly modeled by the *priK* and *pubK* functions from the set of agents to the set of keys.

The set *symKeys* formalizes symmetric keys. According to its definition, a key is an asymmetric key if and only if it has the same decryption and encryption keys [1]:

$$\text{Set key}: \ symKeys = \{key\ k.\ K = invKey(k)\} \tag{1}$$

B. Agents and Threat Model

A security protocol is a sequences of steps designed to achieve certain goals at the time of its completion. Broadly speaking, security protocols aim to provide secure communication through an unsecure network. The network may contain a *Spy* who can intercept all messages and prevent their delivery. He can also tamper with them by decomposing concatenated messages and opening up ciphers sealed with keys he knows. Then, he can use the learnt message components to form new messages at will by concatenation and encryption. He can also collude with some agents and knows their long term secrets. However the capabilities of the *Spy* are specified in the threat model in which the protocol is studied.

Steps of a protocol are executed by the agents who run the protocol. Three types of agents are defined in the Inductive method: *Server*, *Spy* and *Friend i*. *Server* models the trusted third party required in most symmetric cryptography protocols, *Spy* indicates the adversary in the environment and *Friend i* formalizes an unlimited number of friendly agents indexed by natural numbers *i*.

The threat model of the Inductive Method is an extension of Dolev-Yao's threat model. The *Spy* in this threat model, in addition to the capabilities of a Dolev-Yao's adversary can collude with a set of compromised agents. The set of compromised agents is specified by the set *bad*. Definition of the *bad* set is as follows:

$$\text{Set agent}: bad = \{Spy\} \cup \{agent\ a.\ a \neq Server\} \tag{2}$$

Since the *Spy* knows his own long-term secrets, he belongs to this set. In addition, Trusted servers are always assumed to be uncompromised, namely not to belong to the *bad* set.

C. Messages

Running each protocol step requires the transmission of a message, possibly encrypted, between the peers. Messages may include various components such as cryptographic keys, timestamps and ciphers.

In the Inductive Method, seven types of messages are defined: agent names, guessable numbers (modeling

timestamps), random numbers (modeling nonces), cryptographic keys, hashed messages, concatenated messages and ciphers. While the first four message types are the basic types, the three later types are recursive constructors.

An important point about encrypted messages is that if two ciphers are equal, then the corresponding clear texts would be equal too and the corresponding encryption keys are also the same. Message types are specified as follow:

```
Type msg = Agent agent
         | Number natural
         | Nonce natural
         | Key key
         | Hash msg
         | {msg, msg}
         | Crypt key msg
```
(3)

D. Message Operators

The three operators *parts*, *synth*, and *analz* are introduced to manage sets of messages and implementing the *Spy*'s capabilities. The operator *parts* extracts all components from a given set of messages by decomposition and decryption. The operator *synth* formalizes message creation from known components, and the *analz* operator formalizes the act of breaking up messages into their components by decomposition and decryption where the decryption key is available. Inductive definition of the *analz* operator is defined as follows:

```
Inductive Set : analz :: Set msg => Set msg
 for H :: Set msg
   X ∈ H ==> X ∈ analz H
 | {|X,Y|} ∈ analz H ==> X ∈ analz H
 | {|X,Y|} ∈ analz H ==> Y ∈ analz H
 | Decrypt : [|Crypt K X ∈ analz H; Key (invKey K) ∈ analz H|]
       ==> X ∈ analz H
```
(4)

It can be observed that the *Decrypt* rule can obtain the clear text of a cipher in the message set H only if its decryption key belongs to H. On the other hand, based on this definition, encryption is assumed to be perfect.

E. Traces and Events

A history of the network traffic can be represented by the list of the events that occurred throughout that history. Such a list is called a trace. The set of all possible traces of unbounded length is a formal model of the protocol.

The Inductive Method allows for three types of events formalizing the acts of sending, noting, or receiving a message (Says, Notes, and Gets).

F. Agent's Knowledge of Messages

Agent's knowledge of messages is formalized by the agent's static knowledge, namely what he knows before any protocol session takes place. The later, formalizes the agent's dynamic knowledge, namely what he obtains from inspecting protocol traces.

Agent's initial (static) knowledge consists of all the messages, long-term secrets and keys the agent knows before engaging in any sessions of the protocol. For example, a friendly agent knows all public keys and only its own private key. The *Spy* knows all compromised agents' private keys (he is assumed to collude with compromised agents), and all public keys.

Agent's dynamic knowledge of messages contains messages that he acquire from a protocol trace. So the set of all message components that the *Spy* can derive from the observation of the traffic in the trace evs can be modeled by *analz*(*knows Spy evs*).

At the beginning of the protocol when the trace is empty, all the agents only know their own initial knowledge. During the protocol execution, the agents may dynamically expand their knowledge based on the events occurred in the network. For example, any messages ever sent by anyone and any messages ever noted by a compromised agent belong to the *Spy*'s dynamic knowledge but other agents only know what they send to anyone, what they receive and what they note in a trace.

G. The Used Operator

The *used* operator formalizes the set of all message components that either belong to some agent's initial knowledge or appeared on some trace. So freshness of a message *m* in a trace *evs* can be formalized by not belonging *m* to the set of *used evs*.

IV. BLIND SIGNATURE

Blind signature requires that a signer be able to sign a document without knowing its contents. This intuitively corresponds to signing a document with the eyes closed. In security protocols that anonymity of the sender is a major concern, blind signature can be employed. Two such examples are e-voting and electronic cash. To illustrate the concept, we look at the voting scheme in more detail.

In an e-voting protocol, on one hand, the voting center will be concerned of duplicate or fraudulent votes, and on the other hand, the voter will be concerned about the anonymity of his vote. A solution can be to have a trusted Election Authority that authenticates the owner of a vote, namely it is responsible for checking validity and non-duplicity of votes. Then the voting center accepts any votes with the signature of the Election Authority.

The concern of the voter can be solved using blind signatures. The Election Authority should be able to sign on a blinded vote sent by the voter and the voter should be able to extract a valid signature on the original unblinded vote.

Precisely speaking, any blind signature schema is a security

the one who requests for signing a message. For example a simplified version of the FOO protocol which is an e-voting protocol based on blind signature is as follows [15]:

1) $V \rightarrow A : V, \sigma V(\chi(v, b))$
2) $A \rightarrow V : \sigma A(\chi(v, b))$
3) $V: \sigma A(v)$

In the first step, a voter V selects a vote and blinds it by a blinding function χ and a random blinding factor b. then he sings the blinded message and sends it beside his id to the authority A.

In the second step, A investigates whether V has the right to vote, it has not voted yet and his signature is valid. If all of these conditions hold, A signs the blinded message and sends it back to the voter.

Finally, V unblinds the received message and obtains the vote signed by A.

V. FORMAL MODEL OF BLIND SIGNATURE

The inductive method previously allowed only three types of keys: asymmetric keys, symmetric keys and session keys. We formalize blind signature as a symmetric encryption that the symmetric key is not shared with any other agents, namely it is exclusive. In other words, only the owner of the blinding factor can blind and unblind a message using his blinding factor. Another issue that should be addressed is that blinding factor is assumed to be unique.

In order to model blind signature, we define the function *blindFac* from the set of agents to the set of keys (5) that maps each blinding factor into its owner. To address the uniqueness property of the blinding factors, we specify that the *blindFac* function is injective (5).

DEF1: Function blindFac : "agent => Key"
blindFac is injective (5)

Using Axiom 1, we define that blinding factor is a symmetric key, so it has the same encryption and decryption keys and all the theorems and lemmas related to the symmetric keys hold for blinding factors too. Consequently based on the perfectness of encryption, no one can reveal the contents of a blinded message.

Axiom 1 : blindFac X ∈ symKeys (6)

The only issue which remains is to specify that blinding factor is exclusive. We will meet this requirement in the next section where we want to define the agents' static knowledge.

Based on this formalization, the message M blinded by the agent A's blinding factor can be modeled by *Crypt*(*blindFac* A)M. Then the blinded message can be signed by the *priK* function mentioned before.

VI. STATIC KNOWLEDGE OF AGENTS

As mentioned in the previous section, blinding factor of an agent is not shared with any other agents. We redefine the *initState* function which formalizes the static knowledge of agents, in such a way to address this property.

Moreover, threat model of the Inductive model allows the *Spy* to collude with the set of compromised agents. To remain consistent with this model, compromised agents should reveal their blinding factors to the *Spy* since the beginning of protocol execution. So the *Spy*'s initial knowledge should contain the blinding factor of *bad* agents.

Concluding above requirements, The *Spy* knows the blinding factors of compromised agents, private keys of bad agents and all the public keys. Friendly agents and the *Server* knows its own blinding factor, his private key and all the public keys.

DEF2: Function initialState:
initState_Server: Key (All pubK ∪ priK server ∪ blindFac Server)
|
initState_Friend i: Key (All pubK ∪ priK Friend i ∪ blindFac (Friend i)) (7)
|
initState_Spy: Key (All pubK ∪ priK bad ∪ blindFac bad)

Now we move on to prove some lemmas that are used in the following sections. Lemma1 states that the Spy knows the blinding factor of all the bad agents. This lemma can be easily derived from DEF2.

lemma 1: A ∈ bad ==> Key (blindFac A) ∈ initialState Spy (8)

Lemma 2 states that each agent knows his own blinding factor before any protocol session takes place. If the agent is a friendly agent or the *Server*, it can be easily proved using DEF2, else if the agent is the *Spy*: he knows blinding factors of *bad* agents and according to the definition of *bad* set, the *Spy* is a member of this set, so he knows his key.

lemma 2: Key (blindFac A) ∈ initialState A (9)

VII. THEOREMS OF THE USED FUNCTION

The *used* function, formalizes the set of all message components that are used in a trace. At the beginning of protocol execution, the trace is empty; therefore the set of used messages is equal to the set of *initState* of all the agents. So we expect that blinding factor of each agent belongs to the set of used messages (10).

lemma 3: " Key (blindFac A) ∈ used evs" (10)

The lemma can be proved using (11), (12). Since the blinding factor of agent A belongs to the set of A's *initState* message components (11) and the set of his *initState* messages

is a subset of *used* messages (12), blinding factor is a member of used messages.

lemma 4 : Key (blindFac A) ∈ parts(initState A) (11)

lemma 5: initState A ⊆ used evs (12)

VIII. COMPATIBILITY WITH THE INDUCTIVE METHOD KEYS

Blinding factor is introduced as a new key type so it is necessary to prove that the set of *blindFac* keys are completely disjoint from any other keys previously modeled in the Inductive Method. In particular, we should prove there are not any equal blinding factor and asymmetric key. Formally speaking we should prove that:

Theorem 1: blindFac A ≠ priK C (13)

The proof can be done using an axiom in the theory of asymmetric keys which states that *priK* ≠ *pubK*, the definition of *invkey* and *symKeys*, and the axiom1.

According to the definition of the *invkey* function, in case of asymmetric keys, it turns the key into its corresponding asymmetric half. Using the axiom in the theory of asymmetric keys, we can conclude that *invkey* of an asymmetric key is not equal to that key. But the basic property of the key K as a symmetric key is that *invkey* (k) = k. Therefore the range of symmetric keys and asymmetric keys are disjoint. According to Axiom1, blinding factor is a symmetric key, consequently we can prove that its range is disjoint from asymmetric keys and it differs from any public and private keys.

Having proved theorem 1, the following theorem can be proved easily and theorems related to the *priK* can also be proved similarly.

Theorem 2: pubK A ∉ Range (blindFac AA) (14)

Another key type that is formalized in the inductive method is the session key. A session key is a fresh symmetric key that some protocols distribute it to their peers. By the word fresh, it means that the key has not been used in the current trace of the protocol. Because the blinding factor is also a symmetric key, it is essential to prove that the range of blinding factors and session keys are disjoint. The following theorem states it formally:

Theorem 3: Key K ∉ used evs ==> K ∉ range blindFac (15)

This theorem is proved using lemma3 which states that a blinding factor is in the set of used messages for any trace of the protocol so it is also used for the trace *evs* and it differs from session keys.

IX. COMPATIBILITY WITH THE THREAT MODEL

In this section we provide some theorems to show that the formalization of the blind signature is compatible with the threat model and satisfies the properties and behaviors expected.

The function *analz* is particularly important in formalizing the threat model of the inductive method. It represents a potentially unlimited series of decomposing concatenated messages and decryptions by available keys and as already mentioned *analz*(*knows Spy* evs) represents the set of all message components that the *Spy* can derive from the network traffic.

As the *Spy* knows the blinding factor of compromised agents, it can be proved that he can obtain components of the observed messages blinded by the compromised agents.

Formally speaking, if A is a compromised agent, and the message blinded by his blinding factor belongs to the set of message components analyzed by the *Spy* from the trace evs, then the unblinded message is also available to the Spy :

Theorem 4: [| Crypt (blindFac A) X ∈ analz (knows Spy evs)
; A ∈ bad |]
==> X ∈ analz (knows Spy evs) (16)

In order to prove the above theorem, we should first prove simpler theorems and lemmas. The theorem 5 is a simpler version of theorem4 which states that if the *Spy* has the blinding factor, he can decrypt the blinded message. Specifically, if the blinding factor and the message blinded by it belong to the set of messages H, then the *Spy* can recursively uses the operator *analz* to obtain the unblinded message X:

Theorem 5 : [| Crypt (blindFac A) X ∈ analz H;
Key(blindFac A) ∈ analz H |]
==> X ∈ analz H (17)

According to the definition of the *analz* operator, ciphers can be decrypted if and only if the decryption key is available. If we prove that the decryption key of a blinding factor is equal to it, based on the assumptions of theorem 5, we can conclude that the decryption key is available and so prove theorem5. The issue is formally stated in the following lemma:

lemma 6: invKey (blindFac A) = blindFac A (18)

The proof of lemma6 is straightforward using axiom1 and the definition of symmetric keys.

We observe that the *Spy*'s knowledge is omitted in the theorem4.In the next session we will investigate the Spy's knowledge in more detail and find some lemmas which link between this theorem and the *Spy*'s knowledge.

X. AGENT'S DYNAMIC KNOWLEDGE

The function *knows* recursively represents how the knowledge of each agent (the *Spy* included) is expanded during the protocol execution, namely formalizes the dynamic knowledge of agents.

Prior to the protocol execution, the trace of events is empty

and the knowledge of an agent is equal to its initial knowledge. During the protocol execution, based on the events occurred in the network and the agent who causes the event to occur, dynamic knowledge of agents maybe added. It can be proved by induction that the set of agent's initial knowledge in a trace is a subset of his dynamic knowledge on that trace:

$$\text{lemma 7: initialState A} \subseteq \text{Knows A evs} \tag{19}$$

By introducing the blinding factor and consequently extending the initial knowledge of agents, we proved in lemma2 that the blinding factor of an agent belongs to his initial knowledge. So using lemma6 and lemma2, it is proved that the blinding factor of an agent belongs also to his dynamic knowledge for any trace evs:

$$\text{Theorem 6: Key (blindFac A)} \in \text{knows A evs} \tag{20}$$

Similarly we expect that the *Spy* knows the compromised agents' blinding factors in any trace of evs. This requirement is expressed formally in the following lemma:

$$\begin{aligned}&\text{lemma 8: A} \in \text{bad}\\ &\quad \Longrightarrow \text{Key (blindFac A)} \in \text{knows Spy evs}\end{aligned} \tag{21}$$

The lemma can be proved by induction on the length of the trace evs: For the base case when the trace is empty, according to the definition of the function *knows*, dynamic knowledge of an agents is equal to his initial knowledge and based on lemma1, if the agent A is a compromised agent, then the *Spy* knows the A's blinding factor in any trace evs.

For the inductive steps, if the trace has been extended by any event, then the set of *Spy*'s dynamic knowledge is a super set of his previous knowledge set. Then using the base case, compromised agents' blinding factor also belongs to this expanded knowledge set of the *Spy*.

Now, let's move on to prove the theorem4. If we replace the message set H by the term *knows Spy* evs, a variant of the theorem5 which is closer to the theorem4 can be proved easily. In addition based on the lemma8, blinding factor of the compromised agent A belongs to the knowledge set of the *Spy*, namely the set H. Consequently, theorem4 is proved using the variant of theorem5.

XI. DERIVING SIGNED MESSAGE FROM SIGNED BLINDED MESSAGE

We have not addressed yet the key property of the blinding signature: using the blinding factor, it is possible to derive the signed message from the signed blinded message.

If the agent who derives the signed message is the owner of the blinding factor, the property can be modeled implicitly in formalizing the protocol steps. In this case, when the agent receives the signed blinded message, he can send the signed message in the following steps of the protocol.

In the case of formalizing this property in our threat model, the *Spy* should be able to derive the signed messages from the signed blinded message. More precisely, if the blinding factor r is available for the *Spy*, he can unblind the message X blinded by r and signed by the key K and obtain the message X signed by K. formally speaking, using r it is possible to derive *Crypt* K X from *Crypt* K (*Crypt* r X).

In our present model, the Spy can only unblind the blinded message and it is not possible to formalize this capability of him. So it is required to add some assumptions to our model, these assumptions are specified in the following axiom:

$$\begin{aligned}&\text{Axiom2 : [| Crypt (priK A) (Crypt (blindFac V) X)} \in \text{analz H;}\\ &\qquad \text{Key(blindFac V)} \in \text{analz H |]}\\ &\quad \Longrightarrow \text{Crypt (priK A) X} \in \text{analz H}\end{aligned} \tag{22}$$

Similar to theorem4, we expect that the *Spy* could obtain the signed message from a signed blinded message, if the message has been blinded by a compromised agent. The following states this issue:

$$\begin{aligned}&\text{Theorem 7: [| B} \in \text{bad;}\\ &\text{Crypt (priK A) (Crypt (blindFac B) X)} \in \text{analz (knows Spy evs)|]}\\ &\quad \Longrightarrow \text{Crypt (priK A) X} \in \text{analz (knows Spy evs)}\end{aligned} \tag{23}$$

As the *Spy* knows the blinding factor of compromised agents, it can be proved that he can obtain components of the observed messages blinded by the compromised agents. The theorem can be proved, using lemma8 which proved that blinding factor of compromised agent is available to the *Spy*.

XII. CONCLUSION

In this paper, we have extended the inductive method by introducing the formalization of Blind Signature, an advanced cryptographic primitive used mostly in e-voting protocols. Blind signature is modeled in the Inductive Method, as an exclusive unique symmetric key that provides the capability of obtaining a signed message from a signed blinded message. Then we showed backward compatibility of our model by already defined keys and threat model and proved that the formalization meets the expected requirements. The model in this study enables us to specify and verify protocols which use blind signature.

REFERENCES

[1] L. C. Paulson, "Proving Properties of Security Protocols by Induction, " Proc. of 10th Computer Security Foundations Workshop, USA, 1997.
[2] L. C. Paulson, "Isabelle A Generic Theorem Prover," Vol. 828, Lecture Notes in Computer Science. Springer, 1994.
[3] L. C. Paulson, "Mechanized Proofs for a Recursive Authentication Protocol," Proc. of 10th IEEE Computer Security Foundations Workshop, 1997, pp. 84-95.
[4] L. C. Paulson, "Relations between Secrets: two Formal Analyses of the Yahalom Protocol" Journal of Computer Security, 2000.

[5] G. Bella and L. C. Paulson, "Mechanising BAN Kerberos by the Inductive Method," Proc. of the International Conference on Computer-Aided Verification, Vol. 1427 of Lecture Notes in Computer Science, Springer , 1998, pp. 416-427.
[6] G. Bella and L. C. Paulson, "Kerberos Version IV: Inductive Analysis of the Secrecy Goals, " Proc. of the 5th European Symposium on Research in Computer Security, Vol. 1485, Springer, 1998. pp. 361-375.
[7] G. Bella and L. C. Paulson, "Using Isabelle to prove Properties of the Kerberos Authentication System, " Proc. of Workshop on Design and Formal Verification of Security Protocols, 1997.
[8] G. Bella, "Message reception in the inductive approach," Technical Report 460, Computer Laboratory, University of Cambridge, 1999.
[9] G. Bella, "Modelling agents' knowledge inductively," Proc. of the 7th Security Protocols Workshop,Springer, 2000, pp. 85–94.
[10] G. Bella, "Mechanising a protocol for smartcards," Proc. of the 1st International Conference on Research in Smartcards, Springer, 2001, pp. 19–33.
[11] G. Bella, L.C. Paulson, "Mechanical Proofs about a Non-repudiation Protocol," Proc. of Theorem Proving in Higher Order Logics, Vol. 2152, Springer, 2001, pp. 91-104.
[12] G. Bella, F. Massacci, L. C. Paulson, "Verifying the SET registration protocols," Journal of Selected Areas in Communications, Vol. 21, No. 1, 2003, pp. 77–87.
[13] G. Bella, F. Massacci, L. C. Paulson, "An Overview of the Verification of SET," Journal of Information Security, Vol. 4, no. 1, pp. 17–28, 2005.
[14] G. Bella, F. Massacci, L. C. Paulson, "Verifying the SET Purchase Protocols," Journal of Automated Reasoning, Vol. 36, No.1, 2006, pp. 5–37.
[15] A. Fujioka, T. Okamoto, and K. Ohta, "A Practical Secret Voting Scheme for Large Scale Elections," Proc. Advances in Cryptology, Springer, Berlin, 1992, pp. 244-251.

Hermite Polynomial Representation for Finite Fields of Characteristic Three

Sedat Akleylek, Ferruh Özbudak, Canan Özel

***Abstract*—In this paper, we give Hermite polynomial representation for finite fields of characteristic three. We explain how we obtain an arithmetic design for finite field multiplication and modular reduction in $\mathbb{F}_{3^n}$. We show that this representation allows us to perform faster modular reduction in some cases.**

***Index Terms*—representation of finite fields with characteristic three, Hermite polynomials, polynomial multiplication, modular reduction.**

I. Introduction

Arithmetic of finite fields is utilized by the majority of the cryptographic systems [1]. The complexity of the algorithms in these systems is dependent on the arithmetic operations. The efficient implementations of these operations determine the efficiency of the whole system. Many cryptosystems such as RSA, AES, elliptic curve cryptography and also recently pairing based cryptography uses the basic arithmetic operations in finite fields [2]. Binary extension fields and the arithmetic of these fields are extensively studied. Also the importance of general extension field arithmetic have been recently increasing in consequence of the progress in the pairing based cryptography. For instance, Tate Pairing is efficiently computable and achieves its maximum security in finite fields of characteristic three over supersingular elliptic curves [3]. Therefore, the studies on the arithmetic operations on extension fields of $\mathbb{F}_3$ have been recently widespread [4], [5].

By using the polynomial basis representation, the elements of an extension field $\mathbb{F}_{3^n}$ are represented as polynomials of degree $n-1$, where the coefficients of the polynomials are in $\mathbb{F}_3$. Analogous to the binary extension fields, polynomial basis representation needs an irreducible polynomial of degree n with the coefficients from $\mathbb{F}_3$. The main operation of $\mathbb{F}_{3^n}$ is multiplication which contains polynomial multiplication over $\mathbb{F}_3$ and modular reduction with respect to the irreducible polynomial.

In binary extension fields, some special polynomial representations have been proposed to make the field arithmetic efficient. These are Dickson polynomial representation [6], [7], modified redundant representation [8], Charlier polynomial representation [9] and Hermite polynomial representation [10].

S. Akleylek, F. Özbudak and C. Özel are with the Institute of Applied Mathematics, Middle East Technical University, Ankara, 06531, Turkey. e-mail: akleylek, ozbudak, ccimen@metu.edu.tr.

S. Akleylek is also with the Department of Computer Engineering, Ondokuz Mayıs University, Samsun, Turkey.

F. Özbudak is also with the Department of Mathematics, Middle East Technical University, 06531, Ankara, Turkey.

In this paper, we deal with the representation of certain extension fields of $\mathbb{F}_3$. This representation is based on Hermite polynomials. We present the method of multiplication and reduction of Hermite polynomials and we give the complexities of these arithmetic operations. We choose irreducible Hermite binomials to represent the finite field and we obtain some irreducible binomials in Hermite form which allows us an efficient modular reduction.

This paper is organized as follows: in Section 2, we describe Hermite polynomials and give some results on Hermite polynomials in $\mathbb{F}_3[x]$. We present the method of multiplying two polynomials in Hermite representation. In section 3, we give the multiplication and reduction complexities in view of the number of multiplication and addition. We conclude the paper in Section 4.

II. Preliminaries

In this section, we give preliminaries and Hermite representation of finite fields of characteristic three.

Definition 1: [11] The probabilists Hermite polynomials are $H_0(x)=1$, $H_1(x)=x$ and for $n \geq 2$

$$H_n(x) = x \cdot H_{n-1}(x) - (n-1) \cdot H_{n-2}(x)$$

We give the Hermite polynomials in $\mathbb{F}_3[x]$ for $n \leq 10$ in Table 1.

TABLE I
Hermite polynomials in $\mathbb{F}_3[x]$

$H_0(x)$	1
$H_1(x)$	x
$H_2(x)$	x^2+2
$H_3(x)$	x^3
$H_4(x)$	x^4
$H_5(x)$	x^5+2x^3
$H_6(x)$	x^6
$H_7(x)$	x^7
$H_8(x)$	x^8+2x^6
$H_9(x)$	x^9
$H_{10}(x)$	x^{10}

Remark 1: We note that $deg(H_n(x)) = n$. Since Hermite polynomials have a recursive structure, it is shown in Table 1 that all Hermite polynomials in $\mathbb{F}_3$ have the forms

$$\begin{aligned} H_{3k}(x) &= x^{3k} \\ H_{3k+1}(x) &= x^{3k+1} \\ H_{3k+2}(x) &= x^{3k+2}+2x^{3k} \end{aligned}$$

for $k \in \mathbb{N}$.

Let $H_n(x) = \beta_n$ be the n-th Hermite polynomial in $\mathbb{F}_3[x]$ with degree n. Our aim is to represent the elements of finite field $\mathbb{F}_{3^n}$ by using Hermite polynomials in $\mathbb{F}_3[x]$. We use the elements represented with standart polynomial representation. Let $a(x) = a'_{n-1}x^{n-1} + a'_{n-2}x^{n-2} + .. + a_0$ where $a'_i \in \mathbb{F}_3$. $a(x)$ can be represented by using Hermite polynomials as $a = a_{n-1}\beta_{n-1} + .. + a_0\beta_0$. Algorithm 1 gives the way of conversion of the coefficients from standart polynomial representation to Hermite polynomial representation.

Algorithm 1 Conversion of Representation of an Element

Input: $a(x) = \sum_{i=0}^{n-1} a'_i x^i$
Output: $(a_0, a_1, ..., a_{n-1})$ where $a = \sum_{i=0}^{n-1} a_i\beta_i$

1: $T \leftarrow a$
2: **for** $i = n$ downto 1 **do**
3: **if** $deg(T) = i$ then
4: **if** $a'_i = 1$ then $a_i \leftarrow 1$, $T \leftarrow T + 2\beta_i$
5: **else if** $a'_i = 2$ then $a_i \leftarrow 2$, $T \leftarrow T + \beta_i$
6: **end if**
7: **else** $a_i \leftarrow 0$
8: **end if**
9: **end for**
10: $a_0 \leftarrow T$

A. Hermite Basis

We convert the representation of elements to Hermite polynomial representation. We need to introduce the multiplication $\cdot$ on Hermite polynomial representation over $\mathbb{F}_{3^n}$ to obtain the basis elements.

Theorem 1: Let $H_n(x) = \beta_n$ be the n-th Hermite polynomial in $\mathbb{F}_3[x]$, where $n \geq 0$. Then for all $i, j \geq 0$ the Hermite polynomials $\{\beta_0, \beta_1, ..., \beta_{n-1}, ..\}$ satisfies the following equation

$$\beta_i \cdot \beta_j = \beta_{i+j} + l \cdot (k \cdot \beta_{i+j-2} + 2 \cdot m \cdot \beta_{i+j-4}) \quad (1)$$

where $l, k, m \in \mathbb{F}_3$ is defined as

$$l = \begin{cases} 0 & \text{if } i \text{ or } j \equiv 0 \bmod 3 \\ 1 & \text{otherwise.} \end{cases}$$

$$k = \begin{cases} 1 & \text{if } i \equiv j \bmod 3 \\ 2 & \text{otherwise.} \end{cases}$$

$$m = \begin{cases} 1 & \text{if } i, j \equiv 2 \bmod 3 \\ 0 & \text{otherwise.} \end{cases}$$

Let us give the sketch of the proof. We take each Hermite polynomial $H_n(x)$ in $\mathbb{F}_3[x]$ as β_n. As noted in Remark 1, $\forall k \in \mathbb{N}$, $\beta_{3k} = x^{3k}$, $\beta_{3k+1} = x^{3k+1}$ and $\beta_{3k+2} = x^{3k+2} + 2x^{3k+2}$. If we compute all the cases with respect to the residues of i and j (mod 3) respectively, then we get the equation. As a result, the multiplication of Hermite polynomials, β_i and β_j changes with respect to the indices i,j (mod 3).

Any finite field $\mathbb{F}_{3^n}$ is isomorphic to $\mathbb{F}_3[x]/f(x)$ where $f(x)$ is an irreducible polynomial of degree n. The standart representation of elements of $\mathbb{F}_3[x]/f(x)$ is done by using the polynomial basis $\{1, x, x^2, ..., x^{n-1}\}$. Now, we show that $\{\beta_0, \beta_1, ..., \beta_{n-1}\}$ is a linearly independent set and contitutes a basis of $\mathbb{F}_{3^n}$.

Proposition 1: The set $\{\beta_0, \beta_1, ..., \beta_{n-1}\} \in \mathbb{F}_{3^n}$ is linearly independent.

Proof: In consequence of the recursive structure of Hermite polynomials, in the set $\{\beta_0, \beta_1, ..., \beta_{n-1}\}$, each polynomial β_i has degree i. Therefore, β_i can be expressed as a linear combination of only the polynomials $\{\beta_0, \beta_1, ..., \beta_{i-1}\}$. However, in this set none of the polynomials has degree i. If we generalize this, any of the polynomial can be expressed as a linear combination of $\{\beta_0, \beta_1, ..., \beta_{n-1}\}$. This means that the set is linearly independent. ■

Theorem 2: Let $f = f_n\beta_n + .. + f_0\beta_0$ be an irreducible polynomial of degree n where each $f_i \in \mathbb{F}_3$. The set $\{\beta_0, \beta_1, .., \beta_{n-1}\}$ is a basis of $\mathbb{F}_{3^n} \cong \mathbb{F}_3[x]/f(x)$.

Proof: $\mathbb{F}_{3^n}$ is an extension field of $\mathbb{F}_3$ and also considered as a vector space over $\mathbb{F}_3$. By using Algorithm 1, we can write each element of $\mathbb{F}_{3^n}$ uniquely as a linear combination of $\{\beta_0, \beta_1, .., \beta_{n-1}\}$. We have already shown in Proposition 1 that this set is linearly independent. Hence, the set $\{\beta_0, \beta_1, .., \beta_{n-1}\}$ is a basis of $\mathbb{F}_{3^n} \cong \mathbb{F}_3[x]/f(x)$. ■

III. Multiplication of Polynomials in Hermite Representation

In this section, we describe the multiplication of Hermite polynomials for finite fields of characteristic three and explore the complexity of the multiplication. It is well-known that multiplication of finite field elements can be performed in two steps: first multiplication of polynomials and then modular reduction with respect to the irreducible polynomial that is chosen before [12]. We give the multiplication and the reduction operations, respectively. Throughout this section, $M(n)$ and $A(n)$ denote the minimum number of multiplications and the minimum number of additions for corresponding algorithm for two n-term polynomials multiplication. The following theorem gives the required number of multiplications and additions to multiply polynomials in Hermite basis.

Theorem 3: Let $a = a_{n-1}\beta_{n-1} + ... + a_0\beta_0$ and $b = b_{n-1}\beta_{n-1} + ... + b_0\beta_0$ be n-term polynomials over $\mathbb{F}_3$ and $a \cdot b = c_{2n-2}\beta_{2n-2} + ... + c_0\beta_0$. By using any multiplication method, the coefficients of the polynomial c are computed with

$$\begin{aligned} M(n) &+ M(n - \lceil \tfrac{n}{3} \rceil - \lfloor \tfrac{n - \lceil \frac{n}{3} \rceil}{2} \rfloor) \\ &+ 4 \cdot \lfloor \tfrac{n - \lceil \frac{n}{3} \rceil}{2} \rfloor \cdot (n - \lceil \tfrac{n}{3} \rceil - \lfloor \tfrac{n - \lceil \frac{n}{3} \rceil}{2} \rfloor) \\ &+ 3 \cdot M(\lfloor \tfrac{n - \lceil \frac{n}{3} \rceil}{2} \rfloor) \end{aligned}$$

multiplications and

$$A(n) + A(n-\lceil\frac{n}{3}\rceil-\lfloor\frac{n-\lceil\frac{n}{3}\rceil}{2}\rfloor)+A(\lfloor\frac{n-\lceil\frac{n}{3}\rceil}{2}\rfloor) + 2\cdot\lfloor\frac{n-\lceil\frac{n}{3}\rceil}{2}\rfloor\cdot(n-\lceil\frac{n}{3}\rceil-\lfloor\frac{n-\lceil\frac{n}{3}\rceil}{2}\rfloor) + 2\cdot\lceil\frac{2n-4}{3}\rceil+\lfloor\frac{(2n-3)-\lceil\frac{2n-4}{3}\rceil}{2}\rfloor \quad (3)$$

additions.

Proof: By using Theorem 1, the coefficients are computed as follows,

$$\begin{aligned} c_0 &= a_0b_0+a_1b_1+2a_2b_2\\ c_1 &= a_0b_1+a_1b_0+2a_2b_1+2a_1b_2\\ c_2 &= a_0b_2+a_2b_0+a_1b_1+a_2b_2\\ &\vdots\\ c_{2n-3} &= a_{n-2}b_{n-1}+a_{n-1}b_{n-2}\\ c_{2n-2} &= a_{n-1}b_{n-1} \end{aligned}$$

If we compare this multiplication with standard polynomial basis representation, we can see extra terms. All these terms come from the multiplication of the basis elements $\beta_i\cdot\beta_j$ where $0\le i,j\le n-1$ and $i,j\not\equiv 0 \pmod 3$. The multiplication differs with respect to the values of $i \pmod 3$ and $j \pmod 3$, ie. if $i,j\equiv 1 \pmod 3$ then $\beta_i\cdot\beta_j=\beta_{i+j}+\beta_{i+j-2}$ or if $i,j\equiv 2 \pmod 3$ then $\beta_i\cdot\beta_j=\beta_{i+j}+\beta_{i+j-2}+2\cdot\beta_{i+j-4}$. Therefore, the number of the extra terms are related to the number of the indices which are smaller than n and equal to one or two (mod 3). The number of indices that are equal to two (mod 3) is $\lfloor\frac{n-\lceil\frac{n}{3}\rceil}{2}\rfloor$ and the number of indices that are equal to one (mod 3) is $n-\lceil\frac{n}{3}\rceil-\lfloor\frac{n-\lceil\frac{n}{3}\rceil}{2}\rfloor$. The extra terms are computed with the multiplication of the polynomials contains those numbers of terms, so the total multiplication complexity is determined as the sum of these multiplications.

Similarly, in the total addition complexity, we have additions to combine these extra terms to the ordinary multiplication terms. These are related to the indices of c_i where $0\le i\le 2n-4$ and the remainder of these indices from the division with three. ■

Remark 2: Some of this multiplication complexity comprises scalar multiplication, ie. multiplication by two. If we seperate the number of scalar multiplication from the total multiplication complexity, it is equal to:

$$2\cdot\lfloor\frac{n-\lceil\frac{n}{3}\rceil}{2}\rfloor\cdot(n-\lceil\frac{n}{3}\rceil-\lfloor\frac{n-\lceil\frac{n}{3}\rceil}{2}\rfloor)+M(\lfloor\frac{n-\lceil\frac{n}{3}\rceil}{2}\rfloor)$$

Recall that since it is just a shift operation, in hardware applications multiplication by two is free [2].

By the choice of the multiplication method, some or all elements of extra terms may be computed in the first part of the algorithm, ie. in n-term polynomial product, so the complexities added to $M(n)$ and $A(n)$ may be smaller than the given ones in the theorem. We explain the theorem with an example, by using the Karatsuba multiplication method [13]. Karatsuba Algorithm decreases the number of coefficient multiplications compared to the schoolbook or ordinary multiplication method by using the divide-conquer idea recursively. Example 1 shows the required multiplications for 4-term polynomials over $\mathbb{F}_p$ where $p\ge 2$.

Example 1: Let $a(x)=a_3x^3+...+a_0$ and $b(x)=b_3x^3+...+b_0$ be 4-term polynomials over $\mathbb{F}_p$ where $p\ge 2$. Karatsuba algorithm computes the product $c(x)=c_6x^6+..+c_0$ with the following multiplications:

$$\begin{aligned} m_0 &= a_0b_0\\ m_1 &= a_1b_1\\ m_2 &= a_2b_2\\ m_3 &= a_3b_3\\ m_4 &= (a_0+a_1)(b_0+b_1)\\ m_5 &= (a_0+a_2)(b_0+b_2)\\ m_6 &= (a_1+a_3)(b_1+b_3)\\ m_7 &= (a_2+a_3)(b_2+b_3)\\ m_8 &= (a_0+a_1+a_2+a_3)(b_0+b_1+b_2+b_3) \end{aligned}$$

By appropriate additions of m_i's the coefficients of c are obtained. Here, Karatsuba algorithm uses 9 multiplications and 24 additions [13].

Now, in the second example we multiply two 4-term polynomials in Hermite basis representation by using Karatsuba multiplication method.

Example 2: Let $a=a_3\beta_3+a_2\beta_2+a_1\beta_1+a_0\beta_0$ and $b=b_3\beta_3+b_2\beta_2+b_1\beta_1+b_0\beta_0$ be 4-term polynomials over $\mathbb{F}_3$. Let $a\cdot b=c=c_6\beta_6+c_5\beta_5+...+c_0\beta_0$. Then

$$\begin{aligned} c_0 &= a_0b_0+a_1b_1+2a_2b_2\\ c_1 &= a_0b_1+a_1b_0+2a_2b_1+2a_1b_2\\ c_2 &= a_0b_2+a_2b_0+a_1b_1+a_2b_2\\ c_3 &= a_0b_3+a_3b_0+a_1b_2+a_2b_1\\ c_4 &= a_1b_3+a_3b_1+a_2b_2\\ c_5 &= a_2b_3+a_3b_2\\ c_6 &= a_3b_3 \end{aligned}$$

The extra terms in this multiplication are $a_1b_1+2a_2b_2$, $2a_2b_1+2a_1b_2$ and a_2b_2. By applying Karatsuba algorithm for performing an ordinary polynomial multiplication as in Example 1, we compute the terms except these extra terms by using 9 multiplications and 24 additions. Now we compute the extra costs.

We recall that a_1b_1 and a_2b_2 are obtained. To compute $2a_2b_2$, we need 1 multiplication. To compute $2a_2b_1+2a_1b_2$, we do

$$2\cdot[(a_1+a_2)\cdot(b_1+b_2)-a_1b_1-a_2b_2]$$

The cost is 2 multiplications and 4 additions. Also we need 4 additions to add these terms to the general result. So we need totally 3 multiplications and 8 additions as an extra cost. As

a result, by using Karatsuba algorithm we need $9+3=12$ multiplications and $24+8=32$ additions to multiply $c=a\cdot b$.

By this way, we give the upper bound for the complexity of the multiplication of two elements in Hermite basis representation. Now, we explore the reduction part of the multiplication of the elements in $\mathbb{F}_{3^n}$.

A. Irreducible Hermite Binomials

The Hermite polynomials in $\mathbb{F}_3$ are given in Table I for $n \leq 10$. Because of the recursive structure of the Hermite polynomials, we can say that the polynomials including constant terms are only $H_0(x)$ and $H_1(x)$ or we call them β_0 and β_1. We explore low weight irreducible Hermite polynomials for the performance of the reduction operation, so we look for the Hermite binomials. Since irreducible polynomials should include the constant term, there are two forms of the Hermite binomials that are $\beta_n+\beta_0$ and $\beta_n+\beta_2$. We give selected irreducible Hermite binomials in Table II.

TABLE II
IRREDUCIBLE HERMITE BINOMIALS

$\beta_3+\beta_2$	$\beta_4+\beta_2$	$\beta_{11}+\beta_0$
$\beta_{12}+\beta_2$	$\beta_7+\beta_2$	$\beta_{26}+\beta_0$
$\beta_{15}+\beta_2$	$\beta_{19}+\beta_2$	$\beta_{35}+\beta_0$
$\beta_{60}+\beta_2$	$\beta_{28}+\beta_2$	$\beta_{119}+\beta_0$
$\beta_{111}+\beta_2$	$\beta_{67}+\beta_2$	$\beta_{146}+\beta_0$
$\beta_{183}+\beta_2$	$\beta_{151}+\beta_2$	$\beta_{242}+\beta_0$

We list irreducible binomials with respect to the indices $n \pmod 3$. Note that, there are two forms of irreducible binomials and we can group these forms with respect to the indices in mod 3. In the first column, the binomials are in the form $\beta_n+\beta_2$, where $n\equiv 0 \pmod 3$. In the second column, the binomials are in the form $\beta_n+\beta_2$, where $n\equiv 1 \pmod 3$ and in the last column, they are in the form $\beta_n+\beta_0$, $n\equiv 2 \pmod 3$. The reduction operation is different due to the chosen binomials from each column of the Table II, because the multiplication of Hermite polynomials differs with respect to the values of the indices in mod 3, as it is given in Theorem 1.

1) Reduction: Let us call the irreducible Hermite binomial f. By using f, reduction operation with respect to modulo f can be performed as follows:

We deal with each binomial form respectively, so first let's take $f=\beta_n+\beta_2$ where $n\equiv 0 \pmod 3$ and let $n\leq i\leq 2n-2$. Then,

$$\begin{aligned}\beta_n\cdot\beta_{i-n} &= \beta_i\\ 2\beta_2\cdot\beta_{i-n} &= \beta_i\\ \beta_i &= 2\beta_{i-n}.\beta_2\end{aligned}$$

We formulate this by using Theorem 1 as follows:

$$\beta_i = 2\beta_{i-n+2} + r\cdot(s\cdot\beta_{i-n}+t\cdot\beta_{i-n-2}) \qquad (4)$$

$$r=\begin{cases}0 & \text{if } i-n\equiv 0 \bmod 3\\ 1 & \text{otherwise.}\end{cases}$$

$$s=\begin{cases}1 & \text{if } i-n\equiv 1 \bmod 3\\ 2 & \text{if } i-n\equiv 2 \bmod 3\end{cases}$$

$$t=\begin{cases}1 & \text{if } i-n\equiv 2 \bmod 3\\ 0 & \text{otherwise.}\end{cases}$$

Remark 3: If $n\equiv 0 \pmod 3$ then by theorem 1, l is zero and note that $\beta_n=2\cdot\beta_2$.

Now, let $n\equiv 1 \pmod 3$ and let $f=\beta_n+\beta_2$. The reduction of β_i where $n\leq i\leq 2n-2$ differs with respect to the value of $i-n \pmod 3$. Let's give the reduction formulas for the values zero, one and two, respectively.

If $i-n\equiv 0 \pmod 3$:

$$\begin{aligned}\beta_n\cdot\beta_{i-n} &= \beta_i\\ \beta_i &= 2\beta_2\cdot\beta_{i-n}\\ \beta_i &= 2\beta_{i-n+2}\end{aligned}$$

If $i-n\equiv 1 \pmod 3$:

$$\begin{aligned}\beta_n\cdot\beta_{i-n} &= \beta_i+\beta_{i-2}\\ 2\beta_2\cdot\beta_{i-n} &= \beta_i+\beta_{i-2}\\ \beta_i &= 2\beta_2\cdot\beta_{i-n}+2\beta_{i-2}\\ \beta_i &= 2\beta_{i-n+2}+\beta_{i-n}+2\beta_{i-2}\end{aligned}$$

If $i-n\equiv 2 \pmod 3$:

$$\begin{aligned}\beta_n\cdot\beta_{i-n} &= \beta_i+2\beta_{i-2}\\ 2\beta_2\cdot\beta_{i-n} &= \beta_i+2\beta_{i-2}\\ \beta_i &= 2\beta_2\cdot\beta_{i-n}+\beta_{i-2}\\ \beta_i &= 2\beta_{i-n-2}+2\beta_{i-n}+\beta_{i-n-2}+\beta_{i-2}\end{aligned}$$

If we combine these, we get the equation:

$$\beta_i = 2\beta_{i-n+2}+u\cdot(v\cdot\beta_{i-n}+w\cdot\beta_{i-n-2}+2v\cdot\beta_{i-2}) \quad (5)$$

$$u=\begin{cases}0 & \text{if } i-n\equiv 0 \bmod 3\\ 1 & \text{otherwise.}\end{cases}$$

$$v=\begin{cases}1 & \text{if } i-n\equiv 1 \bmod 3\\ 2 & \text{if } i-n\equiv 2 \bmod 3\end{cases}$$

$$w=\begin{cases}1 & \text{if } i-n\equiv 2 \bmod 3\\ 0 & \text{otherwise.}\end{cases}$$

Now let $f=\beta_n+\beta_0$, where $n\equiv 2 \pmod 3$. Since the value of $n\equiv 2 \pmod 3$, the multiplication changes with respect to the values of $i-n \pmod 3$, where $n\leq i\leq 2n-2$. Let us write this seperately again.

If $i-n\equiv 0 \pmod 3$:

$$\begin{aligned}\beta_n\cdot\beta_{i-n} &= \beta_i\\ 2\beta_0\cdot\beta_{i-n} &= \beta_i\\ \beta_i &= 2\beta_{i-n}\end{aligned}$$

If $i-n\equiv 1 \pmod 3$:

$$\begin{aligned}\beta_n\cdot\beta_{i-n} &= \beta_i+2\beta_{i-2}\\ 2\beta_0\cdot\beta_{i-n} &= \beta_i+2\beta_{i-2}\\ \beta_i &= 2\beta_{i-n}+\beta_{i-2}\end{aligned}$$

If $i-n \equiv 2 \pmod 3$:

$$\begin{aligned} \beta_n \cdot \beta_{i-n} &= \beta_i + \beta_{i-2} + 2\beta_{i-4} \\ 2\beta_0 \cdot \beta_{i-n} &= \beta_i + \beta_{i-2} + 2\beta_{i-4} \\ \beta_i &= 2\beta_{i-n} + 2\beta_{i-2} + \beta_{i-4} \end{aligned}$$

If we combine these in a formula:

$$\beta_i = 2\beta_{i-n} + h \cdot (y \cdot \beta_{i-2} + z \cdot \beta_{i-4}) \quad (6)$$

$$h = \begin{cases} 0 & \text{if } i-n \equiv 0 \bmod 3 \\ 1 & \text{otherwise.} \end{cases}$$

$$y = \begin{cases} 1 & \text{if } i-n \equiv 1 \bmod 3 \\ 2 & \text{if } i-n \equiv 2 \bmod 3 \end{cases}$$

$$z = \begin{cases} 1 & \text{if } i-n \equiv 2 \bmod 3 \\ 0 & \text{otherwise.} \end{cases}$$

We perform the reduction operations by choosing all possible irreducible Hermite binomials as some are given in the Table II. Since we have three kinds of irreducible Hermite binomials, we get three reduction formulas in equations 4, 5 and 6. Each reduction formulas changes due to the difference $i-n$ and so the value of the index $i \pmod 3$, which is the index of reduced element β_i. In the form $\beta_n+\beta_2$ where $n \equiv 0 \pmod 3$, the multiplication of $\beta_n \cdot \beta_{i-n}$ directly gives β_i, so we can reduce β_i in one step for this form. However, in the other forms reduction is not completed in one step that we can see from equations 5 and 6. The terms β_{i-2}, β_{i-4} should be reduced until the indices drop into the interval $[0, n-1]$. We do not carry on these reductions, since it depends on the value of the index i.

The following table gives the reduction complexity for each form of the irreducible Hermite binomials.

TABLE III
REDUCTION COMPLEXITY

Form	# Constant Multiplications	# Additions
$\beta_n + \beta_2$ ($n \equiv 0 \bmod 3$)	4	2
$\beta_n + \beta_2$ ($n \equiv 1 \bmod 3$)	6*	3*
$\beta_n + \beta_0$ ($n \equiv 2 \bmod 3$)	4*	2*

Remark 4: Since the reductions in equations 5 and 6 are not completed, we give the signed numbers in Table III which are the numbers of constant multiplications and additions for one step of the reduction. The total number of multiplications and additions for these binomials are computed with multiplying these numbers by the number of reduction steps.

As a result, between these binomials, $\beta_n+\beta_2$, where $n \equiv 0 \pmod 3$ has the least number of constant multiplications and the least number of additions.

IV. CONCLUSION

In this paper, we give Hermite polynomial representation for finite fields of characteristic three. We explain how we obtain an arithmetic design for finite field multiplication and modular reduction in $\mathbb{F}_{3^n}$. We show that this representation allows us to perform efficient modular reduction if we select the irreducible Hermite binomial $\beta_n + \beta_2$, where $n \equiv 0 \pmod 3$. Hermite trinomials also can be chosen as low weight irreducible polynomials. However, we realize that in this case extra multiplications and additions are obtained redundantly in the reduction operation due to the multiplication on Hermite polynomial representation and this increases the reduction complexity.

ACKNOWLEDGMENT

Sedat Akleylek and Ferruh Özbudak were partially supported by TUBITAK under the Grant No. TBAG-109T672.

REFERENCES

[1] I.F. Blake, G. Seroussi, N.P. Smart, Elliptic curves in cryptography *London Mathematical Society Lecture Note Series 265*, Cambridge Univ. Press, 1999
[2] H. Cohen, G. Frey, Handbook of Elliptic and Hyperelliptic Curve Cryptography, *Discrete Math. Appl., Chapman Hall/CRC*, 2006)
[3] T. Kerins, W.P. Marnane, E. M. Popovici and P.S.L.M. Barreto. Efficient Hardware for the Tate Pairing Calculation in Characteristic Three. *CHES 2005*, pp. 412-426, 2005.
[4] K. Harrison, D. Page and N. Smart. Software implementation of finite fields of characteristic three, for use in pairing-based cryptosystems.*LMS Journal of Computation and Mathematics*, 5 (2002), 181-193.
[5] R. Granger, D. Page and M. Stam. Hardware and software normal basis arithmetic for pairing based cryptography in characteristic three. *IEEE Transactions on Computers*, 54 (2005), 852-860.
[6] M.A. Hasan and C. Negre. Subquadratic Space Complexity Multiplication over Binary Fields with Dickson Polynomial Representation.*WAIFI 2008, LNCS 5130*, pp.88-102, 2008.
[7] M.A. Hasan and C. Negre. Low Space Complexity Multiplication over Binary Fields with Dickson Polynomial Representation. *IEEE Trans. on Computers*, vol.60, no.4, pp.602-607, 2011.
[8] S. Akleylek, F. Özbudak, Modified Redundant Representation for Designing Arithmetic Circuits with Small Complexity. *IEEE Trans. Computers* 61(3): 427-432 (2012)
[9] S. Akleylek, M. Cenk, F. Özbudak Polynomial Multiplication over Binary Fields Using Charlier Polynomial Representation with Low Space Complexity. *INDOCRYPT* 2010: 227-237
[10] S. Akleylek, M. Cenk, F. Özbudak, A New Representation of Elements of Binary Fields with Subquadratic Space Complexity Multiplication of Polynomials, submitted, 2010.
[11] D. Drake, The Combinatorics of Associated Hermite Polynomials, European Journal of Combinatorics, vol.30 no.4, pp.1005-1021, 2009.
[12] D. Hankerson, A. Menezes and S. Vanstone, Guide to Elliptic Curve Cryptography, *Springer*, 2004.
[13] A. Weimerskirch, C. Paar, Generalizations of the Karatsuba Algorithm for Efficient Implementations. http://eprint.iacr.org/2006/224, 2006.

Alternate Models of Elliptic Curves: A Survey

M. Ashraf and B. B. Kırlar

***Abstract*—In the recent years, alternate models of elliptic curves have been studied. Such well-known models are Edwards curves, Jacobi intersections and Jacobi quartics, Hessian curves, Huff curves, and their variants to the more common Weierstrass curve. These models sometimes allow for more efficient computation on elliptic curves or provide other features of interest to cryptographers, such as resistance to side-channel attacks. In this paper, we survey the alternate models of elliptic curves. We first give the definition of such elliptic curve models, group law along with computational cost, the suggested improvements in each model and then countermeasures to side channel attacks if any.**

***Index Terms*—alternate models of elliptic curves, unified addition formulae, computational cost.**

I. Introduction

FROM the advent of elliptic curve cryptosystems, independently by Miller (1985) and Koblitz (1987), arithmetic of elliptic curves have been so much interest from cryptographic researchers. Along this period, they proposed many methods to speed up the arithmetic of elliptic curves. These methods can be divided into four different categories:

- Use optimum underlying finite field extensions,
- Use optimum coordinates for representation of group elements,
- Use efficient arithmetic methods,
- Use alternate models of elliptic curves.

In this work, we are dealing with the alternate models of elliptic curves to the more common Weierstrass curve: Edwards curves, Jacobi intersections and Jacobi quartics, Hessian curves, Huff curves, and their variants. These models allow for more efficient computation on elliptic curves such that the group structure of these curves have already been studied in [3], or provide other features of interest to cryptographers, such as resistance to side-channel attacks. These attacks reveal secret information of an elliptic curve cryptosystem based on the point multiplication operation, in which a point is multiplied by a scalar. The basic method for implementing point multiplication is the *double-and-add technique*, which uses a binary representation of the scalar and performs a sequence of point additions and point doublings depending on the bits of the scalar. In double-and-add point multiplication, a point doubling is done for every bit of the key k, but a point addition is done only when a bit of the key is 1. If, in a side-channel analysis, a point addition is distinguishable from a point doubling, then the bits of the secret key can be determined. This is done by analyzing side channel information such as power consumption [24], running time [23], differential fault analysis [9], electromagnetic emissions [1] and so on. As a countermeasure of this attack, one can use the unified addition formula which means point addition formula that can be used for doublings. The unified formulae for point addition and point doubling use the same sequence of field operations and hence are indistinguishable.

Edwards introduced the normal form of elliptic curves together with an explicit addition law in [13]. He also showed that every elliptic curve over a non-binary field is birationally equivalent to a curve in Edwards form over an extension of the field, and in many cases over the original field. In [2], Bernstein and Lange introduced the notion of Edwards curves which is covering more curves than original Edwards curves when those defined on finite fields. Twisted Edwards curve was introduced by Bernstein et al. in [7] as a generalization of Edwards curves. Hisil et al. introduced the Extended Twisted Edwards Coordinates, and obtained efficient point addition algorithms in [19]. These algorithms provide a natural protection from side channel attacks based on Simple Power Analysis (SPA). Bernstein et al. [6] introduced Edwards curves over finite fields of characteristic 2, and obtained addition and doubling formulae.

Jacobi form of the elliptic curves are introduced as the intersection of two quadrics in projective space of dimension 3 by Liardet and Smart in [25]. They showed that these curves could provide a defence against Simple and Differential Power Analysis (SPA/DPA) style attacks. The twisted Jacobi intersections which contains Jacobi intersections as a special case is introduced by Feng et al. in [16]. Billet and Joye [8] reinvestigated the Jacobi Form suggested by Liardet and Smart. They showed that the addition law is directly derived from the underlying quartics.

Hessian curves are investigated as a step towards resistance against side-channel attacks by Joye and Quisquater in [21]. The efficient arithmetic on Hessian elliptic curves are studied in [26] and [17]. They proposed efficient point multiplication algorithms using the Hessian form over finite fields of characteristic 3. In 2010, the family of generalized Hessian curves are proposed by Farashahi and Joye [14]. They showed that these curves cover more isomorphism classes of elliptic curves and that have efficient unified addition formulas. In [5], Bernstein, Kohel, and Lange introduced the twisted Hessian form that is similar to the generalized Hessian curves up to the order of the coordinates.

Huff model of elliptic curve is introduced by Huff [18] over rational fields $\mathbb{Q}$ in 1948. Joye et al. [22] improved these curves to the fields of characteristic different than 2. They obtained point addition and doubling formulae on Huff curves. The generalized form of Huff curve is introduced by Feng and Wu

Manuscript received March 06, 2012.
Muhammad Ashraf is with the Institute of Applied Mathematics, METU, Ankara, Turkey, e-mail: ashraf6061@gmail.com
Barış Bülent Kırlar is with the Department of Mathematics, Süleyman Demirel University, Isparta, Turkey, e-mail: bariskirlar@sdu.edu.tr.

in [15]. Ciss and Sow [11] investigated the new generalized Huff curve that the addition law in projective coordinates is as fast as in the previous particular cases. In 2011, Devigne and Joye [12] obtained the unified point addition formula for Huff curves over fields of characteristic 2.

This paper is organized as follows. In section II, we give Weierstrass form of elliptic curves and its group law. In section III, Edwards curves and their variants are discussed. In section IV, Jacobi intersection and Jacobi quartic with related modifications and improvements are discussed. In section V, Hessian curves are elaborated. In section VI, Huff curves and its generalizations are described. In section VII, we compare the alternate models of elliptic curves and conclude the paper.

II. Preliminaries

An elliptic curve in affine coordinates of simplified Weierstrass form over the finite field $\mathbb{F}$ with $char(\mathbb{F}) \neq 2, 3$ is defined by

$$E \ : \ y^2 = x^3 + ax + b, \tag{1}$$

where $a, b \in \mathbb{F}$. If we apply the process of homogenization with $x = X/Z$ and $y = Y/Z$ for $Z \neq 0$ to (1), we obtain the homogeneous equation in projective coordinates given by

$$E \ : \ Y^2Z = X^3 + aXZ^2 + bZ^3, \tag{2}$$

where $a, b \in \overline{\mathbb{F}}$ (the algebraic closure of $\mathbb{F}$). The curve E has exactly one point with coordinate Z equal to zero, namely $(0:1:0)$. This point is so called point at infinity and denoted by ∞. The curve E has an additive group structure determined by the fact that ∞ is an identity element and $P, Q, R \in E$: $P + Q + R = \infty$ if and only if R lies in the line joining P to Q in the projective space. The group operation in this group structure is usually called *chord-and-tangent rule* that the explicit formula for point addition and point doubling of the curve E are obtained as follows: Let $P = (x_1, y_1)$ and $Q = (x_2, y_2)$ be the points on E with $P, Q \neq \infty$ and $Q \neq -P$. Then

- If $P \neq Q$, then $P + Q = (x_3, y_3)$, where

$$\begin{cases} x_3 = (\frac{y_2 - y_1}{x_2 - x_1})^2 - x_1 - x_2 \\ y_3 = (\frac{y_2 - y_1}{x_2 - x_1})(x_1 - x_3) - y_1 \end{cases}$$

- If $P = Q$, then $2P = (x_3, y_3)$, where

$$\begin{cases} x_3 = (\frac{3x_1^2 - a}{2y_1})^2 - 2x_1 \\ y_3 = (\frac{3x_1^2 - a}{2y_1})(x_1 - x_3) - y_1 \end{cases}$$

Formulas that do not involve field inversions for adding and doubling points in projective coordinates can be derived by first converting the points to affine coordinates, then using the formulae above to add the affine points, and finally clearing denominators. The computational cost of point addition and point doubling in projective coordinates are $12\mathbf{M} + 2\mathbf{S}$ and $5\mathbf{M} + 6\mathbf{S}$, respectively. Until today, much more point representations were used in simplified Weierstrass form of elliptic curves for fast computations, such as Jacobian, Chudnovsky and mixed coordinates. The mixed addition formulae can also be obtained by replacing $Z_2 = 1$ in this form that reduces the total costs to $9\mathbf{M} + 2\mathbf{S}$. In 2002, Brier and Joye [10] obtained the unified point addition formulae for simplified Weierstrass curves in projective coordinates such that the computational cost is $11\mathbf{M} + 5\mathbf{S} + 1\mathbf{D}$.

For the rest of the paper, we enumerate the cost of field operations in terms of multiplication **M**, squaring **S**, multiplication by a constant **D**, and addition/subtraction **a** in $\mathbb{F}$.

III. Normal Form of Elliptic Curves

In this section, we will discuss salient features of Edwards curves and their variants in respect of point addition and point doubling.

A. Edwards Curves

Edwards [13] introduced a new model of elliptic curves over $\mathbb{F}$ with $\text{char}(\mathbb{F}) \neq 2$ which is defined by

$$E(\mathbb{F}) : \ x^2 + y^2 = c^2(1 + x^2y^2), \tag{3}$$

where $c \in \mathbb{F}$. He obtained an efficient explicit formula for point addition of these curves as follows: Let $P = (x_1, y_1)$ and $Q = (x_2, y_2)$ be two points on $E(\mathbb{F})$. Then $P + Q = (x_3, y_3)$, where

$$\begin{cases} x_3 = \dfrac{x_1y_2 + x_2y_1}{c(1 + x_1x_2y_1y_2)}, \\ y_3 = \dfrac{y_1y_2 - x_1x_2}{c(1 - x_1x_2y_1y_2)}. \end{cases}$$

Edwards showed that all elliptic curves over non-binary finite field $\mathbb{F}$ can be transformed to Edwards curves if $\mathbb{F}$ is algebraically closed. However, over the finite field $\mathbb{F}$, only a small number of elliptic curves can be expressed in this form.

Bernstein and Lange [2] improved the notion of Edwards form defined by

$$E(\mathbb{F}) : \ x^2 + y^2 = 1 + dx^2y^2, \tag{4}$$

where $d \in \mathbb{F} \setminus \{0, 1\}$. They showed that more than 1/4 of all isomorphism classes of elliptic curves over the finite field $\mathbb{F}$ could be transformed to Edwards curve over the same field. They presented fast explicit formulae for point addition as follows: Let $P = (x_1, y_1)$ and $Q = (x_2, y_2)$ be two points on $E(\mathbb{F})$. Then $P + Q = (x_3, y_3)$, where

$$\begin{cases} x_3 = \dfrac{x_1y_2 + x_2y_1}{1 + dx_1x_2y_1y_2}, \\ y_3 = \dfrac{y_1y_2 - x_1x_2}{1 - dx_1x_2y_1y_2}. \end{cases}$$

These formulae are strongly unified. The point $(0, 1)$ is the identity element of addition law. The point $(0, -1)$ has order 2. The points $(1, 0)$ and $(-1, 0)$ have order 4. The inverse of the point (x_1, y_1) on $E(\mathbb{F})$ is $(-x_1, y_1)$.

In order to avoid the inversion in addition formulae given above, the notion of Edwards curves in projective coordinates [2] is defined by

$$(X^2 + Y^2)Z^2 = (Z^4 + dX^2Y^2). \tag{5}$$

The point addition for (5) is obtained by the following formulae: Let $P = (X_1 : Y_1 : Z_1)$ and $Q = (X_2 : Y_2 : Z_2)$ be two points on (5), then $P + Q = (X_3 : Y_3 : Z_3)$, where

$$\begin{cases} X_3 = Z_1Z_2(Z_1^2Z_2^2 - dX_1X_2Y_1Y_2)[(X_1 + Y_1)(X_2 + Y_2) \\ \qquad -X_1X_2 - Y_1Y_2], \\ Y_3 = Z_1Z_2(Z_1^2Z_2^2 + dX_1X_2Y_1Y_2)(Y_1Y_2 - X_1X_2), \\ Z_3 = (Z_1^2Z_2^2 - dX_1X_2Y_1Y_2)(Z_1^2Z_2^2 + dX_1X_2Y_1Y_2). \end{cases}$$

These formulae are also unified. The point $(0 : 1 : 1)$ is the identity element of addition law. The inverse of $(X : Y : Z)$ is $(-X : Y : Z)$. The computational cost for addition, doubling, and unified addition is $10\mathbf{M} + 1\mathbf{S} + 1\mathbf{D} + 7\mathbf{a}$, $3\mathbf{M} + 4\mathbf{S} + 6\mathbf{a}$, and $10\mathbf{M} + 1\mathbf{S} + 1\mathbf{D} + 7\mathbf{a}$, respectively. The mixed addition formulae can also be obtained by replacing $Z_2 = 1$ in the above formulae that reduces the total costs to $9\mathbf{M} + 1\mathbf{S} + 1\mathbf{D} + 7\mathbf{a}$. The presence of point of order 4 in the group of elliptic curves in equation (5), reduces the number of elliptic curves in Edwards model over $\mathbb{F}$. To overcome this problem Bernstein et al. [7] introduced further variation of Edwards curves which is so called Twisted Edwards curves.

B. Twisted Edwards Curves

Let $\mathbb{F}$ be a field with char($\mathbb{F}$)$\neq$ 2. Then Twisted Edwards curve is defined by

$$E_{E,a,d}: \; ax^2 + y^2 = 1 + dx^2y^2, \tag{6}$$

where $a,\ d \in \mathbb{F}\backslash\{0\}$. The point addition for (6) is obtained by the following formulae: Let $P = (x_1, y_1)$ and $Q = (x_2, y_2)$ be two points on $E_{E,a,d}$. Then $P + Q = (x_3, y_3)$, where

$$\begin{cases} x_3 = \dfrac{x_1y_2 + x_2y_1}{1 + dx_1x_2y_1y_2}, \\ y_3 = \dfrac{y_1y_2 - ax_1x_2}{1 - dx_1x_2y_1y_2}. \end{cases}$$

These formulae are unified. The point $(0, 1)$ is the identity element of addition law and the inverse of the point (x, y) on $E_{E,a,d}(\mathbb{F})$ is $(-x, y)$. If a is square in $\mathbb{F}$ and d is non-square in $\mathbb{F}$, then the addition law for Twisted Edwards curve is complete, i.e, it works for all pairs of inputs.

In order to avoid inversion in addition formulae given above, twisted Edwards curves in projective coordinates is defined by

$$(aX^2 + Y^2)Z^2 = Z^4 + dX^2Y^2. \tag{7}$$

For $Z_1 \neq 0$, the homogeneous point $(X_1 : Y_1 : Z_1)$ represents the affine point $(X_1/Z_1, Y_1/Z_1)$ on $E_{E,a,d}$. Bernstein et al. [7] obtained the following explicit formulae for addition and doubling on twisted Edwards curves in projective coordinates as follows: Let $P = (X_1 : Y_1 : Z_1)$ and $Q = (X_2 : Y_2 : Z_2)$ be two points on (7), then $P + Q = (X_3 : Y_3 : Z_3)$, where

$$\begin{cases} X_3 = (X_1Y_2 - Y_1X_2)(X_1Y_1Z_2^2 + X_2Y_2Z_1^2), \\ Y_3 = (Y_1Y_2 + aX_1X_2)(X_1Y_1Z_2^2 - X_2Y_2Z_1^2), \\ Z_3 = Z_1Z_2(X_1Y_2 - Y_1X_2)(Y_1Y_2 + aX_1X_2), \end{cases}$$

and $2P = (X_3 : Y_3 : Z_3)$, where

$$\begin{cases} X_3 = (aX_1^2 + Y_1^2 - 2Z_1^2)[(X_1 + Y_1)^2 - X_1^2 - Y_1^2] \\ Y_3 = (aX_1^2 + Y_1^2)(aX_1^2 - Y_1^2), \\ Z_3 = (aX_1^2 + Y_1^2)(aX_1^2 + Y_1^2 - 2Z_1^2). \end{cases}$$

The computational cost of point addition and point doubling are $11\mathbf{M} + 2\mathbf{D} + 9\mathbf{a}$ and $3\mathbf{M} + 4\mathbf{S} + 1\mathbf{D} + 7\mathbf{a}$, respectively. It turns out that a mixed addition requires $9\mathbf{M} + 2\mathbf{D} + 9\mathbf{a}$ by setting $Z_2 = 1$.

The unified addition formulae for twisted Edwards curves in projective coordinates are also obtained as follows: Let $P = (X_1 : Y_1 : Z_1)$ and $Q = (X_2 : Y_2 : Z_2)$ be two points on (7), then $P + Q = (X_3 : Y_3 : Z_3)$, where

$$\begin{cases} X_3 = Z_1Z_2(Z_1^2Z_2^2 - dX_1X_2Y_1Y_2)[(X_1 + Y_1)(X_2 + Y_2) \\ \qquad -X_1X_2 - Y_1Y_2], \\ Y_3 = Z_1Z_2(Z_1^2Z_2^2 + dX_1X_2Y_1Y_2)(Y_1Y_2 - aX_1X_2), \\ Z_3 = (Z_1^2Z_2^2 + dX_1X_2Y_1Y_2)(Z_1^2Z_2^2 - dX_1X_2Y_1Y_2), \end{cases}$$

The computational cost of unified addition is $10\mathbf{M}+1\mathbf{S}+2\mathbf{D}+7\mathbf{a}$.

Another way to avoid inversions is to define inverted coordinates as follows:

$$(X^2 + aY^2)Z^2 = X^2Y^2 + dZ^4. \tag{8}$$

where $XYZ \neq 0$. The homogeneous point $(X_1 : Y_1 : Z_1)$ with $X_1Y_1Z_1 \neq 0$ represents the affine point $(Z_1/X_1, Z_1/Y_1)$ on $E_{E,a,d}$. In [4], Bernstein, and Lange introduced these inverted coordinates for the case $a = 1$, and observed that the coordinates save time in addition. Bernstein et al. generalized to arbitrary a in [7]. They also obtained the following explicit formulae for unified addition and doubling on twisted Edwards curves in inverted coordinates as follows: Let $P = (X_1 : Y_1 : Z_1)$ and $Q = (X_2 : Y_2 : Z_2)$ be two points on (8), then $P + Q = (X_3 : Y_3 : Z_3)$, where

$$\begin{cases} X_3 = Z_1Z_2(X_1X_2 + aY_1Y_2)(X_1Y_1Z_2^2 - Z_1^2X_2Y_2), \\ Y_3 = Z_1Z_2(X_1Y_2 - Y_1X_2)(X_1Y_1Z_2^2 + Z_1^2X_2Y_2), \\ Z_3 = (X_1Y_1Z_2^2 - Z_1^2X_2Y_2)(X_1Y_1Z_2^2 - Z_1^2X_2Y_2), \end{cases}$$

and $2P = (X_3 : Y_3 : Z_3)$, where

$$\begin{cases} X_3 = (X_1^2 + aY_1^2)(X_1^2 - aY_1^2), \\ Y_3 = [(X_1 + Y_1)^2 - X_1^2 - Y_1^2](X_1^2 + aY_1^2 - 2dZ_1^2), \\ Z_3 = (X_1^2 - aY_1^2)[(X_1 + Y_1)^2 - X_1^2 - Y_1^2]. \end{cases}$$

The unified addition formulae for twisted Edwards curves in inverted coordinates are also obtained as follows: Let $P = (X_1 : Y_1 : Z_1)$ and $Q = (X_2 : Y_2 : Z_2)$ be two points on (7), then $P + Q = (X_3 : Y_3 : Z_3)$, where

$$\begin{cases} X_3 = (X_1X_2Y_1Y_2 + dZ_1^2Z_2^2)(X_1X_2 - aY_1Y_2), \\ Y_3 = (X_1X_2Y_1Y_2 - dZ_1^2Z_2^2)[(X_1 + Y_1)(X_2 + Y_2) \\ \qquad -X_1X_2 - Y_1Y_2], \\ Z_3 = Z_1Z_2(X_1X_2 - aY_1Y_2)[(X_1 + Y_1)(X_2 + Y_2) \\ \qquad -X_1X_2 - Y_1Y_2], \end{cases}$$

The computational cost of point addition, point doubling and unified addition are $11\mathbf{M}+2\mathbf{D}+9\mathbf{a}$, $3\mathbf{M}+4\mathbf{S}+2\mathbf{D}+6\mathbf{a}$, and $9\mathbf{M}+1\mathbf{S}+2\mathbf{D}+7\mathbf{a}$, respectively. The mixed addition formulae can also be obtained by replacing $Z_2=1$, which gives an obvious saving of $2\mathbf{M}$ since $Z_1\cdot Z_2=Z_1$, leading to a total cost of $9\mathbf{M}+2\mathbf{D}+9\mathbf{a}$.

Hisil et al. [19] introduced the extended Twisted Edwards coordinates by defining an auxiliary coordinate $t=xy$ to represent a point (x,y) on $E_{E,a,d}$ in extended affine coordinates (x,y,t). One can pass to the projective representation $(X:Y:T:Z)$ which satisfies (7) and corresponds to the extended affine point $(X/Z,Y/Z,T/Z)$ with $Z\neq 0$. The auxiliary coordinate T has the property $T=XY/Z$. Let $P=(X_1:Y_1:T_1:Z_1)$ and $Q=(X_2:Y_2:T_2:Z_2)$ be two points on (7) with $Z_1\neq 0$ and $Z_2\neq 0$, then $P+Q=(X_3:Y_3:T_3:Z_3)$, where

$$\begin{cases} X_3=(X_1Y_2+Y_1X_2)(Z_1Z_2-dT_1T_2),\\ Y_3=(Y_1Y_2-aX_1X_2)(Z_1Z_2+dT_1T_2),\\ T_3=(Y_1Y_2-aX_1X_2)(X_1Y_2+Y_1X_2),\\ Z_3=(Z_1Z_2-dT_1T_2)(Z_1Z_2+dT_1T_2).\end{cases}$$

These formulae are unified that derived from the addition formulae on $E_{E,a,d}$. It is deduced from [2] and [7] that these formulae are also complete when d is not a square in $\mathbb{F}$ and a is a square in $\mathbb{F}$. The identity element is represented by $(0:1:0:1)$. The negative of $(X:Y:T:Z)$ is $(-X:Y:-T:Z)$. The computational cost of point addition, point doubling and unified addition are $9\mathbf{M}+1\mathbf{D}+7\mathbf{a}$, $4\mathbf{M}+4\mathbf{S}+1\mathbf{D}+7\mathbf{a}$, and $9\mathbf{M}+2\mathbf{D}+7\mathbf{a}$, respectively. The mixed addition formulae can also be obtained by setting $Z_2=1$ in the above formulae, reduces the total costs to $8\mathbf{M}+1\mathbf{D}+7\mathbf{a}$. This means that one can add $(X_1:Y_1:T_1:Z_1)$ and an extended affine point (x_2,y_2,x_2y_2), which is equally written as $(x_2:y_2:x_2y_2:1)$.

C. Binary Edwards Curves

Let $\mathbb{F}$ be a field with char($\mathbb{F}$)$=2$. Then Binary Edwards curve is defined by

$$E_{B,d_1,d_2}:\ d_1(x+y)+d_2(x^2+y^2)=xy+xy(x+y)+x^2y^2,$$

where $d_1\neq 0$ and $d_2\neq d_1^2+d_1$. The point addition is obtained by the following formulae: Let $P=(x_1,y_1)$ and $Q=(x_2,y_2)$ be two points on E_{B,d_1,d_2}. Then $P+Q=(x_3,y_3)$, where

$$\begin{cases} x_3=\frac{d_1(x_1+x_2)+d_2(x_1+y_1)(x_2+y_2)+(x_1+x_1^2)(x_2(y_1+y_2+1)+y_1y_2)}{d_1+(x_1+x_1^2)(x_2+y_2)},\\ y_3=\frac{d_1(y_1+y_2)+d_2(x_1+y_1)(x_2+y_2)+(y_1+y_1^2)(y_2(x_1+x_2+1)+x_1x_2)}{d_1+(y_1+y_1^2)(x_2+y_2)}.\end{cases}$$

The addition law on E_{B,d_1,d_2} is strongly unified. The point $(0,0)$ is the identity element of addition law and the inverse of the point (x,y) on E_{B,d_1,d_2} is (y,x). The computational cost of addition and doubling in projective coordinates are $21\mathbf{M}+1\mathbf{S}+4\mathbf{D}$ and $2\mathbf{M}+6\mathbf{S}+3\mathbf{D}$, respectively. When $t^2+t+d_2\neq 0$ for all $t\in\mathbb{F}$, the addition law on the binary Edwards curve $E_{B,d_1,d_2}(\mathbb{F})$ is complete. The mixed addition formulae lead to a total cost of $13\mathbf{M}+3\mathbf{S}+3\mathbf{D}$ that can be obtained by $(X_3:Y_3:Z_3)=(X_1:Y_1:Z_1)+(x_2,y_2)$, where $(X_1:Y_1:Z_1)$ and (x_2,y_2) on $E_{B,d_1,d_2}(\mathbb{F})$. Bernstein et al. introduced different methods for computing point addition and point doubling with that of computational costs in [6].

IV. Jacobi Curves

Jacobi curves gained special attention due to resistance against SPA attacks. In this section, the various forms of Jacobi curves are discussed in respect of point addition and point doubling.

A. Jacobi Intersections

Liardet and Smart [25] introduced the Jacobi Intersections over the finite field $\mathbb{F}$ with char($\mathbb{F}$)$\neq 2$ which are defined by

$$E_{J,b}(\mathbb{F}):\begin{cases} x^2+y^2=1,\\ bx^2+t^2=1,\end{cases}\qquad(9)$$

where $b\in\mathbb{F}$ and $b(1-b)\neq 0$. They obtained an explicit unified formulae for point addition on $E_{J,b}$ as follows: Let $P=(x_1,y_1,t_1)$ and $Q=(x_2,y_2,t_2)$ be two points on $E_{J,b}(\mathbb{F})$. Then $P+Q=(x_3,y_3,t_3)$, where

$$\begin{cases} x_3=\frac{x_1y_2t_2+x_2y_1t_1}{y_2^2+x_2^2t_1^2},\\ y_3=\frac{y_1y_2-x_1t_1x_2t_2}{y_2^2+x_2^2t_1^2},\\ t_3=\frac{t_1t_2-bx_1y_1x_2y_2}{y_2^2+x_2^2t_1^2},\end{cases}$$

and $2P=(x_3,y_3)$, where

$$\begin{cases} x_3=\frac{2x_1y_1t_1}{y_1^2+x_1^2t_1^2},\\ y_3=\frac{y_1^2-x_1^2t_1^2}{y_1^2+x_1^2t_1^2},\\ t_3=\frac{t_1^2-bx_1^2y_1^2}{y_1^2+x_1^2t_1^2}.\end{cases}$$

The point $(0,1,1)$ is the identity element of addition law and the inverse of the point (x,y,t) on $E_{J,b}$ is $(-x,y,t)$.

The affine version of Jacobi Intersections has inherent greater computational cost due to the field inversion involved in addition formulae. In order to avoid inversions in addition formulae, Jacobi Intersections in projective coordinates [25] is defined by

$$E_{J,b}(\mathbb{F}):\begin{cases} X^2+Y^2=Z^2,\\ bX^2+T^2=Z^2,\end{cases}\qquad(10)$$

with the map $(x,y,t)=(X/Z,Y/Z,T/Z)\mapsto(X:Y:T:Z)$ for $Z\neq 0$. The unified point addition for (10) is obtained by the following formulae: Let $P=(X_1:Y_1:T_1:Z_1)$ and $Q=(X_2:Y_2:T_2:Z_2)$ be two points on (10), then $P+Q=(X_3:Y_3:T_3:Z_3)$, where

$$\begin{cases} X_3=X_1Z_1Y_2T_2+Y_1T_1X_2Z_2,\\ Y_3=Y_1Z_1Y_2Z_2-X_1T_1X_2T_2,\\ T_3=T_1Z_1T_2Z_2-bX_1Y_1X_2Y_2,\\ Z_3=Z_1^2Y_2^2+X_2^2T_1^2.\end{cases}$$

The point $(0:1:1:1)$ is the identity element of addition law and the inverse of the point $(X:Y:T:Z)$ on $E_{J,b}$ is $(-X:Y:T:Z)$. In this case, the computational cost of point addition, point doubling, and unified addition are $13\mathbf{M}+2\mathbf{S}+1\mathbf{D}+7\mathbf{a}$, $4\mathbf{M}+3\mathbf{S}+5\mathbf{a}$, and $13\mathbf{M}+2\mathbf{S}+1\mathbf{D}+7\mathbf{a}$, respectively. The mixed addition formulae can also be obtained by replacing $Z_2=1$ in the above formulae that reduces the total costs to $11\mathbf{M}+2\mathbf{S}+1\mathbf{D}+7\mathbf{a}$.

B. Twisted Jacobi Intersections

In [16], the twisted Jacobi Intersections which contains Jacobi intersections as a special case was introduced by Feng et al. These curves encompass more number of elliptic curves and have explicit formulae for addition and doubling with almost as fast as the Jacobi Intersections. The twisted Jacobi Intersections over $\mathbb{F}$ with $\mathrm{char}(\mathbb{F})\neq 2$ are defined by

$$E_{J,a,b}(\mathbb{F}):\begin{cases} ax^2+y^2=1,\\ bx^2+t^2=1,\end{cases} \tag{11}$$

where $a,b\in\mathbb{F}$ and $ab(a-b)\neq 0$. They obtained an explicit unified addition formulae on $E_{J,a,b}$ as follows: Let $P=(x_1,y_1,t_1)$ and $Q=(x_2,y_2,t_2)$ be two points on $E_{J,a,b}(\mathbb{F})$. Then $P+Q=(x_3,y_3,t_3)$, where

$$\begin{cases} x_3=\dfrac{x_1y_2t_2+x_2y_1t_1}{y_2^2+ax_1^2t_1^2},\\ y_3=\dfrac{y_1y_2-ax_1t_1x_2t_2}{y_2^2+ax_1^2t_1^2},\\ t_3=\dfrac{t_1t_2-bx_1y_1x_2y_2}{y_2^2+ax_1^2t_1^2}.\end{cases}$$

The point $(0,1,1)$ is the identity element of addition law and the inverse of the point (x,y,t) on $E_{J,a,b}$ is $(-x,y,t)$.

The twisted Jacobi Intersections in projective coordinates [25] is defined by

$$E_{J,a,b}(\mathbb{F}):\begin{cases} aX^2+Y^2=Z^2,\\ bX^2+T^2=Z^2.\end{cases} \tag{12}$$

with the map $(x,y,t)=(X/Z,Y/Z,T/Z)\mapsto(X:Y:T:Z)$ for $Z\neq 0$. The unified point addition on (12) is obtained by the following formulae: Let $P=(X_1:Y_1:T_1:Z_1)$ and $Q=(X_2:Y_2:T_2:Z_2)$ be two points on (12), then $P+Q=(X_3:Y_3:T_3:Z_3)$, where

$$\begin{cases} X_3=X_1Z_1Y_2T_2+Y_1T_1X_2Z_2\\ Y_3=Y_1Z_1Y_2Z_2-aX_1T_1X_2T_2,\\ T_3=T_1Z_1T_2Z_2-bX_1Y_1X_2Y_2,\\ Z_3=Z_1^2Y_2^2+aX_2^2T_1^2.\end{cases}$$

The point $(0:1:1:1)$ is the identity element of addition law and the inverse of the point $(X:Y:T:Z)$ on $E_{J,a,b}$ is $(-X:Y:T:Z)$. In this case, the computational cost of addition, doubling, and unified addition are $12\mathbf{M}+11\mathbf{a}$, $3\mathbf{M}+4\mathbf{S}+1\mathbf{D}+7\mathbf{a}$, and $13\mathbf{M}+2\mathbf{S}+5\mathbf{D}+13\mathbf{a}$, respectively. For a mixed point addition, the number of required multiplications drops to $10\mathbf{M}+11\mathbf{a}$.

C. Jacobi Quartics

Jacobi Quartic [8] curves over the finite field $\mathbb{F}$ with $\mathrm{char}(\mathbb{F})\neq 2,3$ are first defined by

$$E_{J,k}:\ y^2=k^2x^4-(k^2+1)x^2+1, \tag{13}$$

where $k\neq 0,\pm 1$. As usual to improve the security parameter that is to increase number of elliptic curves, a modification in Jacobi Quartic was introduced by Hisil et al. in [20]. The modified Jacobi Quartic curves are so called extended Jacobi Quartic curves which are defined by

$$E_{J,d,a}:\ y^2=dx^4+2ax^2+1, \tag{14}$$

where $a,d\in\mathbb{F}$ with $\mathrm{char}(\mathbb{F})\neq 2,3$. They showed that arithmetic on Jacobi Quartics is faster as compared with Jacobi Intersections. Moreover, unified point addition formulae offer additional security against some side channel attacks as well. They adapted the following addition and doubling formulae from [21]. Let $P=(x_1,y_1)$ and $Q=(x_2,y_2)$ be two points on $E_{J,d,a}$, then $P+Q=(x_3,y_3)$, where

$$\begin{cases} x_3=\dfrac{x_1y_2+y_1x_2}{1-dx_1^2x_2^2},\\ y_3=\dfrac{(y_1y_2+2ax_1x_2)(1+dx_1^2x_2^2)+2dx_1x_2(x_1^2+x_2^2)}{(1-dx_1^2x_2^2)^2},\end{cases}$$

and $2P=(x_3,y_3)$, where

$$\begin{cases} x_3=\delta x_1,\\ y_3=\delta(\delta-y_1)-1,\end{cases}$$

where $\delta=2y_1/(2+2ax_1^2-y_1^2)$. The point $(0,1)$ is the identity element of addition law and the inverse of the point (x,y) on $E_{J,d,a}$ is $(-x,y)$.

In order to avoid inversion in addition formulae given above, the extended Jacobi Quartic curves in Jacobian coordinates with $x=X/Z$ and $y=Y/Z^2$ are defined by

$$Y^2=dX^4-2aX^2Z^2+Z^4, \tag{15}$$

where $a,d\in\mathbb{F}$ with $\mathrm{char}(\mathbb{F})\neq 2,3$. Billet and Joye [8] proposed a faster inversion-free unified addition algorithm on (15) as follows: Let $P=(X_1:Y_1:Z_1)$ and $Q=(X_2:Y_2:Z_2)$ be two points on (15), then $P+Q=(X_3:Y_3:Z_3)$, where

$$\begin{cases} X_3=X_1Y_2Z_1+X_2Y_1Z_2,\\ Y_3=[(Z_1Z_2)^2+d(X_1X_2)^2](Y_1Y_2-2aX_1X_2Z_1Z_2)\\ \qquad +2dX_1X_2Z_1Z_2(X_1^2Z_2^2+Z_1^2X_2^2),\\ Z_3=(Z_1Z_2)^2-d(X_1X_2)^2,\end{cases}$$

The identity element of addition law is given by $(0:1:1)$ and the negative of the point $(X:Y:Z)$ is $(-X:Y:Z)$. The computational cost of addition, doubling, and unified addition are $10\mathbf{M}+3\mathbf{S}+1\mathbf{D}$, $1\mathbf{M}+9\mathbf{S}+1\mathbf{D}$, and $10\mathbf{M}+3\mathbf{S}+1\mathbf{D}$, respectively. The total cost of point addition reduces to $8\mathbf{M}+3\mathbf{S}+1\mathbf{D}$ by replacing $Z_2=1$.

An other improvement was obtained by Hisil et al. in [20]. They showed that the extended Jacobi Quartic curves in extended projective coordinates was defined by

$$\begin{cases} X^2-TZ=0,\\ Y^2-dT^2-2aX^2-Z^2=0,\end{cases} \tag{16}$$

or simply

$$Y^2Z^2 = dX^4 + 2aX^2Z^2 + Z^4, \tag{17}$$

where T is omitted in the latter case. In this case, a point $(x, y) \in E_{J,d,a}(\mathbb{F})$ corresponds to the point $(X : Y : T : Z)$, where $T = X^2/Z$. The identity element is represented by $(0 : 1 : 0 : 1)$ and negative of $(X : Y : T : Z)$ is $(-X : Y : T : Z)$. They obtained the following explicit formulae for addition and doubling on the extended Jacobi Quartic curves in extended projective coordinates as follows: Let $P = (X_1 : Y_1 : T_1 : Z_1)$ and $Q = (X_2 : Y_2 : T_2 : Z_2)$ be two points on (17), then $P + Q = (X_3 : Y_3 : T_3 : Z_3)$ with $Z_1 \neq 0$, $Z_2 \neq 0$ and $P \neq Q$, where

$$\begin{cases} X_3 = (X_1Y_2 - Y_1X_2)(T_1Z_2 - Z_1T_2), \\ Y_3 = (T_1Z_2 + Z_1T_2 - 2X_1X_2)(Y_1Y_2 - 2aX_1X_2 \\ \qquad +Z_1Z_2 + dT_1T_2) - Z_3, \\ T_3 = (T_1Z_2 - Z_1T_2)^2, \\ Z_3 = (X_1Y_2 - Y_1X_2)^2, \end{cases}$$

and $2P = (X_3 : Y_3 : T_3 : Z_3)$, where

$$\begin{cases} X_3 = X_1Y_2Z_1 + X_2Y_1Z_2, \\ Y_3 = [(Z_1Z_2)^2 + d(X_1X_2)^2](Y_1Y_2 - 2aX_1X_2Z_1Z_2) \\ \qquad +2dX_1X_2Z_1Z_2(X_1^2Z_2^2 + Z_1^2X_2^2), \\ T_3 = (2X_1Y_1)^2, \\ Z_3 = (Z_1Z_2)^2 - d(X_1X_2)^2. \end{cases}$$

If $a = -1/2$, the computational cost of point addition and point doubling are $7\mathbf{M}+3\mathbf{S}+2\mathbf{D}$ and $8\mathbf{S}$, respectively. The total cost of point addition reduces to $6\mathbf{M} + 3\mathbf{S} + 2\mathbf{D}$ by replacing $Z_2 = 1$.

They also obtained the unified addition formulae for extended Jacobi Quartics in extended projective coordinates. If d is not a square in $\mathbb{F}$, then the unified addition formulae are complete. The computational cost is $8\mathbf{M} + 3\mathbf{S} + 2\mathbf{D} + 17\mathbf{a}$ when $a = -1/2$. More on formulae and operation counts can be found Appendix B in [20].

V. Hessian Curves

In [21], Hessian elliptic curves are investigated by Joye and Quisquater. They obtained the formulae of point addition, point doubling and unified addition. The Hessian elliptic curve over $\mathbb{F}$ with $\mathrm{char}(\mathbb{F}) \neq 2, 3$ is a plane cubic curve given by

$$E_{H,d}(\mathbb{F}) \ : \ x^3 + y^3 + 1 = 3dxy, \tag{18}$$

or in projective coordinates,

$$E_{H,d}(\mathbb{F}) \ : \ X^3 + Y^3 + Z^3 = 3dXYZ, \tag{19}$$

where $d \in \mathbb{F}$ and $d^3 \neq 1$. They obtained the following formulae for addition and doubling on Hessian curves in projective coordinates as follows: Let $P = (X_1 : Y_1 : Z_1)$ and $Q = (X_2 : Y_2 : Z_2)$ be two points on (19), then $P + Q = (X_3 : Y_3 : Z_3)$, where

$$\begin{cases} X_3 = Y_1^2X_2Z_2 - Y_2^2X_1Z_1, \\ Y_3 = X_1^2Y_2Z_2 - X_2^2Y_1Z_1, \\ Z_3 = Z_1^2Y_2X_2 - Z_2^2Y_1X_1, \end{cases}$$

and $2P = (X_3 : Y_3 : Z_3)$, where

$$\begin{cases} X_3 = Y_1(Z_1^3 - X_1^3), \\ Y_3 = X_1(Y_1^3 - Z_1^3), \\ Z_3 = Z_1(X_1^3 - Y_1^3). \end{cases}$$

The point $(1 : -1 : 0)$ is the identity element of addition formulae and the inverse of the point $(X : Y : Z)$ on $E_{H,d}(\mathbb{F})$ is $(Y : X : Z)$. The points $(0 : 1 : -1)$ and $(1 : 0 : -1)$ are two points of order 3.

They also described unified addition algorithm as follows: Let $P = (X_1 : Y_1 : Z_1)$ and $Q = (X_2 : Y_2 : Z_2)$ be two points on (19), then $P + Q = (X_3 : Y_3 : Z_3)$, where

$$\begin{array}{ll} \text{Step 1} & \begin{cases} L_1 \leftarrow X_1;\ L_2 \leftarrow Y_1;\ L_3 \leftarrow Z_1 \\ L_4 \leftarrow X_2;\ L_5 \leftarrow Y_2;\ L_6 \leftarrow Z_2 \end{cases} \\ \text{Step 2} & \begin{cases} L_7 \leftarrow L_1 \cdot L_6;\ L_1 \leftarrow L_1 \cdot L_5;\ L_5 \leftarrow L_3 \cdot L_5 \\ L_3 \leftarrow L_3 \cdot L_4;\ L_4 \leftarrow L_2 \cdot L_4;\ L_2 \leftarrow L_2 \cdot L_6 \end{cases} \\ \text{Step 3} & \begin{cases} L_6 \leftarrow L_2 \cdot L_7;\ L_2 \leftarrow L_2 \cdot L_4;\ L_4 \leftarrow L_3 \cdot L_4 \\ L_3 \leftarrow L_3 \cdot L_5;\ L_5 \leftarrow L_1 \cdot L_5;\ L_1 \leftarrow L_1 \cdot L_7 \end{cases} \\ \text{Step 4} & \begin{cases} X_3 \leftarrow L_2 - L_5;\ Y_3 \leftarrow L_1 - L_4;\ Z_3 \leftarrow L_3 - L_6 \end{cases} \end{array}$$

Owing to the formulae $2(X_1 : Y_1 : Z_1) = (Z_1 : X_1 : Y_1) + (Y_1 : Z_1 : X_1)$ and $(X_1 : Y_1 : Z_1) - (X_2 : Y_2 : Z_2) = (X_1 : Y_1 : Z_1) + (Y_2 : X_2 : Z_2)$, the unified addition algorithm given above can be used also doubling and subtraction as well as addition. The computational cost of these operations are $12\mathbf{M}+3\mathbf{a}$. The total cost of point addition reduces to $10\mathbf{M}+3\mathbf{a}$ by replacing $Z_2 = 1$.

More recently, Farashahi and Joye [14] considered a generalized form of Hessian curves that covers more isomorphism classes of elliptic curves. These curves are similar to the twisted Hessian form [5], introduced by Bernstein, Kohel, and Lange, up to the order of the coordinates. The generalized Hessian curve over $\mathbb{F}$ is defined by

$$E_{H,c,d}(\mathbb{F}) \ : \ x^3 + y^3 + c = dxy, \tag{20}$$

where $c, d \in \mathbb{F}$ with $c \neq 0$ and $d^3 \neq 27c$. A generalized Hessian curve over $\mathbb{F}$ is isomorphic over $\mathbb{F}$ to a Hessian curve if and only if c is a cube in $\mathbb{F}$. It is easy to adapt the addition and doubling formulae for generalized Hessian curves which are so-called Sylvester formulas as follows: Let $P = (x_1, y_1)$ and $Q = (x_2, y_2)$ be two points on $E_{H,c,d}(\mathbb{F})$, then $P + Q = (x_3, y_3)$, where

$$\begin{cases} x_3 = \dfrac{y_1^2x_2 - y_2^2x_1}{x_2y_2 - x_1y_1}, \\ y_3 = \dfrac{x_1^2y_2 - x_2^2y_1}{x_2y_2 - x_1y_1}, \end{cases}$$

and $2P = (x_3, y_3)$, where

$$\begin{cases} x_3 = \dfrac{y_1(c - x_1^3)}{x_1^3 - y_1^3}, \\ y_3 = \dfrac{x_1(c - y_1^3)}{x_1^3 - y_1^3}. \end{cases}$$

Furthermore, the inverse of the point (x_1, y_1) on $E_{H,c,d}(\mathbb{F})$ is the point (y_1, x_1). The generalized Hessian curves in projective coordinates are defined by

$$E_{H,c,d}(\mathbb{F}) \ : \ X^3 + Y^3 + cZ^3 = dXYZ. \tag{21}$$

The point $(1 : -1 : 0)$ is identity element and the inverse of the point $(X : Y : Z)$ on $E_{H,c,d}(\mathbb{F})$ is $(Y : X : Z)$. They obtained point addition and doubling formulae on generalized Hessian curves in projective coordinates as follows: Let $P = (X_1 : Y_1 : Z_1)$ and $Q = (X_2 : Y_2 : Z_2)$ be two points on $E_{H,c,d}(\mathbb{F})$, then $P + Q = (X_3 : Y_3 : Z_3)$, where

$$\begin{cases} X_3 = X_2Z_2Y_1^2 - X_1Z_1Y_2^2, \\ Y_3 = Y_2Z_2X_1^2 - Y_1Z_1X_2^2, \\ Z_3 = X_2Y_2Z_1^2 - X_1Y_1Z_2^2, \end{cases}$$

and $2P = (X_3 : Y_3 : Z_3)$, where

$$\begin{cases} X_3 = Y_1(cZ_1^3 - X_1^3), \\ Y_3 = X_1(Y_1^3 - cZ_1^3), \\ Z_3 = Z_1(X_1^3 - Y_1^3). \end{cases}$$

In this case, the computational cost of point addition is **4M**, **3M**, or **2M** correspond to use of $3, 4$ or 6 processors, respectively. The point addition formulae are complete if the difference of all pairs of points on $E_{H,c,d}(\mathbb{F})$ is not equal the identity. The cost of point doubling is $\mathbf{6M} + \mathbf{3S} + \mathbf{1D}$. The point doubling formulae are complete for all inputs.

The unified addition formulae for generalized Hessian curves in projective coordinates are also obtained as follows: Let $P = (X_1 : Y_1 : Z_1)$ and $Q = (X_2 : Y_2 : Z_2)$ be two points on $E_{H,c,d}(\mathbb{F})$, then $P + Q = (X_3 : Y_3 : Z_3)$, where

$$\begin{cases} X_3 = cY_2Z_2Z_1^2 - X_1Y_1X_2^2, \\ Y_3 = X_2Y_2Y_1^2 - cX_1Z_1Z_2^2, \\ Z_3 = X_2Z_2X_1^2 - Y_1Z_1Y_2^2. \end{cases}$$

The computational cost of unified point addition is $\mathbf{12M} + \mathbf{1D}$. The unified point addition formulae on $E_{H,c,d}(\mathbb{F})$ are complete if c is not a cube in $\mathbb{F}$. It turns out that a mixed addition requires $\mathbf{10M} + \mathbf{1D}$ by setting $Z_2 = 1$.

Farashahi and Joye [14] obtained point addition, doubling and tripling formulae for binary generalized Hessian curves with the computational cost of them. Differential addition, that is, point addition with a known difference was also devised for binary Hessian curves by them.

VI. Huff Model of Elliptic Curves

In this section, we will give the details of the models of Huff curves, especially their group structure and related formulae with associated computational costs.

A. Huff Curves

In [18], Huff investigated the Huff elliptic curves over rational fields $\mathbb{Q}$ in 1948. Joye et al. [22] improved these curves to the finite field $\mathbb{F}$ with $\mathrm{char}(\mathbb{F}) \neq 2$ that are given by

$$ax(y^2 - 1) = by(x^2 - 1), \tag{22}$$

where $a, b \neq 0$ and $a^2 - b^2 \neq 0$. The Huff model of elliptic curves in projective coordinates are defined by

$$aX(Y^2 - Z^2) = bY(X^2 - Z^2), \tag{23}$$

where $a, b \neq 0$ and $a^2 - b^2 \neq 0$. The unified addition formulae on (23) is obtained by the following formulae: Let $P = (X_1 : Y_1 : Z_1)$ and $Q = (X_2 : Y_2 : Z_2)$ be two points on (23), then $P + Q = (X_3 : Y_3 : Z_3)$, where

$$\begin{cases} X_3 = (X_1Z_2 + X_2Z_1)(Y_1Y_2 + Z_1Z_2)(Y_1Z_2 + Y_2Z_1), \\ Y_3 = (X_1X_2 - Z_1Z_2)(Z_1^2Z_2^2 - Y_1^2Y_2^2), \\ Z_3 = (Y_1Z_2 + Y_2Z_1)(X_1X_2 + Z_1Z_2)(Y_1Y_2 - Z_1Z_2). \end{cases}$$

Note that the above formulae are independent of curve parameters $a, b \in \mathbb{F}$. The computational cost of point addition, point doubling, and unified addition are **12M**, $\mathbf{6M} + \mathbf{5S}$, and **11M**, respectively. For a mixed point addition (i.e., when $Z_2 = 1$), the number of required multiplications drops to **10M**.

Joye et al. [22] investigated twist of Huff curves defined by

$$ax(y^2 - d) = by(x^2 - d), \tag{24}$$

where $abd(a^2 - b^2) \neq 0$. These curves are also defined in projective coordinates as follows:

$$aX(Y^2 - dZ^2) = bY(X^2 - dZ^2), \tag{25}$$

where $abd(a^2 - b^2) \neq 0$. They obtained point addition formulae with performing **12M** that one could look at [22].

In order to improve the number of isomorphism classes, a generalized Huff curves was introduced by Wu, and Feng in [15]. It is note worthy that the Huff curve family is included in the generalized Huff curves. These curves over the finite field $\mathbb{F}$ with $char(\mathbb{F}) \neq 2$ are defined by

$$x(ay^2 - 1) = y(bx^2 - 1), \tag{26}$$

where $ab(a - b) \neq 0$. In order to avoid inversion for addition formulae in affine coordinates, the generalized Huff curves in projective coordinates are defined by

$$X(aY^2 - Z^2) = Y(bX^2 - Z^2), \tag{27}$$

with the map $(x, y) \mapsto (X : Y : Z)$ for $Z \neq 0$. In this case, there are three identity elements, namely $(1 : 0 : 0), (0 : 1 : 0)$ and $(a : b : 0)$. The negative of $(X_1 : Y_1 : Z_1)$ is $(X_1 : Y_1 : -Z_1)$. We will discuss addition of any two points in each case by selecting one identity point. Let $P = (X_1 : Y_1 : Z_1)$ and $Q = (X_2 : Y_2 : Z_2)$ be two points on (27) and choose $(1 : 0 : 0)$ as identity element. Then $P + Q = (X_3 : Y_3 : Z_3)$,

where

$$\begin{cases} X_3 = (bX_1X_2 - Z_1Z_2)(bX_1X_2 + Z_1Z_2) \\ \quad (Z_1Z_2 - aY_1Y_2), \\ Y_3 = b(X_1Z_2 + X_2Z_1)(bX_1X_2 + Z_1Z_2) \\ \quad (Y_1Z_2 + Y_2Z_1), \\ Z_3 = b(X_1Z_2 + X_2Z_1)(bX_1X_2 - Z_1Z_2) \\ \quad (aY_1Y_2 + Z_1Z_2). \end{cases}$$

These formulae are unified. The computational cost of point addition and doubling corresponding the identity element $(1 : 0 : 0)$ are $11\mathbf{M} + 3\mathbf{D}$ and $6\mathbf{M} + 5\mathbf{S} + 3\mathbf{D}$, respectively. For a mixed point addition (i.e., when $Z_2 = 1$), the number of required multiplications drops to $10\mathbf{M}+3\mathbf{D}$. For other identity elements, we refer the reader to [15] to examine the related point addition formulae and more.

Ciss, and Sow introduced the new generalized Huff curves over the finite field $\mathbb{F}$ of $\text{char}(\mathbb{F}) \neq 2$ in [11]. These curves are defined by

$$ax(y^2 - c) = by(x^2 - d), \tag{28}$$

where $a, b, c, d \in \mathbb{F}$ with $abcd(a^2c - b^2d) \neq 0$. The new generalized Huff curves contains the generalized Huff's model $ax(y^2 - d) = by(x^2 - d)$ with $abd(a^2 - b^2) \neq 0$ of Joye et al. [22] and the generalized Huff curves $x(ay^2 - 1) = y(bx^2 - 1)$ with $ab(a - b) \neq 0$ of Wu and Feng [15] as a special case. They obtained the addition formulae of new generalized Huff curves in affine coordinates that we omit this paper.

In order to avoid inversion in addition formulae, the new generalized Huff curves in projective coordinates are defined by

$$aX(Y^2 - cZ^2) = bY(X^2 - dZ^2), \tag{29}$$

where $a, b, c, d \in \mathbb{F}$ with $abcd(a^2c - b^2d) \neq 0$. The identity elements are of the form $(X : Y : 0)$. The addition law in projective coordinates is as fast as in the previous particular cases. They obtained point addition and point doubling on (29) by the following formulae: Let $P = (X_1 : Y_1 : Z_1)$ and $Q = (X_2 : Y_2 : Z_2)$ be two points on (29), then $P + Q = (X_3 : Y_3 : Z_3)$, where

$$\begin{cases} X_3 = d(X_1Z_2 + X_2Z_1)(cZ_1Z_2 + Y_1Y_2)^2 \\ \quad (dZ_1Z_2 - X_1X_2), \\ Y_3 = c(Y_1Z_2 + Y_2Z_1)(dZ_1Z_2 + X_1X_2) \\ \quad (cZ_1Z_2 - Y_1Y_2), \\ Z_3 = (d^2Z_1^2Z_2^2 - X_1^2X_2^2)(c^2Z_1^2Z_2^2 - Y_1^2Y_2^2), \end{cases}$$

and $2P = (X_3 : Y_3 : Z_3)$, where

$$\begin{cases} X_3 = 2dX_1(cZ_1^2 + Y_1^2)^2(dZ_1^2 - X_1^2), \\ Y_3 = 2cY_1(dZ_1^2 + X_1^2)^2(cZ_1^2 - Y_1^2), \\ Z_3 = (d^2Z_1^4 - X_1^4)(c^2Z_1^4 - Y_1^4). \end{cases}$$

The computational cost of point addition and point doubling formulae are $12\mathbf{M} + 4\mathbf{D}$ and $7\mathbf{M} + 5\mathbf{S} + 4\mathbf{D}$, respectively. The total cost of point addition reduces to $11\mathbf{M} + 4\mathbf{D}$ by replacing $Z_2 = 1$. For further details we refer the reader to look at [11].

B. Binary Huff Curves

Joye et al. [22] introduced the binary Huff curves over $\mathbb{F}$ with $\text{char}(\mathbb{F}) = 2$ which are defined by

$$ax(y^2 + y + 1) = by(x^2 + x + 1), \tag{30}$$

or in projective coordinates

$$aX(Y^2 + YZ + Z^2) = bY(X^2 + XZ + Z^2), \tag{31}$$

where $ab(a - b) \neq 0$. Devigne and Joye [12] described the addition law for binary Huff curves. They showed that there are three points at infinity satisfying the curve equation, namely $(a : b : 0)$, $(1 : 0 : 0)$, and $(0 : 1 : 0)$. They obtained unified point addition formulae as follows: Let $P = (X_1 : Y_1 : Z_1)$ and $Q = (X_2 : Y_2 : Z_2)$ be two points on (31), then $P + Q = (X_3 : Y_3 : Z_3)$ with

$$\begin{cases} X_3 = (Z_1Z_2 + Y_1Y_2)[(X_1Z_2 + X_2Z_1)(Z_1^2Z_2^2 \\ \quad + X_1X_2Y_1Y_2) + \alpha X_1X_2Z_1Z_2(Z_1Z_2 + Y_1Y_2)], \\ Y_3 = (Z_1Z_2 + X_1X_2)[(Y_1Z_2 + Y_2Z_1)(Z_1^2Z_2^2 \\ \quad + X_1X_2Y_1Y_2) + \beta Y_1Y_2Z_1Z_2(Z_1Z_2 + X_1X_2)], \\ Z_3 = (Z_1Z_2 + X_1X_2)(Z_1Z_2 + Y_1Y_2) \\ \quad (Z_1^2Z_2^2 + X_1X_2Y_1Y_2), \end{cases}$$

where $\alpha = (a + b)/b$ and $\beta = (a + b)/a$. The computational cost of unified point addition is $15\mathbf{M} + 2\mathbf{D}$.

The generalized binary Huff curves over $\mathbb{F}$ with $\text{char}(\mathbb{F}) = 2$ are also defined by Devigne and Joye [12] which are of the form

$$ax(y^2 + fy + 1) = by(x^2 + fx + 1), \tag{32}$$

or in projective coordinates

$$aX(Y^2 + fYZ + Z^2) = bY(X^2 + fXZ + Z^2), \tag{33}$$

where $abf(a - b) \neq 0$. They obtained the unified addition formulae of generalized binary Huff curves in affine coordinates that we omit this paper. For more information and formulae, we refer the reader to [12].

VII. Comparison and Conclusions

In this paper, the alternative models of elliptic curves are surveyed by pinning down group operations, and performance in various coordinate systems. Table 1 summarizes the speeds of addition, doubling, mixed addition and unified addition on alternate models of elliptic curves. The comparison in affine coordinates is skipped so that the cost of field inversion is so expensive. We enumerate the cost of field operations in terms of multiplication $\mathbf{M}$, squaring $\mathbf{S}$, and multiplication by a constant $\mathbf{D}$ in $\mathbb{F}$.

The unified addition formulae offer inherited countermeasure against SPA with comparable performance. In these models, SPA is avoided by employing the unified addition formulae or an algorithmic adaptation of it that behaves in similar fashion during the process of point addition and point doubling.

TABLE I
COST OF ARITHMETIC ON ALTERNATE MODELS OF ELLIPTIC CURVES

EC Model	Coordinates	Addition	Doubling	Mixed Addition ($Z_2 = 1$)	Unified Addition
Weierstrass	Projective	12M + 2S	5M+6S	9M+2S	11M + 5S + 1D
Edwards	Projective	10M+1S+1D	3M+4S	9M+1S+1D	10M+1S+1D
Twisted Edwards	Projective	11M+2D	3M+4S+1D	9M+2D	10M+1S+2D
	Inverted	11M+2D	3M+4S+2D	9M+2D	9M+1S+2D
	Extended	9M+1D	4M+4S+1D	8M+1D	9M+2D
Jacobi Intersections	Projective	13M+2S+1D	4M+3S	11M+2S+1D	13M+2S+1D
Twisted Jacobi Intersections	Projective	12M	3M+4S+1D	10M	13M+2S+5D
Extended Jacobi Quartics	Jacobian	10M+3S+1D	1M+9S+1D	8M+3S+1D	10M+3S+1D
	Extended Projective	7M+3S+2D	8S	6M+3S+2D	8M+3S+2D
Hessian Curves	Projective	12M	12M	10M	12M
Generalized Hessian Curves	Projective	12M+1D	6M+3S+1D	10M+1D	12M+1D
Huff Curves	Projective	12M	6M+5S	10M	11M
Generalized Huff Curves	Projective	11M+3D	6M+5S+3D	10M+3D	11M+3D
New Generalized Huff Curves	Projective	12M+4D	7M+5S+4D	11M+4D	Open Prob

ACKNOWLEDGMENT

We would like to express my sincere gratitude to the anonymous referees for their valuable comments, to Professor Ersan Akyıldız for his diligent guidance and encouragement.

REFERENCES

[1] D. Agrawal, B. Archambeault, J.R. Rao, P. Rohatgi, *The EM Side-Channel(s)*. Cryptographic Hardware and Embedded Systems - CHES 2002, Lecture Notes in Computer Science Vol. 2523, Springer-Verlag, pp. 29-45, 2003.

[2] D. Bernstein, and T. Lange, *Faster addition and doubling on elliptic curves*. Progress in Cryptology - Africacrypt 2007, Lecture Notes in Computer Science Vol. 4833, Springer, pp. 29-50, 2007.

[3] D. Bernstein, and T. Lange, *Explicit Formulas Database*, Available at http://www.hyperelliptic.org/EFD

[4] D. Bernstein, and T. Lange, *Inverted Edwards coordinates*. Applied Algebra, Algebraic Algorithms and Error-Correcting Codes, 17th International Symposium - AAECC-17, Lecture Notes in Computer Science Vol. 4851, Springer, pp. 20-27, 2007.

[5] D. Bernstein, D. Kohel, and T. Lange, *Twisted Hessian curves*. Available at http://www.hyperelliptic.org/EFD/g1p/auto-twistedhessian.html.

[6] D. Bernstein, T. Lange, and R. R. Farashahi, *Binary Edwards Curves*. Cryptographic Hardware and Embedded Systems - CHES 2008, Lecture Notes in Computer Science Vol. 5154, Springer, pp. 244-265, 2008.

[7] D. Bernstein, P. Birkner, M. Joye, T. Lange, and C. Peters, *Twisted Edwards curves*, Progress in Cryptology - Africacrypt 2008, Lecture Notes in Computer Science Vol. 5023, Springer, pp. 389-405, 2008.

[8] O. Billet, and M. Joye, *The Jacobi model of an elliptic curve and side-channel analysis*, AAECC 2003, Lecture Notes in Computer Science Vol. 2643, Springer-Verlag, pp. 34-42, 2003.

[9] E. Biham, and A. Shamir, *Differential fault analysis of secret key cryptosystems*. Advances in Cryptology - Crypto '97, Lecture Notes in Computer Science Vol. 1294, Springer-Verlag, pp. 513-525, 1997.

[10] E. Brier, and M. Joye, *Weierstrass elliptic curves and side-channel attacks*. Public Key Cryptography - PKC 2002, Lecture Notes in Computer Science Vol. 2274, Springer, pp. 335-345, 2002.

[11] A. A. Ciss and D. Sow, *On a New Generalization of Huff Curves*. Available at http://eprint.iacr.org/2011/580.pdf.

[12] J. Devigne, and M. Joye, *Binary Huff Curves*. Topics in Cryptology - CT-RSA 2011, Lecture Notes in Computer Science Vol. 6558, Springer, pp. 340-355, 2011.

[13] H. Edwards, *A normal form for elliptic curves*. Bulletin of the American Mathematical Society 44(3) , pp. 393-422, 2007.

[14] R. R. Farashahi, and M. Joye, *Efficient Arithmetic on Hessian Curves*. Public Key Cryptography - PKC 2010, Lecture Notes in Computer

[15] H. Wu, and R. Feng, *Elliptic curves in Huff's model*. Available at http://eprint.iacr.org/2010/390.pdf, 2010.

[16] R. Feng, M. Nie, and H. Wu, *Twisted Jacobi Intersections Curves*. Available at http://eprint.iacr.org/2009/597.pdf

[17] T. S. Gustavsen, and K. Ranestad, *A Simple Point Counting Algorithm for Hessian Elliptic Curves in Characteristic Three*. Appl. Algebra Eng. Commun. Comput. 17(2), pp. 141150, 2006.

[18] G. Huff, *Diophantine problems in geometry and elliptic ternary forms*. Duke Math. J., 15, pp. 443-453, 1948.

[19] H. Hisil, K. Koon-Ho Wong, G. Carter, and E. Dawson, *Twisted Edwards Curves Revisited*. Advances in Cryptology - Asiacrypt 2008, Lecture Notes in Computer Science Vol. 5350, Springer-Verlag, pp. 326-343, 2008.

[20] H. Hisil, K. Koon-Ho Wong, G. Carter, and E. Dawson, *Jacobi Quartic Curves Revisited*. ACISP 2009, pp. 452-468, 2009.

[21] M. Joye, and J. Quisquater, *Hessian elliptic curves and side-channel attacks*. Cryptographic Hardware and Embedded Systems - CHES 2001, Lecture Notes in Computer Science Vol. 2162, Springer, pp. 402-410, 2001.

[22] M.Joye, M. Tibbouchi, and D. Vergnaud, *Huff's Model for Elliptic Curves*. Algorithmic Number Theory - ANTS-IX, Lecture Notes in Computer Science Vol. 6197, Springer, pp. 234-250, 2010.

[23] P. C. Kocher, *Timing Attacks on Implementations of Diffie-Hellman, RSA, DSS, and Other Systems*. Advances in Cryptology - Crypto '96, Lecture Notes in Computer Science Vol. 1109, Springer, pp. 104-113, 1996.

[24] P. Kocher, J. Jaffe, and B. Jun, *Differential Power Analysis*. Advances in Cryptology - Crypto'99, Lecture Notes in Computer Science Vol. 1666, Springer-Verlag, pp. 388-397, 1999.

[25] P. Liardet, and N. Smart, *Preventing SPA/DPA in ECC systems using the Jacobi form*. Cryptographic Hardware and Embedded Systems - CHES 2001, Lecture Notes in Computer Science Vol. 2162, Springer-Verlag, pp. 391-401, 2001.

[26] N. Smart, and E. J. Westwood, *Point Multiplication on Ordinary Elliptic Curves over Fields of Characteristic Three*. Appl. Algebra Eng. Commun. Comput. 13(6), pp. 485-497, 2003.

Optimal Frekans Atlamalı Diziler

Seda Kahraman ve Zülfükar Saygı

***Özet*—Bu çalışmanın amacı, Frekans Atlamalı Kod Bölüşümlü Çoklu Erişim[1] (FH-CDMA), Bluetooth ve ultra geniş bant gibi popüler sistemlerde kullanılan Optimal Frekans Atlamalı Dizilerin (FHS lerin) oluşturulmasıdır. Literatürde optimalliği belirleyen sınırlar bulunmaktadır. Bu çalışmada bahsedilen optimallik Lempel-Greenberger ve Peng-Fan anlamındadır. FHS lerin oluşturulmasında kullanılan cebirsel, kombinatorik vs. gibi bir çok metod vardır. Bunların içinden cebirsel bir üretim metodu olan İz Fonksiyonu ile üretim yapan 4 makale incelenmiş ve bunların MAGMA ile gerçekleştirimi yapılarak örnekleri incelenmiştir. Ayrıca yeni optimal dizilerin ve dizi çiftlerinin varlığı araştırılmıştır.**

***Anahtar Kelimeler*—Frekans atlamalı diziler, Hamming korelasyonu, optimal frekans atlamalı diziler, İz fonksiyonu, optimal frekans atlamalı dizi çiftleri, optimal frekans atlamalı dizi ailesi.**

***Abstract*—The aim of this paper is the constructions of optimal frequency hopping sequences (FHS) that are used in Frequency Hopping Code Division Multiple Access (FH-CDMA) systems, Bluetooth and ultra wide band. There are some bounds in the literature to determine the optimality. The optimality in this work is referred to Lempel-Greenberger and Peng-Fan. There are some constructions techniques for FHSs such that algebraic, combinatorial, etc. We have examined 4 different papers in which the Trace function is used for the constructions and we have implemented the corresponding MAGMA codes. Also new optimal sequences and sequence pairs are investigated.**

***Index Terms*—Frequency hopping sequences, Hamming correlation, optimal frequency hopping sequences, Trace function, optimal FHS pairs, optimal FHS family.**

I. Giriş

FREKANS atlamalı diziler, Frekans Atlamalı Yayılı İzge (FHSS) sistemlerinde kullanılmaktadır. FHSS sistemleri, karıştırıcı önleme[2], güvenli ve çoklu erişim sağlama özellikleri ile ordu radyo iletişimi, mobil iletişim, modern radar ve deniz radarı yankı-konum sistemlerinde[3] yaygın olarak kullanılır [2], [8]. Frekans Atlamalı Kod Bölüşümlü Çoklu Erişim (FH-CDMA), Bluetooth ve ultra geniş bant gibi popüler sistemler en önemli kullanım alanlarıdır [4], [10], [11], [12]. FHSS önemli bir modülasyon tekniğidir. Bu tekniğin geliştirilmesini sağlayan en önemli sebep Yakın-Uzak Probleminin [19] etkisini oldukça azaltarak çoklu erişime imkan sağlamasıdır. Bu teknikte vericiler frekanslar arasında atlayarak veri gönderdiği için aynı anda aynı frekansı kullanmaya çalışmadıkları sürece çakışma olmadan alıcıya veri aktarabileceklerdir. Çakışma olmaması için de FHSS de kullanılan frekans atlamalı dizilerin optimal olması gerekir. Yani iyi bir Hamming Korelasyonuna sahip olmalıdırlar. FHSS sistemlerinde optimalliğin yanısıra diziyi üreten LFSR nin boyu olarak tanımlanan doğrusal karmaşıklığın da büyük olması beklenir [5]. Bu çalışmada incelenen makaleler sadece optimallik üzerinde durmuşlardır. Çalışmalarda kullanılan optimallik Lempel-Greenberger ve Peng-Fan anlamındadır. FHS lerin oluşturulmasında kullanılan cebirsel, kombinatorik vs. gibi bir çok metod vardır. Detaylı bilgi ve referanslar için [17] çalışması incelenebilir. Bunların içinden cebirsel bir üretim metodu olan İz Fonksiyonu ile üretim yapan 4 makale incelenmiş ve bunların MAGMA ile gerçekleştirimi yapılarak örnekleri incelenmiştir. Ayrıca yeni optimal dizilerin varlığı araştırılmıştır.

Gerçek hayat uygulamalarında kullanmak için çeşitli uzunluklarda diziler gerekebilir. Bu nedenle farklı dizi uzunlukları için optimal dizilerin bilinmesi önemlidir. Literatürde farklı metodlarla Lempel-Greenberger sınırına göre optimal dizi üreten çalışmalar (optimal çift ve aile üretenlerden) daha fazladır (bkz. [4], [13], [1], [15], [14]). Bunun yanında optimal aile üreten sadece bir kaç üretim metodu vardır [9].

A. Genel Bilgiler ve Tanımlar

Olabilecek bütün frekans değerlerinden oluşan $\mathbb{F} = \{f_0, f_1, \cdots, f_{t-1}\}$ kümesine *Alfabe* denir. $\mathbb{F}$ bir alfabe ve S kümesi de $\mathbb{F}$ üzerinde uzunluğu v olan bütün dizilerin kümesi olsun. S nin herbir elemanına $\mathbb{F}$ üzerinde v-uzunluğunda *Frekans Atlamalı Dizi* denir. Kısaca FHS ile gösterilir.

Tanım 1 (Hamming Korelasyonu). $X = (x_0, x_1, \ldots, x_{v-1})$ ve $Y = (y_0, y_1, \ldots, y_{v-1})$ şeklinde iki frekans atlamalı $X, Y \in S$ dizisi verildiğinde, bunlar arasındaki *Hamming Korelas- yonu* $H_{X,Y}$ aşağıdaki şekilde tanımlanır:

$$H_{X,Y}(t) = \sum_{i=0}^{v-1} h[x_i, y_{i+t}] \quad , \quad 0 \le t < v. \tag{1}$$

Burada

$$h[a,b] = \begin{cases} 1 & \text{,eğer } a = b \text{ ise} \\ 0 & \text{,diğer durumlar} \end{cases} \tag{2}$$

şeklindedir ve indis pozisyonundaki her işlem mod v de yapılır.

Herhangi iki FHS nin $0 \le t < v$ kaymışı için Hamming korelasyonu tanımlandı. Bu tanımdan yararlanarak aşağıdaki tanımlar verilmiştir.

Tanım 2. Birbirinden farklı her $X, Y \in S$ FHS leri için:
Hamming Oto-Korelasyonu:

$$H(X) = \max_{1 \le t < v} \{H_{XX}(t)\}$$

Hamming Çapraz-Korelasyonu:

$$H(X,Y) = \max_{0 \le t < v} \{H_{XY}(t)\}$$

S. Kahraman, Matematik Bölümü, TOBB Ekonomi ve Teknoloji Üniversitesi.
Z. Saygı, Matematik Bölümü, TOBB Ekonomi ve Teknoloji Üniversitesi.

[1]Frequency Hopping Code Division Multiple Access
[2]antijamming
[3]sonar echo-location systems

Dizi çiftleri için Hamming Korelasyonu:

$$M(X,Y) = \max\{H(X), H(Y), H(X,Y)\}$$

Dizi aileleri için Hamming Korelasyonu:

$$M(F) = \max\{\max_{X\in F} H(X), \max_{X,Y\in F, X\neq Y} H(X,Y)\}$$

eşitlikleri ile tanımlanır.

Hamming korelasyonu çakışmaları sayan bir fonksiyondur. İletişimdeki problemlerin mümkün olduğunca az olması için çakışma sayısının mümkün olduğunca az olması gerekmektedir. Bu nedenle aşağıdaki optimallik kriterleri belirlenmiştir.

Optimallik Kriterleri:

O.1 Her $X' \in S$ için $H(X) \leq H(X')$ sağlanıyorsa $X \in S$ dizisine *Optimal* denir

O.2 Her $X', Y' \in S$, $X' \neq Y'$ için $M(X,Y) \leq M(X',Y')$ sağlanıyorsa X, Y ayrık dizilerine *Optimal Çift* denir.

O.3 $\mathbb{F}$ deki her ayrık çift optimal çift ise $\mathbb{F} \subset S$ alt kümesine *Optimal Aile* denir.

Optimallik kriterlerine dikkat edilirse optimalliği kontrol etmek özellikle dizinin boyu v büyüdüğünde çok zordur. Bu nedenle Hamming Korelasyonları için sınırlar bulunmuştur. Bu çalışmada literatürde en çok kullanılan iki sınır kullanılmıştır. Eğer Hamming korelasyon değeri sınıra eşit ise dizi, dizi çifti veya aileleri için optimaldir denir.

Buradan itibaren uzunluğu v, alfabe boyu q ve hamming oto korelasyonu $\lambda = H(X)$ olan dizileri (v,q,λ) ile, q elemanlı alfabe üzerinde tanımlı v uzunluğunda N diziden oluşan ve hamming korelasyonu $\lambda = M(F)$ olan dizi ailesini $(v,N,\lambda : q)$ ile göstereceğiz.

Lemma 1 (Lempel-Greenberger Sınırı(1974)). [1] *$|\mathbb{F}| = q$ olmak üzere her v uzunluğundaki $X \in S$ frekans atlamalı dizisi için, ϵ, $v \equiv \epsilon \pmod q$ denkliğini sağlayan en küçük negatif olmayan tamsayı olmak üzere;*

$$H(X) \geq \left\lceil \frac{(v-\epsilon)(v+\epsilon-q)}{q(v-1)} \right\rceil \quad (3)$$

eşitsizliği sağlanır.

Lemma 2 (Peng-Fan Sınırı(2004)). [3] *$F \subset S$, q boyutlu alfabe üzerinde tanımlı v uzunluğundaki N diziden oluşan dizi ailesi olsun. $I = \lfloor vN/q \rfloor$ olarak tanımlanırsa*

$$M(F) \geq \left\lceil \frac{(vN-q)v}{(vN-1)q} \right\rceil \quad (4)$$

ve

$$M(F) \geq \left\lceil \frac{2IvN - (I+1)Iq}{(vN-1)N} \right\rceil \quad (5)$$

sağlanır.

Tanım 3. $\mathbb{F}_q$, q elemanlı cisim ve $\mathbb{F}_{q^m}$ onun sonlu genişlemesi olsun. $\alpha \in \mathbb{F}_{q^m}$ olmak üzere $Tr_{\mathbb{F}_{q^m}/\mathbb{F}_q} : \mathbb{F}_{q^m} \to \mathbb{F}_q$ iz fonksiyonu

$$Tr_{\mathbb{F}_{q^m}/\mathbb{F}_q}(\alpha) = \alpha + \alpha^q + \alpha^{q^2} + \cdots + \alpha^{q^{m-1}}$$

şeklinde tanımlanır.

II. Literatürde İz Fonksiyonu ile Üretilen FHS ler

Bu bölümde [5], [6], [7] ve [9] makalelerinde iz fonksiyonu yardımıyla oluşturulan FHS ler incelenecektir. Bu makalelerdeki üretim metodlarında sırasıyla $l = 2$, $l = q-1$, $l \mid (q-1)$ ve $l = q^2 - 1$ alınarak uzunlukları $v = \frac{q^m-1}{l}$ olan optimal FHS ler elde edilmiştir. Bu FHS lerin karşılaştırılmaları detaylı olarak [18] çalışmasında incelenmiştir. Uygulamalarda kullanılacak dizi uzunluğuna bağlı olarak bu yöntemlerden uygun olanı seçilebilir.

A. [5] Makalesindeki Üretim Metodu

p bir tek asal sayı ve r pozitif tamsayı olmak üzere $q = p^r$ olsun. $m \geq 3$ pozitif tek tamsayısı verilsin ve α, $\mathbb{F}_{q^m}$ nin ilkel elemanı olmak üzere $\beta = \alpha^{2s}$ olsun. Burada s, $ebob(s, q^m - 1) = 1$ özelliğini sağlayan bir pozitif tamsayıdır. Her $a \in \mathbb{F}_{q^m}^*$ için

$$c_a = \left(Tr_{q^m/q}(a), Tr_{q^m/q}(a\beta), \cdots, Tr_{q^m/q}(a\beta^{v-1})\right)$$

dizileri Lemma 1 deki Lempel-Greenberger Sınırına göre optimal $(\frac{q^m-1}{2}, q, \frac{q^{m-1}-1}{2})$-FHS lerdir. Ayrıca $a \in \mathbb{F}_{q^m}^*$ bir karesel eleman, $a' \in \mathbb{F}_{q^m}^*$ bir karesel olmayan eleman olmak üzere c_a ve $c_{a'}$ optimal çifttir.

Örnek 1. $p = 5$, $r = 1$ olsun. O halde $q = 5^1 = 5$ olarak bulunur. $m = 3$ olsun ve $\mathbb{F}_{5^3}^*$ cismini oluşturmak için $x^3 + 3x + 3$ ilkel polinomunu alalım. $ebob(s, q^m - 1) = ebob(1, 5^3 - 1) = 1$ olduğundan $s = 1$ olarak alalım. MAGMA gerçekleştirimi ile elde edilen $(62, 5, 12)$ dizilerinden $a = 1$ ve $a' = -1$ için diziler aşağıdaki gibidir:

c_1 = (2, 1, 2, 2, 4, 1, 1, 1, 4, 1, 2, 0, 1, 2, 4, 2, 0, 3, 0, 3, 4, 4, 2, 3, 0, 1, 1, 0, 0, 4, 1, 3, 4, 3, 3, 1, 4, 4, 4, 1, 4, 3, 0, 4, 3, 1, 3, 0, 2, 0, 2, 1, 1, 3, 2, 0, 4, 4, 0, 0, 1, 4)

c_{-1} = (3, 4, 3, 3, 1, 4, 4, 4, 1, 4, 3, 0, 4, 3, 1, 3, 0, 2, 0, 2, 1, 1, 3, 2, 0, 4, 4, 0, 0, 1, 4, 2, 1, 2, 2, 4, 1, 1, 1, 4, 1, 2, 0, 1, 2, 4, 2, 0, 3, 0, 3, 4, 4, 2, 3, 0, 1, 1, 0, 0, 4, 1).

1 karesel eleman olduğundan -1 karesel olmayan eleman olduğundan $\{c_1, c_{-1}\}$ optimal çift verir.

B. [6] Makalesindeki Üretim Metodu

q bir asalın kuvveti ve m bir pozitif tamsayı olsun. g, $\mathbb{F}_{q^m}^*$ nin bir üreteci olsun. $\alpha = g^{q-1}$ ve dizinin uzunluğu $v = \frac{q^m-1}{q-1}$ olarak tanımlansın.Her $0 \leq i \leq q-2$ için,

$$S_i^{m,q} = Tr_{q^m/q}(g^i \alpha^t), \quad 0 \leq t \leq v-1$$

dizisini tanımlayalım. Her bir $S_i^{m,q}$, $\mathbb{F}_q$ alfabesi üzerinde v uzunluğunda dizidir. Şimdi

$$S^{m,q} = S_i^{m,q} : \ 0 \leq i \leq q-2$$

tanımlansın. Eğer $ebob\left(q-1, \sum_{i=0}^{m-1} q^i\right) = 1$ sağlanırsa $S^{m,q}$, Lemma 2 daki Peng-Fan Sınırına göre optimal

$\left(\frac{q^m-1}{q-1}, q-1, \frac{q^{m-1}-1}{q-1}; q\right)$ FHS ailesi elde edilir. Ayrıca bu ailenin her bir elemanı Lemma 1 daki Lempel-Greenberger Sınırına göre optimaldir.

Örnek 2. $q = 4$, $m = 2$ olsun. O halde $q^m = 4^2$ olarak bulunur. $\mathbb{F}_{4^2}^*$ cismini oluşturmak için $x^2 + x + t^2$ ilkel polinomunu alalım. $ebob\left(q-1, \sum_{i=0}^{m-1} q^i\right) = ebob\left(3, \sum_{i=0}^{m-1} q^i = \frac{q^m-1}{q-1} = \frac{4^2-1}{4-1} = 5\right) = 1$ olduğundan MAGMA gerçekleştirimi ile elde edilen optimal (5,3,1;4) FHS ailesi t, $\mathbb{F}_2$ üzerinde 2. dereceden $x^2 + x + 1$ ilkel polinomun kökü olmak üzere aşağıdaki gibidir:

$S_0^{2,8} = (0,\ t,\ t^2,\ t^2,\ t)$

$S_1^{2,8} = (1,\ 1,\ t^2,\ 0,\ t^2)$

$S_2^{2,8} = (1,\ 0,\ 1,\ t,\ t)$

C. [7] Makalesindeki Üretim Metodu

p bir asal sayı ve r pozitif tamsayı olmak üzere $q = p^r$ ve $m,\ l,\ l \mid (q-1)$ ve $ebob\left(\frac{q^m-1}{q-1}, l\right) = 1$ özelliklerini sağlayan pozitif tamsayılar olsun. Yine kabul edelim ki α, $\mathbb{F}_{q^m}$ nin ilkel elemanı, s, $ebob\,(s, q^m-1) = 1$ özelliğini sağlayan bir pozitif tamsayı ve $\beta = \alpha^{l_s}$ olsun. $v = \frac{q^m-1}{l}$ olmak üzere her $g \in \mathbb{F}_{q^m}^*$ için

$$c_g = \left(Tr_{q^m/q}(g), Tr_{q^m/q}(g\beta), \cdots, Tr_{q^m/q}(g\beta^{v-1})\right)$$

dizileri Lemma 1 daki Lempel-Greenberger Sınırına göre optimal $(\frac{q^m-1}{l}, q, \frac{q^{m-1}-1}{l})$-FHS dizileridir.

Örnek 3. $p = 2$ ve $r = 3$ olsun. $\mathbb{F}_2$ üzerinde 3. dereceden $x^3 + x + 1$ ilkel polinomunun kökü v ile $\mathbb{F}_q = \mathbb{F}_8$ cismini oluşturalım. $m = 2$ alınırsa $q^m = 8^2$ olarak bulunur. $\mathbb{F}_{8^2}$ cismini oluşturmak için x^2+vx+v ilkel polinomunu alalım ve α bu polinomun kökü olsun. $l = 7$ olarak şeçilirse $7 \mid (8-1)$ ve $ebob\left(\frac{8^2-1}{8-1}, 7\right) = 1$ sağlanır. MAGMA gerçekleştirimi ile elde edilen optimal (9,8,1)-FHS dizilerinden bazıları aşağıdaki gibidir:

$c_\alpha = (v,\ 0,\ v,\ v^5,\ v^4,\ v^6,\ v^6,\ v^4,\ v^5)$

$c_{\alpha^2} = (v^2,\ v^5,\ 0,\ v^5,\ v^2,\ v,\ v^3,\ v^3,\ v)$

$c_{\alpha^3} = (v^5,\ v^6,\ v^2,\ 0,\ v^2,\ v^6,\ v^5,\ 1,\ 1)$

$c_{\alpha^4} = (v^4,\ v^2,\ v^3,\ v^6,\ 0,\ v^6,\ v^3,\ v^2,\ v^4)$

$c_{\alpha^5} = (v,\ v,\ v^6,\ 1,\ v^3,\ 0,\ v^3,\ 1,\ v^6)$

D. [9] Makalesindeki I. Üretim Metodu

$p = 2$, s pozitif bir tamsayı olmak üzere $q = p^s$ ve $r = q^4$ olsun. $N = q^2 - 1$ ve $v = q^2 + 1$ olarak tanımlansın. α, $\mathbb{F}_r^*$ ın bir üreteci olsun ve $g = \alpha^N$ olarak tanımlansın.Her $0 \le i \le N-2$ için

$$S_i^q = Tr_{r/q}(\alpha^i g^t), \quad 0 \le t \le v-1$$

dizileri tanımlansın. Her bir S_i^q, $\mathbb{F}_q$ üzerinde n uzunluğunda dizilerdir.

$$S^q = S_i^q :\ 0 \le i \le N-1$$

olarak tanımlanırsa, S^q kümesi, Lemma 2 daki Peng-Fan Sınırına göre optimal $(q^2+1, q^2-1, q+1; q)$ FHS ailesi oluşturur.

Örnek 4. $p = 2$, $s = 3$ olsun. $\mathbb{F}_2$ üzerinde 3. dereceden $x^3 + x + 1$ ilkel polinomunun kökü t ile $\mathbb{F}_8$ cismini oluşturalım. $r = 8^4$ olacağından $\mathbb{F}_{8^4}$ cismini oluşturmak için $x^4 + t^4x^3 + t^5x^2 + x + t$ ilkel polinomunu alalım. $N = 8^2 - 1 = 63$ ve $v = 8^2 + 1 = 65$ olur. MAGMA gerçekleştirimi ile elde edilen optimal (65,63,9;8) FHS ailesinin dizilerinden bazıları aşağıdaki gibidir:

$S_0^8 = (0,\ t^4,\ t,\ t^3,\ t^2,\ t^6,\ t^6,\ t^4,\ t^4,\ t^4,\ t^5,\ t,\ t^5,\ 1,\ t,\ t^5,\ t,\ t^6,\ t,\ t^2,\ t^3,\ t^4,\ t^2,\ t,\ t^3,\ t^6,\ 1,\ t^4,\ t^2,\ t^2,\ t^3,\ t^5,\ t^2,\ t^2,\ t^5,\ t^3,\ t^2,\ t^2,\ t^4,\ 1,\ t^6,\ t^3,\ t,\ t^2,\ t^4,\ t^3,\ t^2,\ t,\ t^6,\ t,\ t^5,\ t,\ 1,\ t^5,\ t,\ t^5,\ t^4,\ t^4,\ t^4,\ t^6,\ t^6,\ t^2,\ t^3,\ t,\ t^4)$

$S_1^8 = (t^4,\ t^4,\ t^3,\ t,\ t,\ t^5,\ t^5,\ t^6,\ 1,\ t^4,\ 0,\ 1,\ t^6,\ t^3,\ t^2,\ t^4,\ t^3,\ t^6,\ t^2,\ 1,\ t^3,\ t^5,\ t^5,\ 0,\ t^3,\ t,\ 1,\ 0,\ t,\ t^3,\ t^5,\ t,\ 0,\ 0,\ 0,\ t,\ t^5,\ t^3,\ t,\ 0,\ 1,\ t,\ t^3,\ 0,\ t^5,\ t^5,\ t^3,\ 1,\ t^2,\ t^6,\ t^3,\ t^4,\ t^2,\ t^3,\ t^6,\ 1,0,\ t^4,\ 1,\ t^6,\ t^5,\ t^5,\ t,\ t,\ t^3)$

$S_2^8 = (t,\ 0,\ t,\ 0,\ t^6,\ t^2,\ t^2,\ t^3,\ t^2,\ t^6,\ t^3,\ t^2,\ t^3,\ 0,\ t^5,\ 1,\ 1,\ t^2,\ t,t^6,\ 0,\ 0,\ 1,\ t^3,\ t^5,\ t^3,\ t^6,\ t^6,\ t^4,\ 1,\ t,\ t^4,\ t^6,\ t^5,\ t^5,\ t^6,\ t^4,\ t,\ 1,\ t^4,\ t^6,\ t^6,\ t^3,\ t^5,\ t^3,\ 1,\ 0,\ 0,\ t^6,\ t,\ t^2,\ 1,\ 1,\ t^5,\ 0,\ t^3,\ t^2,\ t^3,\ t^6,\ t^2,\ t^3,\ t^2,\ t^2,\ t^6,\ 0)$

$S_3^8 = (t,\ t^4,\ t^4,\ t,\ t^6,\ 0,\ t,\ t^4,\ 0,\ t^6,\ t^3,\ t^2,\ t^5,\ t^6,\ 1,\ t^6,\ 1,\ t^4,\ t^4,\ t^3,\ 0,\ t^6,\ t^2,\ t^6,\ t^6,\ 0,\ t^2,\ t^3,\ 1,\ t,\ t^2,\ t^5,\ t^5,\ t^5,\ 0,\ t^5,\ t^5,\ t^5,\ t^2,\ t,\ 1,\ t^3,\ t^2,\ 0,\ t^6,\ t^6,\ t^2,\ t^6,\ 0,\ t^3,\ t^4,\ t^4,\ 1,\ t^6,\ 1,\ t^6,\ t^5,\ t^2,\ t^3,\ t^6,\ 0,\ t^4,\ t,\ 0,\ t^6)$

$S_4^8 = (t^2,\ t^3,\ 0,\ t^3,\ t^2,\ t^5,\ 0,\ t,\ t^5,\ t^2,\ t^4,\ 1,\ t^4,\ t,\ t^6,\ t^5,\ t^4,\ t^5,\ t^5,\ t^6,\ t^6,\ t^3,\ t^4,\ t^6,\ t^6,\ 1,\ 0,\ 0,\ t^3,\ 0,\ 1,\ t^5,\ 1,\ t^2,\ t^4,\ t^4,\ t^2,\ 1,\ t^5,\ 1,\ 0,\ t^3,\ 0,\ 0,\ 1,\ t^6,\ t^6,\ t^4,\ t^3,\ t^6,\ t^6,\ t^5,\ t^5,\ t^4,\ t^5,\ t^6,\ t,\ t^4,\ 1,\ t^4,\ t^2,\ t^5,\ t,\ 0,\ t^5)$

E. [9] Makalesindeki II. Üretim Metodu

p bir tek asal, s ve m pozitif tamsayılar olmak üzere $q = p^s$ ve $r = q^m$ olsun. Ayrıca kabul edelim ki N, $r-1$ in pozitif çift tamsayı böleni ve $v = \frac{r-1}{N}$ olsun. α, $\mathbb{F}_r^*$ ın bir üreteci olsun ve $g = \alpha^N$ olarak tanımlansın. Her $0 \le i \le N-2$ için

$$S_i^{q,m} = Tr_{r/q}(\alpha^i g^t), \quad 0 \le t \le v-1$$

dizileri tanımlansın. Her bir S_i^q, $\mathbb{F}_q$ üzerinde v uzunluğunda dizilerdir.

$$S^{q,m} = S_i^{q,m} :\ 0 \le i \le N-1$$

olarak tanımlandığında, $S^{q,m}$ kümesi, $ebob(v, N) = 1$, $q-1 \equiv \frac{N}{2} \pmod N$, $ebob\left(\frac{r-1}{q-1}\ (mod\ N), N\right) = 2$ ve $N > \frac{q-1}{q}\sqrt{r}$

şartları sağlanırsa Lemma 2 daki Peng-Fan Sınırına göre optimal $\left(\frac{r-1}{N}, N, \frac{(r-q+(q-1)\sqrt{r})}{qN}; q\right)$ FHS ailesi oluşturur.

Örnek 5. $p = 3$, $s = 2$ için $\mathbb{F}_3$ üzerinde 2. dereceden $x^2 + 2x + 2$ ilkel polinomun kökü t ile $\mathbb{F}_9$ cismini oluşturalım. $m = 2$ olsun. $\mathbb{F}_{9^2}$ cismini oluşturmak için $x^2 + t^5x + t^3$ ilkel polinomunun kökünü alalım. $N = 16 \mid (9^2 - 1)$ seçilirse $v = \frac{81-1}{16} = 5$ olur. $ebob(v, N) = ebob(5, 16) = 1$, $9 - 1 = 8 \equiv \frac{18}{2} = 8 \pmod{16}$, $ebob\left((\frac{81-1}{9-1} = 10 \ (mod\ 16), 16)\right) = 2$ ve $N = 16 > \frac{8}{9}\sqrt{9} = 8$ sağlandığından parametre seçimimiz doğrudur. MAGMA gerçekleştirimi ile hesaplanarak elde edilen optimal (5,15,1;9) FHS ailesinin dizileri aşağıdaki gibidir:

$S_0^{9,2} = (2,\ t^7,\ t^5,\ t^5,\ t^7)$

$S_1^{9,2} = (t,\ 1,\ 2,\ t^5,\ 0)$

$S_2^{9,2} = (2,\ 2,\ t^6,\ t^3,\ t^6)$

$S_3^{9,2} = (t^3,\ 2,\ 0,\ 1,\ t^7)$

$S_4^{9,2} = (t^5,\ t^2,\ t^5,\ t^3,\ t^3)$

$S_5^{9,2} = (0,\ t^7,\ t^6,\ t^2,\ t^3)$

$S_6^{9,2} = (2,\ t^2,\ t^2,\ 2,\ t)$

$S_7^{9,2} = (t^5,\ t,\ t^2,\ 0,\ t^6)$

$S_8^{9,2} = (t,\ t^3,\ 1,\ t^3,\ t)$

$S_9^{9,2} = (t,\ 0,\ t^5,\ 2,\ 1)$

$S_{10}^{9,2} = (t^7,\ t^2,\ 1,\ 1,\ t^2)$

$S_{11}^{9,2} = (2,\ t^3,\ t^7,\ 1,\ 0)$

$S_{12}^{9,2} = (t^7,\ t^7,\ t,\ t^6,\ t)$

$S_{13}^{9,2} = (t^6,\ t^7,\ 0,\ t^3,\ t^2)$

$S_{14}^{9,2} = (1,\ t^5,\ 1,\ t^6,\ t^6)$

$S_{15}^{9,2} = (0,\ t^2,\ t,\ t^5,\ t^6)$

III. NÜMERİK HESAPLAMALAR

Bu bölümde yaptığımız nümerik dizi üretme çalışmalarından bahsedilecektir. Sonrasında ise çalıştığımız parametreler tablo şeklinde aktarılacaktır. p bir asal sayı ve r pozitif tamsayı olmak üzere $q = p^r$ olsun. Ayrıca kabul edelim ki, m pozitif tamsayı olmak üzere $\mathbb{F}_{q^m}$ sonlu cismi verilsin ve α, $\mathbb{F}_{q^m}$ nin bir ilkel elemanı olmak üzere $\beta = \alpha^{ls}$ olsun. Burada s, $ebob\,(s, q^m - 1) = 1$ özelliğini sağlayan bir pozitif tamsayı, l ise $q^m - 1$ in pozitif bir tamsayı bölenidir. Oluşturduğumuz MAGMA kodu her $a \in \mathbb{F}_{q^m}^*$ için

$$(Tr_{q^m/q}(a), Tr_{q^m/q}(a\beta), \cdots, Tr_{q^m/q}(a\beta^{v-1}))$$

dizileri oluşturulup bunların Hamming Korelasyonlarını hesaplar ve sınırlarla karşılaştırarak optimalliğine karar verir.

[5], [6], [7] ve [9] makalelerindeki üretim metodlarında sırasıyla $l = 2$, $l = q - 1$, $l \mid (q - 1)$ ve $l = q^2 - 1$ için optimal dizi üretimi yapılmaktadır. Biz ise çalışmalarımızda tüm $l \mid (q^m - 1)$ değerleri için diziler oluşturarak optimalliklerini inceledik. Tablolarda p bir asal, q bir asalın kuvveti, m genişlemesinin mertebesi olmak üzere l, $(q^m - 1)$ i bölen bir tamsayıdır ($\frac{q^m-1}{l}$ dizilerin boyunu verir). Tabloların son sütunlarında parametreler [5], [6], [7] ve [9] makalelerinde işlenmiş ise referansı verilmektedir. Ayrıca, dizilerde dizi uzunluğunu $\frac{q^m-1}{l} \leq q$, dizi çiftlerinde dizi uzunluğunu $\frac{q^m-1}{l} \leq \frac{q}{2}$ olacak şekilde veren parametreleri *aşikar* olarak nitelendirdik. Bunların dışındaki optimal dizi veya çift oluşturan parametreleri de *yeni* olarak nitelendirdik.

TABLO I
P=2 İÇİN ELDE EDİLEN NÜMERİK SONUÇLAR

q	m	l	Optimal Dizi	Optimal Çift	Açıklama
4	2	3	var	var	[6], [7]
		5	var	yok	aşikar
4	3	3	yok	yok	
		7	yok	yok	
		9	var	yok	yeni
		21	var	yok	aşikar
4	4	3	var	var	[6], [7]
		5	yok	yok	
		15	yok	yok	
		17	var	yok	yeni
		51	var	var	yeni
		85	var	yok	aşikar
8	2	3	yok	yok	
		7	var	var	[6], [7]
		9	var	yok	aşikar
		21	var	var	aşikar
8	3	7	var	var	[6], [7]
		73	var	yok	aşikar
16	2	3	var	var	[6], [7]
		5	var	var	[6], [7]
		15	var	var	[6], [7]
		17	var	yok	aşikar
		51	var	var	aşikar
		85	var	var	aşikar

TABLO II
P=3 İÇİN ELDE EDİLEN NÜMERİK SONUÇLAR

q	m	l	Optimal Dizi	Optimal Çift	Açıklama
3	2	2	yok	yok	
		4	var	yok	aşikar
3	3	2	var	var	[5], [7]
		13	var	yok	aşikar
3	4	2	yok	yok	
		4	yok	yok	
		5	yok	yok	
		8	yok	yok	
		10	var	yok	yeni
		16	yok	yok	
		20	yok	yok	
		40	var	yok	aşikar
9	2	2	yok	yok	
		4	yok	yok	
		5	yok	yok	
		8	yok	yok	
		10	var	yok	aşikar
		16	yok	yok	
		20	var	var	aşikar
		40	var	var	aşikar

TABLO III
P=5 İÇİN ELDE EDİLEN NÜMERİK SONUÇLAR

q	m	l	Optimal Dizi	Optimal Çift	Açıklama
5	2	2	yok	yok	
		3	yok	yok	
		4	yok	yok	
		6	var	yok	aşikar
		8	var	var	yeni
		12	var	var	aşikar
5	3	2	var	var	[5], [7]
		4	var	var	[6], [7]
		31	var	yok	yeni
		62	var	yok	aşikar

TABLO IV
P=7 İÇİN ELDE EDİLEN NÜMERİK SONUÇLAR

q	m	l	Optimal Dizi	Optimal Çift	Açıklama
7	2	2	yok	yok	
		3	var	var	[7]
		4	yok	yok	
		6	yok	yok	
		8	var	yok	aşikar
		12	var	yok	
		16	var	var	aşikar
		24	var	var	aşikar
7	3	2	var	var	[5], [7]
		3	yok	yok	
		6	yok	yok	
		9	yok	yok	
		18	yok	yok	
		19	yok	yok	
		38	yok	yok	
		57	var	yok	aşikar
		114	var	var	aşikar
		171	var	var	aşikar

TABLO V
P=11 İÇİN ELDE EDİLEN NÜMERİK SONUÇLAR

q	m	l	Optimal Dizi	Optimal Çift	Açıklama
11	2	2	yok	yok	
		3	yok	yok	
		4	yok	yok	
		5	var	var	[7]
		6	yok	yok	
		8	yok	yok	
		10	yok	yok	
		12	var	yok	aşikar
		15	yok	yok	
		20	var	yok	aşikar
		24	var	var	aşikar
		30	var	var	aşikar
		40	var	var	aşikar
		60	var	var	aşikar

TABLO VI
P=13 İÇİN ELDE EDİLEN NÜMERİK SONUÇLAR

q	m	l	Optimal Dizi	Optimal Çift	Açıklama
13	2	2	yok	yok	
		3	var	var	[7]
		4	yok	yok	
		6	yok	yok	
		7	yok	yok	
		8	yok	yok	
		12	yok	yok	
		14	var	yok	aşikar
		21	var	yok	aşikar
		24	var	var	[9]
		28	var	var	aşikar
		42	var	var	aşikar
		56	var	var	aşikar
		84	var	var	aşikar

TABLO VII
P=17 İÇİN ELDE EDİLEN NÜMERİK SONUÇLAR

q	m	l	Optimal Dizi	Optimal Çift	Açıklama
17	2	2	yok	yok	
		3	yok	yok	
		4	yok	yok	
		6	yok	yok	
		8	yok	yok	
		9	yok	yok	
		12	yok	yok	
		16	yok	yok	
		18	var	yok	aşikar
		24	var	yok	aşikar
		32	var	var	yeni
		36	var	var	aşikar
		48	var	var	aşikar
		72	var	var	aşikar
		96	var	var	aşikar
		144	var	var	aşikar

TABLO VIII
P=19 İÇİN ELDE EDİLEN NÜMERİK SONUÇLAR

q	m	l	Optimal Dizi	Optimal Çift	Açıklama
19	2	2	yok	yok	
		3	var	var	[7]
		4	yok	yok	
		5	yok	yok	
		6	yok	yok	
		8	yok	yok	
		9	var	var	[7]
		10	yok	yok	
		12	yok	yok	
		15	yok	yok	
		18	yok	yok	
		20	var	yok	aşikar
		24	yok	yok	
		30	var	yok	aşikar
		36	var	yok	aşikar
		40	var	var	aşikar
		45	var	yok	aşikar
		60	var	var	aşikar
		72	var	var	aşikar
		90	var	var	aşikar
		120	var	var	aşikar
		180	var	var	aşikar

IV. SONUÇ

Bu çalışmada, FH-CDMA, Bluetooth ve ultra geniş bant gibi popüler sistemlerde kullanılan Optimal Frekans Atlamalı Diziler ve bu dizilerin iz fonksiyonu ile oluşturulmasıyla ilgili literatür incelenmiş ve metodların MAGMA ile gerçekleştirimleri yapılarak örnekler verilmiştir. Ayrıca parametrelerde yapılan yeniliklerle yeni optimal dizilerin varlığı araştırılmıştır. Bazı parametreler için, incelenen dört makalede bulunmayan optimal dizi veya çiftlere rastlanılmıştır. Bunların genelleştirilmesiyle ilgili çalışmalarımız devam etmektedir.

TEŞEKKÜRLER

Bu çalışma TÜBİTAK 109T344 referans numaralı proje tarafından desteklenmiştir. Projedeki desteklerinden dolayı TÜBİTAK'a teşekkür ederiz.

REFERANSLAR

[1] Lempel A., Greenberger H. *Families of Sequences with Optimal Hamming Correlation Properties*, IEEE Trans.Inf. Theory, vol.IT-20 , pp 90-94, 1974.
[2] Wenhua M., Yixian Y. *Families of FH sequences based on pseudorandom sequences over GF(p)*, International Conference on Communication Technologies (ICCT '00), vol. 1, Paper S33.4, pp 536-538, August 2000.
[3] Peng D., Fan P. *Lower Bounds on the Hamming Auto- and Cross Correlations of Frequency-Hopping Sequences*, IEEE Trans. Inf. Theory, vol. 50, no. 9, pp 2149-2154, September 2004.
[4] Chu W., Colbourn C.J. *Optimal frequency-hopping sequences via cyclotomy*, IEEE Trans.Inf. Theory, vol. 51, no. 3, pp 1139-1141, March 2005.
[5] Ding C., Miosio M.J., Yuan J. *Algebraic Constructions of Optimal Frequency Hopping Sequences*, IEEE Trans. Inf. Theory, vol. 53, no. 7, pp 2606-2610, July 2007.
[6] Ding C., Yin J. *Sets of Optimal Frequency Hopping Sequences*, IEEE Trans. Inf. Theory, vol. IT-54, no. 8, pp 3741-3745, August 2008.
[7] Ge G., Miao Y., Yao Z. *Optimal Frequency Hopping Sequences: Auto- and Cross-Correlation Properties*, IEEE Trans. Inf. Theory, vol. 55, no. 2, pp 867-879, February 2009.
[8] Zhang Y., Ke P., Zhang S. *Optimal Frequency-Hopping Sequences Based on Cyclotomy*, First International Workshop on Education Technology and Computer Science (ETCS '09), vol. 1, pp 1122-1126, March 2009.
[9] Ding C., Fuji-Hara R., Fujiwara Y., Jimbo M., Mishima M.*Sets of Frequency Hopping Sequences: Bounds and Optimal Constructions*, IEEE Trans.Inf. Theory, vol.55, no.7, pp 3297-3304, July 2009 .
[10] Chung J., Yang K. *Optimal Frequency-Hopping Sequences With New Parameters*, IEEE Trans.Inf. Theory, vol. 56, No. 4, pp 1685-1693, April 2010.
[11] Juntao G., Yupu H., Xuelian L. *The Linear Span of a Class of Optimal Frequency Hopping Sequences*, Natural Science Foundation of China, pp. 147-151, March 2011.
[12] Zhou Z., Tang X., Peng D., Parampalli U. *New Constructions for Optimal Sets of Frequency-Hopping Sequences*, IEEE Trans.Inf. Theory, vol. 57, No. 6, pp 3831-3840, June 2011.
[13] Fuji-Hara R., Miao Y., Mishima M. *Optimal Frequency Hopping Sequences:A Combinatorial Approach*, IEEE Trans. Inf. Theory, vol. 50, no. 10, pp 2408-2420, October 2004.
[14] Udaya P., Siddiqi M. U. *Optimal large linear span frequency hopping patterns derived from polynomial residue class rings*, IEEE Trans. Inf. Theory, vol. 44, no. 4, pp 1492-1503, April 1998.
[15] Kumar P.V. *Frequency-hopping code sequence designs having large linear span*, IEEE Trans.Inf. Theory, vol. 34, no. 1, pp 146-151, January 1988.
[16] Computational Algebra Group, MAGMA Computational Algebra System(V2.10-22). 'http://magma.maths.usyd.edu.au/magma/'.
[17] S. Kahraman, Optimal Frekans Atlamalı Diziler, M.S. Tezi, Mat. Böl., TOBB ETÜ, Ank., 2011.
[18] K. Bayraktar, Frekans Atlamalı Diziler, M.S. Tezi, Mat. Böl., TOBB ETÜ, Ank., 2010.
[19] F. Halsall, *Data Communications, Computer Networks and Open Systems*. USA: Addison-Wesley, 1995.

Cyclotomic Sayılar ve Sidel'nikov Dizileri

Kamil Otal, Zülfükar Saygı ve Çetin Ürtiş

***Özet*—p asal sayı, M ile n pozitif tamsayılar ve $M|(p^n-1)$ olsun. p^n-1 periyotlu M-li Sidel'nikov dizilerinin [11] faz dışı otokorelasyon dağılımı değerleri ile cyclotomic sayılar arasında birebir ilişki mevcuttur [9] . Yüksek hızlı bilgi transferinde iyi korelasyon değerlerine sahip M-li dizilere olan ihtiyaç, dolaylı olarak yüksek mertebeden cyclotomic sayıların hesaplanması ihtiyacını doğurmuştur. Nitekim Chung, Kim, Lim ve Chung [10] mertebe 5 cyclotomic sayıları $p \not\equiv 1 (\mathrm{mod}\, 5)$ için hesaplayıp bu sayıları 5-li Sidel'nikov dizilerinin faz dışı otokorelasyon dağılımı değerlerini hesaplamada kullanmıştır. Mertebe 7 cyclotomic sayılar için Katre ve Rajwade [7] nin verdikleri sonuç kullanılarak $p \equiv 1 (\mathrm{mod}\, 7)$ kısıtıyla hesaplama yapılabilir. Bu çalışmada hem Katre ve Rajwade nin verdiği sonuç kullanılacak şekilde hem de aksi durum için, yani $p \not\equiv 1 (\mathrm{mod}\, 7)$ için örnekler verilip Sidel'nikov dizilerinin faz dışı otokorelasyon dağılımı değerleri hesaplanmıştır.**

***Anahtar Kelimeler*—cyclotomy, cyclotomic sayı, uniform cyclotomy, Sidel'nikov dizileri, otokorelasyon, otokorelasyon dağılımı.**

I. GİRİŞ

Yüksek hızlı veri transferinde, genelde M-li modülasyon tasarları iletim standardı olarak kabul görmektedir. Yüksek hızlı veri transferine olan ihtiyacın artmasıyla birlikte, iyi hata düzeltme değerlerine sahip M-li kodlara ve iyi korelasyon özelliklerine sahip M-li dizilere olan ihtiyaç da artmıştır. M-li Sidel'nikov dizileri [11] de bu konuda oldukça kullanışlı dizilerdendir.

Kim, Chung, No ve Chung [9] $M|(p^n-1)$ olmak üzere periyodu p^n-1 olan M-li Sidel'nikov dizilerinin otokorelasyon dağılımı değerleri ile cyclotomic sayılar arasındaki birebir ilişkiyi göstermişlerdir. Böylelikle cyclotomic sayıları hesaplama problemi konunun ilgi alanına girmiştir.

Cyclotomic sayılar birçok alanda uygulaması bulunan cebirsel argümanlardandır. Bu sayıları tanım üzerinden hesaplama işi, mertebe büyüdükçe meşakkatli bir hal almaktadır. Bu yüzden cyclotomic sayılar, sonlu cisimlerin bazı temel özellikleri kullanılarak elde edilen Diyofant denklemler ile ifade edilmeye çalışılmaktadır.

p^n elemanlı sonlu cisim $\mathbb{F}_{p^n}$ için mertebe 2, 3, 4, 6, 8 cyclotomic sayılar [4]'de derlenmiştir, mertebe 5 ve mertebe 7 cyclotomic sayılar ise [7]'de $p \equiv 1 (\mathrm{mod}\, 5, 7)$ kısıtıyla verilmiştir.

Chung, Kim, Lim, No ve Chung [10] mertebe 5 cyclotomic sayıları $p \not\equiv 1 (\mathrm{mod}\, 5)$ için de hesaplayıp çözümü her sonlu cisime genişletmişler ve bunu Sidel'nikov dizilerinin faz dışı otokorelasyon dağılımı değerlerini belirlemede kullanmışlardır. Dolayısıyla problem mertebe 5 için de tamamlanmıştır.

K. Otal, Matematik Bölümü, TOBB Ekonomi ve Teknoloji Üniversitesi.
Z. Saygı, Matematik Bölümü, TOBB Ekonomi ve Teknoloji Üniversitesi.
Ç. Ürtiş, Matematik Bölümü, TOBB Ekonomi ve Teknoloji Üniversitesi.

Bu çalışmada, öncelikle Sidel'nikov dizileri ve otokorelasyon fonksiyonları hakkında kısa bir ön bilgi verilmiş, sonrasında cyclotomy hakkındaki temel bilgiler ile mertebe 7 cyclotomic sayılar hakkındaki mevcut son bilgiler verilmiştir. Son olarak da farklı durumlar için mertebe 7 cyclotomic sayı örnekleri verilip bunlarla Sidel'nikov dizilerinin faz dışı otokorelasyon değerleri hesaplanmıştır. Bu çalışmanın nihai amacı mertebe 7 cyclotomic sayıları [10] da olduğu gibi tespit edip Sidel'nikov dizilerinin faz dışı otokorelasyon değerlerine uygulamaktır.

II. ÖN BİLGİLER

p bir asal sayı, M ile n pozitif tamsayı, $M|(p^n-1)$ ve $f=\frac{p^n-1}{M}$ olsun. α, $\mathbb{F}_{p^n}$ nin bir ilkel elemanı olmak üzere sıfırdan farklı bir $b \in \mathbb{F}_{p^n}$ elemanının **indeksi** $\mathrm{ind}(b)=t$, $b=\alpha^t$ şartını sağlayan $t \in \{0,1,...,p^n-1\}$ olarak tanımlanır. ω_M ile M. dereceden birim kök, yani $e^{2\pi\sqrt{-1}/M}$ değeri belirtilsin. $\mathbb{F}_{p^n}$ nin M mertebeli **çarpımsal karakteri** ψ,

$$\psi(\alpha^t)=\omega_M^t \text{ ve } \psi(0)=0, \quad t \in \mathbb{Z}$$

şeklindedir. ψ^i ile ψ^j nin **Jacobi toplamı**

$$J(\psi^i,\psi^j)=\sum_{x\in\mathbb{F}_{p^n}} \psi^i(x)\psi^j(1-x)$$

ile verilir. Burada bazen $J(i,j)$ gösterimi de kullanılır.

$\mathbb{F}_{p^n}$ nin

$$S_k=\left\{\alpha^{Ms+k}-1 : s=0,1,...,f-1\right\}$$

alt kümeleri verilsin ($k=0,1,...,M-1$). **M-li Sidel'nikov dizisi** $s(t)$, herhangi bir sabit $k_0=\{0,1,...,M-1\}$ için

$$s(t)=\begin{cases} k, & \alpha^t \in S_k,\ k=0,1,...,M-1 \\ k_0, & t=\mathrm{ind}(-1) \end{cases} \tag{1}$$

şeklinde tanımlanır [11]. Bu dizinin periyodu p^n-1 dir.

$$N_k=|\{t : s(t)=k,\ 0\le t\le p^n-2\}|$$

ifadesi dikkate alınırsa, $k_0=0$ durumunda her $k=0,1,...,M-1$ için $N_k=f$ olduğu görülür. Yani M-li Sidel'nikov dizisi dengelidir.

$u(t)$, periyodu N olan M-li bir dizi olsun. $u(t)$ nin **otokorelasyon fonksiyonu**

$$R(\tau)=\sum_{t=0}^{N-1}\omega_M^{u(t)-u(t+\tau)},\ \tau=0,1,...,N-1$$

şeklinde tanımlanır.

III. CYCLOTOMY

$\mathbb{F}_{p^n}$ üzerinde α ilkeline göre M. **mertebe cyclotomic sınıflar**

$$C_j = \left\{\alpha^{Ms+j} : s = 0, 1, ..., f-1\right\}$$

kümeleri olarak verilir ($j = 0, 1, 2, ..., M-1$). M. **mertebeden cyclotomic sayılar** da

$$(i,j)_M = |\{z \in C_i : z+1 \in C_j\}|$$

şeklinde tanımlanır. M değerinin belli olduğu durumlarda (i,j) ile de gösterilir.

Lemma 1. [4], [5]

1) *Her* $K, L \in \mathbb{Z}$ *için* $(i+KM, j+LM)_M = (i,j)_M$
2) $(i,j)_M = (M-i, j-i)_M$
3) $(i,j)_M = \begin{cases} (j,i)_M, & f \text{ çift} \\ (j+\frac{M}{2}, i+\frac{M}{2})_M, & f \text{ tek} \end{cases}$
4) $\sum_{j=0}^{M-1}(i,j)_M = \begin{cases} f-1, & f \text{ çift ve } i=0 \\ f-1, & f \text{ tek ve } i=\frac{M}{2} \\ f, & \text{diğer durumlarda} \end{cases}$
5) $\sum_{i=0}^{M-1}(i,j)_M = \begin{cases} f-1, & j=0 \\ f, & \text{diğer durumlarda} \end{cases}$
6) $\underset{\alpha \text{ ilkeli ile}}{(ki,kj)_M} = \underset{\alpha^k \text{ ilkeli ile}}{(i,j)_M}$

Bu lemmanın son maddesinden de görüleceği üzere, cyclotomic sayılar ilkel elemanın seçimine göre sadece konum değiştirirler. Bu konum değiştirme dikkate alınmadığında cyclotomic sayıların ilkel elemanının seçiminden bağımsız olduğu söylenebilir. Nitekim cyclotomic sayıları Diyofant denklemleri cinsinden ifade etme problemi ilk başlarda ilkel elemanın seçiminden bağımsız olarak çözülmeye çalışılmıştır (örneğin [1], [2], [3], [4], vs.).

Bu lemma kullanılınca 49 tane yedinci mertebeden cyclotomic sayının kendi aralarında şöyle bir bağıntıya sahip oldukları görülür.

$$T_1 := (0,1) = (1,0) = (6,6)$$
$$T_2 := (0,2) = (2,0) = (5,5)$$
$$T_3 := (0,3) = (3,0) = (4,4)$$
$$T_4 := (0,4) = (4,0) = (3,3)$$
$$T_5 := (0,5) = (5,0) = (2,2)$$
$$T_6 := (0,6) = (6,0) = (1,1)$$
$$T_7 := (1,2) = (2,1) = (6,1) = (1,6) = (6,5) = (5,6)$$
$$T_8 := (1,3) = (3,1) = (6,2) = (2,6) = (5,4) = (4,5)$$
$$T_9 := (1,4) = (4,1) = (6,3) = (3,6) = (4,3) = (3,4)$$
$$T_{10} := (1,5) = (5,1) = (6,4) = (4,6) = (3,2) = (2,3)$$
$$T_{11} := (3,5) = (5,3) = (2,4) = (4,2) = (2,3) = (3,2)$$

Yani $T_0 := (0,0)$ ile birlikte 12 farklı sayı vardır.

Lemma 2. [4], [5], [6] *Jacobi toplamları ile cyclotomic sayılar arasında*

$$M^2(i,j) = \sum_{u,v=0}^{M-1}(-1)^{uf}\omega_M^{-iu-jv}J(\psi^u, \psi^v)$$
$$J(\psi^i, \psi^j) = \sum_{u,v=0}^{M-1}\omega_M^{iu+jv}(u,v)$$

şeklinde bir ilişki vardır.

Teorem 3. [6], [7] $p \equiv 1 \pmod 7$ *olsun.* $(k,7) = 1$ *için* σ_k, $\mathbb{Q}(\omega_7)$ *nin* $\omega_7 \longmapsto \omega_7^k$ *olacak şekildeki otomorfizması olsun.* $\lambda(r)$, $r \pmod 7$ *nin en küçük negatif olmayan tamsayı değerini göstersin.* $1 \le m \le 5$ *sabit bir tamsayı olsun.* α *bir ilkel eleman olmak üzere* $b = \alpha^f$ *olsun.* $H = \sum_{i=0}^{6} a_i\omega_7^i \in \mathbb{Z}[\omega_7]$ *olsun.*

1) $p^n = \sum_{i=0}^{6} a_i^2 - \sum_{i=0}^{6} a_i a_{i+1}$,
2) $\sum_{i=0}^{6} a_i a_{i+1} = \sum_{i=0}^{6} a_i a_{i+2} = \sum_{i=0}^{6} a_i a_{i+3}$
3) $1 + a_0 + a_1 + ... + a_6 = 0 \pmod 7$
4) $a_1 + 2a_2 + ... + 6a_6 = 0 \pmod 7$
5) $p \nmid \prod_{\lambda((m+1)k)>k} H^{\sigma_k}$
6) $p \mid \bar{H} \prod_{\lambda((m+1)k)>k} (b - \omega_7^{\sigma_{k^{-1}}})$

şartları sağlansın (Burada $\bar{H}$ *ile* H *nin kompleks eşleniği belirtilmektedir,* k^{-1} *değeri de* $\pmod 7$ *de hesaplanmıştır). O zaman bu* α *ilkeli için* $H = J(1,m)$ *olur. Bu önermenin diğer yönü de doğrudur.*

$J(1,m)$ ile diğer tüm $J(i,j)$ değerleri üretilebilir. Böylelikle, Jacobi toplamları ile cyclotomic sayılar arasındaki ilişki kullanılarak $p \equiv 1 \pmod 7$ şartını sağlayan mertebe 7 cyclotomic sayılar hesaplanabilir.

Baumert ve Mills [8] $p \not\equiv 1 \pmod M$ durumunda bazı özel şartlar altında kullanışlı bir teorem vermişlerdir.

Eğer $p^t \equiv -1 \pmod M$ olacak şekilde bir t tamsayısı mevcut ise $\mathbb{F}_{p^n}$ üzerinde M. mertebeden cyclotomic sayılar **uniform**dur.

Teorem 4. [8] $\mathbb{F}_{p^n}$ *üzerinde* M. *mertebe cyclotomic sayılar uniform olsun. Bu durumda ya* p *ya da* f *çifttir, ayrıca* n *değeri de çifttir. Üstelik* $\eta = \frac{p^{n/2}-1}{M}$ *olmak üzere*

$$(0,0) = \eta^2 - (M-3)\eta - 1$$
$$(0,i) = (i,0) = (i,i) = \eta^2 + \eta, \quad i \neq 0 \text{ için}$$
$$(i,j) = \eta^2, \quad 0 \neq i \neq j \neq 0 \text{ için}$$

şeklindedir.

Bu teorem cyclotomic sayıları 3 şekilde belirlediği için hesaplamada büyük kolaylık sağlar. Örneğin $M = 7$ için, eğer cyclotomic sayılar uniform ise yukarıda belirtilen T_i değerlerinden sadece T_0, T_1, T_7 değerlerini hesaplamak, diğerlerini de bulmak için yeterli olacaktır.

IV. 7-Lİ SIDEL'NIKOV DİZİLERİNİN OTOKORELASYON DAĞILIMLARI

Teorem 5. [9] $y = \alpha^\tau \in \mathbb{F}_{p^n} - \{0,1\}$ *olmak üzere* $\psi(\frac{1}{1-y}) = \omega_M^u$ *ve* $\psi(\frac{y-1}{y}) = \omega_M^v$ *olsun.* $p^n - 1$ *periyotlu* M*-li*

Sidel'nikov dizisi $s(t)$ nin aşikar olmayan ($\tau \not\equiv 0 (\mathrm{mod}\, p^n-1)$) otokorelasyon fonksiyonu $R(\tau) = R_{u,v}$,

$$R_{u,v} = \begin{cases} -(\omega_M^{u+k_0}-1)(\omega_M^{v-k_0}-1), & \psi(-1)=1 \\ (\omega_M^{u+k_0}+1)(\omega_M^{v-k_0}+1), & \psi(-1)=-1 \end{cases}$$

şeklindedir.

Teorem 6. [9] *$N(R_{u,v})$ ile $R(\tau) = R_{u,v}$ şartını sağlayan $y = \alpha^\tau \in \mathbb{F}_{p^n} - \{0,1\}$ lerin sayısı belirtilsin. p^n-1 periyotlu M-li Sidel'nikov dizisinin faz dışı otokorelasyon dağılımı aşağıdaki gibidir.*

$\psi(-1) = 1$ *ise*

1) $N(0) = \sum_{i=1}^{M-1} ((i, i+k_0)_M + (i,k_0)_M) + (0,k_0)_M$
2) $N(R_{k,k}) = (2k, k+k_0)_M$, $1 \le k \le M-1$
3) $N(R_{u,v}) = (u+v, v+k_0)_M + (u+v, u+k_0)_M$, $1 \le u < v \le M-1$

$\psi(-1) = -1$ *ise*

1) $N(-2) = \sum_{\substack{i=0 \\ i \neq M/2}}^{M-1} ((\frac{M}{2}+i, i+k_0)_M + (\frac{M}{2}+i, \frac{M}{2}+k_0)_M) + (0, \frac{M}{2}+k_0)_M$
2) $N(R_{k,k}) = (2k, k+k_0)_M$, $0 \le k \le M-1$ *ve* $k \neq M/2$
3) $N(R_{u,v}) = (u+v, v+k_0)_M + (u+v, u+k_0)_M$, $1 \le u < v \le M-1$ *ve* $u \neq \frac{M}{2}, v \neq \frac{M}{2}$

Örnek 7. $p \equiv 1 (\mathrm{mod}\, 7)$ şartını sağlayacak şekilde, $\mathbb{F}_{29}$ üzerinde $\alpha = 2$ ilkeliyle oluşturulan mertebe 7 cyclotomic sayılar

$$\begin{aligned} 0 &= T_0 = T_2 = T_3 = T_5 = T_6 = T_8 = T_9 \\ 1 &= T_1 = T_7 = T_{10} = T_{11} \\ 2 &= T_4 \end{aligned}$$

şeklinde belirlenir. Yine bu ilkel eleman ile (1) kullanılarak üretilen 7-li Sidel'nikov dizisi

$$s = (1,5,1,3,0,2,5,4,2,3,2,2,3,6,k_0,0,5,5,6,1,1,4,6,4,3,0,6,4)$$

olur. Ayrıca mertebe 7 çarpımsal karakter $\psi(2^t) = \omega_7^t$, $\psi(0) = 0$ şeklinde olup $\psi(-1) = \psi(2^{14}) = 1$ çıkar ve böylelikle $k_0 = 0$ için Teorem 6 kullanılarak bu dizinin otokorelasyon dağılımları $R(\tau)$

0,	6 kez	$\omega_7+\omega_7^2-\omega_7^3-1$,	1 kez
$-(\omega_7-1)^2$,	1 kez	$\omega_7^2+\omega_7^3-\omega_7^5-1$,	2 kez
$-(\omega_7^2-1)^2$,	1 kez	$\omega_7^2+\omega_7^4-\omega_7^6-1$,	1 kez
$-(\omega_7^3-1)^2$,	0 kez	$\omega_7^2+\omega_7^5-2$,	0 kez
$-(\omega_7^4-1)^2$,	0 kez	$\omega_7^2+\omega_7^6-\omega_7-1$,	2 kez
$-(\omega_7^5-1)^2$,	1 kez	$\omega_7^3+\omega_7^4-2$,	2 kez
$-(\omega_7^6-1)^2$,	1 kez	$\omega_7^3+\omega_7^5-\omega_7-1$,	1 kez
$\omega_7+\omega_7^2-\omega_7^3-1$,	1 kez	$\omega_7^3+\omega_7^6-\omega_7^2-1$,	1 kez
$\omega_7+\omega_7^3-\omega_7^4-1$,	0 kez	$\omega_7^4+\omega_7^5-\omega_7^2-1$,	2 kez
$\omega_7+\omega_7^4-\omega_7^5-1$,	1 kez	$\omega_7^4+\omega_7^6-\omega_7^3-1$,	0 kez
$\omega_7+\omega_7^5-\omega_7^6-1$,	2 kez	$\omega_7^5+\omega_7^6-\omega_7^4-1$,	1 kez

şeklinde hesaplanır. Dikkat edilirse 3 farklı karakterde sayı bulunmasına rağmen cyclotomic sayılar uniform değildir.

Örnek 8. $p \not\equiv 1 (\mathrm{mod}\, 7)$ durumuna örnek olarak, $\mathbb{F}_{64} = \mathbb{F}_2(\theta)$ cismi üzerinde (θ, x^6+x^5+1 polinomunun bir kökü) θ ilkel elemanı kullanılarak oluşturulan mertebe 7 cyclotomic sayılar

$$\begin{aligned} 0 &= T_3 = T_5 = T_6 = T_{10} \\ 1 &= T_8 \\ 2 &= T_0 = T_1 = T_2 = T_4 = T_7 = T_9 = T_{11} \end{aligned}$$

şeklinde belirlenir. Yine bu ilkel eleman kullanılarak üretilen 7-li Sidel'nikov dizisi

$$\begin{aligned} s = \; & (k_0,2,4,6,1,6,5,2,2,6,5,0,3,6,4,5,4,5,5,5,3, \\ & 0,0,1,6,0,5,2,1,4,5,4,1,3,3,1,3,0,3,3,6,6, \\ & 0,4,0,1,2,2,5,4,0,5,3,2,4,1,2,5,1,4,3,2,1) \end{aligned}$$

olur. Burada karakteristik 2 olduğundan $-1 = 1$ dir. Dolayısıyla k_0 değeri 1 in indeksi olan sıfır hanesine konmuştur. Ayrıca mertebe 7 çarpımsal karakter ψ için $\psi(-1) = \psi(1) = 1 = -1$ çıkar. Yani $k_0 = 0$ için Teorem 6 deki formüllerden ikisi de kullanılabilir. Hesaplandığında periyodu 63 olan bu 7-li dizinin otokorelasyon dağılımları $R(\tau)$

0,	14 kez	$\omega_7+\omega_7^2-\omega_7^3-1$,	2 kez
$-(\omega_7-1)^2$,	2 kez	$\omega_7^2+\omega_7^3-\omega_7^5-1$,	4 kez
$-(\omega_7^2-1)^2$,	2 kez	$\omega_7^2+\omega_7^4-\omega_7^6-1$,	1 kez
$-(\omega_7^3-1)^2$,	2 kez	$\omega_7^2+\omega_7^5-2$,	2 kez
$-(\omega_7^4-1)^2$,	2 kez	$\omega_7^2+\omega_7^6-\omega_7-1$,	4 kez
$-(\omega_7^5-1)^2$,	2 kez	$\omega_7^3+\omega_7^4-2$,	2 kez
$-(\omega_7^6-1)^2$,	2 kez	$\omega_7^3+\omega_7^5-\omega_7-1$,	1 kez
$\omega_7+\omega_7^2-\omega_7^3-1$,	1 kez	$\omega_7^3+\omega_7^6-\omega_7^2-1$,	1 kez
$\omega_7+\omega_7^3-\omega_7^4-1$,	4 kez	$\omega_7^4+\omega_7^5-\omega_7^2-1$,	4 kez
$\omega_7+\omega_7^4-\omega_7^5-1$,	1 kez	$\omega_7^4+\omega_7^6-\omega_7^3-1$,	4 kez
$\omega_7+\omega_7^5-\omega_7^6-1$,	4 kez	$\omega_7^5+\omega_7^6-\omega_7^4-1$,	1 kez

şeklinde çıkar.

Not 9. Son örnekte $x^6+x^4+x^3+x+1$ veya x^6+x+1 polinomlarının kökleri olan ilkel elemanlar kullanıldığında da aynı otokorelasyon dağılımlarının elde edildiği görülür.

Karşılaşılan temel zorluk: [10] makalesinde mertebe 5 için hesaplama yapılırken $p \not\equiv 1 (\mathrm{mod}\, 5)$ durumunda cyclotomic sayıların 3 farklı şekilde mevcut olduğu görülmüştür. Oysa 5. mertebeden cyclotomic sayılar Lemma 1 kullanıldığında 7 şekilde belirlenir. Bu durum, $p \not\equiv 1 (\mathrm{mod}\, 5)$ iken mertebe 5 cyclotomic sayıların hep uniform olmasından kaynaklanmaktadır. Çünkü $2^2 \equiv -1 (\mathrm{mod}\, 5)$, $3^2 \equiv -1 (\mathrm{mod}\, 5)$, $4^1 \equiv -1 (\mathrm{mod}\, 5)$ şeklindedir. Mertebe 7 durumunda ise $p \equiv 3,5,6 (\mathrm{mod}\, 7)$ için 7. mertebeden cyclotomic sayılar uniform olur fakat $p \equiv 2,4 (\mathrm{mod}\, 7)$ olduğunda uniform olmazlar.

Örnek 10. $p = 11 \equiv 4 (\mathrm{mod}\, 7)$ olmak üzere $\mathbb{F}_{11^3}$ üzerinde minimal polinomu x^3+2x+9 olan ilkel elemanla oluşturulan

7. mertebeden cyclotomic sayılar

$$27 = T_0$$
$$24 = T_1 = T_2 = T_4 = T_7 = T_9 = T_{11}$$
$$30 = T_3 = T_5 = T_6$$
$$28 = T_8$$
$$36 = T_{10}$$

şeklinde belirlenir. Yani 5 farklı sayı vardır. Oysa uniform durumunda 3 tane idi.

Bu durum [10] makalesindeki sonucu mertebe 7 için genelleştirmeyi zorlaştırmaktadır.

V. SONUÇ

Verilen p^n elemanlı $\mathbb{F}_{p^n}$ sonlu cismi için tanımlanmış 7-li Sidel'nikov dizilerinin otokorelasyon dağılımları 7. mertebeden cyclotomic sayılar hesaplanarak en genel durumlar için verilmeye çalışılacaktır. Bu amaçla cyclotomic sayılar ile Sidel'nikov dizilerinin otokorelasyonu arasındaki ilişki incelenmiştir. İki farklı örnek üzerinden gerekli mertebe 7 cyclotomic sayılar hesaplanarak korelasyon dağılımları gözlenmiştir.

TEŞEKKÜRLER

Bu çalışma TÜBİTAK 109T344 referans numaralı proje tarafından desteklenmiştir. Projedeki desteklerinden dolayı TÜBİTAK'a teşekkür ederiz.

REFERANSLAR

[1] C. F. Gauss, *Disquisitiones Arithmeticae*, Yale University Press, 1966.
[2] L. E. Dickson, *"Cyclotomy, higher congruences and Waring's problem I," American J. of Math.,* vol. 57, no. 2, pp. 391-424, 1935
[3] L. E. Dickson, *"'Cyclotomy, higher congruences and Waring's problem II," American J. of Math.,* vol. 57, no. 3, pp. 463-474, 1935
[4] T. Storer, *Cyclotomy and Difference Sets, Lectures in Advanced Mathematics.* Chicago, IL:Markham, 1967.
[5] B. C. Berndt, R. J. Evans, K. S. Williams, *Gauss and Jacobi Sums,* New York: J. Wiley and Sons Company, 1997.
[6] J. C. Parnami, M. K. Agrawal, A. R. Rajwade, *"Jacobi sums and cyclotomic numbers for a finite field," Acta Arithmetica,* vol. 41, pp. 1-13, 1982.
[7] S. A. Katre and A. R. Rajwade, *"Complete solution of the cyclotomic problem in F_q for any prime modulus $l, q = p^\alpha, p \equiv 1(\mathrm{mod}\, l)$," Acta Arithmetica,* vol. 45, pp. 183-199, 1985.
[8] L.D. Baumert, W. H. Williams and R. L. Ward, *"Uniform cyclotomy," Journal of Number Theory,* vol. 14, pp. 67-81, 1982.
[9] Y.-S. Kim, Y.-S. Chung, J.-S. No, and H. Chung, *"On the autocorrelation distribution of Sidel'nikov sequences," IEEE Trans. Inf. Theory,* vol. 51, no. 9, pp. 3303-3307, September 2005.
[10] Y.-S. Chung, Y.-S. Kim, T.-H. Lim, J.-S. No, and H. Chung, *"Cyclotomic numbers of order 5 over F_{p^n}," in Proceedings of International Symposium on Information Theory (ISIT) 2005,* pp. 1962-1966.
[11] V. M. Sidel'nikov, *"Some k-valued pseudo-random sequences and nearly equidistant codes," Probl. Inf. Transm.,* vol. 5, no. 1, pp. 12-16, 1969.

Notes on Bent Functions in Polynomial Forms

Onur Koçak†, Onur Kurt, Neşe Öztop†, Zülfükar Saygı††

***Abstract*—The existence and construction of bent functions are two of the most widely studied problems in Boolean functions. For monomial functions $f(x) = Tr_1^n(\lambda x^s)$, these problems studied extensively and it is shown that the bentness of the monomial functions is complete for $n \leq 20$. However, in the binomial function case, i.e. $f(x) = Tr_1^n(ax^{s_1}) + Tr_1^k(bx^{s_2})$, this characterization is not complete and there are still open problems.**

In this paper, we give a summary of the literature on the bentness of binomial functions and show that there exist no bent functions of the form $Tr_1^n(ax^{r(2^m-1)}) + Tr_1^m(bx^{s(2^m+1)})$ where $n = 2m$, $gcd(r, 2^m + 1) = 1$, $gcd(s, 2^m - 1) = 1$. Also, we give a bent function example of the form $f_{a,b}(x) = Tr_1^n(ax^{2^m-1}) + Tr_1^2(bx^{\frac{2^n-1}{3}})$ for $n = 4$ although it is stated in [8] that there is no such bent function of this form for any value of a and b.

***Index Terms*—Boolean function, Bent functions, Walsh-Hadamard Transform, Dillon exponents, Kloosterman Sums.**

I. Introduction

The class of bent functions is a special set of functions that achieve the highest possible non-linearity among Boolean functions. Such functions are of great importance for cryptography and coding theory. Therefore, the existence of bent functions is a widely studied problem. When considering the polynomial form, monomial bent functions, which are of the form $Tr_1^n(ax^s)$ are studied extensively by [1], [2], [3], [6] and all monomial bent functions are known if $n \leq 20$. After reaching such a point, community started to pay attention on binomial bent functions of the form $Tr_1^n(ax^{s_1}) + Tr_1^k(bx^{s_2})$. These functions are examined in [5], [7], [8], [9], [13], [14] and the existence conditions of bent functions are given for some values of the parameters n, k, s_1 and s_2. However, the characterization of binomial bent functions is not complete and open problems remain.

In this paper, we give a brief summary of current studies on binomial bent functions. Moreover, we give existence and nonexistence results for some specific forms of bent functions families.

The paper is organized as follows: Section II is devoted to the notation used in the rest of the paper and necessary knowledge. In the third section, in order to give the historical background, we mention the known results on monomial bent functions. Next, in Section IV, we investigate the bentness of the functions $f_{a,b}(x) = Tr_1^n(ax^{2^m-1}) + Tr_1^k(bx^{\frac{2^n-1}{t}})$, give some examples and results on specific values of k, t and m.

O.Koçak, O.Kurt and N.Öztop, are with the Department of Cryptography, Institute of Applied Mathematics, Middle East Technical University, e-mail: {onur.kocak, konur, noztop}@metu.edu.tr

Z.Saygı is with the Department of Mathematics, TOBB Economics and Technology University, e-mail: zsaygi@etu.edu.tr

† The authors are supported by TÜBİTAK under Fellowship Program No. 2211.

†† The author is supported by TÜBİTAK under Grant No. TBAG–109T344.

II. Notation and Preliminaries

A. Boolean Functions and Polynomial Forms

Let $f : \mathbb{F}_{2^n} \to \mathbb{F}_2$ be a Boolean function in n variables. The *truth table* of f is defined as the vector $(f(x_0), f(x_1), \ldots, f(x_{2^n-1}))$. The number of non-zero coordinates in the truth table is called the *Hamming weight* $wt(f)$ of f, or weight in short. Equivalently, one can define weight as

$$wt(f) = \sum_{x \in \mathbb{F}_{2^n}} f(x).$$

The support of f, denoted by $supp(f)$, is the set of inputs $x \in \mathbb{F}_{2^n}$, such that $f(x) = 1$:

$$supp(f) = \{x \in \mathbb{F}_{2^n} | f(x) = 1\}.$$

It is easy to see that $\#supp(f) = wt(f)$.

Any Boolean function f can be uniquely represented in a polynomial form as

$$f(x) = \sum_{r \in R} Tr_1^{o(r)}(a_r x^r) + \epsilon(1 + x^{2^n-1}),$$

$\forall x \in \mathbb{F}_{2^n}$, $a_r \in \mathbb{F}_{2^{o(r)}}$ where $Tr_1^n(x) = \sum_{i=0}^{n-1} x^{2^i}$, the trace function from $\mathbb{F}_{2^n}$ to $\mathbb{F}_2$, is the sum of the conjugates of $x \in \mathbb{F}_{2^n}$, R is the set of *cyclotomic coset leaders* r, $o(r)$ is the size of the coset that contains r and ϵ is the modulo 2 value of $wt(f)$.

Note that bent functions defined on $\mathbb{F}_{2^n}$ exist only for even values of n. Moreover, it is well known that their Hamming weights are even. Therefore, $\epsilon = 0$ and their polynomial form is

$$f(x) = \sum_{r \in R} Tr_1^{o(r)}(a_r x^r) \quad \forall x \in \mathbb{F}_{2^n}.$$

B. Bent Functions

The *Walsh-Hadamard transform* of f is the discrete Fourier transform of $(-1)^f$. It is defined for the value $\omega \in \mathbb{F}_{2^n}$ as follows:

$$W_f(\omega) = \sum_{x \in \mathbb{F}_{2^n}} (-1)^{f(x) + Tr_1^n(\omega x)}.$$

Definition 1. *A Boolean function $f : \mathbb{F}_{2^n} \to \mathbb{F}_2$ is said to be bent if $W_f(\omega) = \pm 2^{\frac{n}{2}}$ for all $\omega \in \mathbb{F}_{2^n}$.*

The classical binary Kloosterman sums on $\mathbb{F}_{2^m}$ are defined as follows:

Definition 2. *Let $a \in \mathbb{F}_{2^m}$. The binary Kloosterman sum associated with a is*

$$K_m(a) = \sum_{x \in \mathbb{F}_{2^m}} (-1)^{Tr_1^m\left(ax+\frac{1}{x}\right)}$$

Proposition 1. *[10] Let m be a positive integer. The set $\{K_m(a),\ a \in \mathbb{F}_{2^m}\}$ is the set of all the integers multiple of 4 in the range $\left[-2^{\frac{m+2}{2}}+1, 2^{\frac{m+2}{2}}+1\right]$.*

III. Monomial Bent Functions

Let $f : \mathbb{F}_{2^n} \to \mathbb{F}_2$ be a Boolean function such that $f(x) = Tr_1^n(ax^s)$ for a given positive integer s and for some $a \in \mathbb{F}_{2^n}$. Functions of this form are called monomial functions. The exponent s is said to be a bent exponent if there exists $a \in \mathbb{F}_{2^n}^*$ such that $Tr_1^n(ax^s)$ is bent. In order f to be bent, the following two conditions should be satisfied [2]:

- $gcd(s, 2^n - 1) \neq 1$.
- either $gcd(s, 2^{n/2}+1) = 1$ or $gcd(s, 2^{n/2} - 1) = 1$.

All known bent exponents s for power functions, with $o(s) = n$, are given in Table I.

TABLE I
ALL KNOWN BENT EXPONENTS, s, $o(s) = n$

s	Condition	Reference
$2^i + 1$	$\frac{n}{gcd(n,i)}$ even, $1 \leq i \leq \frac{n}{2}$	[11]
$r \cdot (2^{n/2} - 1)$	$gcd(r, 2^{n/2}+1) = 1$	[1], [2], [6], [10]
$2^{2i} - 2^i + 1$	$gcd(n, i) = 1$	[12]
$(2^{n/4} + 1)^2$	$n = 4r$, r odd	[2], [4]
$2^{n/3} + 2^{n/6} + 1$	$n = 0 \ mod\ 6$	[3]

Also, Canteaut *et al.* [3] showed by computer experiments that there is no other exponent s for $n \leq 20$.

A specific form of monomial functions, $f_a^{(r)}$, namely monomial Dillon functions, can be represented as

$$\forall x \in \mathbb{F}_{2^n},\ f_a^{(r)}(x) = Tr_1^n(ax^{r(2^m-1)}),\ a \in \mathbb{F}_{2^n}^*, n = 2m.$$

Bentness of these functions has been first studied by Dillon [1] for the case $r = 1$. Then, Leander [2] next Charpin and Gong [6] investigated the bentness of monomial Dillon functions in the case $gcd(r, 2^m+1) = 1$. The following theorem shows the relation between the bentness of monomial Dillon functions and Kloosterman sums.

Theorem 1. *[1], [6] Suppose that $a \in \mathbb{F}_{2^m}^*$. The function $f_a^{(r)}$ defined on $\mathbb{F}_{2^n}$ by $f_a^{(r)}(x) = Tr_1^n(ax^{r(2^m-1)})$ where $gcd(r, 2^m + 1) = 1$ is bent if and only if the Kloosterman sum on $\mathbb{F}_{2^m}$ denoted by K_m satisfies $K_m(a) = 0$.*

In this paper, we focus on the bent functions with Dillon exponents.

IV. Bent Functions of the form $Tr_1^n(ax^{(2^m-1)}) + Tr_1^k(bx^{\frac{2^n-1}{t}})$

Binomial functions of the form $f_{a,b}(x) = Tr_1^n(ax^{2^m-1}) + Tr_1^k(bx^{\frac{2^n-1}{t}})$ have been previously studied by Mesnager [8] and Wang [9] *et al.* Both authors presented some results on the construction of binomial bent functions. In this section, we investigate bentness of $f_{(a,b)}$ when $t|2^m + 1$ and when $t|2^m - 1$. We cover the previous work, give some examples for both cases and state a result on the existence of bent functions of the form $f_{(a,b)}$.

A. $Tr_1^n(ax^{(2^m-1)}) + Tr_1^k(bx^{\frac{2^n-1}{t}})$, where $o(\frac{2^n-1}{t}) = k$ and $t|2^m + 1$

Mesnager [8] showed that the bentness of

$$f_{a,b}(x) = Tr_1^n(ax^{(2^m-1)}) + Tr_1^2(bx^{\frac{2^n-1}{3}})$$

$a \in F_{2^n}^*$, $b \in F_4$, $n = 2m$, can be characterized via Kloosterman sums for $m > 3$, m odd. If $K_m(a) = 4$, then $f_{a,1}, f_{a,\beta}$ and f_{a,β^2} are bent while if $K_m(a) \neq 4$ then $f_{a,1}, f_{a,\beta}$ and f_{a,β^2} are not bent. Wang *et al.* [9] followed similar approach given in [8] and showed that

$$g_{a,b}(x) = Tr_1^n(ax^{(2^m-1)}) + Tr_1^4(bx^{\frac{2^n-1}{5}})$$

is bent for some values of a and b, where $a \in \mathbb{F}_{2^n}^*$, $b \in \mathbb{F}_{2^4}$, $n = 2m$ and $m \equiv 3 \ mod\ 4$. The following function can be given as an example of a bent function of this form:

$$Tr_1^{12}(x^{63}) + Tr_1^4(\beta x^{819})$$

where $\beta = \alpha^{273}$ is a root of the primitive polynomial x^4+x+1 and α is a root of the primitive polynomial $x^{12}+x^6+x^4+x+1$.

Both these approaches are quite similar and depend on the fact that 3 or 5 do not only divide $2^n - 1$ but also $2^m + 1$. Mesnager [14] proved this idea for general case

$$h_{a,b}(x) = \sum_{r \in R} Tr_1^n(a_r x^{r(2^m-1)}) + Tr_1^k(bx^{s(2^m-1)})$$

where $n = 2m$ is an even integer, R is a subset of representatives of the cyclotomic classes modulo $2^m + 1$, $a_r \in \mathbb{F}_{2^m}^*$, $b \in \mathbb{F}_{2^k}$ and $s = \frac{2^m+1}{t}$. Note, $o(s(2^m-1)) = k$, i.e. k is the size of the cyclotomic coset of s modulo $2^m + 1$. The proof for the general case depends on Dickson polynomials.

B. $Tr_1^n(ax^{(2^m-1)}) + Tr_1^k(bx^{\frac{2^n-1}{t}})$, where $o(\frac{2^n-1}{t}) = k$ and $t|2^m - 1$

In [8], Mesnager studied the functions of the form

$$f_{a,b}(x) = Tr_1^n(ax^{(2^m-1)}) + Tr_1^2(bx^{\frac{2^n-1}{3}})$$

and found some results when m is odd. Because of the fact that 3 divides $2^m - 1$ when m is even, this case seems much harder than the case for m odd. Therefore, the bentness of $f_{a,b}$ for even values of m has not been characterized yet. On the other hand, it is claimed in [8] by conducting exhaustive search that for $n = 8, 12$, there exist bent Boolean functions of the form $f_{a,b}(x) = Tr_1^n(ax^{(2^m-1)}) + Tr_1^2(bx^{\frac{2^n-1}{3}})$, but there is no bent function of this form for $n = 4$. However, our computer experiments resulted in the existence of a bent function for $n = 4$ and it is shown in *Remark 1*.

Remark 1. *$f_{a,b}(x) = Tr_1^4(ax^3) + Tr_1^2(bx^5)$ is bent for $a = 1$ and $b = 1$ where $\mathbb{F}_{2^4} = \mathbb{F}_2(\alpha)$ and α is a root of the primitive polynomial $x^4 + x + 1$ over $\mathbb{F}_{2^4}$.*

Algebraic normal form of $f(x)$ is

$$f(x) = Tr_1^4(x^3) + Tr_1^2(x^5) = x_1 + x_2x_3 + x_1x_4$$

where $x = (x_1, x_2, x_3, x_4)$. The truth table and Walsh spectrum of $f(x)$ can be seen from Table II.

TABLE II

x	$Tr_1^4(x^3)$	$Tr_1^2(x^5)$	$f(x)$	$W_f(x)$
0	0	0	0	4
1	0	0	0	-4
α	1	1	0	4
$\alpha+1=\alpha^4$	1	1	0	-4
α^2	1	1	0	4
$\alpha^2+1=\alpha^8$	1	1	0	-4
$\alpha^2+\alpha=\alpha^5$	0	1	1	-4
$\alpha^2+\alpha+1=\alpha^{10}$	0	1	1	4
α^3	1	0	1	4
$\alpha^3+1=\alpha^{14}$	1	1	0	4
$\alpha^3+\alpha=\alpha^9$	1	0	1	4
$\alpha^3+\alpha+1=\alpha^7$	1	1	0	4
$\alpha^3+\alpha^2=\alpha^6$	1	0	1	4
$\alpha^3+\alpha^2+1=\alpha^{13}$	1	1	0	4
$\alpha^3+\alpha^2+\alpha=\alpha^{11}$	1	1	0	-4
$\alpha^3+\alpha^2+\alpha+1=\alpha^{12}$	1	0	1	-4

The following functions are numerical examples for $f_{a,b}$ when 3 divides 2^m-1 :

- For $n=8$, $m=4$, $k=2$ and $t=3$

$$Tr_1^8(\alpha^{51}x^{15})+Tr_1^2(x^{85})$$

where α is a root of the primitive polynomial $x^8+x^4+x^3+x^2+1$.

- For $n=12$, $m=6$, $k=2$ and $t=3$

$$Tr_1^{12}(\alpha^{195}x^{63})+Tr_1^2(x^{1365})$$

where α is a root of the primitive polynomial $x^{12}+x^6+x^4+x+1$.

Consider the case $t=2^m-1$. Then,

$$f_{a,b}(x)=Tr_1^n(ax^{2^m-1})+Tr_1^m(bx^{2^m+1}).$$

It is known that if $f_{a,b}(x)$ is bent, then $W_f(w)=\pm 2^m$, $\forall w$. Before looking at the Walsh-Hadamard transform, it is worth to note two well-known facts one of which is about the Kloosterman sums.

Proposition 2. *[1]*

$$\sum_{u\in\mathbb{U}}(-1)^{Tr_1^n(au)}=1-K_m(a),$$

where $\mathbb{U}$ is the cyclic group of order 2^m+1 and $a\in\mathbb{F}_{2^m}^*$.

Proposition 3. *Any $x\in\mathbb{F}_{2^n}^*$ can be written as $x=uy$ with $y\in\mathbb{F}_{2^m}^*$ and $u\in\mathbb{U}$ where $\mathbb{U}$ is the cyclic group of order 2^m+1.*

Computation of the Walsh-Hadamard transform for $w=0$ shows

$$\begin{aligned}
W_f(0) &= \sum_{x\in\mathbb{F}_{2^n}}(-1)^{Tr_1^n(ax^{2^m-1})+Tr_1^m(bx^{2^m+1})}\\
&= \sum_{u\in\mathbb{U}}\sum_{y\in\mathbb{F}_{2^m}^*}(-1)^{Tr_1^n(a(uy)^{2^m-1})+Tr_1^m(b(uy)^{2^m+1})}+1\\
&= \sum_{u\in\mathbb{U}}(-1)^{Tr_1^n(au^{2^m-1})}\sum_{y\in\mathbb{F}_{2^m}^*}(-1)^{Tr_1^m(by^2)}+1\\
&= \sum_{u\in\mathbb{U}}(-1)^{Tr_1^n(au)}\sum_{y\in\mathbb{F}_{2^m}^*}(-1)^{Tr_1^m(by)}+1\\
&= (1-K_m(a))(-1)+1\\
&= K_m(a)
\end{aligned}$$

In order for $f_{a,b}(x)$ to be bent, $W_f(0)=K_m(a)=\pm 2^m$. However, by Proposition 1, we know that $K_m(a)$ is in the interval $[-2^{\frac{m+2}{2}}+1, 2^{\frac{m+2}{2}}+1]$ $\forall a\in\mathbb{F}_{2^m}^*$. One can easily show that, for any value of $m>2$, $\pm 2^m$ is out of Kloosterman sums bounds. To illustrate, the boundaries for $K_m(a)$ and the Walsh spectrum values are given in Table III for distinct values of m. This observation is stated in *Proposition 4*.

TABLE III

m	$K_m(a)$	$W_f(0)$
2	[-3, 5]	± 4
3	[-4.65, 6.65]	± 8
4	[-7, 9]	± 16
5	[-10.31, 12.31]	± 32
6	[-15, 17]	± 64

Proposition 4. *Boolean functions of the form*

$$f_{a,b}(x)=Tr_1^n(ax^{r(2^m-1)})+Tr_1^m(bx^{s(2^m+1)})$$

where $gcd(r,2^m+1)=1$, $gcd(s,2^m-1)=1$ are not bent for any a, $b\in\mathbb{F}_{2^m}^*$.

V. Conclusion

The classification and characterization of bent functions in polynomial forms is a hard problem. Despite the existence of notably many specified bent functions, there are still open problems and unclassified bent functions remain. In this note, we have studied previous characterization of some binomial functions of the form $f_{(a,b)}(x)=Tr_1^n(ax^{(2^m-1)})+Tr_1^k(bx^{\frac{2^n-1}{3}})$ where t divides either 2^m+1 or 2^m-1. Mesnager [14] investigated the former case and presented some conditions on bentness of this function family. The latter case has not been characterized yet. In this study, we showed for specific values of t, where $t=2^m-1$, that there is no bent function of the form $Tr_1^n(ax^{(2^m-1)})+Tr_1^m(bx^{2^m+1})$. As a future work, it is planned to study the characterization of $f_{(a,b)}$ in the case t divides 2^m-1 which still has open problems.

References

[1] J. F. Dillon, *Elementary Hadamard Difference Sets*, PhD Dissertation, University of Maryland 1974.
[2] G. Leander, *Monomial bent functions*, IEEE Trans. Inf. Theory, vol. 2, no. 52, pp. 738-743, 2006.
[3] A. Canteaut, P. Charpin, and G. Kyureghyan, *A new class of monomial bent functions*, Finite Fields Applicat., vol. 14, no. 1, pp 221-241, 2008.
[4] P. Charpin and G. Kyureghyan, *Cubic monomial bent functions: A subclass of M*, SIAM J. Discr. Math., vol. 22, no. 2, pp. 650-665,2008.
[5] S. Mesnager, *A new class of bent boolean functions in polynomial forms*, in Proc. Int. Workshop on Coding and Cryptography, WCC 2009, pp. 5-18, 2009.
[6] P. Charpin, G. Gong, *Hyperbent functions, Kloosterman Sums and Dickson Polynomials*, IEEE Trans. Inform. Theory 9(54), 4230-4238 (2008).
[7] S. Mesnager, *A new family of hyper-bent boolean functions in polynomial form*, M. G. Parker Ed., in Proc. Twelfth Int. Conf. Cryptography and Coding, Cirencester, United Kingdom. IMACC 2009, Heidelberg, Germany, 2009, vol. 5921, LNCS, pp. 402-417.
[8] S. Mesnager, *A new class of bent and hyper-bent boolean functions in polynomial forms*, Des. Codes Cryptography, 59(1-3):265-279, 2011.
[9] B. Wang, C. Tang, Y. Qi, Y. Yang, M. Xu, *A New Class of Hyper-bent Boolean Functions with Multiple Trace Terms*, Cryptology ePrint Archive, Report 2011/600, 2011. http://eprint.iacr.org/.

[10] G. Lachaud, J. Wolfmann, *The Weights of the Orthogonals of the Extended Quadratic Binary Goppa Codes* IEEE Trans. Inf. Theory, vol. 36, no 3, pp. 686-692, 1990.
[11] R.Gold, *Maximal Recursive Sequences with 3-valued Recursive Cross-Correlation Functions* IEEE Trans. Inf. Theory, vol. 14, no 1, pp. 154-156, 1968.
[12] J.F. Dillon, H. Dobbertin, *New Cyclic Difference Sets with Singer Parameters* Finite Fields and Their Applications, vol.10, no 3, pp. 342-389, 2004.
[13] B. Wang, C. Tang, Y. Qi, and Y. Yang, *A generalization of the class of hyper-bent Boolean functions in binomial forms*, Cryptology ePrint Archive, Report 2011/698, 2011. http://eprint.iacr.org/.
[14] S. Mesnager, J.-P. Flori, *A note on hyper-bent functions via Dillon-like exponents*, Cryptology ePrint Archive, Report 2012/033, 2012. http://eprint.iacr.org/.

Security Margin of 5-Round DEAL

Orhun Kara

***Abstract*—DEAL is a block cipher designed by L. Knudsen. It is a Feistel network with 128-bit block and 128-bit, 192-bit and 256-bit keys. The round function of DEAL is DES encryption and the number of rounds is six for 128 and 192 bit key lengths. Knudsen claimed that the 6-round DEAL and the 5-round DEAL provide 121 bit and 88 bit securities respectively. In this paper, we mount a reflection attack to 5-round DEAL with a time complexity of 2^{72} encryptions for 128-bit key length. The attack works approximately 2^{72} keys. We need 2^{65} chosen plaintexts the identify if a key is weak. The attack is mounted only if the key is weak. We have derived a 3-round distinguisher to mount the attack.**

***Index Terms*—block cipher, self similarity, reflection attack, DEAL, weak key**

I. Introduction

DEAL is a block cipher designed by L. Knudsen. It is a Feistel network with a block length of 128-bit and key lengths of 128-bit, 192-bit and 256-bit. The round function of DEAL is DES encryption and the number of rounds is six for 128 and 192 bit key lengths. Knudsen claimed that the 6-round DEAL and the 5-round DEAL provide 121 bit and 88 bit securities respectively [13].

In this paper, we mount a reflection attack on 5-round DEAL to show that 5-round DEAL provides 72 bit security for some keys. The reflection attack on DEAL is given in [10]. While the attack was successful for 6-round DEAL-192 and 8-round DEAL-256, it failed for 6-round DEAL-128 due to the very few number of weak keys in the 128- bit version. Indeed, the attack has been exploited the 5-round distinguisher which imposes too many conditions on round keys. Hence, the cost of the identification step goes far beyond the number of weak keys, rendering the attack unsuccessful.

In this paper, we exploit 3-round distinguisher to increase the number of weak keys dramatically. However, it is not given how to construct a 3-round distinguisher for the classical reflection attack in the original paper, [10]. The statements in [10] are given for the Feistel networks with palindromic round keys where there are at least two pairs of palindromic keys. Hence the reflection attack in [10] works for the ciphers of round numbers more than five and the distinguisher is based on at least 5 rounds. However, we make use of three-round distinguisher to mount an attack on 5-round DEAL. So, we derive a new statement, Theorem 1, which provides a 3-round distinguisher.

We have seen that the probability that one half of the plaintext is equal to one half of the corresponding ciphertext no more deviates from the random pattern. Hence, the conventional reflection attack does not work. However, we derive a new version of the attack by means of Theorem 1 and mounted the attack on 5-round DEAL.

We use 2^{65} chosen plaintexts to identify whether the key is weak. If it is identified as a weak key, then we recover the key with 2^{72} time complexity, using 2^{56} blocks of memory for DEAL-128. The number of weak keys is 2^{72}, which is more then the cost of the identification step.

The paper is organized as follows. We give a brief description of DEAL-128 in the next section. Section III covers the new results on the reflection attack on DEAL. We give the attack on 5-round DEAL in this section. Finally, we conclude the paper with Section VI.

II. Brief Description of DEAL-128

DEAL, submitted to AES contest, is a Feistel network with 128-bit block length [13]. That is, at each round, one half of the input is encrypted by a round function and added to the other half and the result with the half incorporated into the round function together form the output of the round. The round function of DEAL is DES so that the DES encryption chips can be used for DEAL also which provided DEAL an advantage over the other AES contestants for the interoperability.

The key lengths of DEAL are 128-bit, 192-bit and 256-bit. The number of rounds is six for the 128-bit and 192-bit versions whereas it is 8 for the 256-bit version. In this paper we analyze 5-round DEAL for the 128-bit version.

We give the high level description of DEAL-128. The other versions are quite similar. For the 128-bit version, the key, K, is divided into two 64-bit parts as K_0 and K_1. The six round keys, $RD_{K_1}, ..., RD_{K_6}$, are computed by using DES. An 56-bit constant value, s, is used as the DES key to produce the round keys. The round keys are then calculated from the 64-bit raw data given as

$$\begin{aligned}
RD-RAW_{K_1} &= DES_s(K_0)\\
RD-RAW_{K_2} &= DES_s(K_1 \oplus RD_{K_1})\\
RD-RAW_{K_3} &= DES_s(K_0 \oplus RD_{K_2} \oplus strng(1))\\
RD-RAW_{K_4} &= DES_s(K_1 \oplus RD_{K_3} \oplus strng(2))\\
RD-RAW_{K_5} &= DES_s(K_0 \oplus RD_{K_4} \oplus strng(4))\\
RD-RAW_{K_6} &= DES_s(K_1 \oplus RD_{K_5} \oplus strng(8))
\end{aligned}$$

where $strng(i)$ denotes the integer i as the bit string. Only 56 bits of each $RD-RAW_{K_i}$ is used in the i-th round of DEAL, yielding to the round key RD_{K_i}. We remark that the final round ends with a swap unlike conventional use of Feistel networks.

There are some theoretical attacks on DEAL. The attack by Knudsen [13] is a meet-in-the-middle attack which requires 2^{168} encryptions with 2^{173} bytes of memory for 6-round

Manuscript received March 10, 2012.
Orhun Kara is with TÜBİTAK BİLGEM Gebze, 41470 Kocaeli Turkey, e-mail: orhun,@uekae.tubitak.gov.tr

DEAL. On the other hand, the impossible differential attack on DEAL requires 2^{121} DES encryption with 2^{70} chosen plaintexts and 2^{68} bytes of memory, utilizing the impossible differentials of 5 round Feistels with bijective round functions [13]. In [15], Lucks uses similar techniques and mounts chosen ciphertext attack instead of chosen plaintext attack on DEAL so as to gain information from the first round key. In [12], Kelsey and Schneier discuss the existence of equivalent keys and mount a related key attack.

III. Reflection Attack on 5-Round DEAL-128

Define the Feistel structure as $x_i = R_{k_{i-1}}(x_{i-1}) \oplus x_{i-2}$ recursively with the initial conditions given by $x = (x_0, x_1)$. The initial condition $x = (x_0, x_1)$ is the plaintext, the function R is the round function of the Feistel network and $\oplus$ is the "XOR" operation. The i-th round operation is defined as

$$(x_i, x_{i+1}) = (x_i, R_{k_i}(x_i) \oplus x_{i-1}) \quad (1)$$

for $i \leq r$. The final output (x_r, x_{r+1}) is the corresponding ciphertext of the plaintext (x_0, x_1). The stream $x_0, x_1, ..., x_r, x_{r+1}$ is called the encryption stream of (x_0, x_1) with respect to K.

The reflection attack in [10] mounted on 6-round DEAL exploits the palindromic properties of the round keys given as

$$RD_{K_2} = RD_{K_6} \quad (2)$$
$$RD_{K_3} = RD_{K_5} \quad (3)$$

However, all the keys do not produce such palindromic round keys. The probability that these equalities hold is roughly 2^{-112}. When Equations 2 and 3 hold, the last five rounds of DEAL has 2^{64} fixed points (without the final swap). Then one can mount a reflection attack given in [10]. However, this attack is not successful for 128-bit DEAL since the number of weak keys, which are the keys producing the subkeys satisfying Equations 2 and 3, is around 2^{16}. So, identifying a weak key costs much more than the number of weak keys. Remark that the total cost of recovering a weak key among several keys, if exists, consists of the cost of identifying the weak key with the cost of recovering it. Hence, the overall complexity exceeds that of exhaustive search.

One natural extension of the attack is to increase the number of weak keys. This can be done by loosing one of the equalities between subkeys. In this section, we introduce a new reflection attack on 5-round DEAL-128 by imposing only one equality on subkeys. Hence the probability of this condition will raise to 2^{-56}. In this case, the number of weak keys is approximately 2^{72} for 128 bit DEAL. Hence we are able to possess a resource of 2^{72} encryptions for the identification.

Consider the 5-round DEAL-128 by revoking the last round. Assume that

$$RD_{K_2} = RD_{K_4}. \quad (4)$$

This happens with a probability of 2^{-56}. We will have a 3-round reflection for the rounds 2, 3 and 4 in this case. However, we can not use the theorems in Section IV of [10] since the theorems are not valid for a 3-round distinguisher. For instance, it is given in [10] that

$$\Pr(x_0 = x_r) = 2^{-\frac{n}{2}}(2 - 2^{-\frac{n}{2}})$$

which is a distinguisher in order to identify a weak key for the Feistel networks with palindromic subkeys and bijective round functions. Because, $\Pr(x_0 = x_r)$ in the case of a weak key is more than twice as much as $\Pr(x_0 = x_r)$ in random case. The conventional reflection attack given in [10] exploits this distinguisher. However, the probability $\Pr(x_0 = x_r)$ will no more be able to be distinguished from the random case when the number of rounds satisfying the palindromic subkeys is three and the round function is a permutation. Therefore, the attack given in [10] will not work in this case.

We derive another statement to mount a reflection attack on 5-round DEAL-128 where there is a 3-round reflection property.

Theorem 1: Let $(x_0, x_1, x_2, x_3, x_4, x_5)$ be the encryption stream of a 4-round n bit block Feistel network whose round function is a random permutation for any key. Assume $k_1 = k_3$. Then we have

a) $x_0 = x_4$ if and only if $x_1 = x_3$.

b) $\Pr(x_0 = x_4) = 2^{n/2}$ (which is random) and $\Pr(R_{k_2}(x_2) = 0 \,|\, x_0 = x_4) = 1$.

Proof: Consider a Feistel network of 4-round with an encryption stream $(x_0, x_1, x_2, x_3, x_4, x_5)$ where $k_1 = k_3$. Assume $x_0 = x_4$. Then $F_{k_1}(x_1) = F_{k_3}(x_3)$ since $x_0 = F_{k_1}(x_1) \oplus x_2$ and $x_4 = F_{k_3}(x_3) \oplus x_2$. On the other hand, F is a permutation by the assumption. So, $x_1 = x_3$. Assume, on the contrary that $x_1 = x_3$. Then,

$$x_4 = F_{k_3}(x_3) \oplus x_2 = F_{k_3}(x_1) \oplus x_2 = F_{k_1}(x_2) \oplus x_2 = x_0.$$

So, we have proved that $x_0 = x_4$ if and only if there is fixed point for the first three rounds. So, $x_0 = x_4$ implies that $R_{k_2}(x_2) = 0$. This fact is given in [7], [16], [17]. Hence $\Pr(R_{k_2}(x_2) = 0 \,|\, x_0 = x_4) = 1$. On the other hand, $x_0 = x_4$ only if $R_{k_2}(x_2) = 0$. Because $x_0 = x_4$ means (x_0, x_1) is a fixed point and a fixed point occurs only if $R_{k_2}(x_2) = 0$. The probability that $R_{k_2}(x_2) = 0$ is roughly $2^{n/2}$ for a random permutation F. Hence $\Pr(x_0 = x_4) = 2^{n/2}$. ■

Corollary 1: Assume $k_1 = k_3$ for a given 4-round n bit block Feistel network with an encryption stream $(x_0, x_1, x_2, x_3, x_4, x_5)$. Assume also that the round functions are all permutations. The equality $x_0 = x_4$ holds if and only if $x_1 = R_{k_4}(x_4) \oplus x_5$.

Proof: Let $(x_0, x_1, x_2, x_3, x_4, x_5)$ be the encryption stream of a 4-round Feistel network with permutation round functions such that $k_1 = k_3$. Assume that $x_0 = x_4$. Then $x_1 = x_3$ by Theorem 1. On the other hand $x_3 = F_{k_4}(x_4) \oplus x_5$. Hence, $x_1 = F_{k_4}(x_4) \oplus x_5$. Conversely, if $x_1 = R_{k_4}(x_4) \oplus x_5$ then $x_1 = x_3$ and hence $x_0 = x_4$ again by Theorem 1. ■

Let us remark that Corollary 1 states that whenever we have an equality between the right part of the plaintext and the left part of the ciphertext, we have an input-output pair for the last round function. This was not always true when the number of rounds is larger than 4. There was a probability that the equality between the right and the left parts of plaintexts and ciphertexts respectively might happen randomly, not due to a

fixed point. In this case, the equality $x_1 = R_{k_r}(x_r) \oplus x_{r+1}$ would most probably be not satisfied.

Corollary 2: Assume $k_1 = k_3$ for a given 4-round n bit block Feistel network. For a given x_1, let $P_{x_1} = \{(x_0, x_1) | x_0 \in GF(2^{n/2})\}$. That is, P_{x_1} is the set of plaintexts whose first halves take all the values and second halves equal to a fixed x_1. Then there is only one element (x_0, x_1) of P_{x_1} such that the right half of the ciphertext of the encryption of (x_0, x_1) is x_0 and the ciphertext is $(x1 \oplus F_{k_4}(x_0), x_0)$.

Proof: Let $P_{x_1} = \{(x_0, x_1) | x_0 \in GF(2^{n/2})\}$. Then the left part of P_{x_1} takes all the possible values. On the other hand $x_2 = F_{k_1}(x_1) \oplus x_0$. Hence, x_2 takes all the values possible exactly once. Going on so, $F_{k_2}(x_2)$ takes all the values exactly once since F_{k_2} is a permutation. Hence there exists only one x_2 such that $F_{k_2}(x_2) = 0$. Let x_0 be the left part of the corresponding plaintext for this x_2. Then (x_0, x_1) is a fixed point by Theorem 1. This means that $x_4 = x_0$ and $x_5 = x1 \oplus F_{k_4}(x_0)$. ■

We are ready to mount a reflection attack on 5-round DEAL (WLOG assume there is no final swap). Let $\alpha \in GF(2^{64})$ be any fixed element. Then encrypt all the plaintexts whose right parts are equal to α. If subkeys satisfy, $RD_{K_2} = RD_{K_4}$ then we expect a three-round reflection for the 2nd, the 3rd and the 4th rounds of DEAL. On the other hand there exits x such that (α, x) is expected to be a fixed point by Theorem 1 and Corollary 2. Hence, we observe α at the right half of the ciphertext. Among all the encryptions of 2^{64} chosen plaintext, α is occurred only once as the right half of a ciphertext. In this case, we are sure that a fixed point occurs by Theorem 1.

On the other hand, store the values $(k, DES_k(\alpha))$ sorted by $DES_k(\alpha)$ when k takes all the values. So there are 2^{56} blocks. This can be considered as the pre-computation phase of the attack since it can be performed at any time, particularly before collecting the real data.

Let (x, α) be the plaintext whose encryption is (y, α). Then we have a fixed point for the intermediate three rounds and hence

$$DES_{k_1}(\alpha) \oplus DES_{k_5}(\alpha) = x \oplus y$$

by Theorem 1. Similarly, choose another value β and encrypt all the plaintexts whose right halves are β. Then we have another equation for β:

$$DES_{k_1}(\beta) \oplus DES_{k_5}(\beta) = x \oplus y$$

where the encryption of (x, β) is (y, β). Solve the equation

$$DES_{k_1}(\alpha) \oplus DES_{k_5}(\alpha) = x \oplus y$$

by guessing k_1 and recovering k_5 from the table $(k, DES_k(\alpha))$ sorted by $DES_k(\alpha)$. There are roughly 2^{48} solutions for (k_1, k_5). On the other hand, these solutions must satisfy the equation deduced by β. The right keys always satisfy the equation. Any arbitrary key pair satisfies the equation with a probability of 2^{-64}. Hence, the probability that there is a wrong key pair satisfying both the equations is approximately 2^{-16}.

If there is no key pair satisfying both equations then our assumption is wrong. That is, we have no equality: $RD_{K_2} \neq RD_{K_4}$. In this case we terminate the attack with 2^{65} chosen plaintexts. If there is a key pair satisfying both equations then we conclude that $RD_{K_1} = k_1$. This gives 56 bit information of the main key. Search the remaining 72 bits of the key exhaustively if the key is identified as a weak key. Let us remark that there may be solutions to (k_1, k_5) for some keys even though $RD_{K_2} \neq RD_{K_4}$ since the probability of finding a solution among 2^{112} subkey candidates is 2^{-16} in this case.

The data complexity of the attack is 2^{65} chosen plaintexts. We need a memory of 2^{56} pairs of the form $(k, DES_k(\alpha))$. Each pair is 15 bytes. At the end we recover the key with 2^{72} time complexity if the key is weak. That is, $RD_{K_2} = RD_{K_4}$. The exhaustive search on 72 bits is done only once at 2^{16} identification steps.

IV. Conclusion

We have analyzed the security margin of 5-round DEAL by means of a self-similarity attack. We have mounted a reflection attack on 5-round DEAL with a time complexity of 2^{72} encryptions if the key is a weak key for DEAL-128. The attack works for approximately 2^{72} keys and we have used 2^{65} chosen plaintexts to identify if the attack works for a given key, before mounting the attack.

We have needed a 3-round distinguisher to mount a reflection attack successfully on 5-round DEAL. However, the reflection attack on Feistel networks given in [10] does not work for a 3-round distinguisher. So, we have derived a new version of the reflection attack for the Feistel networks. This new derivative makes use of 3-round distinguisher and can be successfully mounted on 5-round DEAL faster than the brute force in terms of the overall complexity.

Acknowledgment

We would like to thank the anonymous reviewers for their comments.

References

[1] E. Biham. New Types of Cryptanalytic Attacks Using Related Keys. *J. of Cryptology*, Vol.7, pp.229-246, 1994.
[2] E.Biham, O. Dunkelman and N. Keller. Improved Slide Attacks. In *Proc. FSE'07*, LNCS 4593, pp. 153-166, Springer, 2007.
[3] E.Biham, O. Dunkelman and N. Keller. Related-Key Boomerang and Rectangle Attacks. In *Proc. of EUROCRYPT 2005*, LNCS 3494, pp. 507-525, Springer, 2005.
[4] E.Biham, O. Dunkelman and N. Keller. A Unified Approach to Related-Key Attacks. In *Proc FSE'08*, LNCS 5086, pp73-96, Springer, 2008.
[5] A. Biryukov and D. Wagner. Slide Attacks. In *Proc. FSE'99*, LNCS 1636, pp.245-259, Springer, 1999.
[6] A. Biryukov and D. Wagner. Advanced Slide Attacks. In *Proc. EUROCRYPT 2000*, LNCS 1807, pp.589-606, Springer, 2000.
[7] D. Coppersmith. The Real Reason for Rivest's Phenomenon. In *Proc. CRYPTO'85*, LNCS 218, pp. 535-536, Springer, 1985.
[8] E.K. Grossman and B. Tuckerman. Analysis of a Weakened Feistel-like Cipher. In Proc. *International Conference on Communications*, pp. 46.3.1-46.3.5, Alger Press Limited, 1978.
[9] S. Furuya. Slide Attacks with a Known-Plaintext Cryptanalysis. In Proc. Information and Communication Security 2001, LNCS 2288, pp. 214-225, Springer, 2002.
[10] O. Kara. Reflection Cryptanalysis of Some Ciphers. In *Proc. Indocrypt'08*, LNCS 5365, pp. 294-307, Springer, 2008.
[11] B.S. Kaliski, R.L. Rivest and T. Sherman. Is DES a Pure Cipher? (Results of More Cycling Experiments on DES). In *Proc. CRYPTO'85*, LNCS 218, pp. 212-222, Springer, 1985.
[12] J. Kelsey and B. Schneier. Key-Schedule Cryptanalysis of DEAL. In *Proc. SAC'99*, LNCS 1758 pp.118-134, Springer, 2000.

[13] L. Knudsen. DEAL - a 128-Bit Block Cipher. Avaliable at http://www.ii.uib.no/ larsr/aes.html.
[14] L. Knudsen. Cryptanalysis of LOKI91. In *Proc. of AUSCRYPT'92*, LNCS 718, pp 196-208, Springer, 1993.
[15] S. Lucks. On the Security of 128-Bit Block Cipher DEAL. In *Proc. FSE'99*, LNCS 1636, pp.60-70, Springer, 1999.
[16] J.H. Moore and G.J. Simmons. Cycle Structure of the DES with Weak and Semi-Weak Keys. In *Proc. CRYPTO'86*, LNCS 263, pp.9-32, Springer, 1986.
[17] J.H. Moore and G.J. Simmons. Cycle Structure of the DES for Keys Having Palindromic (or Antipalindromic) Sequences of Round Keys. *IEEE Transactions on Software Engineering*, pp. 262-273,No 13,1987.

How Biased Are Linear Biases

Adnan Baysal and Orhun Kara

***Abstract*—In this paper we re-visit the Matsui's linear cryptanalysis. The linear attack on the full round DES was the first attack that has been verified experimentally. Matsui extended one-round linear approximations to a linear mask of plaintext-ciphertext pairs by means of his piling-up lemma. The assumption of the lemma, the independence of the random variables in the round approximations, is hopefully fulfilled for the full round DES. So the experiment was successful. However, there exist some ciphers whose linear approximations may have completely different biases than those calculated by the piling-up lemma. We work out a case study where the biases of the linear approximations cannot be calculated through the lemma. We derive the theoretical infrastructures which lead us to compute the overall bias. We verify the theoretical results by performing some experiments on a toy cipher. For the verification, we mount a linear attack on the cipher and construct two linear approximations having the same plaintext-ciphertext masks. We show that the biases of the approximations are different from what the piling-up lemma asserts.**

***Index Terms*—block cipher, linear cryptanalysis, nonlinearity, DES, linear hull, linear approximation**

I. Introduction

Matsui's linear cryptanalysis is the second successful attack on the full round DES, exploiting the biases of the linear approximations between plaintext, ciphertext and key bits [12]. These linear approximations are constructed by extending one-round linear approximations whose input-output masks cancel out one by one so that there is no interior variable left in the combined linear approximation. Matsui introduces the piling-up lemma to compute the overall bias of the combined linear approximation.

The piling-up lemma works when the random variables in the linear approximations are independent. It is interesting to see that this condition is not fulfilled for all ciphers. Hopefully, Matsui has shown experimentally that his approximations work for an arbitrary key on DES [13].

In this paper, we examine the Matsui's linear cryptanalysis. We construct a set of random variables and calculate the biases between them. We divide the random variables into two sets and assume that any two distinct variables in different sets are independent. On the other hand, the random variables in one set are equal to each other with certain probabilities, and hence we can construct a linear approximation for each set. We compute the biases for the approximations. We show that the biases are not equal to the biases computed by the piling-up lemma even though the random variables are independent. We design a toy cipher and construct two linear approximations for the cipher whose random variables act in accordance with the model we introduce. Finally, we calculate the biases experimentally and verify our theoretical results.

The paper is organized as follows: In Section II, we give a brief overview of the linear cryptanalysis and show how it is mounted on DES. Also, we depict a high level description of DES in this section. We introduce the notion of hull effect and the related works on the hull effect in Section III. In Section IV we describe our case study and give the theoretical infrastructure. We verify the theoretical results by performing some experiments in Section V. Finally we conclude the paper with section VI.

Manuscript received March 26, 2012.

Adnan Baysal and Orhun Kara are with TÜBİTAK BİLGEM Gebze, 41470 Kocaeli Turkey, e-mails: {abaysal,orhun}@uekae.tubitak.gov.tr

II. An Overview of Linear Attack on DES

Linear attack is one of the most effective cryptanalysis methods on block ciphers. The first, and maybe the most prominent sample of the method is the attack mounted on DES by Matsui [12]. Matsui show that the full round DES is vulnerable to the linear cryptanalysis if the attacker has 2^{47} known plaintexts. He also conducted an experiment and implemented the attack successfully [13], verifying his results related to attack complexities and success rates.

The linear cryptanalysis exploits the biased equations between linear combinations of certain plaintext bits and ciphertext bits. Consider a linear equation of the form

$$\begin{aligned} &P[i_1] \oplus \cdots \oplus P[i_m] \oplus C[j_1] \oplus \cdots \oplus C[j_s] \\ &= K[l_1] \oplus K[l_2] \oplus \cdots \oplus K[l_t] \end{aligned} \quad (1)$$

where $P[i]$, $C[i]$ and $K[i]$ are the i-th bits of the plaintext, the ciphertext and the key respectively. The operation $\oplus$ is the XOR operation. Let Equation 1 be satisfied with a probability $\frac{1}{2} + \epsilon$. Matsui introduces an algorithm which he calls "Algorithm 1" to reveal one bit information of the key. Assume that $\epsilon > 0$.

If the number of plaintext-ciphertext pairs which make the left hand side of Equation 1 equal to 0 is more than half of all the plaintext-ciphertext pairs then we conclude that

$$K[l_1] \oplus K[l_2] \oplus \cdots \oplus K[l_t] = 0.$$

Otherwise, that is, if the number of plaintext-ciphertext pairs where the right half Equation 1 is equal to 1 is more than half of the all the plaintext-ciphertext pairs, then,

$$K[l_1] \oplus K[l_2] \oplus \cdots \oplus K[l_t] = 1.$$

If the bias, ϵ, is negative, Algorithm 1 complements the results above.

Algorithm 1 retrieves one bit of information from the key which is the value of the linear combination

$$K[l_1] \oplus K[l_2] \oplus \cdots \oplus K[l_t].$$

The success rate depends on the data complexity. It is given as

$$\int_{-2\sqrt{N}|\epsilon|}^{\infty} \frac{1}{\sqrt{2\pi}} \exp(-x^2/2)dx$$

where N is the number of the plaintexts and exp is the Euler function. Let us remark that this success rate is almost one when N is proportional to ϵ^{-2}. For instance, when $N \approx \epsilon^{-2}$ the success rate is around 98 %.

For a given cipher, one of the natural questions is how to find equations of the form given in Equation 1, if such equations exist with significant biases. Matsui answered this question in the case of DES and found a linear characteristic with a bias of $\epsilon = -1,49 \cdot 2^{-24}$ for the 16-round DES. To find such a characteristic, Matsui analyzed the "nonlinearity degree" of the S-boxes of DES. He introduced the following definition to measure how nonlinear an S-box is [12]:

Definition 1: Let S be an S-box of n-bit input, m-bit output. For a given $\alpha \in GF(2)^n$ and $\beta \in GF(2)^m$, define the number $N_S(\alpha, \beta)$ as the number of times out of 2^n inputs such that an XORed value of the input bits masked by α is equal to an XORed value of the output bits masked by β. In other words,

$$N_S(\alpha,\beta) = |\{x| \oplus_{i=0}^{n} x[i] \cdot \alpha[i] = \oplus_{j=0}^{m} S(x)[j] \cdot \beta[j]\}|$$

where $\cdot$ is bitwise AND operation.
The values $N_S(\alpha,\beta)$ are expected to be around 2^{n-1} for a highly nonlinear S -Box. Otherwise, there are some α masks in the input and β masks in the output such that the linear equation given by $N_S(\alpha,\beta)$ would be highly biased, that is, the absolute value of its bias, say ϵ, is quite larger than 0. For instance, the fifth S-Box of DES satisfies $N_{S_5}(16,15) = 12$ among all the 64 input patterns. That is, the fourth input bit of the S-Box is equal to the sum of all the output bits with a probability $\frac{1}{2} - \frac{20}{64}$ if the input is random.

A. A Brief Description of DES

DES is one of the most famous block ciphers which has been used worldwide prevalently since 1976. It can be considered as the ancestor of all the modern block ciphers. DES has 64-bit block length and 56-bit key length. It is a Feistel network. That is, the plaintext is divided into two equal part, say the left half and the right half, and then the output of right part through the round function F is XOR'ed to the left part. Then the left and right parts are swapped. This procedure is repeated 16 times where a different round key is incorporated into the round function F in each round.

The round function F first expands the 32-bit input, which is the right part of the internal state, to 48-bit value and then this expansion is XOR'ed with the current round key. The eight 6×4-bit S-Boxes are then applied. The S-Box outputs are permuted bitwise by a particular permutation to constitute the 32-bit output of the F function. The Feistel structure of DES is depicted in Figure 1.

B. Linear Cyptanalysis of DES

Matsui introduced several linear characteristics for certain number of rounds of DES. In this section we give one of them. The method to find an input/output mask with a biased equation is to extend the biased linear approximations of F to the full cipher. For example, if X, K are the data and the key inputs to the DES Feistel function F, then it is given in [12] that;

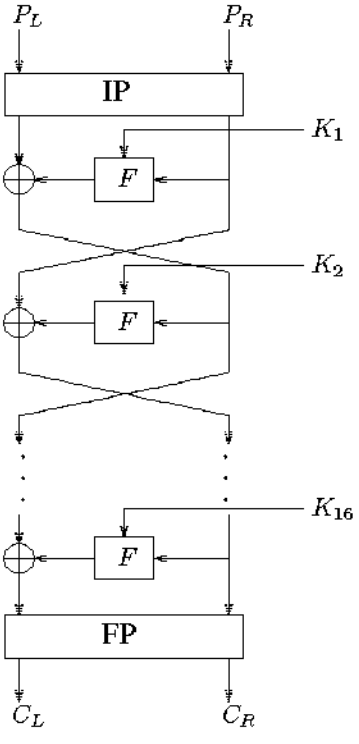


Fig. 1. Feistel structure of DES.

$$A : X[15] \oplus F(X,K)[7,18,24,29] = K[22]$$

with a probability of $\frac{1}{2} - \frac{20}{64}$ due to the fifth S-box of F since $N_{S_5}(16,15) = 12$. Another one-round characteristic can be given as

$$B : X[27,28,30,31] \oplus F(X,K)[15] = K[42,43,45,46]$$

with a probability $\frac{1}{2} - \frac{10}{64}$. Remark that this one-round approximations is valid for any round so we can construct a linear approximation for several rounds by combining one round approximations like the examples above. A linear approximation for 5-round DES which uses the approximations above is depicted in Figure 2.

Matsui introduced a lemma, piling-up lemma, to compute the bias of the new linear approximation obtained by combining one-round approximations. It is given as

Lemma 1: Let X_i be independent random variables for $1 \leq i \leq n$. Let $\Pr(X_i = 0) = \frac{1}{2} + \epsilon_i$. Then

$$\Pr(\oplus_{i=1}^{n} X_i = 0) = \frac{1}{2} + 2^{n-1} \prod_{i=1}^{n} \epsilon_i.$$

Using the piling-up lemma and the 1-round characteristics A and B, as in the 5-round characteristic depicted in Figure 2, we get;

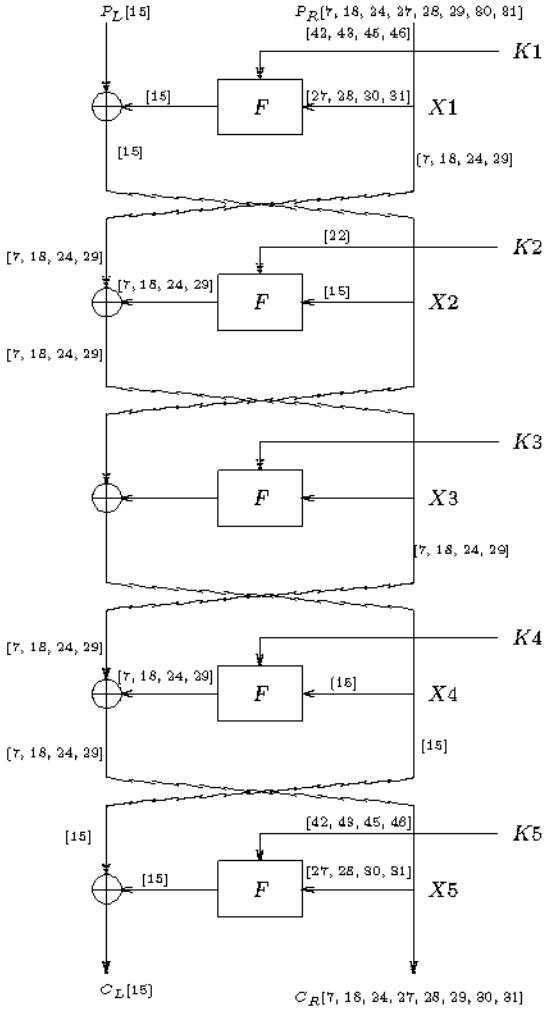


Fig. 2. A five round linear characteristic for DES using above approximations, in the $BA - AB$ form.

$$X_1[27,28,30,31] \oplus F(X_1,K_1)[15] = K_1[42,43,45,46], \epsilon_1$$
$$X_2[15] \oplus F(X_2,K_2)[7,18,24,29] = K_2[22], \epsilon_2$$
$$X_4[15] \oplus F(X_4,K_4)[7,18,24,29] = K_4[22], \epsilon_3$$
$$X_5[27,28,30,31] \oplus F(X_5,K_5)[15] = K_5[42,43,45,46], \epsilon_4$$

Here ϵ_i's are the biases of each equation and by A and B, $\epsilon_1 = \epsilon_4 = -\frac{10}{64}$, and $\epsilon_2 = \epsilon_3 = -\frac{20}{64}$. Using the fact that $X_1 = P_R$, $X_2 = F(X_1,K_1) \oplus P_L$ and for $i \geq 1, X_{i+2} = X_i \oplus F(X_{i+1},K_{i+1})$, we can eliminate the intermediate values at these equations and finally get

$$\begin{aligned} P_L[15] \oplus P_R[7,18,24,27,28,29,30,31] \oplus \\ C_L[15] \oplus C_R[7,18,24,27,28,29,30,31] = \\ K_1[42,43,45,46] \oplus K_2[15] \oplus \\ K_4[15] \oplus K_5[42,43,45,46] \end{aligned} \quad (2)$$

where Equation 2 has bias approximately equal to $2^{-5.71}$. Using this 5-round characteristic and 2^{12} plaintext-ciphertext pair, one can recover the right hand side of the Equation 2 with the success probability equal to almost one, using Algorithm 1.

One discussion has been raised about the assumption of Matsui's piling-up lemma. It is a question that the random variables in the one-round linear approximations may not be independent. Hence the actual bias may be quite different than the calculated bias by the piling-up lemma. For example, Selçuk noted for some Feistel networks that, some biases calculated by the piling-up lemma can be quite different than those derived by the experimental results [1].

The independence of the variables in the linear approximations has been studied well. However, the stability of the probabilities for one-round approximations after plunging in the cipher is not examined.

III. Linear Hull

The definition of approximate linear hull (ALH), or simply linear hull, was first introduced by Nyberg [9]. Linear hull appears in the case that there are multiple linear characteristics with the same data mask but different key masks. The opposite of this idea, i.e. benefiting from linear approximations with different data masks and the same key mask (multiple linear approximations) is explained and applied in [2], [3], [4] and [5]. The idea of multiple linear approximations is further improved by Hermelin, Cho, and Nyberg in [10] and [11], and their attack is called as Multidimensional Linear Cryptanalysis.

In [14], Murphy claimed that there is no linear hull effect in the linear cryptanalysis. But, Leander later proved that the linear hull does indeed effect the security of a cipher, and thus should always be taken into account [7]. In his work, Leander claims that calculating the average time complexity of a linear characteristic by using the average over all keys is not appropriate since this average is usually infinite (due to the case that there is at least one key with zero bias). He claims that one should take into account of the median of the complexities to prove the security against linear cryptanalysis [7].

Assume we analyze a block cipher in which there is a linear hull with two linear characteristics whose biases are dominating (i.e other characteristics have negligible biases). Since the input bits (plaintext bits) of these characteristics are the same, there must be a function (such as an S-box) F whose input masks for those characteristics are the same, whereas the output masks are different. Similarly, starting from the ciphertext and going backwards, necessarily there is a function G such that the input masks differ and output masks are the same. Consider a scenario in which there is only one such F and G. Also, assume that the linear approximations between these functions are independent. Calling this middle part U, we get the model in Figure 3.

For Figure 3, we can assume that the only key difference of the characteristics is caused by the part U. Depending on the actual key values which affects this difference, the overall bias of the model changes. The reason behind this effect is studied theoretically in Section IV and practically verified in Section V.

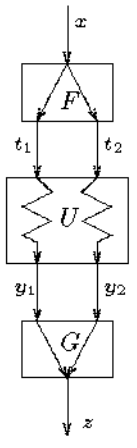


Fig. 3. An example scenario of a linear hull. x, t_1, t_2, y_1, y_2 and z represent 1-bit masked values.

IV. A Case Study

In this section, we define some random variables and the relations between these variables. Then we derive some statements in order to use for the construction of certain linear approximations which are affecting each other. The variables and probabilities are constructed in order to have a better understanding of the linear hull structure depicted in Figure 3.

Let x, y_1, y_2 and z be binary random variables. Then

Proposition 1: Assume $\Pr(x = y_1) = \frac{1}{2} + \epsilon$ and $\Pr(x = y_2) = \frac{1}{2} - \epsilon$ for some $\epsilon > 0$. Assume also that these events are independent. If $\Pr(z = y_1 | y_1 \neq y_2) = \frac{1}{2}$ which is independent of x and $\Pr(z = y_1 | y_1 = y_2)$ is also independent of x, then we have $\Pr(z = x) = \frac{1}{2}$.

Proof: The probability $\Pr(x = z)$ is given as

$$\begin{aligned}&\Pr(x = z | x = y_1 \text{ and } x = y_2) \Pr(x = y_1 \text{ and } x = y_2)\\ &+ \Pr(x = z | x = y_1 \text{ and } x \neq y_2) \Pr(x = y_1 \text{ and } x \neq y_2)\\ &+ \Pr(x = z | x \neq y_1 \text{ and } x = y_2) \Pr(x \neq y_1 \text{ and } x = y_2)\\ &+ \Pr(x = z | x \neq y_1 \text{ and } x \neq y_2) \Pr(x \neq y_1 \text{ and } x \neq y_2).\end{aligned}$$

On the other hand we assume that the events $x = y_1$ and $x = y_2$ are independent. Hence the probability $\Pr(x = z)$ will be equal to

$$\begin{aligned}&\Pr(x = z | x = y_1 \text{ and } x = y_2) \Pr(x = y_1) \Pr(x = y_2)\\ &+ \Pr(x = z | x = y_1 \text{ and } x \neq y_2) \Pr(x = y_1) \Pr(x \neq y_2)\\ &+ \Pr(x = z | x \neq y_1 \text{ and } x = y_2) \Pr(x \neq y_1) \Pr(x = y_2)\\ &+ \Pr(x = z | x \neq y_1 \text{ and } x \neq y_2) \Pr(x \neq y_1) \Pr(x \neq y_2).\end{aligned}$$

We have

$$\begin{aligned}&\Pr(x = z | x = y_1 \text{ and } x \neq y_2) \Pr(x = y_1) \Pr(x \neq y_2)\\ &+ \Pr(x = z | x \neq y_1 \text{ and } x = y_2) \Pr(x \neq y_1) \Pr(x = y_2).\\ &= (\frac{1}{2} + \epsilon)^2 (\Pr(x = z | x = y_1 \text{ and } x \neq y_2)\\ &+ (\frac{1}{2} - \epsilon)^2 (\Pr(x = z | x \neq y_1 \text{ and } x = y_2))\end{aligned}$$

and

$$\begin{aligned}&\Pr(x = z | x = y_1 \text{ and } x = y_2) \Pr(x = y_1) \Pr(x = y_2)\\ &+ \Pr(x = z | x \neq y_1 \text{ and } x \neq y_2) \Pr(x \neq y_1) \Pr(x \neq y_2)\\ &= (\frac{1}{4} - \epsilon^2)((\Pr(x = z | x = y_1 \text{ and } x = y_2) +\\ &+ Pr(x = z | x \neq y_1 \text{ and } x \neq y_2)).\end{aligned}$$

However

$$\Pr(x = z | x = y_1 \text{ and } x = y_2) =$$

$$\Pr(z = y_1 | x = y_1 = y_2) = \Pr(z = y_1 | y_1 = y_2)$$

since it is independent of x, and similarly

$$Pr(x = z | x \neq y_1 \text{ and } x \neq y_2) = \Pr(z \neq y_1 | y_1 = y_2).$$

Hence

$$\begin{aligned}&\Pr(x = z | x = y_1 \text{ and } x = y_2)\\ &\quad + Pr(x = z | x \neq y_1 \text{ and } x \neq y_2) = 1.\end{aligned}$$

We conclude that

$$\begin{aligned}&\Pr(x = z | x = y_1 \text{ and } x = y_2) \Pr(x = y_1) \Pr(x = y_2)\\ &+ \Pr(x = z | x \neq y_1 \text{ and } x \neq y_2) \Pr(x \neq y_1) \Pr(x \neq y_2)\\ &= (\frac{1}{4} - \epsilon^2). \qquad (3)\end{aligned}$$

On the other hand, it is given that $\Pr(z = y_1 | y_1 \neq y_2) = \frac{1}{2}$. So,

$$\Pr(x = z | x = y_1 \text{ and } x \neq y_2) = \frac{1}{2}$$

and

$$\Pr(x = z | x \neq y_1 \text{ and } x = y_2) = \frac{1}{2}.$$

This gives as

$$\begin{aligned}&(\frac{1}{2} + \epsilon)^2 (\Pr(x = z | x = y_1 \text{ and } x \neq y_2))\\ &+ (\frac{1}{2} - \epsilon)^2 (\Pr(x = z | x \neq y_1 \text{ and } x = y_2))\\ &= \frac{1}{2}((\frac{1}{2} + \epsilon)^2 + (\frac{1}{2} - \epsilon)^2)\\ &= \frac{1}{4} + \epsilon^2. \qquad (4)\end{aligned}$$

Summing the probabilities given in Equation 3 and Equation 4 we conclude that $\Pr(x = z) = \frac{1}{2}$. ■

A similar proposition can be proven as:

Proposition 2: Let $\Pr(x = y_1) = \Pr(x = y_2) = \frac{1}{2} + \epsilon$ for some $\epsilon > 0$. Assume that these events are independent. If $\Pr(z = y_1 | y_1 \neq y_2) = \frac{1}{2}$ and $\Pr(z = y_1 | y_1 = y_2) = \sigma$ which are independent of x, then we have $\Pr(z = x) = \frac{1}{2} + \epsilon(2\sigma - 1)$.

Proof: We give the sketch of the proof since it is similar to the proof of Proposition 1. We have $\Pr(z = x)$ given as

$$\begin{aligned}&\Pr(x = z | x = y_1 \text{ and } x = y_2) \Pr(x = y_1) \Pr(x = y_2)\\ &+ \Pr(x = z | x = y_1 \text{ and } x \neq y_2) \Pr(x = y_1) \Pr(x \neq y_2)\\ &+ \Pr(x = z | x \neq y_1 \text{ and } x = y_2) \Pr(x \neq y_1) \Pr(x = y_2)\\ &+ \Pr(x = z | x \neq y_1 \text{ and } x \neq y_2) \Pr(x \neq y_1) \Pr(x \neq y_2).\end{aligned}$$

On the other hand we have

$$\begin{aligned} & \Pr(x=z|x=y_1 \text{ and } x\neq y_2)\Pr(x=y_1)\Pr(x\neq y_2) \\ + \; & \Pr(x=z|x\neq y_1 \text{ and } x=y_2)\Pr(x\neq y_1)\Pr(x=y_2). \\ = \; & (\frac{1}{2}+\epsilon)^2(\Pr(x=z|x=y_1 \text{ and } x\neq y_2) \\ + \; & (\frac{1}{2}-\epsilon)^2(\Pr(x=z|x\neq y_1 \text{ and } x=y_2)) \\ = \; & (\frac{1}{2}+\epsilon)^2\frac{1}{2}+(\frac{1}{2}-\epsilon)^2\frac{1}{2}=\frac{1}{4}-\epsilon^2 \end{aligned}$$

and

$$\begin{aligned} & \Pr(x=z|x=y_1 \text{ and } x=y_2)\Pr(x=y_1)\Pr(x=y_2) \\ + \; & \Pr(x=z|x\neq y_1 \text{ and } x\neq y_2)\Pr(x\neq y_1)\Pr(x\neq y_2) \\ = \; & (\frac{1}{2}+\epsilon)^2\cdot\sigma+(\frac{1}{2}-\epsilon)^2\cdot(1-\sigma). \end{aligned}$$

Hence we conclude that

$$\begin{aligned} & \Pr(x=z)=(\frac{1}{2}+\epsilon)^2\cdot\sigma+(\frac{1}{2}-\epsilon)^2\cdot(1-\sigma) \\ + \; & \frac{1}{4}-\epsilon^2=\frac{1}{2}+\epsilon(2\sigma-1) \end{aligned}$$

■

Note that if the probabilities $\Pr(z=y_1|y_1\neq y_2)=\frac{1}{2}$ and $\Pr(z=y_1|y_1=y_2)=\sigma$ are swapped, that is, if $\Pr(z=y_1|y_1=y_2)=\frac{1}{2}$ and $\Pr(z=y_1|y_1\neq y_2)=\sigma$ then the results in Proposition 1 and Proposition 2 will also be swapped. That is, we have $\Pr(z=x)=\frac{1}{2}+\epsilon(2\sigma-1)$ in Proposition 1 and $\Pr(z=x)=\frac{1}{2}$ in Proposition 2. The proof is rather knotty. However, it is very similar to the proof of Proposition 1. So, we skip it.

We generalize the statements in Proposition 1 and Proposition 2 to add another pair of random variable, this time loosing the independence condition for the new variables.

Theorem 1: For given binary random variables x,t_1,t_2,y_1,y_2,z, let $\Pr(x=t_1 \text{ and } x\neq t_2)=\Pr(x\neq t_1 \text{ and } x=t_2)$. Assume $\Pr(t_1=y_1)=\frac{1}{2}+\epsilon$, $\Pr(t_2=y_2)=\frac{1}{2}-\epsilon$ for some $\epsilon>0$ and they are independent of each other and of x. Let $\Pr(z=y_1|y_1\neq y_2)=\frac{1}{2}$ which is independent of x and $\Pr(z=y_1|y_1=y_2)$ be also independent of x. Then we have $\Pr(z=x)=\frac{1}{2}$.

Proof: Let $Pr(x=t_1=t_2)=p_1$, $Pr(x=t_1\neq t_2)=p_2$, $Pr(x=t_2\neq t_1)=p_3$ and $Pr(x\neq t_1=t_2)=p_4$. Recall that we have $p_2=p_3$ by the assumption and $p_1+p_2+p_3+p_4=1$. Also, define $\Pr(z=y_1|y_1=y_2)=p$. Then $\Pr(z\neq y_1|y_1=y_2)=1-p$. With these parameters we write

$$\begin{aligned} & \Pr(z=x)= \\ & p_1(p(\frac{1}{4}-\epsilon^2)+\frac{1}{2}((\frac{1}{2}+\epsilon)^2+(\frac{1}{2}-\epsilon)^2)+(1-p)(\frac{1}{4}-\epsilon^2)) \\ & +p_2(p(\frac{1}{2}+\epsilon)^2+\frac{1}{2}(\frac{1}{4}-\epsilon^2+\frac{1}{4}-\epsilon^2)+(1-p)(\frac{1}{2}-\epsilon)^2) \\ & +p_3(p(\frac{1}{2}-\epsilon)^2+\frac{1}{2}(\frac{1}{4}-\epsilon^2+\frac{1}{4}-\epsilon^2)+(1-p)(\frac{1}{2}+\epsilon)^2) \\ & +p_4(p(\frac{1}{4}-\epsilon^2)+\frac{1}{2}((\frac{1}{2}+\epsilon)^2+(\frac{1}{2}-\epsilon)^2)+(1-p)(\frac{1}{4}-\epsilon^2)). \end{aligned}$$

Hence $\Pr(z=x)$ is given as

$$\begin{aligned} & p_1(\frac{1}{4}-\epsilon^2+\frac{1}{4}+\epsilon^2)+p_2(\frac{1}{2}+\epsilon(2p-1)) \\ + \; & p_3(\frac{1}{2}-\epsilon(2p-1))+p_4(\frac{1}{4}-\epsilon^2+\frac{1}{4}+\epsilon^2) \\ = \; & \frac{p_1+p_4}{2}+p_2(\frac{1}{2}+\epsilon(2p-1)+\frac{1}{2}-\epsilon(2p-1)) \end{aligned}$$

and this equals to $\frac{p_1+p_4}{2}+p_2$. However, $p_1+2p_2+p_4=p_1+p_2+p_3+p_4=1$. Hence, $\Pr(z=x)=\frac{1}{2}$. ■

Theorem 1 explains how the biases of two characteristics can be perished together. These two characteristics have biases in the opposite directions. The natural question is what the combined bias is when the characteristics have both positive or negative biases. We give the combined biases in the following statement.

Theorem 2: For given binary random variables x,t_1,t_2,y_1,y_2,z, let $\Pr(x=t_1 \text{ and } x=t_2)-\Pr(x\neq t_1 \text{ and } x\neq t_2)=\rho$. Assume $\Pr(t_1=y_1)=\Pr(t_2=y_2)=\frac{1}{2}+\epsilon$ and they are independent of each other and of x. Let $\Pr(z=y_1|y_1\neq y_2)=\frac{1}{2}$ and $\Pr(z=y_1|y_1=y_2)=\sigma$ which are independent of x. Then $\Pr(z=x)=\frac{1}{2}+\epsilon\rho(2\sigma-1)$.

Proof: Let $Pr(x=t_1=t_2)=p_1$, $Pr(x=t_1\neq t_2)=p_2$, $Pr(x=t_2\neq t_1)=p_3$ and $Pr(x\neq t_1=t_2)=p_4$. We have $p_1+p_2+p_3+p_4=1$ and it is given that $\Pr(z=y_1|y_1=y_2)=\sigma$. Then $\Pr(z\neq y_1|y_1=y_2)=1-\sigma$. Then

$$\begin{aligned} & \Pr(z=x)= \\ & p_1((\frac{1}{4}-\epsilon^2)+\sigma(\frac{1}{4}+\epsilon^2)+(1-\sigma)(\frac{1}{2}-\epsilon)^2) \\ & +p_2(\frac{1}{2}((\frac{1}{2}+\epsilon)^2+(\frac{1}{2}-\epsilon)^2)+\sigma(\frac{1}{4}+\epsilon^2) \\ & +(1-\sigma)(\frac{1}{4}-\epsilon^2)) \\ & +p_3(\frac{1}{2}((\frac{1}{2}+\epsilon)^2+(\frac{1}{2}-\epsilon)^2)+\sigma(\frac{1}{4}+\epsilon^2) \\ & +(1-\sigma)(\frac{1}{4}-\epsilon^2)) \\ & +p_4((\frac{1}{4}-\epsilon^2)+\sigma(\frac{1}{4}-\epsilon^2)+(1-\sigma)(\frac{1}{2}+\epsilon)^2) \end{aligned}$$

Clearing out the parameters, $\Pr(z=x)$ will be equal to

$$(p_2+p_3)/2+p_1(1/2+\epsilon(2\sigma-1))+p_4(1/2-\epsilon(2\sigma-1)).$$

Then we conclude that

$$\Pr(z=x)=\frac{1}{2}+\epsilon(2\sigma-1)(p_1-p_4)$$

since $p_1+p_2+p_3+p_4=1$. On the other hand $p_1-p_4=\rho$. Hence,

$$\Pr(z=x)=\frac{1}{2}+\epsilon\rho(2\sigma-1).$$

■

V. Experimental Results

In this section, we analyze a fictious cipher in which there are two linear characteristics with the same data (plaintext and ciphertext) mask but different key masks. This gives the so-called *linear hull* affect [9].

A. The analyzed cipher

The fictious cipher, depicted in Figure 4, has 32-bit block length. Plaintext is XORed with the whitening key at the beginning of the encryption. Then the round function is applied four times. The cipher is an SPN structure. The round function consists of 4 8×8 S-boxes and a bitwise permutation. We apply 6-bit S-boxes after the permutation to the bits which we do not use in the approximations to randomize the passive bits in the input masks. In Figure 4, $S8$ is an 8-bit and $S6_i$'s are 6-bit S-boxes. Bold lines (which are entering to any of the $S6_i$'s) are 6-bit values whereas other data lines are 1 bit variables. Each XORed key part has a length of 8-bits (K_i, where $i = 1 \ldots 20$).

The input of the round function is 32-bit data and 32-bit round key. The S-box layer of 8-bit S-boxes, which is also used at the end of the encryption, is applied to the data in the beginning of the round function. Then 7-bit left cyclic rotate operation is applied. After that, a combination of key XORing, 6-bit S-box operation and 6-bit diffusions are applied in the following manner:

Let the data after the 8-bit S-box and 7-bit cyclic rotate be named as $D_1||D_2||D_3||D_4$ where D_i's are 8 bit parts from left to right. These names will also serve as the state at that block in the forthcoming operations. Similarly let $K_{i+1}||K_{i+2}||K_{i+3}||K_{i+4}$ be the round key. First, $K_{i+2}||K_{i+3}$ is XORed to $D_2||D_3$. Then $S6_2$ and $S6_3$ are applied to the rightmost 6-bit parts D_2 and D_3 respectively. The output of the $S6_2$ is XORed to the rightmost 6-bit of D_1, then the resulting value is passed to the $S6_1$. The output of $S6_1$ is XORed to the rightmost 6-bit of the current state at D_2. After that, K_{i+1} is XORed to the state at D_1. Similar operations applied between D_3 and D_4.

The analyzed cipher is constructed in a way that there is a linear hull with two dominating linear characteristics. To provide this property, first we draw the paths of these two characteristics, then we construct an 8 bit S-box –namely $S8$– in a way that this S-box have the desired linear approximations with high biases. Bits not entering into these approximations distributed randomly, causing other linear approximations to have smaller biases.

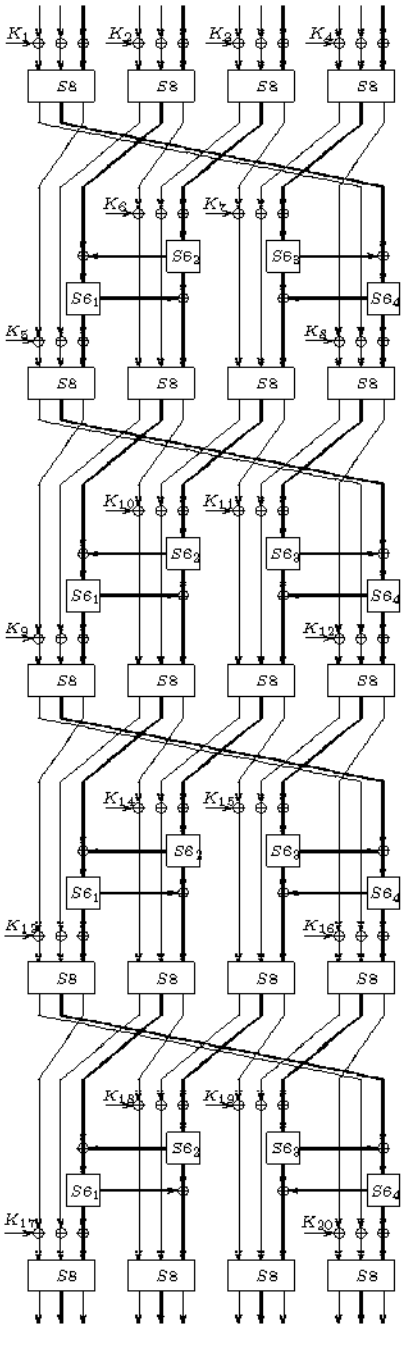


Fig. 4. The fictious block cipher's overall structure.

B. Construction of the linear hull

Let the input bits of the $S8$ be written as $x_1||x_2 \ldots ||x_8$, and output bits as $y_1||y_2 \ldots ||y_8$. Then we have:

$$\Pr(x_1 = y_1) = \Pr(x_1 = y_8) = \frac{3}{4},$$

$$\Pr(x_2 = y_1) = \Pr(x_2 = y_8) = \frac{3}{4},$$

$$\Pr(x_1 = y_1 \text{ and } x_1 \neq y_8) = \frac{1}{4},$$

$$\Pr(x_1 = y_8 \text{ and } x_1 \neq y_1) = \frac{1}{4},$$

$$\Pr(y_8 = x_1 | x_1 \neq x_2) = \frac{1}{2},$$

Using the equations above, we construct a pair of linear characteristics. For any data block, X, $X[j]$ denotes the leftmost j–th bit of X, where indices begin at 1. P and C denote the plaintext and ciphertext respectively. The round keys K_j's are assumed to be independent, i.e., the key length of the cipher is 160-bit.

$$P[1] \oplus C[8] = K_1[1] \oplus K_5[1] \oplus K_9[1] \oplus K_{13}[1] \oplus K_{17}[1] \quad (5)$$

$$P[1] \oplus C[8] = K_1[1] \oplus K_8[2] \oplus K_{11}[2] \oplus K_{14}[2] \oplus K_{17}[2] \quad (6)$$

The pair of the linear characteristics given in Equation 5 and Equation 6 is constructed in order to form an example for the model in Figure 3. F can be seen as the leftmost S-box of the first round whereas the leftmost S-box of the final S-box layer plays the role of G. U, on the other hand, is the middle 3 rounds which are the independent part of our characteristics. Call the right hand side of (5) and (6)–i.e. the key bits– K_L and K_R respectively.

If we call the ouput of the ith cyclic rotate operation by X_i $(i = 1, \ldots 4)$, the variables used in *Theorem* 1 and *Theorem* 2 can be assigned to our case in the following manner:

$$x = P[1], t_1 = X_1[1], t_2 = X_1[26],$$

$$y_1 = X_4[1], y_2 = X_4[2], \text{and } z = C[8].$$

C. Mounting linear attack

Using the classical assumptions of linear cryptanalysis and the piling-up lemma, we can calculate the overall biases of (5) and (6) as follows;

$$\epsilon_1 = \epsilon_2 = 2^4(2^{-2})^5 = 2^{-6}$$

where ϵ_1 and ϵ_2 are the biases of (5) and (6) respectively. Here, each characteristics have 5 active S-boxes and all active S-boxes have a bias of 2^{-2}. So both characteristics have probability $\frac{1}{2} + 2^{-6}$ by the piling-up lemma.

We implement Algorithm 1 of [12] and see that the plaintext-ciphertext mask has the bias different then the bias, 2^{-6}, computed by the piling-up lemma for any key. The actual bias of $P[1] \oplus C[8]$ (the left hand side of the linear characteristics) is around 2^{-5} for some keys. We classified these keys. On the other hand, the bias perishes for some other keys. Indeed, when both biases in both characteristics are positive, then the overall bias is increased to 2^{-5}. Otherwise, it perishes. The results of the experiments are depicted in Table I. The success rate of Algorithm 1 is 50% whereas it is expected to be almost one since we use much more than 2^{12} data.

Table I shows that if the linear combination of the key bits of two characteristics are equal then the bias is increased by a factor of two. If the linear combination of the key bits are not equal, then the bias becomes 0.

The case in which the linear combinations of the key bits are not equal is explained through Theorem 1. The difference in the linear combinations of the key bits causes two approximations having biases of opposite signs, i.e., one of them has probability $\frac{1}{2} + \epsilon$, and the other one has $\frac{1}{2} - \epsilon$, where $\epsilon = 2^{-4}$. Other assumptions of the theorem are also satisfied by the S-box. So the overall bias is expected to be zero by Theorem 1. Indeed, the experimental results have been verified the result. We have observed a bias of less then 2^{-10} when 2^{20} data were used and a bias of less then 2^{-12} when 2^{24} data were used as in Table I.

TABLE I
EXPERIMENTAL RESULTS ON THE FICTIOUS CIPHER. BIASES ARE COMPUTED ACCORDING TO EQUATION (5), I.E FOR THE EVENT $P[1] \oplus C[8] = K_L$

		Biases for (K_L,K_R) pair (see Sec. V-B)			
Exp #	**Data**	**(0,0)**	**(0,1)**	**(1,0)**	**(1,1)**
1	2^{20}	$2^{-5.0086}$	$2^{-12.3276}$	$-2^{-10.2154}$	$2^{-4.9830}$
2	2^{20}	$2^{-5.0192}$	$2^{-10.3598}$	$2^{-10.3927}$	$2^{-4.9866}$
3	2^{20}	$2^{-5.0023}$	$2^{-11.8605}$	$2^{-11.2252}$	$2^{-5.0199}$
4	2^{20}	$2^{-5.0195}$	$-2^{-10.8102}$	$2^{-10.7426}$	$2^{-5.0207}$
5	2^{24}	$2^{-5.0109}$	$2^{-14.5344}$	$-2^{-13.8251}$	$2^{-4.9955}$
6	2^{24}	$2^{-5.0093}$	$2^{-11.8148}$	$-2^{-13.0028}$	$2^{-4.9993}$
7	2^{24}	$2^{-5.0187}$	$2^{-12.4594}$	$-2^{-15.3634}$	$2^{-4.9877}$
8	2^{24}	$2^{-5.0034}$	$2^{-12.3449}$	$2^{-12.3276}$	$2^{-5.0046}$

When two linear combinations of the key bits are both zero or both one simultaneously, that is, when the biases of the both approximations are positive or negative then we observe an increase of factor two in each bias as given in Theorem 2. We saw that the bias of one approximation is doubled as the theorem states. That is, the overall bias is calculated by summing the biases. In our example, $\rho = \frac{1}{2}, \sigma = 1$ and $\epsilon = 2^{-4}$. So, the overall bias is calculated as 2^{-5} as we have observed in the experiments.

VI. Conclusion

In this paper, we examined Matsui's linear cryptanalysis and the bias calculation for the extended linear masks through the piling-up lemma. By introducing a case study, we have proved that the lemma does not work all the time . We also have shown the existence of linear hull in the case study. We have derived new statements to calculate the actual biases for our case study and verified our results by conducting some experiments. To do that, we have designed a toy cipher and mount the linear attack on the cipher, yielding two linear approximations whose random variables comply with the assumptions given in the statements derived for the case study.

Acknowledgment

We would like to thank Rıdvan Bakkal and Mehmet Sabır Kiraz for their helpful comments.

References

[1] A.A. Selçuk. *On Bias Estimation in Linear Cryptanalysis.* In *Proc. Indocrypt 2000*, LNCS 1977, pp. 52–66, Springer, 2000.

[2] A. Biryukov, C. D. Cannière, and M. Quisquarter. *On Multiple Linear Approximations.* In M. Franklin (Ed.): *Crypto 2004*, LNCS 3152, pp. 1–22, Springer, 2004.

[3] B. Collard, C. D. Cannière, and M. Quisquater. *Experiments on the Multiple Linear Cryptanalysis of Reduced Round Serpent.* In K. Nyberg (Ed.): *FSE 2008*, LNCS 5086, pp. 382–397, Springer, 2008.
[4] B. S. Kaliski Jr., and M. J. B. Robshaw. *Linear Cryptanalysis Using Multiple Approximations.* In Y. G. Desmedt (Ed.): *Crypto'94*, LNCS 839, pp. 26–39, Springer-Verlag Berlin Heidelberg, 1994.
[5] B. S. Kaliski Jr., and M. J. B. Robshaw. *Linear Cryptanalysis Using Multiple Approximations and FEAL.* In B. Preneel (Ed.): *FSE'94*, LNCS 1008, pp. 249–264, Springer, 1995.
[6] F. Chabaud, S. Vaudenay. *Links Between Differential and Linear Cryptanalysis.* In A. D. Santis (Ed.): *Eurocrypt'94*, LNCS 950, pp. 356–365, Springer, 1995.
[7] G. Leander. *On Linear Hulls,Statistical Saturation Attacks, PRESENT and Cryptanalysis of PUFFIN.* In K. G. Peterson (Ed.): *Eurocrypt 2011*, LNCS 6632, pp. 303–322, Springer, 2011.
[8] J. Nakahara Jr., P. Sepehrdad, B. Zhang, and M. Wang. *Linear (Hull) and Algebraic Cryptanalysis of the Block Cipher PRESENT.* In J. A. Garay, A. Miyaji, and A. Otsuka (Eds.): CANS 2009, LNCS 5888, pp. 58–75, Springer-Verlag Berlin Heidelberg, 2009.
[9] K. Nyberg. *Linear Approximation of Block Ciphers.* In A. D. Santis (Ed.): *Eurocrypt'94*, LNCS 950, pp. 439–444, Springer, 1995.
[10] M. Hermelin, J. Y. Cho, and K. Nyberg. *Multidimensional Extension of Matsui's Algorithm 2.* In O. Dunkelman (Ed.): *FSE 2009*, LNCS 5665, pp. 209–227, Springer, 2009.
[11] M. Hermelin, J. Y. Cho, and K. Nyberg. *Multidimensional Linear Cryptanalysis of Reduced Round Serpent.* In Y. Mu, W. Susilo, and J. Seberry (Eds.): *ACISP 2008*, LNCS 5107, pp. 203-215, Springer-Verlag Berlin Heidelberg, 2008.
[12] M. Matsui. *Linear Cryptanalysis Method of DES Cipher.* In *Proc. EUROCRYPT'93*, LNCS 765, pp. 386–397, Springer, 1994.
[13] M. Matsui. *The First Experimental Cryptanalysis of the Data Encryption Standard.* In *Proc. CRPTO'94*, LNCS 839, pp. 1–11, Springer, 1994.
[14] S. Murphy. *The Effectiveness of the Linear Hull Effect.* Technical Report, RHULMA-2009-19 (2009).
[15] S. Murphy. *The Independence of Linear Approximations in Symmetric Cryptanalysis.* In *IEEE Transactions on Information Theory*,Vol. 22, N0. 12, December 2006.
[16] W. Meier and O. Staffelbach. *Nonlinearity Criteria for Cryptographic Functions.* In *Proc. EUROCRYPT'89*, LNCS 434, pp. 548–562, Springer, 1989.
[17] V. Rijmen, *Cryptanalysis and Design of Iterated Block Ciphers*, Doctoral Dissertation, K.U. Leuven, 1997.

A Scalable Platform for Cryptanalysis of Computationally Intensive Algorithms

Mustafa Hakan Solmaz, Hasan Erdoğan, and Rıza Aykaç

Abstract— **A cryptographic co-processor design methodology is introduced in this study. The co-processor is connected to a microprocessor through a bus interface protocol, namely Processor Local Bus (PLB) protocol of IBM. Since the co-processor is designed to be a modular block, it can be instantiated in any number as long as FPGA fabric is empty. The methodology is demonstrated for exhaustive key search of DES algorithm. A Microprocessor system is designed and realized on ML605, a Xilinx Virtex-6 FPGA Evaluation Board, which captures initial performance of 8 billion key searches per second.**

Index Terms— **Cryptanalysis, DES, Brute force attack, Cryptographic peripheral design.**

I. Introduction

Cryptography is the study of secure communication methods in the presence of adversaries. Classical cryptography existed in the ancient ages in the form of substitution or transposition ciphers. In the computer era cryptography turned into a discipline which heavily uses advanced mathematical methods and computer science practices. While cryptography is the study of introducing secure communication methods, there is a parallel discipline, cryptanalysis, which is trying to extract secret information from encrypted messages. Although there seems to be a negative perception about seeking other people's secret information, cryptanalysis is as important as cryptography. In the absence of cryptanalysis we cannot know how secure our cryptosystem is.

Classical cryptanalysis used basic tools for breaking classical cryptosystems. Frequency analysis can be given as an example to these methods. For example "e" is known to be the most frequent letter in English, while "the" is the most frequent word which ends with "e". In a classical cryptosystem which fails to hide these statistics, frequency analysis can be used to break the cryptosystem provided that the encrypted text is long enough. As with cryptography, modern cryptanalysis also changed face with the advent of high speed computers and electronic computation systems.

Among the methods of modern cryptanalysis we will focus on brute force attack and their applications. A brute force attack or exhaustive key search can be described as follows: Suppose that an attacker has one or more plain text - cipher text pairs and the cryptosystem details except the encryption key. Can he/she find the secret key so that he/she can decrypt other cipher texts for which the plain text is not known? The answer to this question is theoretically yes for all symmetric ciphers. A pseudo flowchart can be described as below:

Let the key space be $K = \{k_1, k_2, k_N\}$ plain text p cipher text c and $d_{k_i}(c)$ be the decryption function with key k_i.

For $i = 1,2,.,N$ loop
  Compute $y = d_{ki}(c)$
  If $y = p$ then return k_i.
End loop

For a key length of N it can be shown that the correct key is found in N/2 iterations on the average [11]. It is also possible to run a brute force attack by using encryption function.

Among the famous applications of brute force attacks are the attempts to break DES algorithm. The first special computer was proposed by Diffie and Helman right after the standardization of DES [4]. Later a distributed network of 100.000 PC's was able to reveal key after 22 hours. Electronic Frontiers Foundation built a machine which also succeeded in finding the key. Most recently a special hardware named as Copacobana was designed by SciEngines Corporation. More than one hundred FPGAs are used in Copacobana to execute exhaustive search algorithms like the one defined above [5], [6].

In this paper we will go through the steps of implementing an exhaustive key search of a crypto algorithm on a commercially available off the shelf (COTS) FPGA board. DES algorithm is chosen since it is the most frequently studied algorithm in literature and there are performance measures to compare against. As FPGA platform we chose Virtex-6 ML605 Evaluation Board, a recent board from Xilinx. Although there is a Virtex-6 family of FPGA on this board the design can easily be ported to any other Xilinx FPGA. It can also be ported to other vendors' FPGAs with some more effort.

The outline of the manuscript is as follows: In the next section we give a brief introduction about embedded

Manuscript received March 11, 2012.
M. H. Solmaz, H. Erdoğan and R. Aykaç are with Information Security Dept, Aselsan Inc.,P.O.Box 1 ,06172 Yenimahalle, ANKARA / TURKEY (e-mail: hsolmaz,herdogan,raykac@aselsan.com.tr).

processors and custom peripheral concepts in an FPGA. In Section 3 DES algorithm implementation is introduced. Section 4 covers the details of custom peripheral for brute force attack designed for exhaustive key search and its interface to an embedded processor. Hardware and software co-design practices are also presented in this section. Section 5 will give performance results and comparisons to other platforms. Section 6 discusses design practices followed during the study. Section 7 closes with conclusion.

II. EMBEDDED PROCESSORS AND CUSTOM PERIPHERALS

A. *Embedded Processors*

Embedded system design and FPGA design were two different branches in the last decade. With the advances of process technologies FPGAs with thousands of configurable blocks became available and embedded system design with FPGAs has emerged as a new branch. Today FPGA vendors are providing soft or hard core processors in their chips. They also provide tool chains for hardware and software development for hardware and software platforms.

The name of the soft-core processor for Xilinx platforms is Microblaze, where as the hard core which is present in certain families is called PowerPC. Microblaze as an example of soft processor is built by combining blocks of Xilinx slices. The advantage of this approach is that you can generate a microprocessor exactly as you need. You do not have to accommodate unused CPU parts.

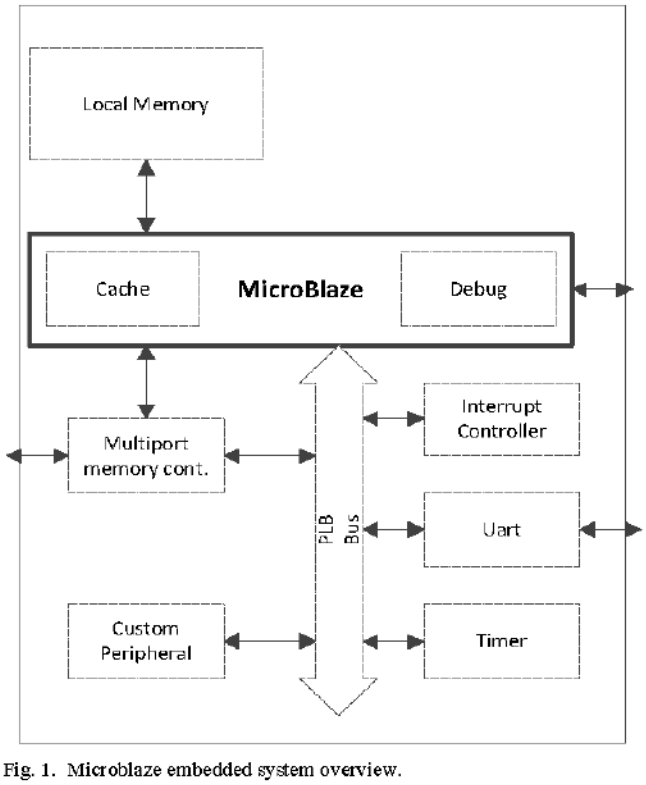


Fig. 1. Microblaze embedded system overview.

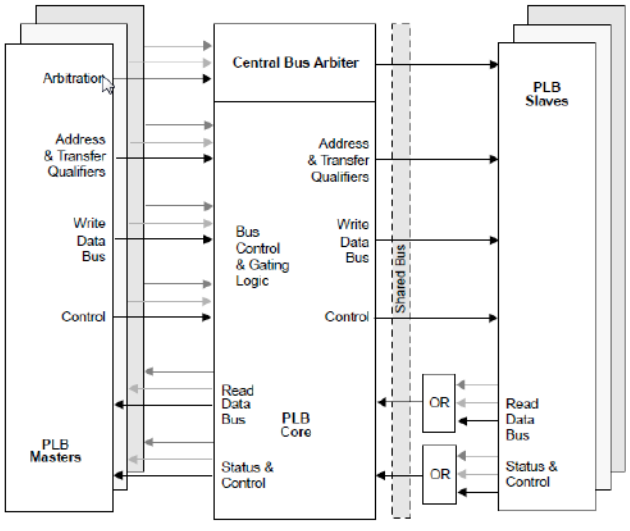


Fig. 2. PLB Overview [1].

Microblaze is a 32-bit Harvard architecture RISC processor. As being Harvard architecture it has a separate program and data bus running concurrently to execute programs or access memory or peripherals. A template for Microblaze system is seen in Fig. 1. Almost every part of this processor system is optional, only the section which contains Microblaze core is mandatory.

In an embedded FPGA design we must partition the design as hardware and software. Time-critic, resource hungry part of the design must be in FPGA fabric. Digital signal processing tasks or cryptographic tasks fall into this category. Interfacing these regions with processor is done through bus protocols, which we will introduce next.

B. *Processor Local Bus*

Processor Local Bus (PLB) is a standard which is introduced by IBM to interface peripherals directly with processor core. As shown in Fig. 1, PLB is the two sided big arrow to which all the peripherals are connected. There are master(s) and slave(s) connected to a PLB bus. The arbitration between masters and slaves is performed on central bus arbitration unit [1],[2] as shown in Fig. 2.

In our system configuration, the processor and custom cryptographic peripheral is connected via PLB. Once configured through PLB interface, our custom peripheral is intended to work at higher speeds.

III. DATA ENCRYPTION STANDARD (DES)

The Data Encryption Standard was selected by NBS (later named as NIST) as official Federal Information Processing Standard (FIPS) in 1976 [8]. Since its key space is too small and subject to several attacks, it is replaced by triple DES, later with AES. An important feature of DES is that it is so widely investigated in cryptology community that it became a tutorial tool for understanding block ciphers and their cryptanalysis.

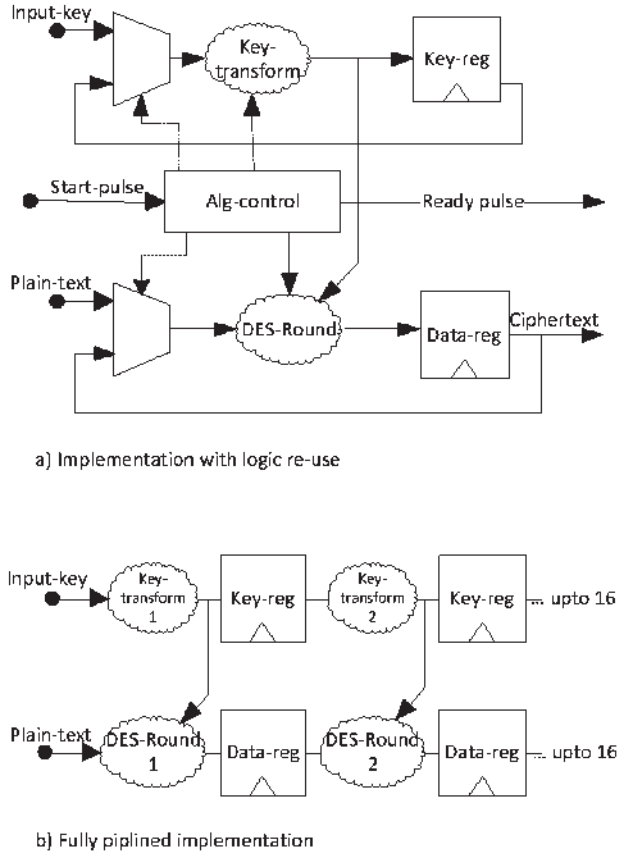


Fig. 3. Logic re-use vs. fully pipelined implementation of DES core.

Leaving the details to [3], [7], and [8], we can say that it contains 16 rounds in each of which a Feistel Network is used. S-boxes and permutations are used for achieving confusion and diffusion properties respectively.

In a straightforward implementation of DES in Virtex-6 FPGA, we obtained an area allocation of 95 slices and synthesis frequency of 350MHz. (Fig.3-a). In this implementation there is a key transform block, a Feistel Network block and a simple control logic which arranges what to do in each cycle. Once an input is given to this architecture it gives output after 16 cycles. Only after 16 cycles a new input can be fed to the module.

Although for practical communication purposes this implementation is fine, for brute force attack a fully pipelined implementation is much better in terms of throughput/area ratio (Fig3-b). Unlike the previous implementation there is not a control block in this implementation. Every key-transform and DES round has its own logic which are separated with register blocks. One can feed new key, plain-text pair into this architecture at every cycle. This architecture yields an output at every clock period after 16 clock cycles when the pipeline is full. We obtained 16 times larger throughput in expense of 10 times FPGA area. This saving is due to control logic absence in fully pipelined architecture.

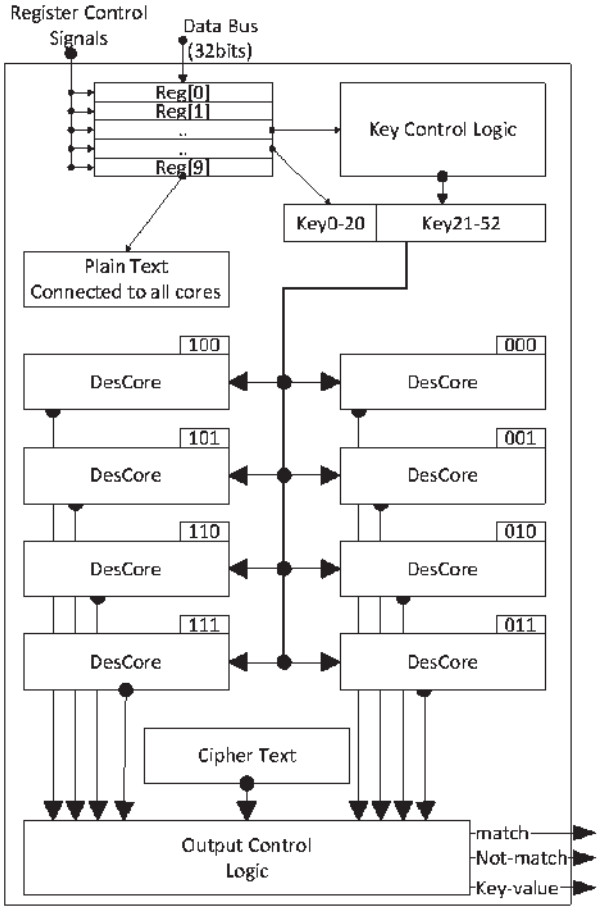


Fig. 4. PLB peripheral designed for brute force attacking to DES algorithm.

IV. Brute Force Attack Peripheral

An exhaustive key search peripheral is designed to include 8 distinct DES cores all of which are designed to run fully pipelined. These cores are managed by key control logic and output control logic blocks as shown in Fig. 4.

Key control logic is responsible to give different key values as an input to the cores. This is achieved by the sharing of the least significant 3 bits of the key separately between each core. Key control logic decides the next 32 bits of the key which starts from zero and distributes the same bits to each core. Page offset is incremented at every cycle until it reaches to 0xFFFFFF value. The key length for DES is 56 bits and the remaining 21 bits, is determined by the processor which controls the brute force attack peripherals connected to it via Processor Local Bus. Processor manages the peripherals to run in the span of all key space formed by mentioned 21 bits.

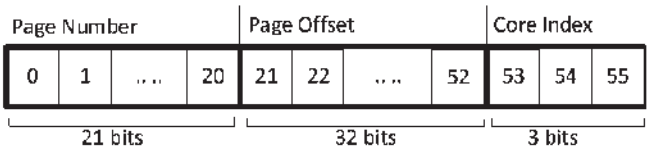


Fig. 5. DES brute force attack key space division.

The most significant 21 bits are called the page number of the keys. The latter 32 bits are called the page offset of the keys. The least significant 3 bits are constant part of the keys, each of which is connected to a DES core (Fig. 5).

The processor or the software side of the system decides the Page number in $[0\ 2^{21}-1]$ range which approximately corresponds to 2 million pages and each brute force attack peripheral spans 2^{35} keys which approximately corresponds to 32 billion.

Output control logic manages the output evaluations of the DES cores. This logic compares the reference cipher text given as an input to the peripheral with the outputs of each core in that peripheral. A core output is the computed cipher text of the plain text with the key determined by the key control logic. This plain text is also given as an input to the peripheral by the processor. Output control logic does at most 2^{35} comparisons for each run with the page number of the key given by the peripheral. If any of the DES cores finds a match between the computed cipher text and reference cipher text, the output control logic returns the key value and a *'match-found'* signal to processor. If none of the cores finds a match, a *'match-not found'* signal is generated. The processor runs the brute force attack peripherals until a match is found. In case of a *'match-found'*, the corresponding key value is read from the peripheral.

In Fig. 6 a "lucky" execution of the brute force attack peripheral core for plain text X"0123456789ABCDEF" and cipher text X"731C4E97EFA7462B" is seen. We know that the correct key for this pair is X"12680000000080". (This is the checksum stripped 56-bit key). For this simulation, brute force attack peripheral is executed with page number X"12680". As will be mentioned later, there are two clocks in the waveform. The slow clock is the interface clock with which the Microblaze processor runs, while the fast clock is for DES cores. Only a pulse-transfer which is seen in the simulation plot is made between clock domains. Once the peripheral starts, the key controller block generates the full key for each pipelined DES core at each cycle. After 16 cycles the comparator module becomes active and outputs from each core is compared against the cipher text. Once X"0000000000000000" is obtained as comparison result the corresponding key is returned as the output of the core. It is seen that for this particular case the correct key, X"12680000000080", is found 16 cycles later than the comparator's activation. Since we try 8 keys per cycle, 0x80/8=16 is the number of trials as expected.

V. Implementation And Performance Results

A. ML605 Development Platform

ML605 is an embedded development kit which has an FPGA from Virtex-6 family, XC6VLX240T-1FFG1156, on it. It has several peripherals including DDR3 memory, tri-speed Ethernet interface, SFP connection, USB to UART bridge, a dot matrix led, leds, dip-switches and industry standard FPGA Mezzazine Connector. Among the above we use only USB to

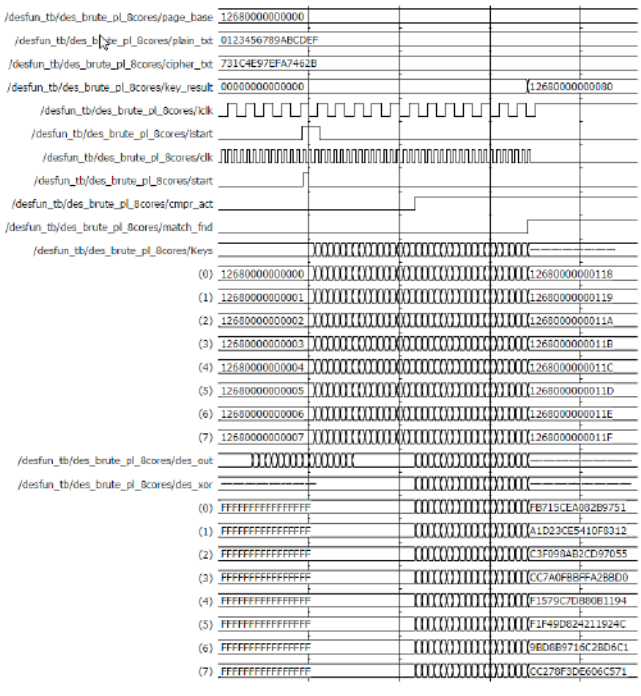


Fig. 6. Simulation result for a short search.

UART bridge and a few leds as peripheral [9]. Our main interest was about the abundant reconfigurable logic which is available on the FPGA.

With Microblaze soft processor, there is a great flexibility to select the combination of peripheral, memory and interface features for our problem solution on a single FPGA.

The ISE Design Suite provided by Xilinx includes the Embedded Development Kit (EDK) and the Software Development Kit (SDK). The EDK includes the tool suite for designing embedded applications with Xilinx platform FPGAs and Microblaze soft processor cores [10]. We developed our system design and wrote some of the HDL codes using EDK. We implemented application software for Microblaze to control brute force attack peripherals with C programming language using SDK.

B. Microprocessor System Overview

A simplified version of the hardware system is seen in Fig. 7. In the center, there is a Microblaze processor as the main control unit. The software of this processor can either run from the internal block memory or from external DDR3 memory which is available on the board. There is a debug interface over which the software can be interrupted, monitored during development phase. All peripherals are connected to Microblaze system through PLB interface. An UART and general purpose IO peripheral is picked from standard library of Xilinx embedded system platform. The rest of the reconfigurable logic area is filled up with custom cryptographic core. In our case we were able to fit 5 DES brute force peripherals into our FPGA with an area utilization of %85.

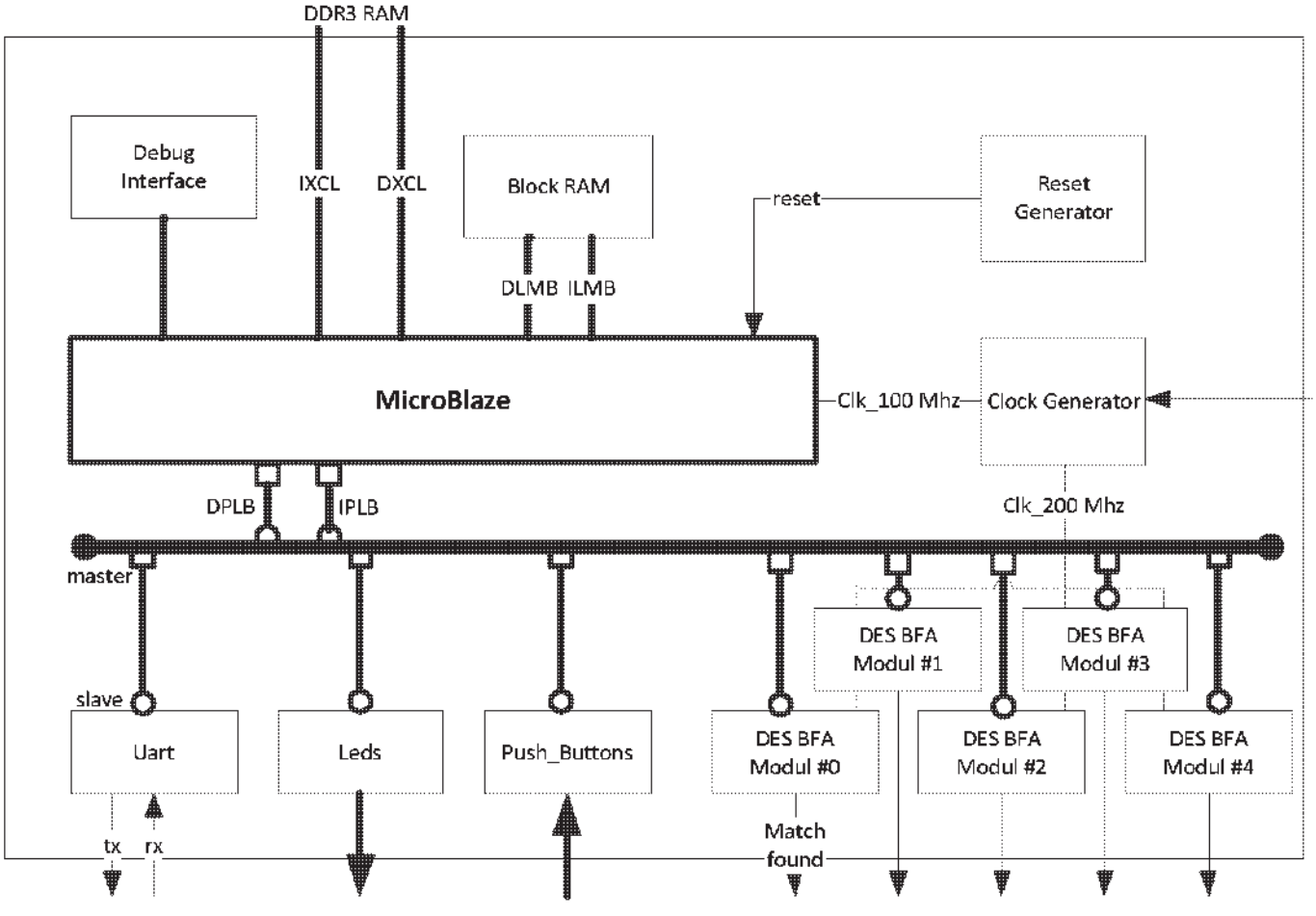


Fig. 7. ML605 Microprocessor system overview.

Synthesis frequency of an FPGA design is a critical parameter in its performance. A high synthesis frequency is desired for high performance. However it is not always possible to obtain a unique high frequency for the whole design. In our case Microblaze seems to be the bottleneck for synthesis frequency which is around 100 MHz. To overcome this limitation we introduced a higher frequency, 200 MHz, which will be the operating frequency of our cryptographic peripherals. DES brute force attack peripherals are designed such that they communicate with the Microblaze system with a slow rate while they execute internally with a faster clock speed.

C. *Performance Results*

We generated the programming file of hardware platform on Virtex-6 FPGA which includes a Microblaze soft processor and 5 brute force attack peripherals. Each peripheral consists of 8 pipelined DES cores running at 200 MHz frequency.

Each brute force attack peripheral finishes the search of the whole page in 21.5 seconds that is 8 cores x 2^{32} keys per 21.5 seconds which yields approximately 1.6 billion keys per second. A system with 5 brute force attack peripherals means that 5 page numbers of the key values are searched simultaneously. This increases the performance of our system to 8 billion keys per seconds. Thus, the correct key of a given open-text, cipher-text pair can be found in 52 days on the average.

To provide a comparison with the Copacobana system, it uses 120 Spartan-3 family FPGAs on 20 different boards with 136MHz working frequency [5]. ML605 has a single Virtex-6 family FPGA with 200MHz working frequency on DES brute force attack cores. Copacobana has a key search performance of approximately 65 billion keys per second [5], whereas our system has 8 billion.

From cost point of view, we can say that ML605 has a comparable performance with respect to Copacobana. In [11] it is calculated that an average search time of less than 9 days is achievable with Copacobana system for € 8980. With our design, parallel execution of 6 boards yields an average duration of 8.6 days with a cost of 6x€1371 = €8226.

Our main interest in this study was to demonstrate a useful methodology for implementing a computationally heavy cryptographic task on an embedded FPGA platform. With this methodology one can bridle huge amounts of configurable logic in a systematic way. The performance can be increased

by focusing on application specific needs after then.

VI. Design Practices

Change of scale in a problem may invalidate a solution which is fine for the previous scale. For example, in a small scale you may design a module, simulate it and observe every behavior of it in simulation and then burn your design into FPGA. For an exhaustive search hardware design, it is no way possible to simulate the whole behavior. It is even not possible to make simulation in most of the Embedded FPGA platforms.

Our approach in this scale is to verify smaller modules in hardware independently. After verifying all small modules, we combined them to get intermediate modules. If a verification problem occurs at a step we only focus on the last integration.

To give an example of above approach, we first designed a single DES core and verified it on hardware. Hardware verification can be done by encapsulating the core with a fixed input and comparison circuit at the output. The module is triggered with a push button and the comparison result is connected to a led which is common to all FPGA boards. If the led blinks after we press the push button on board, we make sure that the module is working as expected (Fig 7). This approach also gives the opportunity to see the speed and area performance of a module independently.

On the other extend we first generate an empty peripheral and see that it can communicate with the processor. After verifying the empty peripheral, we populate it with a verified crypto core.

This approach is also good for team work. For example while one team member is working on software development with an early peripheral, another team member can work on increasing the performance of the peripheral.

VII. Conclusion

In this paper we proposed a contemporary solution for cryptanalysis of computationally intensive algorithms on FPGA platforms. The solution consists of two parts. One is designing a custom peripheral which contains the algorithm; the other part is connecting many instances of this peripheral to a microprocessor system and control the execution of the peripherals through light software. We demonstrated the use of methodology through a well-known application, brute force attacking to DES algorithm. It appeared that we can obtain performance results compared to state-of-the art designs with this methodology.

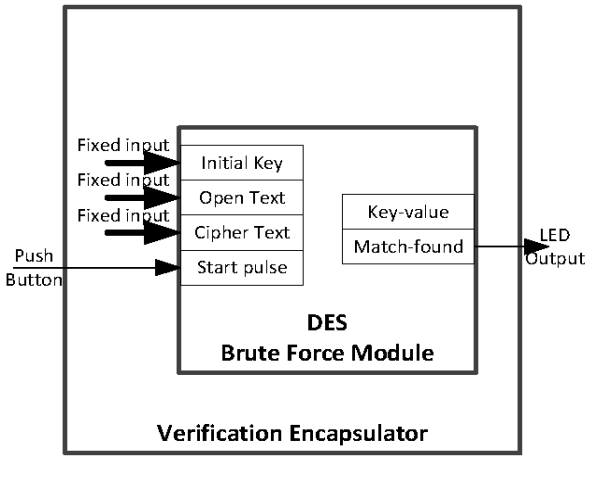


Fig. 7. Independent verification of a design module.

Acknowledgment

We would like to thank Ali Yazıcı and Bikem Temürcü for their support and motivation in this study.

References

[1] IBM Corp., *CoreConnect Bus Architecture Product Brief*, GK10-3116-00, September 1, 1999.
[2] IBM Corp., *128-bit Processor Local Bus Architecture Specifications*, Version 4.6, SA-14-2538-04, July, 2004.
[3] NIST Special Publication 800-67, *Recommendation for the Triple Data Encryption Algorithm (TDEA) Block Cipher*, May 2008.
[4] W. Diffie and M. E. Hellman, "Exhaustive cryptanalysis of the NBS Data Encryption Standard". *COMPUTER*, 10(6):74–84, June 1977.
[5] Tim Güneysu, Timo Kasper, Martin Novotny, Christof Paar, and Andy Rupp. "Cryptanalysis with COPACOBANA". *IEEE Transactions on Computers*, 57(11):1498–1513, 2008.
[6] COPACOBANA—A Cost-Optimized Parallel Code Breaker. http://www.copacobana.org/
[7] Christoph Paar and Jan Pelzl. *Understanding Cryptography, A Textbook for Students and Practitioners*, Springer, 2010.
[8] FIPS PUB 46-3 , DATA ENCRYPTION STANDARD (DES) , October 1999
[9] Xilinx, ML605 Hardware User Guide UG534 (v1.6) July 18, 2011 Available at http://www.xilinx.com/support/documentation/boards_and_kits/ug534.pdf
[10] Getting Started with the Xilinx Virtex-6 FPGA ML605 Evaluation Kit, UG533 (v1.5) October 20, 2011 Available at http://www.xilinx.com/support/documentation/boards_and_kits/ug533.pdf
[11] S. Kumar, C. Paar, J. Pelzl, G. Pfeiffer, A. Rupp, and M. Schimmler. "How to Break DES for € 8,980". In SHARCS Workshop. Cologne, Germany, 2006.

A Proposed Attacking Method on Rabin's Cryptosystem

Dr. Sattar B. Sadkhan / University of Babylon - IRAQ
E-mail:drengsattar@ieee.org

ABSTRACT

In 1979 Rabin proposed his system as a modification to RSA public key cryptosystem. The security of Rabin's scheme based mainly on the difficulty of finding square roots modulo a composite number. This problem equivalents to factoring a large composite number. Rabin's cryptosystem proved to be as hard as factorization. This paper provides a mathematical analysis of Rabin's cryptosystem and shows a proposed attacking procedures on Rabin's cryptosystem.
Keywords:

1- Introduction

In 1976, Diffe and Hellman published a paper about the public key cryptography " new direction in cryptography ", which surprised most cryptologist at that time. They proposed a cryptosystem that does not require a secure channel, but nevertheless offers the possibility for secret communication. Diffe and Hellman proposed such system for distributing the secret key to be used in conventional cryptosystems over the insecure communication channel. The fundamental concept on which they are based is the simple. Rabin's cryptosystem is a public key which based on the same idea of Diffe and Hellman. Rabin's cryptosystem was proved to be as hard as factorization [1] . However decryption is not unique. Williams [3] showed that if (p = q = 3 mod 4), then decryption can be unique in Rabin's cryptosystem, where p and q are the secret prime numbers. Kurosawa et al. showed a cryptosystem that is hard as factorization in which p and q are arbitrary as well as the decryption being unique. Digital signature schemes of Williams and Kurosawa et al. are the same as Rabin's digital signature scheme. They have no advantage over Rabin's scheme [2].

The objective of this paper is to provide a proposed new supporting mathematical tools for attacking Rabin's cryptosystem. The paper contains four sections, section 1 provided the introduction to Rabin's type cryptosystem, while section 2 introduces mathematical analysis of Rabin's cryptosystem, section 3 provides the proposed new attacking procedures on Rabin's cryptosystem and the section 4 contains the conclusion.

2-Mathematical Analysis of Rabin's Cryptosystem

2-1 Rabin's Public Key Cryptosystem.

Michael Rabin discovered a version of RSA, although it is more properly regarded as a public key cryptosystem in its own right. During its early history, this system was considered of theoretical, but not practical interest because of a "fatal flaw" that made it vulnerable to a chosen plaintext attack. However there are ways around the flaw, making this system a real competitor to RSA [4] [9].

In the operation with integers modulo n, using both addition and multiplication modulo n, if n is not a prime, then not every non-zero element has a multiplicative inverse. But also of interest here are the elements that have a square roots. The square root of an element (a) is an element (b) . Some integers have several square roots, and some have none. In fact, number theorists have been interested in these matters for hundreds of years; they even have a special term for a number that has a square root: a quadratic residue [5].

Rabin's cryptosystem encodes a member x of Zn to another member y of Zn by the formula y = x^2 (mod n), where n is the product of two large primes p and q. The security of this cryptosystem is based on the assumption that factoring n is "hard". When working in the ring of integers modulo n, we give a special name to members of the ring that have a square root. We say x is a quadratic residue modulo n if there exists y co-prime to x such that:

$y^2 \equiv x \pmod n$.

Rabin's cryptosystem is based on the difficulty of finding square roots modulo an integer n.

2-2 key Generation method

Each user chooses two prime numbers p and q both congruent to (3 mod 4) and forms the product:

$n = p*q$.

hence the public key is the number (n), and the secret key: the numbers p and q [2].

2-3 Encryption

Let M be the set of all the plain text (messages).

$m = \{m \mid 0 < m \leq n-1\}$, the function E(m) is defined by :

$E(m) = C \equiv m^2 \bmod n$

2-4 Decryption

given the cipher text C, use the following formulas (given below) to calculate the four square roots (mod n) of C , i.e., m_1 , m_2 , m_3 , and m_4 as follows:

$m_1 \equiv C^{(p+1)/4} \bmod p$
$m_2 \equiv (p - C^{(p+1)/4}) \bmod p$
$m_3 \equiv C^{(q+1)/4} \bmod q$
$m_4 \equiv (q - C^{(q+1)/4}) \bmod q$

Then compute the integers (a) and (b) as follows:

$a = q\,(q \bmod p)^{-1} \in Z_p$
$b = p\,(p \bmod q)^{-1} \in Z_p$

The four possible solutions are :

$M_1 \equiv (am_1 + bm_3) \bmod n$
$M_2 \equiv (am_1 + bm_4) \bmod n$
$M_3 \equiv (am_2 + bm_3) \bmod n$
$M_4 \equiv (am_2 + bm_4) \bmod n$

2-5 Efficiency

Encryption with Rabin cryptosystem requires only one squaring (mod n), so Rabin encryption method can be considered more efficient than RSA. The decryption of Rabin cipher text is as expensive as RSA decryption using the Chinese remainder theorem [6].

3- Cryptanalysis of Rabin's Cryptosystem.

The complexity of Rabin's system (the difficulty of breaking it) is exactly equivalent to factoring the number (n). Suppose one has a Rabin encryption / decryption system that hides the two primes inside it. If one can factor the number (n), then the system is broken immediately. Since the above mentioned formulas allow the roots to be calculated. On the other hand, if one has access to a Rabin's crypto system, then taking any message, calculate $c = m^2 \bmod n$, and submit c to the Rabin system. If the system produces all four roots, then (m) and (-m) give no additional information, but either of the two roots minus m will have one of p and q as factors [7].

Given a Rabin public key (*n*), we want to find the private key (*p* , *q*) such that n = p* q. Suppose Cryptanalyst has broken Rabin's cryptosystem with algorithm (R) which computes m = R(c) such that m is a square root of c. The Cryptanalyst chooses a random integer x € {1,2, ….., n-1} with gcd (x , n)=1 and encrypts (x) using the Rabin's cryptosystem to find c = x^2 mod n [1], [8].

If Cryptanalyst happens to find *x* with gcd (x , n) ≠ 1, then she has a factor of *n*. The residue class $m + n\mathbf{Z}$ is *a* square root of (c + n **Z)**, but is not necessarily equal to (x + n **Z)**. However, *m* and *x* will satisfy one of the following pairs of congruence relations [10]:

a) $m \equiv +x \pmod p$ and $m \equiv +x \pmod q$

b) $m \equiv -x \pmod p$ and $m \equiv -x \pmod q$

c) $m \equiv +x \pmod p$ and $m \equiv -x \pmod q$

d) $m \equiv -x \pmod p$ and $m = +x \pmod q$

The four possibilities are

	x	m – x, n) = n
	n-x	m – x, n) = 1
|	$m - x, q \nmid m - x$	m – x, n) = p
∤	$m - x, q \mid m - x$	m – x, n) = q

More generally, factoring integers into primes and taking square roots (mod n) are computationally equivalent. The above algorithm will be successful 50% of the time.

Now suppose we modify our Rabin's cryptosystem so that the plaintext is always of a special form for easy identification among the four possible square roots. Thus if cryptanalyst has broken this modified Rabin's system with algorithm *R*', she/he can compute m = R'(c). The Cryptanalysis (R') algorithm to work, *x* must be of the special form. Then given $c \equiv x \text{ ^2 (mod n)}$ and m = R'(c), the only solution is $m = R'(c) = x$. Since $m = x$, we cannot recover *p* and *q*. Thus, if the plaintext has to be of a special form, Rabin's problem is not equivalent to factoring problem.

3-1 First Lipton's method

Lipton [3] assumed that two plain text m_1 and m_2 are encrypted modulo and the difference between m_1 and m_2 is a constant t , so m_1 and m_2 be obtained as follows :

$C_1 = m_1^2 \bmod n$

$C_2 = m_2^2 \bmod n$

$= (m_1 + t)^2 \bmod n$ then

$m_1 = (c_2 - c_3 - t^2) / 2t \bmod n$

$m_2 = m_1 + t$

3-2 Second Lipton's Method

Lipton [3] assumed that m is encrypted in two different modulo (n_1, n_2), then the analyst could find (m) as follows:

1- Compute x, y such that :-

$x = (y*n_2 + c_2 - c_1) / n_1$, choosing a random value to (y) such that (x) be an integer.

2- Compute the value of (t) where :-

$t = \llcorner -x / n_2 \lfloor$

3- Compute m where:

$m = (c_1 + (x + t* n_2)* n_1)^{1/2}$

3-3 Iteration of Fermat's factorization

This method used to factorize the public key n to its factor (p) & (q) by Fermat's factorization method [4] [8].

3-4 Other attacks

An algorithm that can factor the Rabin modulus can break the cryptosystem and allow any message to be decoded. However, there are more subtle attacks that do not require factoring the modulus. They do not result in breaking the Rabin's cryptosystem but can, in special cases, give enough information to decode some messages. Many attacks on the RSA cryptosystem also can be applied to Rabin's cryptosystem.

One such attack is the broadcast attack. This attack applies to Rabin since Rabin encryption is the same as RSA encryption with e =2. To understand this attack let us suppose that Bob encrypts the same message *m* with two different public keys n_1 and n_2 to get cipher texts C1=m^2 mod n1 and C2= m^2 mod n1. Note that m < n_1, n_2. We solve the system

$C \equiv C1 \pmod{n1}$

$C \equiv C2 \pmod{n1}$

Thus we have $0 \le c < n1\ n2$ and $0 \le m^2 < n1\ n2$ which implies $m = \sqrt{c}$. The idea behind this attack is that taking square roots (mod *n*) is hard, but taking square roots on integers is easy. For RSA this attack can be mounted when the same message is sent (e) times.

In order to get a picture of RSA system we must consider how the cryptanalyst might attack it. The most obvious way of course, is to factor n . If cryptanalyst knows p and q, the system will be broken. There is no known polynomial time algorithm for factoring integers, and the security of the system is closely related to the difficulty of this problem. To justify our confidence in the inability of the cryptanalyst to factor (n) we list the time required to factor integers of various sizes. The assumption made in obtaining Table 1 is that each operation takes (one microsecond). It must not be forgotten that any increase in n produces an increase in complexity of implementation, which concerns not only the hardware, but also the time for encryption / decryption [5] [6].

Table 1 the time needed for factoring integers

Algorithm 1

No. of decimal digits in n	No. of operations to factor	Time needed
	$1.4* 10^{10}$	3.9 hours
	$9.0* 10^{12}$	104 days
	$2.3* 10^{15}$	74 years
	$1.2* 10^{23}$	$3.8*10^{9}$ years
	$1.5* 10^{29}$	$4*10^{15}$ years
	$1.3* 10^{39}$	$4.2*10^{25}$ years

4- The Proposed Attacking Methods on Rabin's Cryptosystem

In Rabin's cryptosystem let (x) be the first integer greater than I satisfying the congruence $\chi^2 \equiv 1 \bmod n$, then cache of (x) and its complement (n-x) are called a generator of (n) .

This method based on finding a generator (x) in the ring (z) of order (n) where n = p*q , and then finding the plain text by the following algorithm :-

Step 1 : the generator = x
Step 2 : I = 1
Step 3 : $M_1 = I$, $M_2 = x$, $M_3 = n-1$, $M_4 = n-x$
Step 4 : I = I +1
Step 5 : $M_1 = I$, $M_2 = (M_{2i-1}+x) \bmod n$, $M_3 = n-1$, $M_4 = n-M_2$

j represent the prime number p.

c- The factorization algorithm to factorize the order of the ring Z_n (n = p*q) in Rabin's cryptosystem is efficient specially when n is large number and with error ≈ 0.0007. using the algorithm 1 and q by using algorithm 2 given below :-

Step 1 : the generator = x
Step 2 : y = n / x-1
Step 3 : y = y / frac. (y)
Step 4 : if frac(y) =0 then y = p else go to step 3

Algorithm 2

Step 1 : the generator = x
Step 2 : y-n / x+1
Step 3 : y = y / frac. (y)
Step 4 : if frac. (y) =0 then y = q else go to step 3

5- Conclusion

Rabin's cryptosystem is a good alternative to the RSA cryptosystem, though both depend on the difficulty of factoring for their security.

a- The definition of the generator is a great contribution in attacking direction because this definition opened many attacking ways on Rabin's cryptosystem.

b- By using the definition of the generator and during the table of plain text preparation we can stop just the cipher text C_j appear which is equal to any C_i(i<j) and the distance between i and J represent the prime number p.

c- The factorization algorithm to factorize the order of the ring Z_n (n=p*q) in Rabin's cyriptosystem is efficient specially when n is large number and with error ≈ 0.0007.

References

[1] Henry B. , Freed P. , " Cipher system", ISBN, publisher, 1982.
[2] Bruce S. , " Applied Cryptography", second edition published by John Wiley & Sons, Inc, 1996.
[3] Williams H.C. , " Some public key crypto-functions as intractable as factorization ", Cryptology No.3, 1985, P.223-237.
[4] Alan G. Konheim , " Cryptography : A primer", John Wiley & Sons, 1982.
[5] Arto S. , " Public key Cryptography", second edition ,1996.
[6] Carl H. Meryer , Stephen M. Matyas , " Cryptography : A new dimension in computer data security", 1982.

[7] Kaoru K. , Toshiya I. , Masashi T., "Public Key Cryptosystem Using A Reciprocal Number With The Same Intractability As Factoring A Large Number ", Cryptologia ,1994
[8] Public-key Cryptography, http://www.quadibloc.com/crypto/publ05.htm
[9] Kurosawa, K. Ito, T. Takeuchi, M. ," Public key cryptosystem using a reciprocal number with same intractability as factoring a large number", Electronics Letters, 23 Issue: 15 , July 2007,
[10] Okamoto T., Uchiyawan S., " A New Public Key Cryptosystem as a secure as Factoring", Proc. of Euorocrypt '99, Lecture Notes in Computer Science, 1403 (1998).

Frei-Chen Maskeleri Tabanlı Yeni Bir Sır Paylaşım Tekniği

Veysel ASLANTAŞ, Ebubekir KAYA

***Özet*—Bu çalışmada Frei-Chen maskeleri tabanlı yeni bir sır paylaşım tekniği geliştirilmiştir. Bu teknikte (5,5) eşik değer kullanılarak sır resmin gürültülü görünüme sahip beş tane pay resimde saklanması sağlanmıştır. Pay resimlerden sır resmi yeniden elde edebilmek için, pay resimlerin tamamına ihtiyaç duyulmaktadır. Eğer 4 veya daha az sayıda pay resim bir araya gelirse sır resim hiç bir şekilde yeniden elde edilemeyecektir. Ayrıca elde edilen pay resimlerin boyutu sır resmin boyutundan daha küçüktür. Geliştirilen tekniğin başarısı uygulamalar üzerinden gösterilmiş ve diğer sır paylaşım teknikleri ile karşılaştırılmıştır.**

***Anahtar Kelimeler*—Bilgi Güvenliği, Frei-Chen Maskeleri, Görüntü İşleme, Sır Paylaşımı**

***Abstract*—In this study, a new secret sharing scheme based Frei-Chen masks is developed. In this scheme, the secret image is hidden using (5,5) threshold scheme in five noisy share images. All share images are required to recover the secret image. If four or fewer share images are combined, secret image can never be recovered. Additionally, the size of the share images is smaller than the size of the secret image. The success of the proposed method is shown via applications and compared to other secret sharing schemes.**

***Keywords*— Frei-Chen Masks, Image Processing, Information Security, Secret Sharing**

I. GİRİŞ

Sır paylaşımı, veri saklamada kullanılan bir yöntemdir. Bu yöntemde saklanan veriler metin, sayısal veya resim içerikli olabilir. Saklanacak verilere sır değer, sır değerlerin saklanması sonucu oluşan yeni verilere ise pay değeri adı verilir. Sır paylaşımında; sır değerin n adet yeni veride saklanması sağlanır. Bu n adet veriden k veya daha fazlası bir araya geldiği zaman yeniden orijinal veriye (sır değere) ulaşılması sağlanır. Bu olaya (k,n) eşik değeri adı verilir.

Sır paylaşımı metodu Shamir ve Blakley tarafından 1979 yılında aynı zamanlarda önerilmiştir [1][2]. Bu metotlarda sır değerin korunması amaçlanmıştır. (k, n) eşik değeriyle sır n paya ayrılmıştır. Bu n payda k ve daha fazlasının bir araya gelmesiyle sır değere yeniden ulaşılması sağlanmıştır. Sır paylaşımı modelinin ortaya atılmasından sonra bu alanda bir çok çalışma yapılmıştır. Noar ve Shamir [3] görsel sır paylaşımı adı verilen (Visual Secret Sharing - VSS) yeni bir şifreleme tekniği önermişlerdir. (k, n) eşik değerli VSS metodunda sır resim, gürültülü bir görünüme sahip n tane pay resme dönüştürülmektedir. Elde edilen pay resimlerde bilginin gizlenmesi sağlanır ve orijinal resim komşu pikseller arasındaki ilişki kullanılarak oluşturulur. Pay resimlerin gürültülü bir görünüme sahip olmasından dolayı sır resme ait bilgi elde edilemez. En az k tane pay resmin bir araya gelmesiyle sır resmin yeniden elde edilmesi sağlanır. Görsel sır paylaşımı metodu ortaya çıktıktan sonra bu alanda çalışmalar devam etmiştir. Blundo [4], görsel sır paylaşımı metodunu gri resimlere uygularken Lukac [5] ise renkli resimlere uygulamıştır.

Thien ve Lin [6] gizli resim paylaşımı metodunu önermişlerdir. Bu metodda sır resim n adet gölge resme ayrılır. Bu gölge resimlerden ($k \leq n$) ve daha fazlasının bir araya gelmesiyle orijinal resim yeniden elde edilir. Bu metotda elde edilen gölge resimlerin boyutu, orijinal resmin boyutundan daha küçüktür. Boyutun küçüklüğü depolamanın önemli olduğu çalışmalarda avantaj sağlamaktadır. Wang ve Su [8] da gizli resim paylaşımı üzerinde Thien ve Lin tabanlı bir metot öne sürmüştür.

Lin ve Tsai [7], Shamir'in sır paylaşımı tabanlı bilgi saklama ve kimliklendirme seviyelerinin daha iyi olduğu bir metot önermiştir. Bu yöntem de güvenliğin sağlandığı üç aşama vardır. Birinci aşamada güvenlik (k, n) eşik değeri ile sağlanır. Burada sır n paya ayrılır. k ve daha fazla payın bir araya gelmesiyle orijinal resim yeniden elde edilir. İkinci aşamada ise bilgiler gizlemede kullanılan resimlerde gizlenir. Son olarak sır resmi yeniden oluşturmadan önce pay sahiplerindeki hata belirlenir ve iyi bir kimliklendirme seviyesine hazırlanılır. Önerilen bu yöntem renkli resimlerde de uygulanabilir. Renkli resimlere uygulandığında çok az bir veri kaybı ile sır resim yeniden oluşturulabilmektedir.

Bai [9] matris tabanlı bir sır paylaşım metodu önermiştir. Önerilen bu yöntemde sır, karesel matriste bulunan elemanlardır. Bu metotta elde edilen pay matrisin boyutu, S sır matrisin boyutundan daha küçüktür. Bai [10] diğer bir çalışmasında Thien ve Lin [6] modeli ile matris tabanlı sır paylaşım modelini bir arada kullanmıştır. Sır resmin boyutunun büyük olduğu durumlarda önerilen bu yöntem avantaj sağlamaktadır.

Wang [11], resimlerde kullanılan ve ölçeklenebilir sır paylaşımı adını verdiği yenilikçi bir metot önermiştir. Sır

Veysel ASLANTAŞ, Erciyes Üniversitesi Mühendislik Fakültesi Bilgisayar Mühendisliği Bölümü, Tel: 0352 4374901, E-posta: aslantas@erciyes.edu.tr
Ebubekir KAYA, Nevşehir Üniversitesi Meslek Yüksekokulu Bilgisayar Programcılığı Bölümü, Tel: 0384 22811 40, E-posta: ebubekir@nevsehir.edu.tr

paylaşımı metotlarının diğer versiyonlarında olan farklı pay resimlerin bir araya gelmesiyle sır resmin yeniden elde edilmesi özelliğine bu modelde esneklik getirilmiştir. Bu durum çoklu sır, öncelik ve ilerici adı verilen üç yöntem ile sağlanmaktadır.

Bu çalışmadanın diğer bölümlerinde şu konular ele alınmıştır: İkinci bölümde Frei-Chen maskeleri anlatılmıştır. Üçüncü bölümde önerilen yöntem açıklanmıştır. Dördüncü bölümde uygulamalara yer verilmiştir. Beşinci bölümde ise değerlendirme yapılmıştır.

II. FREI-CHEN MASKELERİ

Frei-Chen maskeleri bir resmin özelliklerini ortaya çıkaran 3x3 boyutlarında dikey gösterimlerdir. Bu yüzden, bir resmin 3x3'lük her bloğu dokuz Frei-Chen maskesinin toplam ağırlığını göstermektedir [15]. Frei-Chen maskeleri Denklem 1'de verildiği şekildedir.

$$
\begin{aligned}
W_1 &= \frac{1}{\sqrt{8}}\begin{bmatrix} 1 & \sqrt{2} & 1; & 0 & 0 & 0; & -1 & -\sqrt{2} & -1 \end{bmatrix} \\
W_2 &= \frac{1}{\sqrt{8}}\begin{bmatrix} 1 & 0 & -1; & \sqrt{2} & 0 & -\sqrt{2}; & 1 & 0 & -1 \end{bmatrix} \\
W_3 &= \frac{1}{\sqrt{8}}\begin{bmatrix} 0 & -1 & \sqrt{2}; & 1 & 0 & -1; & -\sqrt{2} & 1 & 0 \end{bmatrix} \\
W_4 &= \frac{1}{\sqrt{8}}\begin{bmatrix} \sqrt{2} & -1 & 0; & -1 & 0 & 1; & 0 & 1 & -\sqrt{2} \end{bmatrix} \\
W_5 &= \frac{1}{2}\begin{bmatrix} 0 & 1 & 0; & -1 & 0 & -1; & 0 & 1 & 0 \end{bmatrix} \\
W_6 &= \frac{1}{2}\begin{bmatrix} -1 & 0 & 1; & 0 & 0 & 0; & 1 & 0 & -1 \end{bmatrix} \\
W_7 &= \frac{1}{6}\begin{bmatrix} 1 & -2 & 1; & -2 & 4 & -2; & 1 & -2 & 1 \end{bmatrix} \\
W_8 &= \frac{1}{6}\begin{bmatrix} -2 & 1 & -2; & 1 & 4 & 1; & -2 & 1 & -2 \end{bmatrix} \\
W_9 &= \frac{1}{3}\begin{bmatrix} 1 & 1 & 1; & 1 & 1 & 1; & 1 & 1 & 1 \end{bmatrix}
\end{aligned} \tag{1}
$$

Frei-Chen maskeleri resmin farklı yapısal bilgilerini verir. İlk dört maske kenar, sonraki dört maske hat ve en son maske ortalama değer bilgilerini verir. Dolayısıyla 3x3 boyutundaki bir resim bölgesi (V), bu maskelerin ağırlıklandırılmış (R_i) bir toplamı olarak temsil edilebilir:

$$
V = \sum_{i=0}^{9} R_i W_i, \qquad R_j = V \circ W_j, \qquad j = 1,2,\ldots,9 \tag{2}
$$

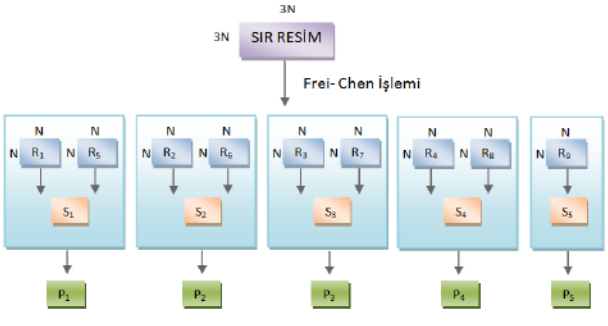
Denklem 2'de verilen "$\circ$" sembolü nokta çarpımı temsil etmektedir.

III. ÖNERİLEN YÖNTEM

Bu çalışmada Frei-Chen maskeleri tabanlı sır paylaşım tekniği geliştirilmiştir. Önerilen teknikte sır resim, beş gölge (pay) resimde saklanmıştır. Gölge resimlerin elde edilmesinde dokuz Frei-Chen maskesi kullanılmıştır. Önerilen teknik, pay resimlerin elde edilmesini sağlayan Gizleme aşaması ve yeniden sır resmin oluşturulmasını sağlayan Birleştirme aşamasından oluşmaktadır.

A. Gizleme Aşaması

Gizleme aşamasında, sır resmin pay resimlerde saklanması sağlanmıştır. Pay resimlerin elde edilmesinde Şekil 1'de verilen şema kullanılmıştır. Bu şemada görüldüğü gibi 3Nx3N boyutunda sır resme Frei-Chen maskeleri uygulanarak NxN boyutunda dokuz resim elde edilmiştir ($R_1, R_2, \ldots, R_9$). R_i, i. Frei-Chen maskesi ile oluşturulan resmi göstermek üzere, R_i resminde meydana gelen değişiklikler sağlama resimlerinde (S_1, S_2, S_3, S_4, S_5) tutulmuştur. S_j, j. sağlama resmini göstermek üzere; boyutu R_i resminin boyutuna eşittir. R_1 ve R_5 kullanılarak S_1, R_2 ve R_6 kullanılarak S_2, R_3 ve R_7 kullanılarak S_3, R_4 ve R_8 kullanılarak S_4 ve R_9 kullanılarak da S_5 resimleri elde edilmiştir. R_i ve S_j resimlerinin kullanılmasıyla ise pay resimleri oluşturulmuştur. P_j, j.pay resmi göstermek üzere; R_1, R_5 ve S_1 kullanılarak P_1; R_2, R_6 ve S_2 kullanılarak P_2; R_3, R_7 ve S_3 kullanılarak P_3; R_4, R_8 ve S_4 kullanılarak P_4; son olarak R_9 ve S_5 kullanılarak P_5 pay resimleri elde edilmiştir.


3N
3N
SIR RESİM
Frei- Chen İşlemi
N
N
N

$$S_{3_{i,j}} = \begin{cases} \alpha, & R_3 \geq 0 \quad ve \quad R_7 \geq 0 \\ \alpha+1, & R_3 \geq 0 \quad ve \quad R_7 < 0 \\ \alpha+2, & R_3 < 0 \quad ve \quad R_7 \geq 0 \\ \alpha+3, & R_3 < 0 \quad ve \quad R_7 < 0 \end{cases}$$

$$S_{4_{i,j}} = \begin{cases} \alpha+4, & R_4 \geq 0 \quad ve \quad R_8 \geq 0 \\ \alpha+5, & R_4 \geq 0 \quad ve \quad R_8 < 0 \\ \alpha+6, & R_4 < 0 \quad ve \quad R_8 \geq 0 \\ \alpha+7, & R_4 < 0 \quad ve \quad R_8 < 0 \end{cases}$$

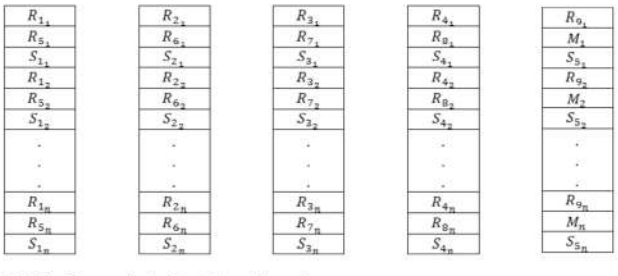
$$S_{5_{i,j}} = \begin{cases} \beta+8, & R_9 \geq 0 \\ \beta+9, & R_9 < 0 \end{cases}$$

Denklem 3-7 arasında S_i resimlerinin oluşturulmasını sağlayan denklemler verilmiştir. Denklemlerde yer alan β değeri [100, 245] aralığında ve α değeri [0, 99] aralığında 10'un katı olan rastgele sayıları göstermektedir.

Pay Resimlerinin Elde Edilmesi:

Bu çalışmada beş pay resim oluşturulmuştur. Pay resimler gürültülü bir görünüme sahiptir. Bu yüzden sır resmin özelliklerini yansıtmamaktadır. P_j, j.pay resmi göstermek üzere; P_1 resmini elde etmek için R_1, R_5 ve S_1 resimleri; P_2 resmini elde etmek için R_2, R_6 ve S_2 resimleri; P_3 resmini elde etmek için R_3, R_7 ve S_3 resimleri; P_4 resmini elde etmek için R_4, R_8 ve S_4 resimleri, P_5 resmini elde etmek için R_9 ve S_5 resimleri kullanılmıştır.

Pay resimlerin elde edilmesinde Şekil 2'de verilen birleşim kullanılmıştır. Her bir pay resmin oluşmasını sağlayan resimlerden sırasıyla birer satır alınarak 3N x N boyutlarında pay resimler elde edilmiştir.

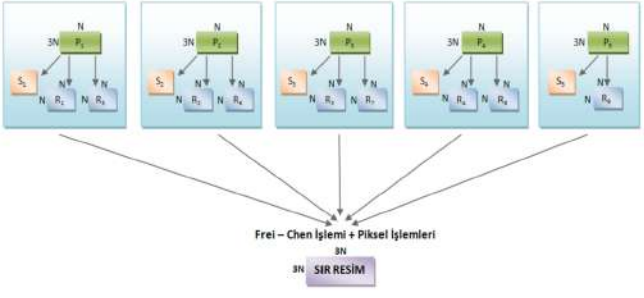


Şekil 2. Pay resimlerin elde edilmesi.

384x384 boyutunda bir resim üzerinde işlem yapılırsa, 128x128 boyutlarında (1/9 oranında) 9 tane R_i ve aynı boyutta 5 tane S_j ile 1 random resim (M) oluşturulmaktadır. 128x128 boyutunda 15 resmi kullanarak 384x128 boyutunda 5 tane pay resim (S_j) elde edilir. Pay resimlerin boyutu orijinal resmin boyutunun 1/3 ü kadardır.

B. Birleştirme Aşaması

Bu bölümde pay resimler kullanılarak sır resmin yeniden elde edilmesi anlatılmıştır. Sır resmin yeniden oluşturulmasında uygulanacak işlem adımları Şekil 3'de verilmiştir.



Şekil 3. Pay resimlerden sır resmin elde edilme aşamaları.

(5) Pay resimlerden R_i ve S_j resimleri ayırt edilmiştir. Bu resimlerin ayırt edilebilmesi için pay resimlerin numaralarının tespit edilmesi gerekmektedir (P_1, P_2, P_3, P_4, P_5). N pay resimlerdeki satır numarasını göstermek üzere; MOD(N, 3)=0 eşitliğini sağlayan satırlardaki pikseller sağlama resimlerine aittir. Sağlama resminin piksellerinden Tablo I' de verilen incelemeler yapılarak pay resim numaraları ve R_i resimleri tespit edilmektedir.

(6) R_i resimlerinin değerini Fre-Chen maskeleri kullanılarak elde edildiği ilk haline dönüştürmek için aşağıda verilen işlemler uygulanmıştır. Modüler işlemlerin sonucu sayıların işareti elde edilmiştir.

TABLO I
S_j PİKSEL DEĞERİ İLE BULUNABİLECEK BİLGİLER

S_j Piksel Değeri	MOD(S_j,10) Sonucu	Sağlama Resimler	Frei-Chen Resimleri
100 - 255	0, 1, 2, 3	S_1	R_1, R_5
100 - 255	4, 5, 6, 7	S_2	R_2, R_6
100 - 255	8, 9	S_5	R_9
0 - 99	0, 1, 2, 3	S_3	R_3, R_7
0 - 99	4, 5, 6, 7	S_4	R_4, R_8

(7) R_i resimleri elde edildikten sonra Denklem 1'de verilen Frei-Chen maskeleri kullanılarak sır resim yeniden elde edilir.

$$\begin{cases} -R_{5_{i,j}}, & \mathrm{mod}(S_{1_{i,j}},10)=1 \\ -R_{1_{i,j}}, & \mathrm{mod}(S_{1_{i,j}},10)=2 \\ -R_{1_{i,j}} \quad ve \quad -R_{5_{i,j}}, & \mathrm{mod}(S_{1_{i,j}},10)=3 \end{cases} \tag{8}$$

$$\begin{cases} -R_{6_{i,j}}, & \mathrm{mod}(S_{2_{i,j}},10)=5 \\ -R_{2_{i,j}}, & \mathrm{mod}(S_{2_{i,j}},10)=6 \\ -R_{2_{i,j}} \quad ve \quad -R_{6_{i,j}}, & \mathrm{mod}(S_{2_{i,j}},10)=7 \end{cases} \tag{9}$$

$$\begin{cases} -R_{7_{i,j}}, & \mathrm{mod}(S_{3_{i,j}},10)=1 \\ -R_{3_{i,j}}, & \mathrm{mod}(S_{3_{i,j}},10)=2 \\ -R_{3_{i,j}} \quad ve \quad -R_{7_{i,j}}, & \mathrm{mod}(S_{3_{i,j}},10)=3 \end{cases} \tag{10}$$

TABLO III
DİĞER YÖNTEMLERLE ÖZELLİK KARŞILAŞTIRMASI

Metod	Wang et al's [16]	Yang's [14]	Yu et al's [13]	Lukac et al's [12]	Önerilen Yöntem
Piksel Genişleme	1	1	1/2	4	1/3
Resim Formatı	İkili, gri ve renkli	İkili	İkili, gri ve renkli	İkili, gri ve renkli	İkili, gri ve renkli

TABLO II
ÖNERİLEN YÖNTEMDE ELDE EDİLEN SONUÇLAR

Resim	Format	Boyut	PSNR
Lena	Gri	300x300	50.2438
Barbara	Gri	300x300	50.0230
Lena	Renkli	300x300	49.9660
Barbara	Renkli	300x300	49.8234

$$\begin{cases} -R_{8_{i,j}}, & \mathrm{mod}\left(S_{4_{i,j}},10\right)=5 \\ -R_{4_{i,j}}, & \mathrm{mod}\left(S_{4_{i,j}},10\right)=6 \\ -R_{4_{i,j}} \quad ve \quad -R_{8_{i,j}}, & \mathrm{mod}\left(S_{4_{i,j}},10\right)=7 \end{cases} \tag{11}$$

Farklı Formattaki Resimlere Uygulanışı:

Tek banttan oluşan resimlerde sır paylaşımı anlatıldığı şekliyle uygulanmaktadır. Eğer resim üç banttan oluşuyorsa her bant için ayrı işlemler yapılarak tekrar bir araya getirilir. Dolayısıyla önerilen sır paylaşım metodunda resim formatı ikili, gri ve renkli olabileceği gibi 8, 16 ve 24 bit özelliğinde de olabilir. Gri ve renkli resimlere önerilen yöntemin uygulanması ile elde edilen sonuçlar Tablo II' de verilmiştir.

IV. UYGULAMA VE SONUÇLARI

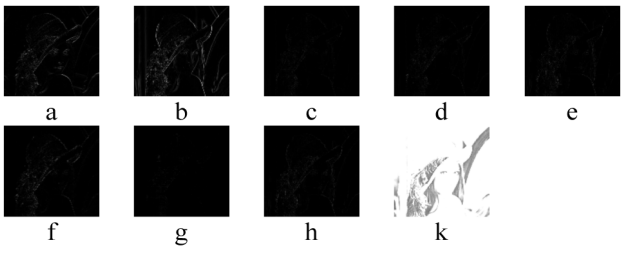
Şekil 4a'da verilen 300x300 boyutundaki resim bu uygulamada kullanılmıştır. Verilen resim 5 pay resimde saklanmıştır. Pay resimlerin elde edilebilmesi için 15 yan resim (R_i, S_j, M) kullanılmıştır. Elde edilen R_i resimleri Şekil 5'de, S_j resimleri Şekil 6'da verilmiştir. Bu resimlerin kullanılmasıyla oluşturulan P_j resimleri ise Şekil 7'de gösterilmiştir. Şekil 4b'de ise yeniden elde edilen sır resim verilmiştir.

R_i ve S_i resimleri 100x100, P_i resimleri ise 300x100 boyutundadır. Sır resmin gizlendiği pay resimlerde boyut 1/3 oranında küçültülmüştür. Sır paylaşımı tekniklerinin uygulanabilirliğini gösteren özelliklerden biri pay resimlerin sır resmin görüntüsünü vermemesidir. Şekil 7'de elde edilen pay resimler özellik olarak sır resme benzemediği görülmektedir. Pay resimlerin bir araya gelmesi ile Şekil 4b de verilen resim elde edilmiştir. Orijinal resim ile yeniden elde ettiğimiz resim arasındaki benzerlik PSNR=50.2438 olduğundan başarılı bir sonuç elde edildiği görülmektedir. Şekil 4'de verilen sır resim dışında, farklı boyut ve şekilde resimlerin kullanılmasıyla elde edilen sonuçlar Tablo II' de verilmiştir. Tablo II' de verilen sonuçlar incelendiğinde gri ve renkli resimlerde önerilen yöntemin iyi sonuçlar verdiği görülmektedir. Sır paylaşım yöntemlerinin başarısını yeniden elde etme dışında pay resimlerin sayısı, pay resimlerinin görünümü, pay resimlerin büyüklüğü, elde edilen toplam piksel sayısı, uygulanabilen resim formatları gibi diğer kriterlerde belirlemektedir. Bu yüzden Tablo III' de geliştirilen tekniğin diğer sır paylaşım teknikleri ile özellik yönünden karşılaştırılması verilmiştir. Tablo III incelendiğinde pay resimlerin boyutunun (Piksel Genişleme) en düşük olduğu yöntem bu çalışmada önerilen yöntemdir. Ayrıca önerilen yöntem diğerlerinde olduğu gibi tüm resim formatlarında uygulanabilmektedir. Bu çalışmada resimlerin yeniden elde edilmesi sırasında oluşan kayıp Tablo II' de verilmiştir. Elde edilen pay resimlerin boyutunun küçültülmesi, farklı resim formatlarına uygulanabilmesi, geliştirilen yöntemin verilen yöntemlere göre daha başarılı olduğunu göstermektedir.



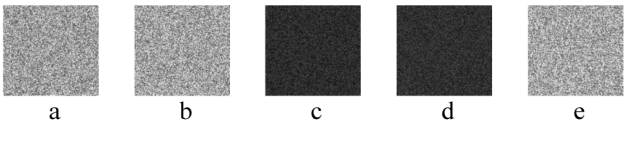
a b

Şekil 4. a- Uygulamada kullanılan sır resim. b- Yeniden elde edilen sır resim



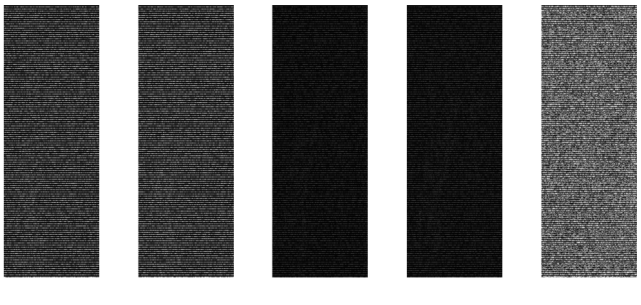
a b c d e f g h k

Şekil 5. Frei-Chen maskeleri kullanılarak oluşturulan resimler (R_i).



a b c d e

Şekil 6. Elde Edilen Sağlama Resimleri (S_i).



V. DEĞERLENDİRME

Bu çalışmada Frei-Chen maskeleri tabanlı sır paylaşım tekniği geliştirilerek gri ve renkli resimlere uygulanmıştır. Çalışmada elde edilen sonuçlar incelendiğinde tüm resim formatlarında PSNR değerinin yaklaşık olarak 50'nin üzerinde olduğu görülmektedir. Bu sonuçlar geliştirilen tekniğin sır paylaşımında çok az bir veri kaybı ile uygulanabileceğini göstermektedir. Geliştirilen teknik üzerinde değişiklikler yapılarak veri kaybının olmadığı veya daha aza indirildiği farklı çalışmalar yapılabilir.

KAYNAKLAR

[1] A. Shamir "How to share a secret," Commun. ACM, vol.22 (11) , pp. 612-613, 1979.
[2] G. R. Blakley, "Safeguarding cryptographic keys," Proc. AFIPS NCC, vol.48, pp.313-317, 1979.
[3] M. Naor, A. Shamir, "Visual cryptography," in Proceedings of Advances in Cryptology − EURPOCRYPT, LNCS 950, pp. 1-12, 1995.
[4] C. Blundo, A. De Santis, and M. Naor, , "Visual cryptography for grey level images" , Inf. Process. Lett., vol. 75, pp. 255–259, 2000.
[5] R. Lukac, K.N. Plataniotis, "Bit-Level Based Secret Sharing For Image Encryption", Pattern Recognition 38 (5), pp. 767–772, 2005.
[6] C.C. Thein and J.C. Lin, "Secret Image Sharing", Computers & Graphics, Vol.26, pp. 765-770, 2002.
[7] C.C. Lin, W.H. Tsai, "Secret image sharing with steganography and authentication," The Journal of Systems and Software, pp. 405–414, November (2004).
[8] R.Z. Wang, C.H. Su, "Secret image sharing with smaller shadow images," Pattern Recognition Lett., 27 6, pp. 551–555, 2006.
[9] L. Bai, "A strong ramp secret sharing scheme using matrix projection," presented at the Second International Workshop on Trust, Security and Privacy for Ubiquitous Computing, Niagara-Falls, Buffalo, NY, 2006.
[10] L. Bai, "A reliable (k, n) image secret sharing scheme," Dependable, Autonomic and Secure Computing, IEEE International Symposium on, vol. 0, pp. 31-36, 2006.
[11] R.Z. Wang, S.J. Shyu, "Scalable secret image sharing," Signal Processing: Image Communication, 22, pp. 363–373, 2007.
[12] R. Lukac, K. N. Plataniotis, "Colour image secret sharing," IEE Electronics Letters, vol. 40, no. 9, pp. 529-530, 2004.
[13] F. X. Yu, H. Luo, J. S. Pan, Z. M. Lu, "Lossless and lossy image secret sharing for data transmission":ISDA2008: Eighth International Conference on Intelligent Systems Design and Applications, Taiwan, November 26-28, 2008.
[14] C. N. Yang, "New visual secret sharing schemes using probabilistic method," Pattern Recognition Letters 25, 481-494, 2004.
[15] Rae-Hong Park, "A fourier interpretation of the frei-chen edge masks," Pattern Recognition Letters, vol. 11, no. 9, pp. 631 – 636, 1990.
[16] D.S.Wang, L. Zhang, N. Ma, X.B. Li, "Two secret sharing schemes based on Boolean operations," Pattern Recognition, vol.40, pp.2776-2785, 2007.

Gizli Görüntü Paylaşımında Kullanılan Eşik Şemalarının Performans Değerlendirilmesi

Güzin Ulutaş, Mustafa Ulutaş ve Vasif V. Nabiyev

Özet—**Ağ üzerinden gerçekleştirilen veri aktarımındaki artış, gizlilik gerektiren verilerin güvenliğinin sağlanması problemini beraberinde getirmiştir. İletilen verinin gizli görüntü olması durumunda veri güvenliği ve hataya karşı toleransı birlikte sağlayabilmek için (k, n) eşik şemaları son yıllarda yapılan çalışmalarda kullanılmaktadır. Gizli görüntü paylaşımı (GGP) alanında, dizinde var olan eşik şemalarını kullanan birçok çalışma yapılmıştır. Bu bildiride, gizli görüntü paylaşımında sıklıkla kullanılan (k, n) eşik şemalarının başarımları göreceli olarak değerlendirilmiştir. Başarım ölçütü olarak, yeniden yapılandırılan gizli görüntünün doğruluğu, pay görüntülerindeki genişleme oranı, pay görüntülerinin gizli görüntü hakkında bilgi içermesi ve yeniden yapılandırma süreleri göz önüne alınmıştır. Elde edilen deneysel sonuçlarda Shamir tabanlı yöntemlerin, diğer yöntemleri kullanan şemalara nazaran değerlendirme kriterleri açısından ön plana çıktığı gözlemlenmiştir.**

Anahtar Kelimeler—**Eşik şemaları, Gizli görüntü paylaşımı, PSNR, Sır Paylaşımı.**

Abstract—**Increase in the amount of data transferred through networks also brings secret data security problem. (k, n) threshold schemes are used to both ensure data security and fault tolerance lately. There are many publications based on secret sharing schemes (SSS) reported in the literature. Relative performances of widely used (k, n) threshold secret sharing schemes are reported in this paper. Distortion of revealed secret, expansion ratio of shares, secret hiding properties without permutation of secret and reconstruction time are considered as the performance metrics. Experimental results indicate that methods based on Shamir's work exhibit desirable properties than that of others in terms of the performance metrics.**

Keywords—**Threshold schemes, Secret image sharing, PSNR, Secret sharing.**

I. GİRİŞ

İnternetin bireyler yada kurumlar arası veri haberleşme amacı ile kullanılmasındaki artış, iletilecek olan verinin gizlilik gerektirdiği durumlarda, veri güvenliğinin sağlanması problemini de beraberinde getirmiştir. Haberleşmede kullanılan ortamın herkes tarafından gözlemlenebilir olması, araştırmacıları veri güvenliği alanında yeni çözümler bulmaya yönlendirmiştir. Dizinde yer alan ve kullanımı yaygın olan iki teknik Kriptografi ve Steganografidir. Kriptografi, gizli veriyi kullanılan matematiksel bir dönüşüm ve anahtar değeri ile, çözümlenemez biçime dönüştürme işlemidir. Yalnız bu yöntemdeki en büyük problem üretilen ortamın şifreli bir ortam olması sebebi ile, ağ üzerinden iletimi esnasında kötü niyetli kişilerin ilgisini çekecek şekilde yüksek entropili olmasıdır. Bu nedenle şifreli verinin yada gizli verinin, dikkat çekmeyen başka bir ortam içerisine saklanması araştırmacılar tarafından önerilmiştir. Steganografi olarak adlandırılan bu yöntem, örten ortam olarak, dikkat çekmeyen bir görüntü, ses dosyası ya da video dosyası kullanmaktadır. Saklamada kullanılan sayısal veri örten ortam, yerleştirme işleminin ardından üretilen veri ise stego ortam olarak adlandırılmaktadır. Steganografinin, diğer yönteme kıyasla en önemli üstünlüğü, ağ üzerinden iletilen stego ortamın kötü niyetli kişilerin ilgisini çekmeyecek şekilde doğal olmasıdır.

Veri güvenliğinin sağlanmasında kullanılan bu iki teknik temelde iki problemi de beraberinde getirmektedir. İlk problem her iki yöntemin uygulanması sonucunda oluşan şifreli yada stego ortamın hataya karşı toleranslı olmamasıdır. Diğer bir deyişle özel bir önlem almadıkça, herhangi bir bozulma olması durumunda, gizli veri yeniden hatasız olarak yapılandırılamayacaktır. Bir diğer problem ise kişiye güven yerine gruba güven mekanizmasının uygulanması gerektiği durumlarda her iki yöntemin de yetersiz kalmasıdır.

1994 yılında Naor ve Shamir tarafından önerilen Görsel Şifreleme (Visual Cryptography) yöntemi, gizli görüntülerin iletiminde ilk olarak hem veri güvenliğini sağlayan hem de gruba güven mekanizmasını uygulayan bir teknik olma özelliğini taşımaktadır [1]. Görsel şifreleme yöntemi gizli görüntüyü n kişi arasında paylaştırır. Katılımcıların asetatlar üzerine bastığı pay görüntülerinin herhangi k tanesinin üst üste getirilmesi gizli görüntünün elde edilmesi için yeterli olmaktadır. Görsel şifreleme, gizli görüntünün yeniden yapılandırılması esnasında yalnız insan görme sisteminden faydalanır. Yöntemin üretmiş olduğu pay görüntülerinin, en ve boy yönünde gizli görüntünün iki katı büyüklüğünde olması genişleme oranı problemi olarak adlandırılır. Dört kat büyüme gerek depolama gereksinimleri gerekse ağ bant genişliği açısından problem oluşturmaktadır. Görsel şifreleme yöntemindeki bir diğer problem ise yeniden yapılandırılan gizli görüntüdeki düşük karşıtlık değeridir.

2002 yılında Thien ve Lin, Gizli Görüntü Paylaşımı olarak adlandırılan ve Shamir'in 1979 yılında önermiş olduğu (k, n) eşik şemalarını kullanan yeni bir teknik önermişlerdir [2]. Yöntem, görsel şifrelemeden farklı olarak, genişleme oranı probleminden etkilenmemekte ve gizli görüntüyü doğru olarak yapılandırabilmektedir. Fakat bu yöntemler, gizli görüntünün elde edilmesi aşamasında insan görme sistemi değil, matematiksel hesaplardan faydalanmaktadır. Gizli görüntü

paylaşım şeması, görüntünün k adet pikselden oluşan bölümlerden oluştuğu varsaymakta ve her bir bölümü Shamir'in yöntemine göre katılımcılar arasında paylaştırmaktadır. Üretilen pay görüntüleri gizli görüntünün $1/k$'sı büyüklüğündedir.

Bu çalışmanın ardından önerilen farklı gizli görüntü paylaşımları da temelde, (k, n) eşik şemalarının kullanımına dayanmaktadır. Eşik şemaları gizli veriyi n kişi arasında paylaştırmakta ve katılımcılardan herhangi k yada daha fazlasının bir araya gelmesi durumunda gizli veriyi yeniden yapılandırabilmektedir [3-6]. k-1 yada daha az pay değerinin bir araya gelmesi gizli veri hakkında herhangi bir bilgi açığa çıkarmayacaktır. Eşik şemaları ilk olarak 1979 yılında Shamir ve Blakley tarafından ayrı zamanlarda önerilmiştir [3, 4]. Shamir'in yöntemi paylaştırma esnasında polinomial interpolasyondan faydalanırken, Blakley'in yöntemi ise düzlem geometrisini kullanmaktadır. Bu çalışmaların ardından 1983 yılında Asmuth-Bloom ve Mignotte ayrı zamanlarda Çinli Kalan Teoremini kullanan eşik şemaları önermişlerdir [5, 6]. Her iki yöntemde özel seçilmiş sıralı ve aralarında asal sayıları paylaştırma işleminde önce belirler. Asmuth-Bloom'un yöntemi rasgelelik içeriyor olması sebebi ile Mignotte'nin yöntemine göre üstünlük içermektedir.

2002 yılından sonra Gizli Görüntü Paylaşımı alanında yapılan çalışmalar, bahsi geçen eşik şemalarını kullanmaktadır [7-14]. Fakat araştırmacılar tarafından çoğunlukla Shamir'in yöntemi, gizli görüntülerin paylaştırılması için seçilmektedir [7-10]. Bu makalede, eşik şemalarının gizli görüntü paylaşımında kullanımı gerçekleştirilmiş ve literatürde ilk olarak hangi eşik şemasının gizli görüntülerin paylaşımında kullanılmasının performans açısından üstünlük sağlayacağı değerlendirilmiştir. Değerlendirme esnasında yeniden yapılandırılan gizli görüntünün doğruluğu, pay görüntülerindeki genişleme oranı, pay görüntülerinin gizli görüntü hakkında bilgi içermesi ve yeniden yapılandırma süreleri göz önüne alınmıştır.

Yayının geri kalan kısmı şu şekilde düzenlenmiştir. İkinci bölümde eşik şemaları hakkında kısa bir bilgi verilecektir. Üçüncü bölümde eşik şemalarının gizli görüntü paylaşımına uyarlanması gerçekleştirilecek ve son olarak da yöntemlerin birbirlerine göre performans değerlendirmesi yapılacaktır.

II. (K, N) SIR PAYLAŞIM ŞEMALARI

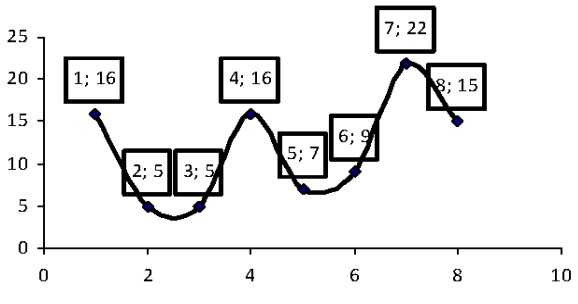
Eşik şemaları olarak da adlandırılan (k, n) sır paylaşım şemaları, gizli veriyi n kişi arasında paylaştırmaktadır [3-6]. Katılımcılara gönderilen pay değerleri gizli veri hakkında herhangi bir bilgi içermez ve en az k tanesinin bir araya gelmesi durumunda gizli veri yeniden yapılandırılır. k-1 yada daha az pay değeri gizli veri hakkında herhangi bir bilgi açığa çıkarmaz. Literatürde var olan eşik şemaları hakkında genel bir bilgi bu bölümde verilecektir.

A. *Shamir'in Eşik Şeması*

Shamir tarafından önerilen eşik şeması yöntemi, polinomial interpolasyona dayanır [3]. Verilen herhangi k adet noktanın $(x_1, y_1)\cdots(x_k, y_k)$, $x_i \neq x_j, 1 \le i < j \le k$ koşulunu sağlamak şartıyla, üzerinden geçtiği k-1 dereceden yalnızca bir $P(x)$ polinomu vardır. Shamir'in yöntemine göre gizli veri S, k-1 dereceden ve pozitif tamsayıların alanında bir polinomun sabit katsayısı olarak belirlenir. Polinom ifadesi (1)'de verilmektedir. Seçilecek olan gizli verinin tanımlı olması gerektiği aralık p değeri ile belirlenir, $s \in (0, p-1]$. Seçilecek olan p değeri asal sayı olmak zorundadır. Geri dönüş esnasında tek bir çözüm elde edilmesi ihtimalini kesinleştirmek için p değerinin asal olarak seçilme zorunluluğu vardır. Polinoma ilişkin katsayı değerleri, $(a_1, a_2, \cdots, a_k)$, rasgele belirlenir.

$$P(x) = \left(S + a_1 x + a_2 x^2 + \cdots + a_{k-1} x^{k-1}\right) \bmod p \qquad (1)$$

$I_1, \cdots, I_n$ olarak gösterilen pay değerleri polinomun farklı x değerlerinde üretmiş olduğu y değerlerinden oluşmaktadır, $I_i = P(x_i), 1 \le i \le n$. Seçilen x değerlerinin birbirinden farklı olması gerekmektedir. Gizli verinin 7 olması ve eşik şemasının (3, 8) olması durumunda yapılandırılacak olan polinom $f(x) = \left(7 + 19x + 21x^2\right) \bmod 31$ şeklindedir. Polinom ikinci dereceden olup, sabit terim hariç diğer katsayıları rasgele seçilmiştir. Polinom tanımlamasında kullanılan asal değer ise, gizli verinin tanımlı olduğu aralığı kapsayacak en büyük asal sayı değeridir. Verilen örnek şema için Shamir'in şemasının geometrik anlamı Şekil 1'de verilmektedir.



Şekil 1. Shamir'in yönteminin (3, 8) şeması için gösterimi

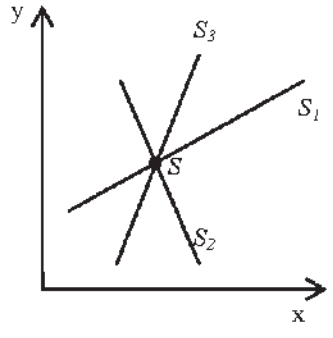
B. *Blakley'in Eşik Şeması*

Blakley'in önermiş olduğu sır paylaşım şemasında, gizli veri GF_q^k vektör uzayında bir elemandır [4]. Katılımcılara dağıtılacak olan paylar ise (2) ile ifade edilen ve gizli veriyi barındıran (k-1) boyutlu hiper düzlemlerdir.

$$\left\{(x_1, \cdots, x_k) \in GF_q^k \,\middle|\, \alpha_1 \cdot x_1 + \cdots + \alpha_k \cdot x_k = \beta\right\} \qquad (2)$$

$\alpha_1, \cdots, \alpha_k, \beta$ değerleri GF_q alanının elemanlarıdır ve pay değerlerini tanımlamada kullanılır. Gizli veri herhangi k payın kesişmesi sonucu yeniden yapılandırılmaktadır. Şekil 2'de (2, 3) eşik şemasının geometrik anlamı gösterilmiştir. Böyle bir şema için katılımcılara gönderilecek olan pay değerleri iki boyutlu uzaydaki doğru denklemleri ile ifade edilir.

Dağıtıcı kişi tarafından, gizli verinin temsil ettiği noktayı kesen n adet doğru denklemi üretilir. Verilen örnek için S ile gösterilen noktayı kesen üç farklı doğru oluşturulmuştur. Doğruları ifade eden katsayılar ise katılımcılara pay değeri olarak gönderilir. Herhangi iki kişinin bir araya gelmesi ile iki doğrunun kesiştirilmesi sonucu gizli veri yeniden yapılandırılır. Blakley'in önermiş olduğu şema mükemmel sır paylaşım şeması özelliği taşımamaktadır. Çünkü k katılımcıdan daha az kişinin bir araya gelmesi, gizli verinin üzerinde yer aldığı doğru denkleminin elde edilmesine sebep olmaktadır. Fakat gizli verinin, bir noktanın yalnız tek bir koordinatı olarak seçilmesi durumunda, bilgi oranı etkilense dahi şema mükemmel hale getirilebilir. Verilen örnekte bir katılımcı, gizli verinin, kendi pay değerinin göstermiş olduğu doğru üzerindeki bir nokta olduğunu bilmektedir.



Şekil 2. Blakley'in yönteminin (2, 3) eşik şeması için gösterimi

C. Asmuth-Bloom'un Eşik Şeması

Asmuth ve Bloom'un 1983'de önerdiği eşik şeması yöntemi de, özel sıralı tamsayıların kullanımına dayanır [5]. Aralarında asal n+1 asal sayı $p_0, p_1 < p_2 < \cdots < p_n$ (3)'te verilen koşulu sağlayacak şekilde seçilmektedir.

$$p_0 \cdot \prod_{i=0}^{k-2} p_{n-i} < \prod_{i=1}^{k} p_i \qquad (3)$$

Katılımcıların kendileri ile ilişkili asal değerleri bilmesi, şemanın düzgün çalışabilmesi için gereklidir. Gizli veri S, Z_{p_0} kümesinin bir elemanı olmak zorundadır. Katılımcılara gönderilecek olan pay değerleri $I_i = (S + \alpha \cdot p_0) \bmod p_i, 1 \le i \le n$ denklik ifadesi kullanılarak hesaplanır. Şemanın rasgeleliğini sağlayan α değeri $S + \alpha \cdot p_0 \in \mathrm{Z}_{p_1 \cdots p_k}$ şartını sağlayacak şekilde seçilir. Yeniden yapılandırma esnasında, herhangi k tane pay değeri, ÇKT yardımıyla gizli verinin elde edilmesinde kullanılmaktadır.

D. Mignotte'nin Eşik Şeması

Mignotte, önermiş olduğu sır paylaşma yönteminde, Mignotte'nin sırası olarak adlandırılan sıralı tamsayıları kullanmıştır [6]. (k, n) eşik şeması için birbirleri arasında asal olan n tamsayı $p_1 < p_2 < \cdots < p_n$, $\prod_{i=0}^{k-2} p_{n-i} < \prod_{i=1}^{k} p_i$ koşulunu sağlayacak şekilde belirlenir. Gizli veri S, $\beta < S < \alpha$ aralığında bir sayı olmak zorundadır. α değeri en küçük k sayının çarpımına karşı düşerken $\alpha = \prod_{i=1}^{k} p_i$, β değeri en büyük k-1 sayının çarpımına eş değerdir $\beta = \prod_{i=0}^{k-2} p_{n-i}$. Pay değerleri $I_i = S \bmod p_i, 1 \le i \le n$ denklik ifadesi yardımıyla belirlenir. Yeniden yapılandırma esnasında herhangi k adet pay değerinin bir araya gelmesi, gizli verinin yeniden yapılandırılması için yeterli olmaktadır. (4)'te verilen denklik sisteminin çözümünde ÇKT kullanılır.

$$\begin{cases} x \equiv I_{i_1} \bmod p_{i_1} \\ \quad \vdots \\ x \equiv I_{i_k} \bmod p_{i_k} \end{cases} \qquad (4)$$

Gizli veri $S < \alpha$ olduğu için, $\mathrm{Z}_{p_{i_1} \cdots p_{i_k}}$'de tanımlıdır. Yalnızca k-1 pay değerinin yeniden yapılandırmada kullanılması durumunda $I_{i_1}, \cdots, I_{i_{k-1}}$, elde edilen denklik ifadesi $S \equiv x_0 \bmod p_{i_1} \cdots p_{i_{k-1}}$ şeklinde olur. x_0 değeri $\bmod p_{i_1} \cdots p_{i_{k-1}}$ tabanındaki tek çözümdür.

III. Eşik Şemalarının Gizli Görüntü Paylaşımında Kullanımı

Bu bölümde var olan eşik şemalarının, gizli görüntü paylaşımı alanına uyarlanması esnasında irdelenecek olan durumların üzerinde durulacak ve tasarlanmaları gerçekleştirilecektir.

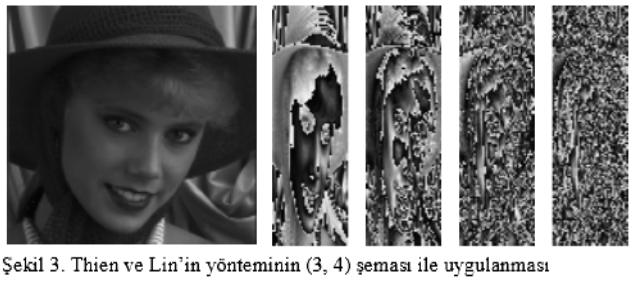
A. Shamir'in Yönteminin GGP'de Kullanımı

2002 yılındaki çalışmanın ardından, literatürde birçok araştırmacı, gizli görüntülerin paylaşımında Shamir'in yönteminden faydalanmıştır [7-10]. Yalnız önerilen yöntemler, Shamir'in şemasındaki polinomu oluştururken katsayıları belirleme şekillerine göre farklılıklar göstermektedir. (1)'de verilen polinom ifadesinde, Shamir'e göre, yalnızca sabit terim gizli veriyi barındırmakta kullanılmaktadır. Diğer terimler ise rasgele olarak seçilmektedir. Fakat 2002 yılındaki çalışmada, polinomun bütün katsayıları gizli görüntü piksel değerlerini kodlamada kullanılmıştır [2]. Katılımcılarla ilişkilendirilmiş olan x değerlerinin sabit olması sebebi ile, üretilen pay görüntülerinde gizli görüntüye benzerlikler vardır. Şekil 3'te verilen gizli görüntünün Shamir'in polinomundaki bütün katsayıların kullanımı ile paylaştırılması sonucu elde edilen pay görüntüleri verilmektedir. Şekilden de gözlemlenebileceği gibi, pay görüntüleri gizli görüntü hakkında bilgi açığa çıkarmaktadır. Thien ve Lin, pay görüntülerindeki benzerliği ortadan kaldırabilmek amacıyla gizli görüntünün

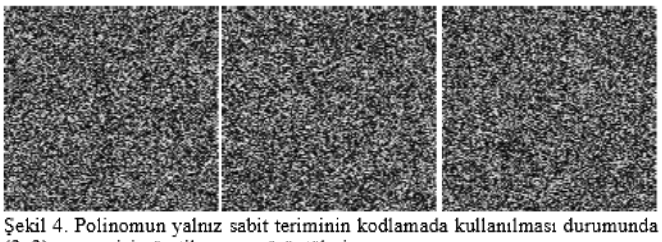
paylaştırılmadan önce permüte edilmesini önermişlerdir. Permütasyon algoritmasının bir anahtar değeri ile kullanılacak olması, sistemin güvenliğini tehlikeye atacaktır.

Polinomun bütün katsayı değerlerini kullanan çalışmanın, permütasyona ihtiyaç duyması sebebi ile son yıllarda yapılan çalışmalar yalnızca sabit değeri gizli veriyi saklamada kullanmaktadır [7-8, 10]. Polinomun sabit teriminin gizli veriyi barındırması durumunda üretilen pay görüntüleri Şekil 4'te verilmiştir. Şekilden de gözlemlenebileceği gibi üretilen pay görüntüleri gizli görüntü hakkında herhangi bir bilgi açığa çıkarmamaktadır.

Literatürde her iki yöntemi de uygulayan farklı şemalar mevcuttur [7-10]. Polinomun tüm katsayılarının kodlamada kullanılması üretilen pay görüntü büyüklüğünün $1/k$ oranında küçülmesini sağlamaktadır. Yalnız üretilen pay görüntülerinin rasgeleliğini sağlamak gerekir. İkinci yöntemin kullanılması durumunda ise, pay görüntülerinin rasgeleliği sağlanmış olacak fakat üretilen görüntü büyüklüğü gizli görüntüye eşit olacaktır.



Şekil 3. Thien ve Lin'in yönteminin (3, 4) şeması ile uygulanması



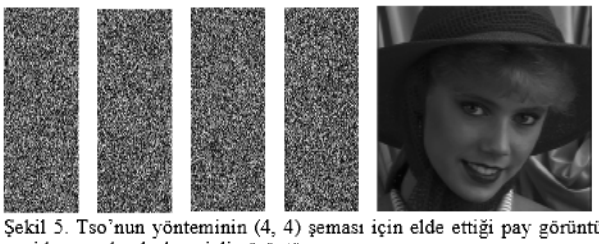
Şekil 4. Polinomun yalnız sabit teriminin kodlamada kullanılması durumunda (3, 3) şeması için üretilen pay görüntüleri

Shamir'in yöntemine dayanan şemaların kodlama esnasında kullandıkları bir diğer yöntem ise, pay görüntüsünü m tabanına çevirmek ve ardından üretilen vektörü, her biri k adet sayıdan oluşan bölümler şeklinde değerlendirmektir. Bu durumda polinomun üretilmesinde kullanılan asal sayı m'den büyük ilk asal sayıdır. Pay değerlerini ifade etmekte kullanılan bit sayısının azalması her ne kadar genişleme oranı probleminin üstesinden gelecek olsa da, sistemin güvenliğini tehlikeye atmaktadır. Gizli görüntüyü ifade etmekte kullanılan m değerinin 17 ve Shamir'in polinomundaki asal değerin de 17 olarak seçilmesi durumunda, herhangi k-1 adet pay değeri kullanılarak gizli görüntünün elde edilme olasılığı $17^{-\lceil \log_{17} 255 \rceil (MN)/(k)}$ şeklindedir. İfadeden de gözlemlenebileceği gibi, pay değerini temsil eden bit sayısını azaltırken aynı zamanda sistemin güvenliğinden ödün verilmektedir.

B. *Blakley'in Yönteminin GGP'de Kullanımı*

Literatürdeki yöntemler çoğunlukla Shamir'in yöntemini kullanırken, 2008 yılında yapılan iki çalışma Blakley'in yöntemini gizli görüntü paylaşımı alanına adapte etmeye çalışmıştır [11, 12]. Her iki yöntemin de paylaştırma adımı esnasında uyguladığı farklı stratejiler ve dolayısıyla elde ettikleri farklı kazanımlar mevcuttur.

Tso çalışmasında gizli görüntüyü paylaştırmadan önce b ile verilen rasgele bir sayı ile kuantalamaktadır [12]. Kuantalama işleminin ardından görüntü permüte edilir ve her biri k pikselden oluşan bölümlere ayrılır. Her bir bölüm $\alpha_1 \cdot x_1 + \cdots + \alpha_k \cdot x_k = \beta$ ile gösterilen k boyutlu uzaydaki düzlemin $(\alpha_2, \alpha_3, \cdots, \alpha_k, \beta)$ katsayılarını belirlemede kullanılır. Katılımcılarla önceden ilişkilendirilmiş sabit x değerleri kullanılarak üretilen farklı α_1 değerleri katılımcılara gönderilecek olan pay değerlerini oluşturur. Tso'nun önermiş olduğu çalışmada permütasyona ihtiyaç duyulmasının sebebi, katılımcılarla ilişkilendirilmiş sabit x değerlerinin olmasıdır. Tso'nun yönteminin Şekil 3'te verilen gizli görüntü'nün (4, 4) şeması kullanılarak paylaştırılması sonucu elde edilen pay görüntüleri Şekil 5'te verilmektedir. Şekilden de gözlemlenebileceği gibi, üretilen pay görüntüleri, eşik değerinin 4 olarak seçilmesinden dolayı, gizli görüntünün $1/4$'ü büyüklüğündedir. Pay görüntülerinin dördünün de kullanılmasıyla elde edilen gizli görüntü de yine Şekil 5'te verilmektedir. Yeniden yapılandırılan görüntünün PSNR değeri yaklaşık olarak 45 dB civarındadır. Gizli görüntüdeki böyle bir bozulma, paylaştırma esnasında kullanılan kuantalama işleminden kaynaklanmaktadır. Yöntemle ilgili bir diğer problem ise sabit x değerlerinin önceden katılımcılara gönderilecek olmasıdır. Böyle bir iletimin de güvenli ağ trafiğinin kullanımı ile gerçekleştirilmesi gerekmektedir.



Şekil 5. Tso'nun yönteminin (4, 4) şeması için elde ettiği pay görüntüleri ve yeniden yapılandırılan gizli görüntü

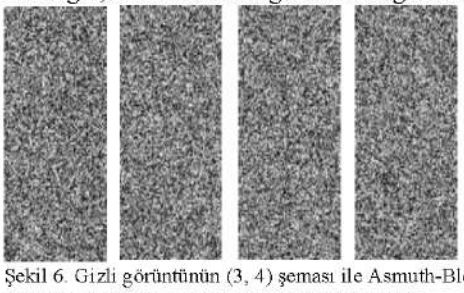
Chen vd.'nin önermiş olduğu yöntemde ise gizli görüntü birbiriyle örtüşmeyen k pikselden oluşan bölümlere ayrılmaktadır [11]. Her bir bölümün k boyutlu uzayda bir noktayı temsil ettiği varsayılır. Bu noktayı kesecek şekilde oluşturulan n farklı hiper düzlem denklem katsayıları ise katılımcılara gönderilecek pay görüntülerinde karşılık düşen piksel parlaklık değerlerini oluşturur. Yalnız araştırmacılar k pikselden oluşan bir bölümü kodlarken, k+1 piksel kullanarak genişleme oranı probleminden etkilenmemek için yeni bir yöntem önermişlerdir. Önerdikleri yönteme göre $(\alpha_1, \alpha_2, \cdots, \alpha_k, \beta)$ değerleri, karşılık düşen pay görüntüsündeki k adet piksel tarafından taşınacaktır.

Denklem katsayılarını kodlamada kullanılacak toplan $8k$ bit

vardır. Pay görüntüsünde karşılık düşen ilk $6+2k$ bit β değerini, $\lfloor (8k-(6+2k))/k \rfloor$ bit değeri $(\alpha_1, \cdots, \alpha_{k-1})$ katsayılarını ve $8k-\lfloor (8k-(6k+2))/k \rfloor (k-1)-(6+2k)$bit ise α_k değerini kodlamada kullanılır. Böylece yöntem tarafından oluşturulan pay görüntü büyüklüğü, gizli görüntü büyüklüğü ile aynı olacaktır. Yöntemin, Tso'nun yöntemine kıyasla en büyük avantajları, yeniden yapılandırılan gizli görüntünün hatasız olması ve x değerlerinin iletilmesi için güvenli bir hat gerektirmemesidir. Aynı zamanda pay görüntülerinin rasgeleliğini sağlamak için fazladan bir permütasyon fonksiyonuna da ihtiyaç duymamaktadır. Tso'nun yönteminin avantajı ise üretmiş olduğu pay görüntülerinin gizli görüntüye oranla $1/k$ oranında küçük olmasıdır.

C. Asmuth-Bloom'un Yönteminin GGP'de Kullanımı

Asmuth-Bloom'un sır paylaşım şeması ilk olarak tarafımızdan yapılan çalışmada gizli görüntü paylaşımı alanında kullanılmıştır [13]. Görüntülerin paylaştırılmasından önce aralarında asal n+1 sayının belirlenmesi gerekmektedir. Piksel parlaklık aralığı [0-255] aralığında olduğu için belirlenen asal değerleri [257-511] aralığındadır. Asmuth-Bloom şemasındaki S ve α değerleri, gizli görüntüde karşılık düşen piksel değerleri kullanılarak elde edilir. Yalnız α değeri, Asmuth-Bloom şemasına rasgelelik katan bir parametredir. Bu değerin sabit olarak belirlenmesi durumunda, pay görüntüleri gizli görüntüye benzerlikler içerecektir. Buna engel olabilmek amacıyla, α değerinin üretiminde hem piksel değeri hem de piksel değerinden önceki piksel değerleri yardımıyla belirlenen rasgele bir değerden faydalanılır. Böylece üretilen pay görüntülerinin rasgeleliği sağlanmaktadır. Asmuth-Bloom şemasını kullanan gizli görüntü paylaşım şeması k değerinden bağımsız olarak sabit büyüklükte pay görüntüleri üretmektedir. Aynı zamanda yöntemin kullanabilecek olduğu n değeri de [257-511] aralığı ile sınırlıdır. Şekil 3'te verilen gizli görüntünün, Asmuth-Bloom şeması yardımıyla (3, 4) şeması kullanılarak paylaştırılması sonucu elde edilen pay görüntüleri Şekil 6'da verilmektedir. Şekilden de gözlemlenebileceği gibi pay görüntüleri rasgelelik içermektedir. Görüntü büyüklükleri ise orijinal gizli görüntünün $(9/16)(\cong 0.56)$'sı büyüklüğündedir. Bu değer, kullanılan k değerinden bağımsızdır.



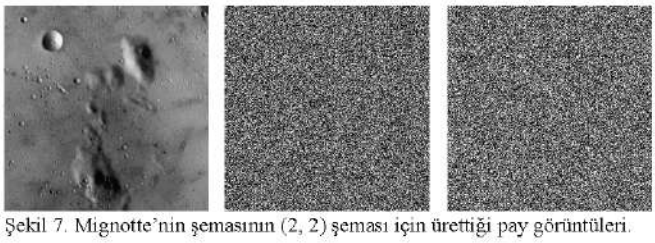
Şekil 6. Gizli görüntünün (3, 4) şeması ile Asmuth-Bloom şeması kullanılarak paylaştırılması sonucu elde edilen pay görüntüleri.

Asmuth-Bloom şemasındaki α parametresi, şemanın gizli görüntü paylaşımı alanına uyarlanması durumunda, Permütasyon fonksiyonuna olan ihtiyacı ortadan kaldıracaktır. Çünkü arka arkaya gelen ve eş değer parlaklık değerine sahip pikseller için bile farklı pay değerleri üretilecektir. Yalnız yöntemin en sorunlu tarafı seçilecek olan asal değerleridir. (3)'te verilen şartın sağlanabilmesi için üretilen pay değerleri 9 bit olmaktadır. Katılımcı sayısı arttıkça asal değerlerin şartı sağlayabilmesi için pay değer aralığının büyütülmesi gerekmekte ve dolayısıyla genişleme oranı artmaktadır.

D. Mignotte'nin Yönteminin GGP'de Kullanımı

Mignotte'nin şemasının gizli görüntü paylaşımında kullanılması durumunda, sıralı ve aralarında asal n adet sayının paylaştırma adımından önce seçilmesi gerekir. Gizli görüntüdeki her bir piksel değeri, şema ile paylaştırılacak olan gizli veriye karşı düşmektedir. S ile gösterilen gizli verinin $\beta < S < \alpha$ aralığına düşmesini garantileyebilmek için, sabit bir değer katsayı olarak kullanılabilir. Sabit değer kullanılması durumunda, pay görüntüleri, gizli görüntüye benzerlikler içerecektir. Buna engel olabilmek amacıyla, yan yana gelen eşit iki piksel değerine karşı farklı pay değerleri üretebilmek için, gizli verinin aralığa düşürülmesi esnasında rasgele bir çarpan kullanılır. Fakat bu durumda pikseller için kullanılan çarpanların karşı tarafta da bilinmesi gerekir. Buna engel olabilmek için [14]'te gerçekleştirilen çalışmada 255'in katı şeklinde çarpanlar eklenmiştir. Alıcı tarafın 255 tabanında modulo alması, eklenen kısmın yok edilmesi için yeterli olacaktır. Mignotte'nin şemasının gizli görüntü paylaşımı alanına uyarlaması ilk olarak 2008 yılında Shyu vd. tarafından gerçekleştirilmiştir. Yalnız bu çalışmanın en önemli problemi, gizli verinin ilgili aralığa düşürülmesi esnasında kullanılan rasgele fonksiyonun ve çekirdek değerinin taraflar arasında önceden belirlenmesi gerektiğidir. [14]'teki çalışmamızda buna engel olunmuş ve tamamen rasgele özellikte pay görüntüleri üretilmiştir.

Şekil 7'de verilen gizli görüntünün (2, 2) şeması kullanılarak paylaştırılması sonucu elde edilen pay görüntüleri verilmektedir. Yumuşak geçişli bir gizli görüntü için bile rasgelelik içeren pay görüntüleri üretilmektedir.



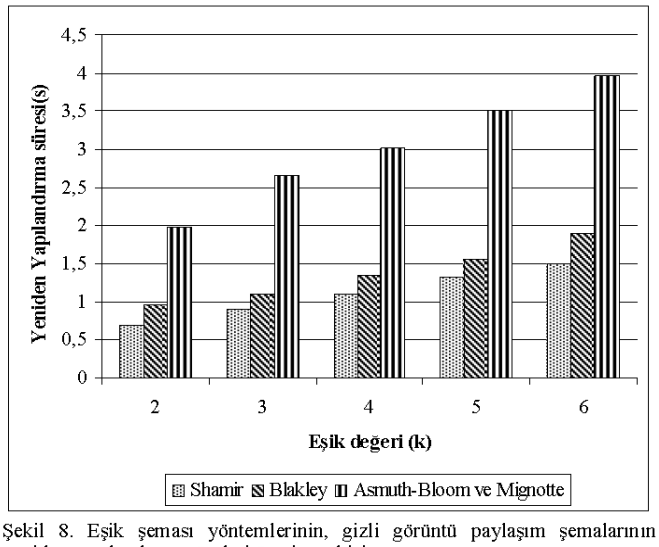
Şekil 7. Mignotte'nin şemasının (2, 2) şeması için ürettiği pay görüntüleri.

Yalnız üretilen pay görüntüleri, gizli görüntü ile birebir aynı büyüklüktedir. Çünkü gizli görüntüdeki her bir piksel değeri pay görüntülerinde bir piksel değeri ile kodlanmaktadır.

IV. Yöntemlerin Genel Olarak Değerlendirilmesi

Shamir'in yöntemini kullanan gizli görüntü paylaşım şemaları ile Asmuth-Bloom ve Mignotte'nin eşik şeması kullanan yöntemler arasındaki en belirgin fark yeniden yapılandırma esnasında yaşanmaktadır. Shamir tabanlı yöntemler, yeniden yapılandırma esnasında Lagrange'ın interpolasyonunu kullanırken, diğer yöntemler ÇKT'ni

kullanmaktadır. Blakley'in yöntemi ise yeniden yapılandırma esnasında lineer denklik sisteminin çözümünü gerçekleştirmektedir. Yeniden yapılandırma süreleri açısından dört yöntemin, gizli görüntü paylaşımında kullanımını değerlendirdiğimizde Şekil 8'deki verilere ulaşılmıştır. Yöntemlerin performans değerlendirmesini yapabilmek amacıyla 128×128 büyüklüğündeki gizli görüntü k=2, 3, 4, 5, 6 değerleri kullanılarak paylaştırılmıştır. Farklı eşik değerlerinde gerek Shamir ve Blakley tabanlı yöntemlerin gerekse ÇKT'ne dayalı yöntemlerin yeniden yapılandırma süreleri ölçülmüştür. Testler sonucunda elde edilen değerler şekilde gösterilmektedir. Şekilden de gözlemlenebileceği gibi hız açısından Shamir ve Blakley tabanlı yöntemler öne çıkmaktadır. Asmuth-Bloom ve Mignotte sır paylaşım yöntemlerinin gizli görüntü paylaşımında kullanımı, pay görüntülerinde karıştırma gerekmeksizin rasgeleliği sağlamasına rağmen işlem zamanı açısından olumlu sonuçlar vermemektedir. Yöntemlerin yeniden yapılandırılan gizli görüntünün doğruluğu, genişleme oranı ve pay görüntülerinin rasgeleliği açısından değerlendirilmesi Tablo 1'de verilmektedir. Shamir'in eşik şemasında, polinomun tüm katsayılarını gizli veriyi kodlamada kullanan yaklaşımlar "Shamir I" olarak adlandırılırken, yalnızca sabit terimi kodlamada kullanan yaklaşımlar "Shamir II" olarak isimlendirilmiştir. Blakley'in yönteminde gizli veriyi k boyutlu uzayda bir nokta olarak kabul eden yöntem "Blakley I", noktayı kesen denklem katsayılarını sabit kabul eden yöntem ise "Blakley II" olarak adlandırılmıştır.



Şekil 8. Eşik şeması yöntemlerinin, gizli görüntü paylaşım şemalarının yeniden yapılandırma süreleri üzerine etkisi.

Shamir ve Blakley tabanlı yöntemlerde yeniden yapılandırılan gizli görüntüde [251-255] aralığındaki piksel parlaklık değerleri kaybedilmektedir. Asmuth ve Mignotte'nin şemalarını kullanan yöntemler ise gizli görüntüyü hatasız olarak yeniden yapılandırabilmektedir. Genişleme oranı açısından baktığımızda, Shamir tabanlı eşik şemasının kullanım şeklinde göre farklı sonuçlar üretilmektedir. Tüm katsayıların gizli görüntüden alınması durumunda genişleme oranı $1/k$ iken aksi durumda 1 olarak rapor edilmektedir. Yalnız genişleme oranındaki kazanım, pay görüntülerinde rasgelelik problemi oluşmasına ve permütasyon kullanılmasına sebep olmaktadır. Blakley'in yöntemini kullanan yöntemlerde ise, paylaştırma algoritmasına göre genişleme oranı değişim göstermektedir.

Asmuth ve Mignotte tabanlı yöntemlerde, genişleme oranı eşik değerinden bağımsız olarak sabittir. Pay görüntülerinin rasgeleliğini sağlamak için Shamir'in yönteminde yalnızca sabit terimi gizli veri saklamada kullanan yöntemler herhangi bir Permütasyon fonksiyonuna ihtiyaç duymazken, tüm katsayıları kullanan yöntemler ise karıştırma fonksiyonu kullanmak zorundadır. Blakley'in yöntemini kullanan Tso'nun çalışması pay görüntülerindeki benzerliği engellemek için karıştırma fonksiyonuna ihtiyaç duymaktadır. Asmuth-Bloom yöntemini kullanan [13]'teki çalışma, α parametresinden rasgeleliği sağlamakta faydalanmaktadır. Mignotte'nin yöntemini kullanan gizli görüntü paylaşım şeması ise, permütasyona ihtiyaç duymamaktadır.

Tablo 1. Yöntemlerin kıyaslanması

	Kodlanabilen piksel parlaklık aralığı	Genişleme oranı	Pay görüntü rasgeleliğinin sağlanması
Shamir I	[0-250]	1/k	Permütasyon
Shamir II	[0-250]	1	--
Blakley I	[0-250]	1	--
Blakley II	[0-250]	1/k	Permütasyon
Asmuth-Bloom	[0-255]	9/16	--
Mignotte	[0-255]	1	--

Sonuç olarak yeniden yapılandırma süresi, genişleme oranı ve önerilen paylaştırma algoritmasının esnekliği açısından bakıldığında, Shamir tabanlı yöntemlerin gizli görüntü paylaşımı alanında daha etkin kullanım alanına sahip olacağı kanaatine varılmaktadır.

KAYNAKÇA

[1] Naor, M. ve Shamir, R., Visual Cryptography, Lecture Notes in Computer Science, 950 (1995) 1–12.
[2] Thien, C. C. ve Lin, J. C., Secret Image Sharing., Computers and Graphics, 26 (2002) 765–770.
[3] Shamir, A., How to Share a Secret, Communications ACM, 22 (1979) 612–613.
[4] Blakley, G. R., Safeguarding Cryptographic Keys, National Computer Conference, Haziran 1979, New York, Bildiriler Kitabı, 313–317.
[5] Asmuth, C. ve Bloom, J., A Modular Approach to Key Safeguarding, IEEE Transactions on Information Theory, 29 (1983) 208–210.
[6] Mignotte, M., How to Share a Secret, Lecture Notes in Computer Science, 149 (1983) 371–375.
[7] Lin, C. C. ve Tsai, W. H., Secret Image Sharing with Steganography and Authentication, Journal of Systems and Software, 73 (2004) 405–414.
[8] Yang, C. N., Chen, T. S., Yu, K. H. ve Wang, C. C., Improvements of Image Sharing with Steganography and Authentication, Journal of Systems and Software, 80 (2007) 1070-1076.
[9] Chang, C. C., Hsieh, Y. P. Ve Lin, C. H., Sharing Secrets in Stego Images with Authentication, Pattern Recognition, 41 (2008) 3130-3137.
[10] Wu, C. C., Hwang, M. S. ve Kao, S.-J., A New Approach to the Secret Image Sharing with Steganography and Authentication, Imaging Science Journal, 57 (2009) 140-151.
[11] Chen, C. C. ve Fu, W. Y., A Geometry Based Secret Image Sharing Approach, Journal of Information Science and Engineering, 24 (2008) 1567-1577.

[12] Tso, H. K., Sharing Secret Images Using Blakley's Concept, Optical Engineering, 47, 7 (2008) 1-3.
[13] Ulutas, M., Nabiyev, V. ve Ulutas, G., A New Secret Image Sharing Technique Based On Asmuth Bloom's Scheme, Application on Information and Communication Technologies, Ekim 2009, Bakü, Bildiriler Kitabı,1-5.
[14] Ulutas, G., Ulutas, M. ve Nabiyev, V., Mignotte'nin Şemasına Dayanan Gizli Görüntü Paylaşma Şeması, Sinyal İşleme ve Uygulamaları, Nisan 2011, Antalya, Bildiriler Kitabı, 291-294.

An Imperceptible Watermarking Scheme based on Double Density Dual-Tree Discrete Wavelet Transform in combination with Singular Value Decomposition

Mary Agoyi and Devrim Seral

Abstract - **Watermarking has been the current solution to Copyright protection and content authentication which has become a major issue in multimedia technology. This study introduces a multimedia watermarking technique based on the combination of double density Dual-Tree discrete wavelet transform (DD-DT-DWT) and singular value decomposition (SVD) method called DD-DT-DWT–SVD. An experiment is carried out to compare Watermarking technique based on DD-DT-DWT–SVD with that of the DWT-SVD. The experimental result shows that watermarking based on DD-DT-DWT–SVD is more imperceptible than watermarking based on DWT-SVD.**

Index Terms - **Watermarking, Discrete Wavelet Transform, Double Density Dual-Tree Discrete Wavelet Transform, Singular Value Decomposition**

I. INTRODUCTION

With the wide use of multimedia technologies and rapid popularity of the Computer and Internet technologies, digital multimedia contents are transmitted via the Internet and other computer technologies. This has lead to different kinds of infringements on the digital contents which include easy access, authorized manipulations, illegal copying, illegal reproduction of original contents and malicious attacks [1]. Digital watermarking is a technology that is known to help protect multimedia contents from illegal copying, manipulation and distribution problems by embedding an information into the digital multimedia content without it been noticed by visual representation [2]. Digital watermarking is grouped into spatial and frequency domain. The spatial domain embeds the watermark into the digital content by pixels modification. Although these technique has low complexity and is easy to implement but it is not robust against attacks and common signal processing operations such as rotating, scaling, cropping, filtering, additive noise and compression.

Manuscript received March 2, 2012.

M. Agoyi is a PhD candidate of Computer Engineering at Cyprus International University, Turkey. (e-mail: magoyi@ ciu.edu.tr).

D. Seral is the Head of Information Systems Engineering Department at Cyprus International University, Turkey. (e-mail: dseral@ciu.edu.tr).

The frequency domain that is similar to spread spectrum communication embeds the watermark by modification of the magnitude coefficient of the digital content according to the embedding algorithm. Though the frequency domain watermarking has higher computational cost but it has proven to be more robust and imperceptible than the spatial domain watermarking [3]. Currently the discrete wavelet transform (DWT), discrete cosine transform (DCT) and the discrete Fourier transform (DFT) are the commonly used frequency domain watermarking, but the DWT is most widely used due to its frequency spread, multi resolution ability and the spatial localized nature of its wavelet [4]. Despite the advantages of DWT, it major drawbacks it that DWT is not shift invariant, small shift in the input signal can lead to variations in the distribution of energy at different scales between the coefficients of the DWT. The wavelets filters are also separable and real causing a poor directional selectivity for diagonal features [5]. In other to overcome this shortcoming double density Dual Tree discrete (DD-DT-DWT) wavelet transform can be used. Double density dual tree DWT processes the properties of double density DWT and dual tree complex DWT. It is based on FIR perfect construction filter banks. It is nearly shift invariant which solves the problem of wavelet coefficients oscillation around singularities [6]. A combination of DD-DT-DWT with singular value decomposition (SVD) can provide a better transparency and robustness. SVD thence to achieve better transparency and robustness since slight variations of singular value does not affect the visual perception of the cover image [1].

II. BACKGROUND REVIEW

A. *DD-DT-DWT*

The Double density Dual-Tree DWT structure consists of two over sampled iterated filter bank operating in parallel and it transform is based on two scaling functions and four distinct wavelets. It processes the properties of double density DWT and Dual Tree Complex DWT [6]. The Double density DWT is based on single scaling function and two distinct wavelets. A

half is the offset factor from one wavelet to the other. The translation of one wavelets integer fall midway between the translation of the other wavelets integer [7], as expressed in (1)

$$\psi_2(t) \approx \psi_1(t-0.5) \quad (1)$$

The Dual Tree Complex DWT (DT-CWT) uses two trees of real filters to generate the real and imaginary parts of the wavelet coefficients separately [8][9]. It has Gabor-like complex value wavelets. This is usually obtained by the conducting of two DWT filter banks in parallel as the real and imaginary parts of a complex transform. The wavelet corresponding to each of the two DWTs form an appropriate Hilbert transforms pair [7] of the form of (2).

$$\psi_g(t) \approx H\{\psi_h(t)\} \quad (2)$$

The DT-CWT introduces limited redundancy and allows the transform to provide appropriate directionally selective filters while preserving the usual properties of perfect reconstruction and efficient computation upon the embedding algorithm. [10]. Both the double density DWT and the dual tree complex DWT are based on FIR perfect construction filter banks and they are nearly shift invariant. There development was motivated by a part of undecimated DWT and special properties of complex wavelet transform respectively. They both outperform the critically sampled DWT in several signal processing applications [11]

B. SVD

In SVD transformation, an image of n x n can be decomposed into three matrices that are of the same size as the original image. Let I be an image then the SVD of I can be given as (3)

$$[U\ S\ V] = \text{SVD}(I)$$
$$I = USV^T \quad (3)$$

Where U and V are the orthogonal matrices with small singular value and S is a diagonal matrix with the larger singular value entries of the image [1].

The three main properties of SVD in digital image processing scheme are that:

1) When a small perturbation is added to an image it singular values do not change significantly due to the stability property of the singular value.
2) Pairs of singular vectors specify the geometry of the image and the singular value specifies the luminance of an image layer.
3) The intrinsic algebraic image properties is represented by the singular values [12]

III. THE PROPOSED APPROACH

The proposed DD-DT-DWT-SVD watermarking scheme is given as follows

A. Watermarking embedding

1) Apply DD-DT-DWT to the original image I to decompose it into sub bands. As given in (4)

$$[\text{HH HL LH LL}] = \text{DD-DT-DWT(I)} \quad (4)$$

Where HH is the high-high frequency band, HL is the high-low frequency band, LH is the low-high frequency band, and LL is the low-low frequency band.

2) Apply SVD to HH as given in (5)

$$[U_1 S_1 V_1] = \text{SVD}(HH)$$
$$HH = U_1 S_1 V_1^T \quad (5)$$

Where U1 and V1 are the orthogonal matrixes of the decomposed high frequency band image and S1 is the diagonal matrix with the higher entries of the decomposed high frequency band of the original image.

3) Apply SVD to the watermark image as given in (6)

$$[U_2 S_2 V_2] = \text{SVD}(W)$$
$$W = U_2 S_2 V_2^T \quad (6)$$

Where U2 and V2 are the orthogonal matrixes of the watermark image and S2 is the diagonal matrix with the higher entries of the watermark image.

4) Modify the singular value of the decomposed original image with the singular value of the watermark image using a scaling factor α, which controls the strength of the watermark to be inserted. This is given in (7)

$$S_3 = S_1 + \alpha S_2 \quad (7)$$

5) The high frequency band of the decomposed image is modified thus given as (8)

$$HH_2 = U_1 S_3 V_1^T \quad (8)$$

6) Inverse DD-DT-DWT (IDD-DT-DWT) is applied to the decomposed image, using the modified high

frequency band HH2 instead of HH as shown in (9) to give the watermarked image

$$I = \text{IDD-DT-DWT}(HH_2\ HL\ LH\ LL) \quad (9)$$

B. Watermarking extraction

1) Apply DD-DT-DWT to the watermarked image W to decompose it into sub bands. As given in (10)

$$[HH_W\ HL_W\ LH_W\ LL_W] = \text{DD-DT-DWT}(W) \quad (10)$$

Where HHw is the high-high frequency band, HLw is the high-low frequency band, LHw is the low-high frequency band, and LLw is the low-low frequency band of the decomposed watermarked image.

2) Apply DD-DT-DWT to the original image to decompose it into sub bands. As given in (11)

$$[HH\ HL\ LH\ LL] = \text{DD-DT-DWT}(I) \quad (11)$$

3) Apply SVD to the high frequency band of the decomposed image as given in (12)

$$[U_1 S_1 V_1] = \text{SVD}(HH)$$
$$HH = U_1 S_1 V_1^T \quad (12)$$

Where U1 and V1 are the orthogonal matrixes of the decomposed high frequency band image and S1 is the diagonal matrix with the higher entries of the decomposed high frequency band of the original image.

4) Apply SVD to the high frequency band of the decomposed watermarked image as given in (13)

$$[U_4 S_4 V_4] = \text{SVD}(HH_w)$$
$$HH_w = U_4 S_4 V_4^T \quad (13)$$

Where U4 and V4 are the orthogonal matrixes of the decomposed high frequency band image and S4 is the diagonal matrix with the higher entries of the decomposed high frequency band of the watermarked image.

5) Apply SVD to the watermark image as given in (14)

$$[U_2 S_2 V_2] = \text{SVD}(W)$$
$$W = U_2 S_2 V_2^T \quad (14)$$

Where U2 and V2 are the orthogonal matrixes of the watermark image and S2 is the diagonal matrix with the higher entries of the watermark image

6) Subtract the singular value of the decomposed original image form the singular value of the watermarked image and divide the values by the scaling factor α to obtain the singular value of the watermark image. This is given in (15)

$$S_5 = (S_4 - S_1)/a \quad (15)$$

7) Combining the singular values of the watermark image using the S5 (which was obtained in step 6) instead of S2 gives the extracted watermark image as given in (16).

$$W_2 = U_2 S_5 V_2^T \quad (16)$$

Where W2 is the extracted watermark image

IV. PERFORMANCE EVALUATION

In order to evaluate the performance of the proposed scheme, imperceptibility is chosen as the evaluation metrics. Watermarking algorithms are usually evaluated with respect to robustness and imperceptibility [13].

Imperceptibility

Imperceptibility is the measure of the quality of the watermarked image. The original image should not be distorted by the presence of the watermark or any kinds of attack [14]. These attacks may include some signal processing operations such as blurring, Gaussian noise, cropping, rotations, salt & pepper noise, contrast adjustment, sharpening, and histogram equalization [15].

To measure the imperceptible capability the peak signal to noise ratio (PSNR) can be used to measure the degradation caused by the watermarked effect [16]. The PSNR, which is measured in decibels, defines the resemblance between an original image and the reconstructed image. The higher the PSNR values of the reconstructed image the closer the resemblance of the reconstructed image to the original image [17].

The PSNR in decibels (dB) of the original image I(s) and the watermarked image W(s) can be calculated using (13)

$$PSNR_{dB} = 10\log\left(\frac{\text{MAX}^2}{MSE}\right) \quad (13)$$

Log is logarithm base 10. MAX is the maximum possible pixel value of the image and MSE is the mean square error [16]. MAX for a gray scale image with

eight bits per pixel is 255. The MSE is the average of the pixel difference between two images [17]. The MSE can be defined as given in (14) below.

$$MSE = \frac{1}{S}\sum_{1}^{s}\left(I(s) - W(s)\right)^2 \qquad (14)$$

Where I(s) is the original image before watermarking and W(s) is the watermarked image.

V. EXPERIMENTAL RESULTS

Several experiments were conducted using a grey scale-level image "Barbara" and a "pepper" image. The "Barbara" and "pepper" images are used as the cover and the watermark image respectively. These images are shown in Fig 1-a and Fig 1-b below



Fig 1-a: Original image Fig 1-b watermark image

The visual quality of the watermarked image for DD-DT-DWT-SVD watermarking technique is compared with that of the watermarked image of DWT-SVD watermarking technique by measuring the PSNR values of the Watermarked image for both algorithms. The watermarked image and their PSNR values for DWT-SVD algorithm and DD-DT-DWT-SVD algorithm is given in Fig 2.



Fig 2 DWT-SVD and DD-DT-DWT-SVD Watermarked

It can be seen form Fig 2 that the PSNR value for DD-DT-DWT-SVD watermarking algorithm is higher than that of the DWT-SVD making DD-DT-DWT-SVD watermarking algorithm a better approach in term of visual quality perception.

In order to further test the imperceptibility of each algorithm, different kinds of attacks are applied to the watermarked images and the PSNR values of the attacked images are measured corresponding to the original images. The various attacks applied to the watermarked images are rotation, histogram equalization, salt & pepper noise, Gaussian noise, blurring, sharpening and contrast adjustment.

The PSNR values corresponding to various attacks on watermarked images are summarized in Table 1.

Table 1: PSNR and CC values for different types of attack for various algorithms

OPERATION		DWT-SVD	DD-DT-DWT-SVD
Watermarked		**56.25**	**74.21**
ATTACKS	Rotation 90°	29.95	30.65
	Rotation 180°	28.52	29.20
	Hist. Equalization	42.08	43.74
	Salt & pepper	37.53	39.09
	Gaussian noise	48.44	49.97
	Blurring	61.90	64.66
	Sharpening	47.32	54.45
	Contrast Adjustment	50.40	51.49

For proper representation, the images of the attacked watermarked images and their corresponding PSNR values for DWT-SVD are given in Fig 3-a and that for DD-DT-DWT-SVD are given in Fig. 3-b.

Data's in Table 1 and the figures in Fig 3-a and Fig 3-b shows that the DD-DT-DWT-SVD watermarking algorithm offers considerably higher PSNR values for almost all the signal processing operations as compared with DWT-SVD watermarking algorithms. Hence DD-DT-DWT-SVD watermarking algorithm is more imperceptible than DWT-SVD watermarking algorithms.

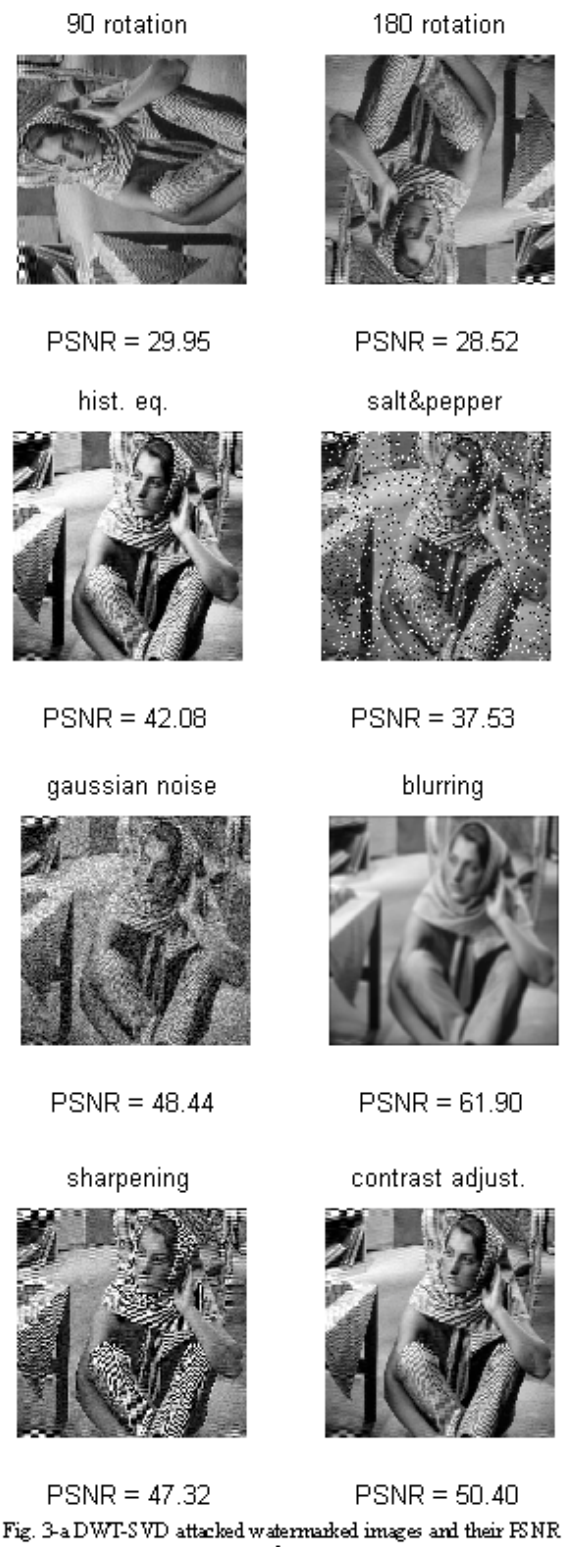


Fig. 3-a DWT-SVD attacked watermarked images and their PSNR values

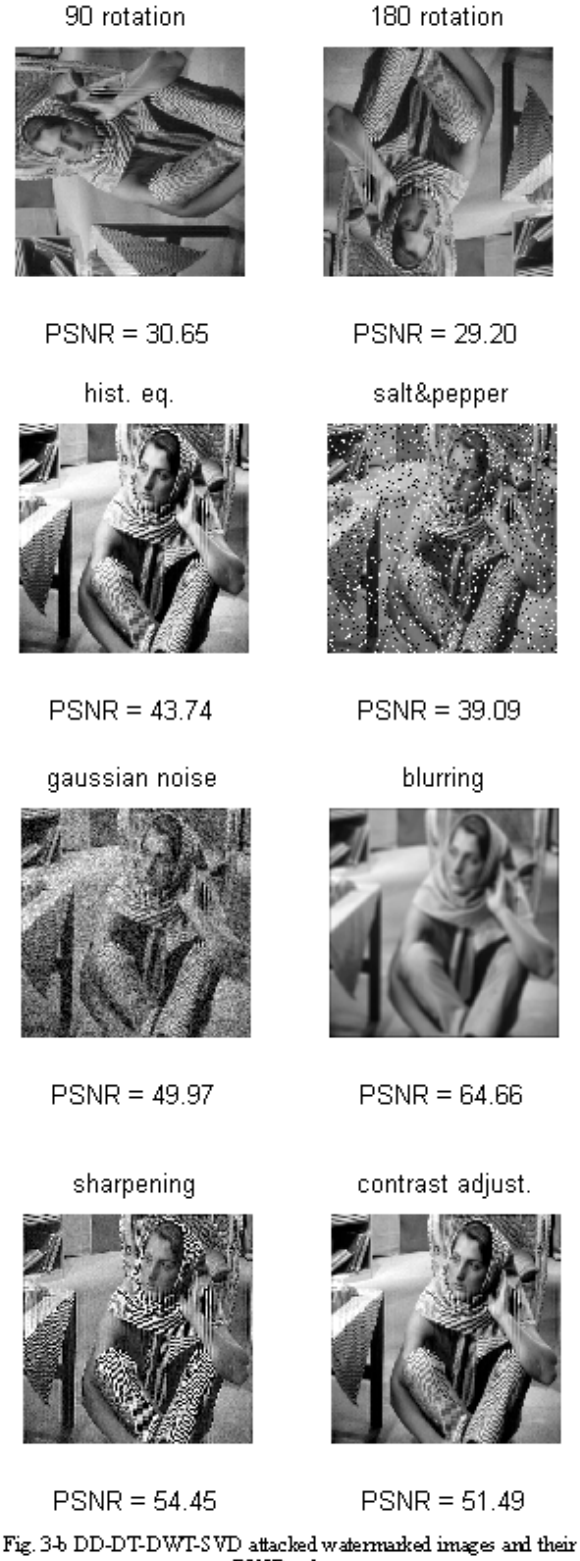


Fig. 3-b DD-DT-DWT-SVD attacked watermarked images and their PSNR values

VI. CONCLUSION

In this paper, a hybrid watermarking technique based on Double density Dual-Tree discrete Wavelet Transform and singular value decomposition has been presented. The experimental result shows that DD-DT-DWT-SVD provides better perceptibility in various signal processing operations as compared to DWT-SVD watermarking algorithms.

REFERENCES

[1] Chih-chin Lai and Cheng-chih Tsai, digital image watermarking using discrete wavelet transform and singular value decomposition, IEEE transactions on instrumental and measurement, vol. 59, no. 11, Nov 2010

[2] Lama Rajab, Tahani Al-Khatib, and Ali Al-Haj, " Video Watermarking Algorithms Using the SVD Transform", European Journal of Scientific Research Vol.30 No.3 ,2009, pp.389-401

[3] B. Chandra Mohan, and S. Srinivas Kumar, A Robust Image Watermarking Scheme using Singular Value Decomposition, Journal of Multimedia, vol. 3, no. 1, May 2008

[4] Say Wei Foo, and Qi DongWorld , "A Normalization-based Robust Image Watermarking scheme using SVD and DCT", International Journal of Information and Communication Engineering, vol.6, Is.4, 2010

[5] N. G. Kingsbury, "Shift invariant properties of the dual tree complex wavelet transform", In: Proc. IEEE ICASSP'99, IEEE Pres. New Jersey, 1999

[6] T. Kumaran and P, Thangavel, "genertic algorithm based watermaking in double density dual tree DWT,proceeding of 2008 International conference on wavelet analysis and pattern recognition, Hong Kong, 2008

[7] Phuong Pham, Li Yu, and Minh Nguyen, "Applying The Dual Tree Complex DWT and Double density DWT for mass Spectrometry feature Extraction and classification", in Bioinformatics and Biomedical Technology (ICBBT), April 16-18, 2010, pp.394-399

[8] Ivan W. Selesnick, Richard G. Baraniuk, and Nick G. Kingsbury, "the dual-tree complex wavelet transform IEEE Signal Processing Magazine, 2005

[9] Sathesh And Samuel Manoharan, A Dual Tree Complex Wavelet Transform Construction And Its Application To Image Denoising, International Journal of Image Processing (IJIP) Volume (3), Issue (6), pp 293-300

[10] S. K. Muttoo, and Sushil Kumar, "A multilayed secure, robust and high capacity image steganographic algorithm", world of computer and information technology journal, vol. 1,No. 6 pg 239-246, 2011

[11] Ivan W. Selesnick. "The Double density Dual-Tree DWT", IEEE Transactions on signal processing, vol. 52, No. 5, may 2004.

[12] Liu Liang and Sun Qi, A new SVD-DWT composite watermarking, ICSP 2006 proceedings

[13] Ejima, M and A. Myazaki, "On the evaluation of performance of digital watermarking in the frequency domain", IEEE International conference on image processing, 2001, pp 546-549

[14] Ali Al-haj, combined DWT-DCT digital image watermarking, journal of computer science, 2007, vol. 3 No. 9, pp 740-746

[15] V.Santhi and A.Thangavelu, "DC Coefficient Based Watermarking Technique for color Images using Singular Value Decomposition", International Journal of Computer and Electrical Engineering, 2011, vol. 3, No. 1, pp 1793-8163

[16] Chunlin Song, Sud Sudirman, Madjid Merabti and David Llewellyn-Jones, "Analysis of Digital Image Watermark Attacks", in Consumer Communications and Networking Conference (CCNC), Jan. 9-12, 2010, pp.1-5

[17] D. Salomon, "Data Compression: the complete reference", Springer, London. 2007, pp.279- 282

[18] Bum-Soo Kim et al, "Robust digital image watermarking method against geometrical attacks", Real-Time Imaging, 9 (2003), pp. 139–149

Mary Agoyi is currently a PhD candidate of Computer Engineering at Cyprus International University. She holds Bsc Physics from Benue state university Nigeria and MSc Information Systems Engineering from Cyprus International University. Her field of interest includes Telecommunication, Networking and Network Security.

Devrim Seral received his undergraduate degree from Faculty of Technical Education (Now Faculty of Technology) Gazi University – Ankara. He received Master of Science degree in 2000 and PhD degree in 2007 from the Institue of Science, Gazi University – Ankara. While studying for his PhD, he was also working in the IT Sector as a System and Internet Engineer. He joined the Faculty of Engineering of Cyprus International University in 2007, where he is presently working as a Lecturer and Head of Department Information Systems Engineering.

Dr. Seral research fields are Operating Systems, Network Load Balancing, Network Security, Computer Security and Mobile computing. He is also a member of IEEE and Association for Computing Machinery.

Rasgele Seçilen S-kutularını Temel Alan Blok Şifrelerin Diferansiyel Kriptanalizi

Fatih ÖZKAYNAK, Ahmet Bedri ÖZER, Sırma YAVUZ

Özet—**Diferansiyel kriptanaliz blok şifreleme sistemlerine uygulanan ilk önemli saldırı tekniklerinden biridir. Birçok şifreleme algoritmasının güvenlik analizi yapılırken bu saldırı tekniği göz önüne alınmaktadır. Ancak birçok kriptanalist şifreleme mimarisinin statik yapısından yararlanarak daha küçük versiyonları üzerine yoğunlaşmakta ve şifreleme sistemi hakkında genel bir ifade elde etmeye çalışmaktadır. Bu çalışmada şifreleme sisteminin statik yapısından kaynaklanan problemleri gidermek için şifreleme mimarisinin her bir adımında rasgele seçilen farklı s-kutusu yapılarını kullanan yeni bir algoritma önerilmiştir. Rasgele yapı içerisinde kullanılmak üzere oluşturulan s-kutusu yapıları kriptolojik olarak benzer özellikler göstermektedir. Bir başka deyişle birbirine eşdeğer şifreleme mimarileri oluşturulmuştur. Oluşturulan s-kutusu yapıları içerisinden seçim işleminin yapılması sürecinde ise kaos teorisinden faydalanılmıştır. Bu işlem ile şifreleme sisteminin analizi daha zorlaştırılmıştır. Teorik analizler ve bilgisayar simülasyonları önerilen yeni algoritmanın diferansiyel kriptanalize karşı daha dirençli olduğunu göstermiştir.**

Abstract—**Differential cryptanalysis is one of the first important attack techniques applied to block encryption systems. This attack technique is taken into consideration while performing security analysis of several encryption algorithms. However, several cryptanalyst in this technique concentrates on the smaller versions by making use of static structure of encryption architectures and tries to obtain a general expression about encryption system. In this study; a new algorithm which uses different s-box structures selected randomly at each step of encryption architecture, is proposed to eliminate the problems arising from static structure of encryption system. S-box structures which are formed to be used within random structure cryptographically exhibit similar features. In other words, encryption architectures equivalent to each other were formed. Chaos theory was used during the period of selection process among the formed s-box structures. The analysis of encryption system was made more difficult with this process. Theoretical analysis and computational simulations showed that the proposed, new algorithm is more resistant to differential cryptanalyses..**

Index Terms—**block ciphers differential cryptanalysis, randomly selected s-boxes, chaos.**

Fatih ÖZKAYNAK, Fırat Üniversitesi Yazılım Mühendisliği Bölümü 23119 Elâzığ, Türkiye (telefon: +904242370000/4227, faks: +904242367064; e-mail: ozkaynak@firat.edu.tr).

Ahmet Bedri ÖZER, Fırat Üniversitesi Bilgisayar Mühendisliği Bölümü, 23119 Elazığ, Türkiye (e-mail: bedriozer@firat.edu.tr).

Sırma YAVUZ, Yıldız Teknik Üniversitesi Bilgisayar Mühendisliği Bölümü 34349 İstanbul, Türkiye (sirma@ce.yildiz.edu.tr).

I. GİRİŞ

BLOK şifreleme algoritmaları modern kriptolojinin en temel yapı taşlarından biridir [1, 2]. Gürbüz bir blok şifreleme algoritması Shonnon'un [3] güvenli iletişim için vurguladığı iki temel kriter olan karıştırma ve yayılma özelliklerini sağlamalıdır. Bir blok şifreleme algoritmasında karıştırma özelliğini sağlamak için genellikle yer değiştirme kutuları olarak bilinen ve kısaca s-kutusu olarak adlandırılan kriptolojik yapılar kullanılmaktadır. Birçok modern blok şifreleme algoritmasında doğrusal olmayan tek eleman s-kutusu olduğu için genellikle kriptanaliz çalışmaları da bu eleman üzerine odaklanmaktadır [4]. Genel olarak s-kutuları n-bitlik bir giriş değerini m-bitlik bir çıkış değerine dönüştüren doğrusal olmayan bijektif (bire bir ve örten) bir dönüşümdür [5]. S-kutularının tasarımı için literatürde birçok yöntem önerilmiştir [6-9]. Modern blok şifreleme algoritmalarında genellikle güçlü cebirsel ilişkilere dayanan s-kutusu tasarım teknikleri kullanılmaktadır [10]. Bu tip katı cebirsel tekniklere dayalı yöntemler kullanıldığında mimarinin statik yapısından yola çıkılarak bazı istatistiksel ilişkiler ortaya çıkarılabilir ve şifreleme sistemine çeşitli saldırılar gerçekleştirilebilir. Diferansiyel kriptanaliz çalışmaları bunun en temel örneklerinden biridir [4]. Şifreleme mimarisi statik bir yapıda tasarlandığından kriptanalist şifreleme mimarisinin daha küçük versiyonları üzerinde çalışarak mimarinin geneli hakkında bir bilgiye sahip olabilir. Bu çalışmada bu problemi ortadan kaldırmak için rasgele seçilen s-kutularını temel alan yeni bir blok şifreleme algoritması önerilmiştir. Önerilen yeni yöntemin, diferansiyel kriptanaliz için başarı olasılığını azalttığı basit bir blok şifreleme mimarisi üzerinde gösterilmiştir.

Önerilen algoritma iteratif bir blok şifreleme algoritmasının her bir iterasyon adımında farklı bir s-kutusu kullanılması prensibine dayanmaktadır. Bunun için öncelikle s-kutularının tasarım aşamasında en yaygın kullanılan yöntemlerden biri olan Nyberg'in ters haritalama yöntemi incelenmiştir. Bu yöntem kullanılarak tasarlanabilecek farklı s-kutuları gösterilmiştir.

Çalışmadaki önemli katkılardan biri de her bir iterasyon adımında oluşturulan s-kutuları içerisinden seçim işlemine karar verilmesi sürecinde kaos teorisinden yararlanılmış olunmasıdır. Birçok kriptoloji uzmanı arasındaki yaygın görüşlerden biri; blok şifreleme mimarisinde kullanılan elemanlar ne kadar rasgele ise şifreleme mimarisinin o kadar güçlü olacağı yönündedir. Ancak rasgele oluşturulan

elemanlar belirli bir yapıya oturtulamadığından bu elemanların kriptolojik olarak test edilmesi aşamasında sıkıntılar ortaya çıkmaktadır. Bu problemin çözümü için kaotik sistemler ideal bir yapıya sahiptir. Çünkü kaotik sistemler gerekirci (deterministtik) bir yapıya sahip olmalarına rağmen rasgele benzeri bir davranış göstermektedir. Başlangıç koşulları ve kontrol parametrelerindeki ufak bir değişiklik ile sistem kısa vadede gerekirci bir yapıya sahip iken uzun vadede tahmin edilemez bir yapı kazanmaktadır.

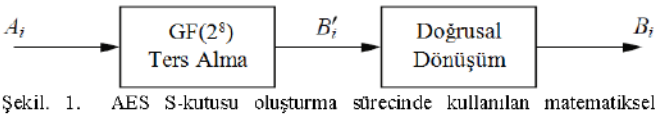
Çalışmanın geri kalan kısmı aşağıdaki gibi organize edilmiştir. İkinci bölümde her bir iterasyon adımında kullanılacak rasgele seçilen s-kutularının nasıl üretileceği gösterilmiştir. Üçüncü bölümde kaos teorisi kısaca tanıtılmış ardından kaotik seçim algoritmasının detayları verilmiştir. Dördüncü bölümde kaotik olarak seçilmiş s-kutularını temel alan basit blok şifreleme mimarisinin diferansiyel kriptanalizi verilmiştir. Elde edilen sonuçlar son bölümde tartışılmıştır.

II. Cebirsel Tabanlı S-Kutuları

Gelişkin şifreleme standardı olarak bilinen AES [10] algoritmasının seçim sürecinde en önemli konulardan biri diferansiyel ve lineer kriptanalize karşı dirençli bir yapının araştırılması olmuştur. Bu tasarım sürecinde Galois cisim aritmetiğinden yararlanılarak Nyberg [6] tarafından önerilen yöntem kullanılmıştır. Bu bölümde öncelikle s-kutusu tasarım aşamasında kullanılan Galois aritmetiği hakkında kısa bir bilgi verilmiş ardından Nyberg'in tasarım yöntemi açıklanmıştır. Bölümün sonunda önerilen yeni yapıda kullanılabilecek s-kutularının nasıl üretildiği ve kriptolojik özellikleri verilmiştir.

A. Galois Aritmetiği

Bazen Galois cismi olarak adlandırılan bir sonlu cisim sonlu sayıda eleman içeren bir kümedir. AES'de sonlu cisim 256 eleman içermektedir ve $GF(2^8)$ olarak gösterilmektedir [11]. Burada 2^8=256 polinom vardır.



Şekil. 1. AES S-kutusu oluşturma sürecinde kullanılan matematiksel dönüşümler.

AES s-kutusu şekil 1'de gösterildiği gibi iki adımlı bir matematiksel dönüşüm kullanılarak oluşturulmuştur. İlk aşamada her bir elemanın $GF(2^8)$ cismi üzerinde tersi alınmıştır. Ters alma işleminde indirgenemez polinom olarak $P(x)=x^8+x^4+x^3+x+1$ polinomu kullanılmıştır. Sıfır elemanının tersi olmadığı için kendisine dönüştürülmüştür. İkinci adımda ise hesaplanan değer sabit bir bit matrisi ile çarpıldıktan sonra yine sabit bir 8-bit vektör ile toplanmıştır. Bu işlem denklem (1)'de gösterilmiştir.

B. $GF(2^8)$'de Oluşturulabilecek Farklı S-kutuları

Barkan ve Biham [12] AES şifreleme sistemine eşdeğer şifreleme sistemleri yazılıp yazılamayacağını araştırmışlardır. Bunun için şifreleme mimarisinde kullanılan bazı yapıların yerine kullanılabilecek alternatifleri göstermişlerdir. Bu yapılar s-kutularının tasarım sürecindeki indirgenemez polinomlar, kolon karıştırma işleminde kullanılan matrisin katsayıları ve doğrusal dönüşümde kullanılabilecek matrislerdir.

$$\begin{pmatrix} b_0 \\ b_1 \\ b_2 \\ b_3 \\ b_4 \\ b_5 \\ b_6 \\ b_7 \end{pmatrix} = \begin{pmatrix} 1 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 1 & 1 & 0 & 0 & 0 & 1 & 1 & 1 \\ 1 & 1 & 1 & 0 & 0 & 0 & 1 & 1 \\ 1 & 1 & 1 & 1 & 0 & 0 & 0 & 1 \\ 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 1 & 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 1 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 \end{pmatrix} \cdot \begin{pmatrix} b'_0 \\ b'_1 \\ b'_2 \\ b'_3 \\ b'_4 \\ b'_5 \\ b'_6 \\ b'_7 \end{pmatrix} + \begin{pmatrix} 1 \\ 1 \\ 0 \\ 0 \\ 0 \\ 1 \\ 1 \\ 0 \end{pmatrix} \quad (1)$$

Buradan hareketle çalışmada önerilen algoritmanın her bir adımında kullanacağımız s-kutularını oluşturmak için sadece indirgenemez polinomları değiştirerek AES s-kutusuyla aynı mantıkla tasarlanmış kriptolojik olarak eşdeğer olan farklı s-kutuları üretilmiştir. $GF(2^8)$'de yazabileceğimiz indirgenemez polinomların listesi tablo 1'de verilmiştir.

C. Oluşturulabilecek S-kutularının Kriptolojik Özellikleri

Tablo 1'de verilen indirgenemez polinomları kullanarak oluşturulacak s-kutularının kriptolojik özelliklerini değerlendirmek için literatürde birçok test kriteri önerilmiştir. Bu kriterlerden en yaygın şekilde kullanılanları s-kutularının bijektif (bire-bir ve örten) olması, doğrusal saldırılara karşı güçlü olması için doğrusal olmama ölçütünün yüksek olması, diferansiyel saldırılara karşı dirençli olması için fark dağılım tablosundaki en büyük değerin küçük olması ve çığ kriterini sağlaması olarak özetlenebilir [13].

Oluşturulan tüm s-kutuları bijektif bir yapıya sahiptir ayrıca izomorfik yapıda olduğu için kriptolojik testlerden diferansiyel ve doğrusal olmama ölçütüne ilişkin test sonuçları benzer çıkacaktır. Oluşturulan tüm s-kutularının diferansiyel düzgünlük değeri 4 iken doğrusal olmama değeri ise 112 olarak hesaplanmıştır.

S-kutularının kriptolojik özelliklerinin değerlendirilmesi aşamasında kullanılan diğer önemli bir test ise çığ kriterinin testidir. Çığ testinde giriş bitlerinde bir bitlik bir değişim meydana geldiği zaman bu değişimin çıkış bitlerini nasıl etkilediği ölçülmektedir. İdealde giriş bitlerinde bir bitlik bir değişim meydana geldiğinde çıkış bitlerinin yarısının değişmesi istenmektedir. Tablo 1'de verilen indirgenemez polinomları kullanarak üretilen tüm s-kutuları ideal değer olan 0.5 değerine çok yakın sonuçlar üretmişlerdir. Üretilen s-kutuları içerisinde en iyi sonuç ise $x^8+x^6+x^5+x+1$ polinomunu kullanarak üretilen 8 numaralı s-kutusu olmuştur.

III. Kaotik Seçim Algoritması

Kaos ekosistemdeki popülasyon artışından elektrik devrelerine, kimyasal reaksiyonlardan mekanik sistemlere kadar bilimin birçok alanında gözlemlenebilen ilginç bir olgudur. Kaos doğrusal olmayan dinamik sistemlerdeki gerekirci ve rasgele benzeri bir süreçtir. Kaotik sistemler periyodik değillerdir ve sonlu olmalarına rağmen belirli bir

değere yakınsamazlar. Kaotik sistemlerin en önemli özelliği başlangıç koşulları ve kontrol parametrelerine aşırı bağımlı olmalarıdır. Kaos doğası gereği rasgele ve tahmin edilemez görülmesine rağmen iç kısmında bir düzen vardır. Aslında genellikle kaos düzen içerisinde düzensizlik yada düzensizlik içerisinde düzen olarak adlandırılabilir. Matematiksel olarak kaos basit gerekirci dinamik bir sistemin rasgeleliği olarak tanımlanabilir [14, 15].

TABLO I
GF(2^8) ÜZERİNDE İNDİRGENEMEZ POLİNOMLAR

Polinom No	İndirgenemez Polinomlar
0	$x^8+x^4+x^3+x+1$
1	$x^8+x^4+x^3+x^2+1$
2	$x^8+x^5+x^3+x+1$
3	$x^8+x^5+x^3+x^2+1$
4	$x^8+x^5+x^4+x^3+1$
5	$x^8+x^5+x^4+x^3+x^2+x+1$
6	$x^8+x^6+x^3+x^2+1$
7	$x^8+x^6+x^4+x^3+x^2+x+1$
8	$x^8+x^6+x^5+x+1$
9	$x^8+x^6+x^5+x^2+1$
10	$x^8+x^6+x^5+x^3+1$
11	$x^8+x^6+x^5+x^4+1$
12	$x^8+x^6+x^5+x^4+x^2+x+1$
13	$x^8+x^6+x^5+x^4+x^3+x+1$
14	$x^8+x^7+x^2+x+1$
15	$x^8+x^7+x^3+x+1$
16	$x^8+x^4+x^3+x^2+1$
17	$x^8+x^7+x^4+x^3+x^2+x+1$
18	$x^8+x^7+x^5+x+1$
19	$x^8+x^7+x^5+x^3+1$
20	$x^8+x^7+x^5+x^4+1$
21	$x^8+x^7+x^5+x^4+x^3+x^2+x+1$
22	$x^8+x^7+x^6+x+1$
23	$x^8+x^7+x^6+x^3+x^2+x+1$
24	$x^8+x^7+x^6+x^4+x^2+x+1$
25	$x^8+x^7+x^6+x^4+x^3+x^2+1$
26	$x^8+x^7+x^6+x^5+x^2+x+1$
27	$x^8+x^7+x^6+x^5+x^4+x+1$
28	$x^8+x^7+x^6+x^5+x^4+x^2+1$
29	$x^8+x^7+x^6+x^5+x^4+x^3+1$

Kaos ve kriptoloji bilimleri arasında doğal bir ilişki bulunmaktadır. Bu ilişki herhangi bir şifreleme sisteminin güvenilir olması için sahip olması gereken özellikler olan karıştırma ve yayılma özellikleri ile kaotik sistemlerin başlangıç koşullarına duyarlı olması ve doğrusal olmaması özellikleriyle örtüşmesinden ortaya çıkmaktadır [16].

Karıştırma ve yayılma özellikleri dinamik sistemlerin sahip olduğu özelliklerdir. Kaotik sistemlerin başlangıç koşulları ve kontrol parametrelerine bağımlılığı bir kaotik sistemden üretilen yörüngeler boyunca yayılma özelliğini sağlar. Başka bir ifade ile herhangi bir yörünge üzerinde alınan her bir değer başlangıç koşulları veya kontrol parametrelerine bağımlıdır. Başlangıç koşulları ve kontrol parametrelerindeki en ufak bir değişiklik ile tamamen farklı yörüngeler oluşacağından bu bağımlılık çok güçlüdür. Sonuç olarak kaotik sistemler başlangıç koşulları ve/veya kontrol parametrelerine bağımlılığı yayılma özelliğine sahiptir [17].

Kaotik sistemlerin ergodiklik özelliği kaotik yörüngenin uzun vadeli davranışının başlangıç koşulları ve kontrol parametrelerine bağımlılığını ortaya koymaktadır. Buradan bir kaotik sistemden üretilen yörüngelerin bir kümesi ile istatistikî olarak başlangıç koşulları ve kontrol parametrelerinin tam değerlerinin çıkarılmasının mümkün olmadığı görülebilir. Sonuç olarak kaotik sistemler karıştırma özelliğini göstermedir [17].

Bu çalışmada kaotik sistem olarak Lojistik harita seçilmiştir. Lojistik haritanın ifadesi denklem (2)'de yörüngesinin davranışı ise şekil 2'de gösterilmiştir [15]. Şifreleme algoritmasında Lojistik haritanın seçilmesindeki en önemli sebeplerden biri kaotik sistemin birinci dereceden bir yapıya sahip olması ve sadece bir başlangıç koşulu, bir kontrol parametresiyle kaotik yörüngenin oluşturulabilmesidir. Bu birçok şifreleme algoritmasının gereksinim duyduğu şifreleme ve şifre çözme sürelerinin azaltılması için önemli bir özelliktir. Ayrıca Lojistik harita düzgün bir dağılıma sahip olması şifreleme mimarisine uygulanacak istatistiksel saldırılara karşı önemli bir etken olacaktır.

$$x_{k+1} = Ax_k(1-x_k), \quad x_0 = 0.2, \quad A = 3.8 \qquad (2)$$

A. Önerilen Algoritma

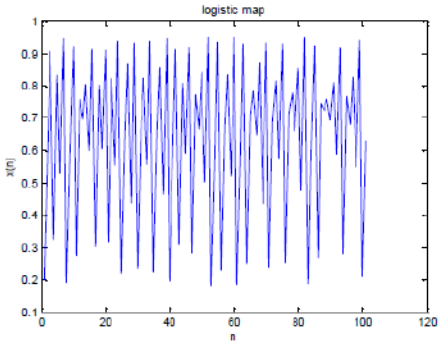
AES şifreleme algoritmasında anahtar uzunluğuna göre iterasyon adım sayısı değişmektedir. Maksimum iterasyon sayısı anahtar uzunluğu 256-bit olduğunda 14 olarak belirlenmiştir. GF(2^8)'de yazılabilecek indirgenemez polinom sayısı tablo 1'de gösterildiği gibi 30 tanedir. Bu indirgenemez polinomlar kullanılarak oluşturulan her bir s-kutusuna 0'dan 29'a kadar numara verilir. Bu durumda her bir iterasyon adımında hangi s-kutusunun seçileceğine karar verilmelidir. Kriptolojik uygulamalarda bu tip bir seçim yapılırken sürecin rasgele olması istenmektedir. Ancak rasgele yapılan bir sürecin kriptolojik özelliklerin değerlendirilmesi aşamasında çeşitli sıkıntılar ortaya çıkmaktadır. Çünkü rasgele bir işlem belirli bir yapıya oturtulamadığından nasıl test edileceği önemli bir soru olarak karşımıza çıkmaktadır. Bu problemi çözmek için seçim sürecinde kaotik sistemlerden yararlanılabilir. Kaos rasgele benzeri bir davranış göstermesine rağmen gerekirci bir yapıya sahiptir. Kaotik sistemin belirlenen başlangıç koşulları ve kontrol parametrelerini kullanarak kaç defa iterasyona sokulacağını şifreleme sisteminin anahtarı belirlemektedir. Dolayısıyla kaotik sistemin kullanılması sisteme ek bir maliyet getirmeyecektir. Kaotik sistem yardımıyla hangi s-kutusunun seçileceğini belirleyen algoritmanın adımları aşağıda adım adım açıklanmıştır. Algoritmanın sözde kodu ise tablo 2'de verilmiştir.

Adım 1) Anahtar planlama algoritmasından gelen 128-bitlik iterasyon adım anahtarı 8-bitlik bloklara bölünür.

Adım 2) Kaotik haritanın kaç sefer iterasyona sokulacağını 8-bit uzunluğunda bloklara bölünen yapı içerisinden seçilen i. blok belirlemektedir. i değeri başlangıçta sıfırdır.

Adım 3) Kaotik haritanın adım 2'de bulunan değer kadar iterasyonu sonucunda hesaplanan çıkış değerinin virgülden sonraki iki basamağına mod 30 işlemi uygulanarak hangi s-kutusunun seçileceğine karar verilir.

Adım 4) Eğer belirlenen s-kutusu daha önce seçilmişse i değeri artırılır ve yeni i. blok için adım 2'den devam edilir. S-kutusu daha önce kullanılmamışsa algoritma sonlandırılır.



Şekil. 2. Lojistik haritanın yörüngesinin davranışı.

IV. Önerilen Kaotik Seçim Algoritmanın Kriptanalizi

Diferansiyel kriptanaliz Biham ve Shamir [4] tarafından blok şifrelerin kriptanalizi için geliştirilen bir seçilmiş açık metin saldırısıdır. Bu saldırı tekniğinde farkları özel olarak seçilmiş açık metinlerin şifreli metinler üzerine etkilerinin incelenmesine bağımlıdır. Diferansiyel kriptanalizde yüksek olasılıklı fark çiftlerinin bulunması amaçlanmaktadır. Bunun için fark dağılım tablosu kullanılmaktadır. XOR tablosu olarak da adlandırılan bu tablo s-kutusunun olası tüm giriş çıkış çiftlerinin her birinin tüm giriş çıkış farklarını göstermektedir.

TABLO 2 KAOS TABANLI S-KUTU SEÇİM ALGORİTMANIN SÖZDE KODU

```
KaotikSkutuSecim(K0||K1||...||K15)
    i, n:=0
    kontrol:=true
    while(kontrol)
        n:= Σ_{j=0}^{i} Decimal(K_j)
        x=KaotikHarita(n) mod 30
        if(x seçilmedi ise) then kontrol:=false
        else i++
    end
end

KaotikHarita(n)
    xEski:=0.2
    for i:=1 to n do
        xYeni:=3.8*xEski*(1-xEski)
        xEski:=xYeni
    end
    xYeni:=0,b1b2b3...bk
    return b1b2
end
```

Önerilen kaotik olarak seçilmiş s-kutularını temel alan blok şifreleme mimarisinin diferansiyel kriptanalizini göstermek için Knudsen ve Robshaw [18] tarafından eğitim amaçlı olarak tanıtılmış basit bir blok şifreleme mimarisi incelenmiştir. Bu blok şifreleme mimarisi 16-bitlik bloklar üzerinde işlem yapan r adımlı iteratif bir blok şifreleme algoritmasıdır. Algoritmanın yapısı tablo 3'de verilmiştir. Blok şifreleme algoritmasında kullanılan s-kutusunun fark dağılım tablosu ise tablo 4'de gösterilmiştir.

Tablo 4'den kolayca görülebileceği gibi giriş çiftleri arasında fark olmadığında çıkış çiftleri arasında da fark olmayacağı 16/16=1 olasılıkla tahmin edilebilir. Tablodan çıkarılabilecek bir diğer önemli ilişkide giriş çiftleri arasında f-bitlik fark olduğunda çıkış çiftleri arasında d-bitlik fark olma olasılığının 10/16 olmasıdır. Bu değer fark dağılım tablosundan çıkarılabilecek maksimum olasılık ilişkisidir. Ancak analiz amacına göre farklı ilişkilerde kullanılabilir. Bu çalışmada giriş çiftleri arasında 2-bitlik fark olduğunda çıkış bitleri arasında 1-bitlik fark olma olasılığının 6/16 ve 2-bitlik fark olma olasılığının 6/16 olması ilişkisi kullanılmıştır.

Yani basit bir örnek üzerinde bu ilişki incelenirse blok şifreleme mimarisine giriş olarak seçilen iki açık metin arasında (0,0,2,0) fark olduğu varsayılmıştır. Yani 16-bitlik giriş 4-bitlik 4 bloğa bölündükten sonra seçilmiş açık metin saldırısına göre 1, 2 ve 4 bloklarda değişim yoktur sadece 3. blokta iki bitlik bir değişim bulunmaktadır. Bu giriş ile 4 iterasyon ilerlendikten sonra 5. adım alt anahtarı olan k_5 $(6/16)^4$ olasılıkla tahmin edilebileceği görülür.

Eğer statik s-kutuları yerine her bir adımda rasgele seçilen s-kutularını kullanan bir yapı kullanılsaydı her bir iterasyon adımda s-kutusu değişeceğinden bu s-kutularına ilişkin fark dağılım tabloları da değişecektir. Bu durumda 5. adım alt anahtarı olan k_5 $(1/16)^4$ olasılıkla hesaplanabilecektir. Sonuç olarak istatistiki ilişki çıkarmak zorlaşacaktır.

İncelenen blok şifreleme mimarisinin kaotik olarak seçilen s-kutularıyla nasıl kullanılacağını göstermek için 4x4 boyutunda s-kutuları $GF(2^4)$ üzerinde tasarlanmıştır. $GF(2^4)$ cismi üzerinde yazabileceğimiz indirgenemez polinomlar denklem (3)'de verilmiştir. Bu indirgenemez polinomları kullanarak AES s-kutusuna benzer mantıkla tasarlanmış s-kutuları tablo 5'de gösterilmiştir. Tablo 5'de verilen s-ilk iki s-kutusu için fark dağılım tabloları ise sırasıyla tablo 6 ve 7'de verilmiştir. Her bir adımda farklı bir s-kutusu kullanıldığında fark dağılım tablolarından istatistiksel ilişki çıkarmanın zorluğu kolayca görülebilir.

$$P_1(x) = x^4 + x + 1$$
$$P_2(x) = x^4 + x^3 + 1 \quad (3)$$
$$P_3(x) = x^4 + x^3 + x^2 + x + 1$$

V. Sonuçlar

Bu çalışmada statik s-kutularını kullanan blok şifreleme mimarisi yerine rasgele seçilen s-kutularını kullanan bir mimari seçildiği zaman diferansiyel kriptananliz başarı olasılığının azaltılabileceği gösterilmiştir.

Blok şifreleme mimarisinin her bir adımında rasgele seçilen s-kutuları $GF(2^8)$ üzerinde yazılabilen indirgenemez

polinomlar kullanılarak AES s-kutusu tasarım mantığına benzer olarak oluşturulmuştur.

Oluşturulan s-kutuları içerisinden seçim işlemi aşamasında ise kaos teorisinden faydalanılmıştır. Kaotik sistemler gerekirci bir yapıya sahip olmasına rağmen rasgele benzeri bir davranış göstermektedir. Kaotik sistemlerin bu özelliği hem sözde rasgele bir seçim yapma imkânı hem de rasgele seçimlerde mümkün olmayan seçimin nasıl yapıldığına dair ifadenin ortaya koyulması probleminin aşılmasını sağlamaktadır. İleride kaotik sistemlerin bu özelliğinden yararlanılarak kriptolojik sistemlerin güçlendirilebileceği düşünülmektedir.

KAYNAKLAR

[1] J. Katz, Y. Lindell, Introduction to modern cryptography: principles and protocols, Chapman & Hall, 2008.
[2] C. Paar, J. Pelzl, Understanding Cryptography A Textbook for Student and Practitioners, Springer, 2010.
[3] CE. Shanon, Communication theory of secrecy systems, Bell Syst Tech J, 28/4 (1949) 656–715.
[4] E. Biham, A. Shamir, Differential Cryptanalysis of DES-like Cryptosystems, Journal of Cryptology 4 (1991) 3-72.
[5] T. Cusick, P. Stanica, Cryptographic Boolean Functions and Applications, Academic Press, 2008.
[6] K. Nyberg, Differentially uniform mappings for cryptography, Proceedings of Eurocrypt'93 Lecture Notes in Computer Science 765 (1994) 55-64.
[7] C. Adams, S. Tavares, The Structured Design of Cryptographically Good S-Boxes, Journal of Cryptography, 3 (1990) 27-41.
[8] K. Nyberg, S-Boxes and Round Functions with Controllable Linearity and Differential Uniformity, Fast Software Encryption, Lecture Notes in Computer Science 1008 (1995) 111-130.
[9] C. Adams, S. Tavares, Good S-Boxes Are Easy To Find, Advances in Cryptography, Lecture Notes in Computer Science 435 (1990) 612-615
[10] J. Daemen, V. Rijmen, AES Proposal: Rijndael, First Advanced Encryption Conference, California, 1998.
[11] R. Lidl, H. Niederreiter, Introduction to finite fields and their applications, Cambridge University Press, Revised edition. 1994.
[12] E. Barkan, E. Biham, In How Many Ways Can You Write Rijndael?, Advances in Cryptology - Asiacrypt2002 Lecture Notes in Computer Science 2501 (2002) 160-175.
[13] F. Özkaynak, A. B. Özer, A Method for Designing Strong S-Boxes Based on Chaotic Lorenz System, Physics Letters A, Vol.374, issue.36, 3733-3738, 2010.
[14] O. Edward, Chaos in Dynamical Systems, Cambridge University Press, New York, 2002.
[15] J. Sprott, Elegant Chaos Algebraically Simple Chaotic Flows. World Scientific, 2010.
[16] L. Kocarev, S. Lian, Chaos Based Cryptography Theory Algorithms and Applications, Springer-Verlag, 2011.
[17] F. Özkaynak, A.B. Özer, S. Yavuz, Kaos Tabanlı Yeni Bir Blok Şifreleme Algoritması, IV. Ağ ve Bilgi Güvenliği Sempozyumu, Ankara, 2011.
[18] L. Knudsen, M. Robshaw, The Block Cipher Companion, Springer, 2011.

TABLO 3 KNUDSEN-ROBSHAW [18] BLOK ŞİFRELEME ALGORİTMASI

x	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
S[x]	6	4	C	5	0	7	2	E	1	F	3	D	8	A	9	B

i	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
P[j]	0	4	8	12	1	5	9	13	2	6	10	14	3	7	11	15

1. $u_0=m$
2. for i:=1 to r-1 do
   a) $a_i=u_{i-1} \oplus k_{i-1}$
   b) a_i dört parçaya bölünür. $a_i=A_0 \| A_1 \| A_2 \| A_3$
   c) $S[A_0] \| S[A_1] \| S[A_2] \| S[A_3]$ hesaplanır.
   d) $y_{15},\ldots,y_0= S[A_0] \| S[A_1] \| S[A_2] \| S[A_3]$ şeklinde .
   e) y_i değeri permute edilir.
   f) u_i değeri $y_{15} \| y_{11} \| \ldots y_4 \| y_0$.
3. Son iterasyon adımı
   a) $a_r=u_{r-1} \oplus k_{r-1}$
   b) a_r dört parçaya bölünür. $a_r=A_0 \| A_1 \| A_2 \| A_3$
   c) $S[A_0] \| S[A_1] \| S[A_2] \| S[A_3]$ hesaplanır.
   d) $y_{15},\ldots,y_0= S[A_0] \| S[A_1] \| S[A_2] \| S[A_3]$ şeklinde yazılır .
   e) Çıkış $y \oplus k$

TABLO 4 KNUDSEN-ROBSHAW S-KUTUSU İÇİN FARK DAĞILIM TABLOSU

	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
0	16	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
1	0	0	6	0	0	0	0	2	0	2	0	0	2	0	4	0
2	0	6	6	0	0	0	0	0	0	2	2	0	0	0	0	0
3	0	0	0	6	0	2	0	0	2	0	0	0	4	0	2	0
4	0	0	0	2	0	2	4	0	0	2	2	2	0	0	2	0
5	0	2	2	0	4	0	0	4	2	0	0	2	0	0	0	0
6	0	0	2	0	4	0	0	2	2	0	2	2	2	0	0	0
7	0	0	0	0	0	4	4	0	2	2	2	2	0	0	0	0
8	0	0	0	0	0	2	0	2	4	0	0	4	0	2	0	2
9	0	0	0	0	0	2	2	2	0	4	2	0	0	0	0	2
A	0	0	0	0	2	2	0	0	0	4	4	0	2	2	0	0
B	0	0	0	2	2	0	2	2	2	0	0	4	0	0	2	0
C	0	4	0	2	0	2	0	0	2	0	0	0	0	0	6	0
D	0	0	0	0	0	0	2	2	0	0	0	0	6	2	0	4
E	0	2	0	4	2	0	0	0	0	0	2	0	0	0	0	6
F	0	0	0	0	2	0	2	0	0	0	0	0	0	10	0	2

TABLO 5 DENKLEM (3)'DE VERİLEN POLİNOMLARI KULLANARAK OLUŞTURULABİLECEK S-KUTULARI

	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
SKUTU1	0	1	9	E	D	B	7	6	F	2	C	5	A	4	3	8
SKUTU2	0	1	C	8	6	F	4	E	3	D	B	A	2	9	7	5
SKUTU3	0	1	F	A	8	6	5	9	4	7	3	E	D	C	B	2

TABLO 6 S-KUTUSU 1 İÇİN FARK DAĞILIM TABLOSU

	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
0	16	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
1	0	2	2	0	2	0	2	0	2	2	0	0	0	0	4	0
2	0	0	0	0	4	0	2	2	0	2	0	2	2	0	0	2
3	0	2	4	0	0	2	2	2	0	0	2	0	0	0	0	2
4	0	0	2	2	0	0	0	0	2	4	2	0	2	0	0	2
5	0	4	0	0	2	0	0	2	2	0	2	0	2	2	0	0
6	0	0	0	2	0	0	4	2	2	0	0	0	0	2	2	2
7	0	0	0	0	0	2	2	0	4	0	2	2	2	0	2	0
8	0	2	2	2	0	0	2	0	0	0	0	2	4	2	0	0
9	0	0	2	2	2	4	0	2	0	0	0	0	2	0	2	0
A	0	0	2	0	0	2	0	4	2	2	0	2	0	2	0	0
B	0	2	0	4	0	0	0	2	0	2	2	2	0	0	2	0
C	0	2	0	2	2	2	0	0	2	0	0	2	0	0	0	4
D	0	2	0	0	0	2	0	0	0	2	0	0	2	4	2	2
E	0	0	2	0	2	0	0	0	0	0	2	4	0	2	2	2
F	0	0	0	2	2	2	2	0	0	2	4	0	0	2	0	0

TABLO 7 S-KUTUSU 2 İÇİN FARK DAĞILIM TABLOSU

	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
0	16	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
1	0	2	0	0	2	0	0	0	0	2	2	2	0	2	4	0
2	0	2	2	2	0	2	0	0	4	0	0	2	0	0	2	0
3	0	0	2	0	0	4	2	0	0	2	2	2	2	0	0	0
4	0	0	0	0	0	2	0	2	2	2	0	0	4	2	2	0
5	0	2	2	0	2	0	2	4	2	2	0	0	0	0	0	0
6	0	0	2	0	2	2	0	2	0	0	0	2	0	4	0	2
7	0	2	0	2	2	2	0	0	0	4	0	0	2	0	0	2
8	0	2	2	0	0	0	0	0	2	0	2	0	2	2	0	4
9	0	2	0	0	0	0	4	2	0	0	0	2	2	0	2	2
A	0	0	2	2	2	0	0	2	0	0	4	0	2	0	2	0
B	0	0	0	0	4	2	2	0	2	0	2	0	0	0	2	2
C	0	4	0	2	0	2	2	2	0	0	2	0	0	2	0	0
D	0	0	0	2	0	0	0	2	2	2	2	4	0	0	0	2
E	0	0	4	2	0	0	2	0	0	2	0	0	0	2	2	2
F	0	0	0	4	2	0	2	0	2	0	0	2	2	2	0	0

Success Probability of The First Attack on Full Round GOST

Orhun Kara, Ferhat Karakoç

***Abstract*—The GOST encryption function is the Russian encryption standard, which is a block cipher of 64-bit block and 256-bit key size. The first attack on the full round GOST is a kind of reflection attack given in [15]. This attack does not work for all the keys. It consists of two steps. The first step is the identification step that determines if the attack works for the given key. The weak key is identified by searching a special type of fixed points. If the encryption function possesses such fixed points then the second step is carried out. This step is the key recovery attack and implemented only if the key is identified as a weak key.**

In this paper, we analyze the success rate of the key recovery step of the attack given in [15]. We compute the success rate and come to a conclusion that the second step is successful with a probability of almost one half. In addition, we implement the second part of the attack for some small scale GOST toy ciphers and verify the theoretical results we come up with. Moreover, we introduce a new key recovery algorithm for the second step and improve the time complexity slightly.

***Index Terms*—block cipher, self-similarity, reflection attack, GOST, weak key**

I. Introduction

The GOST cipher, the Russian encryption standard, is a Feistel network of 64-bit block and 256-bit key size [27]. It has a relatively very simple key schedule. A given key is divided into 8 parts and each part is used as a subkey in a palindromic order. This is a similarity property of the cipher; the similarity due to the palindromic order of the subkeys occurs between round functions of the encryption and those of the decryption. However, self-similarity attacks such as slide attacks or related key attacks could not be mounted on the full round GOST since these attack techniques examine the similarity between round functions of the encryption direction.

One of the self-similarity attack, the reflection attack, exploits the similarities between the round functions of the encryption direction with the corresponding round functions of the decryption direction by means of unexpectedly many number of fixed points. These fixed points are due to the palindromic structure of the round keys [18], [15], [16], [17]. As one of the applications, it succeeded to be the first attack on the full round GOST [15]. The attack does not work for all the keys. It consists of two steps. The former step is the identification step. The key is identified as a weak key in this step. The latter step is the key recovery attack and implemented only if the key is identified as a weak key.

Manuscript received March 26, 2012.

Orhun Kara and Ferhat Karakoç are with TÜBİTAK BİLGEM Gebze, 41470 Kocaeli Turkey, e-mails: {orhun,ferhatk}@uekae.tubitak.gov.tr

The weak key identification process in [15] makes use of the special type of fixed points. In the attack, it has been expected that a special type of fixed points may occur due to weak keys and the second step of the attack has been mounted if the encryption function has possessed such fixed points. On the other hand, there is a probability that these fixed points may exist by chance also. However, this situation was not examined and hence the probability of recovering the key in the second step has been left out in [15]. In this paper, we analyze the success rate of the second step of the attack. We compute the success rate and come to a conclusion that the second step is successful with a probability of almost one half. In addition, we implement the second part of the attack for some small-scale GOST toy ciphers and verify the theoretical results we come up with. Furthermore, we introduce a new key recovery algorithm for the second step. This attack is also a guess and determine type attack. However, we guess the internal states of the cipher instead of subkey bits. We also take advantages of the meet-in-the middle technique while determining the key bits. Altogether, we gain a minor improvement in the time complexity.

The paper is organized as follows. We introduce the notation in the next section. Then we give a brief overview about self-similarity attacks in Section III. Section IV is about a description of GOST cipher. Then the reflection attack on full round GOST is given in Section V. We analyze the success rate of the attack in Section VI. Experimental results are given in Section VII. We introduce a new key recovery attack when the key is identified as a weak key in Section VIII. We conclude the paper with Section IX.

II. Notation

We follow the notation and definitions given in [15]. Let us denote the ith round function of an encryption function E_K with n-bit block length as F_{k_i} for $i = 1, ..., r$ where r is the number of rounds and $k_1, ..., k_r$ are the round keys. Let us define the partial encryption function $F_K[i, j]$ as the encryption starting from round i and finishing at round j. That is,

$$F_K[i, j] = F_{k_j} \circ \cdots \circ F_{k_i} \text{ for } 1 \leq i < j \leq r. \quad (1)$$

These functions are called *intermediate functions*. Let $U_K(i, j)$ be the set of fixed points of the function $F_K[i, j]$. More explicitly,

$$U_K(i, j) = \{x \in GF(2)^n : F_K[i, j](x) = x\}.$$

III. Self-Similarity Attacks

Self-similarity attacks exploit the similarities between building blocks of a cipher iterated several times such as round functions of a block cipher. There are three main kinds of self-similarity attacks: Slide attacks [7], [8], related key attacks [1], [23] and recently discovered reflection attacks [15], [16], [17], [18]. Related key attacks proposed by Biham [1] and independently by Knudsen [23] are based on the powerful assumption that the attacker knows a relation between several keys and can access encryption function with these related keys.

Reflection attack was first presented at a local symposium [16] and on the web [17]. Then, several applications were introduced in [18], [15]. Reflection attack differs from the previous self-similarly attacks in the sense that it exploits certain similarities of some round functions of the encryption direction with the corresponding round functions of the decryption direction. Therefore, it particularly works on some involutionary ciphers such as some Feistel networks and its assumptions can be much weaker than the assumptions of previous self-similarity attacks for some cases. This enables the reflection attack to be mounted on some ciphers even with complicated key schedules.

IV. Brief Description of GOST

GOST, the Russian encryption standard [27], is a 32 round 64 bit Feistel network with 256 bit key. It has a simple key schedule: 256 bit key is divided into eight 32 bit words $k_0, ..., k_7$ and the sequence of round keys is given as $k_0, ..., k_7, k_0, ..., k_7, k_0, ..., k_7, k_7, k_6, ..., k_1, k_0$. The round key is involved by the modular addition in the round function. We do not consider details of the round function. We only assume that it is bijective.

Denote the first eight rounds of GOST as $F_K[1,8]$. Note that $F_K[1,8]$ ends with a swap operation. Then, the GOST encryption function is given as

$$E_K(x) = F_K[8,1] \circ S \circ F_K^3[1,8](x),$$

where S is the swap operation of the Feistel network and $F_K[8,1]$ is the inverse of $F_K[1,8]$.

A. Security Status of GOST

The first single key recovery attack on full round GOST is the reflection attack [15]. Before the discovery of the reflection property of GOST, there was no known attack on a single key which is better than the exhaustive search for full-round GOST. A related key differential cryptanalysis is shown in [20]. The attack is impractical for properly chosen S-boxes. A slide attack has been mounted on 20 round GOST$\oplus$, a variant of GOST defined in [8]. This attack uses 2^{33} known plaintexts and 2^{65} memory space and the key is recovered in 2^{70} encryptions. Another related key differential attack given in [26] has been mounted on 21 round GOST. This attack has a data complexity of 2^{56} chosen plaintexts. A related key differential attack that uses the idea of Seki and Kaneko in [26], is mounted on GOST [22]. The attack is on full-round GOST and recovers 12 bits of the key with 2^{35} chosen plaintexts in 2^{36} steps. However, the attack is based on a powerful assumption that the attacker knows that the two related keys differ in only eight specific bits. Another study by Biham, Dunkelman and Keller is the improved slide attack mounted on GOST [2]. In this attack, they firstly recover the key for 24-round reduced GOST in 2^{63} steps and then extend the attack to 30-round GOST with a workload of 2^{254} encryptions by using almost the entire code book.

Using the reflection property in [15], Isobe et.al. recently proposed an attack on full-round GOST which works for all keys. This attack requires 2^{32} data, 2^{64} memory, and 2^{224} time [14]. Also, there is another recent attack on full-round GOST using a different technique with 2^{64} data, 2^{64} memory and 2^{226} time [9]. Dinur et.al. improved the attack done by Isobe reducing the time complexity to 2^{192} [10].

V. Reflection Attack on Full Round GOST

In this section, we recall the reflection attack on full-round GOST given in [15].

Assume there exists x such that x is a fixed point of both $F_K[1,8]$ and the swap operation S, i.e., $F_K[1,8](x) = x$ and $S(x) = x$. Then, x is also a fixed point of the encryption function E_K. This observation leads to the following attack: Encrypt all 2^{32} plaintexts whose left and right halves are equal and collect the fixed points in a set, say U_E. If U_E is empty, then the attack is not applicable. Otherwise, for any x in U_E solve the equation $F_K[1,8](x) = x$ for K. Note that there are 2^{192} solutions and each of the solutions may be obtained by guessing $k_0, k_1, ..., k_5$ and then determining k_6 and k_7.

Guessing $k_0, k_1, ..., k_5$, we construct a two-round Feistel network with unknown keys k_6 and k_7 and an input-output pair given as $(F_K[1,6](x), x)$. Then, solving the system for k_6 and k_7 is straightforward since the round functions F_{k_6} and F_{k_7} are bijective and their outputs are known. By taking the inverses of F_{k_6} and F_{k_7}, we obtain the inputs and then k_6 and k_7. Consequently, we obtain 2^{192} candidates for the key by solving $F_K[1,8](x) = x$. We recover the correct key by searching over all the candidates by roughly 2^{192} encryptions. We solve $F_K[1,8](x) = x$ for each $x \in U_E$. However, it is most likely that U_E is empty if there exists no fixed point of $F_K[1,8]$ with the equal halves. On the other hand, the expected number of fixed points is one and the probability that any arbitrary value is a fixed point of S is 2^{-32}. Hence, the number of keys satisfying that $\exists\, x$ such that $F_K[1,8](x) = x$ and $S(x) = x$ is roughly 2^{224}.

VI. Success Rate of The Attack

The reflection attack on full-round GOST is given in [15]. However, the success rate of the attack is left out. Indeed, if the function $F_K[1,8]$ has a fixed point of the form $x = (a,a)$ where the former half of x is equal to its latter half, it is definitely a fixed point of the encryption function E. Nevertheless, the attack makes use of the opposite direction of the statement. That is, the attack is mounted if there is a fixed point of E, assuming that it is (probably) a fixed point for also $F_K[1,8]$. In this paper, we examine this direction and find the probability that any fixed point of E is also a fixed point of

$F_K[1,8]$. Let us remark that the attack is not successful for those fixed points of E which are not fixed points of $F_K[1,8]$.

Let the set of the fixed points of the form $x = (a,a)$ of $F_K[1,8]$ be U_F. Recall that U_E is the set of the fixed points of E of the form $x = (a,a)$.

Then, the success rate, $\Pr(S)$, of the attack is given as the conditional probability that U_F is nonempty given that U_E is nonempty. That is,

$$\Pr(S) = \Pr(U_F \neq \emptyset | U_E \neq \emptyset).$$

The following statement gives the success rate explicitly.

Theorem 1: Assume the encryption function E behaves as a random permutation when the function F_K has no fixed point of the form $x = (a,a)$. Then the sucess probability is given as

$$\Pr(S) = \frac{1}{1+(1-2^{-64})^{2^{32}}} \approx \frac{1}{2-2^{-32}}.$$

Proof: We have

$$\Pr(S) = \Pr(U_F \neq \emptyset | U_E \neq \emptyset)$$

which leads to

$$\Pr(S) = \frac{\Pr(U_F \neq \emptyset)}{\Pr(U_E \neq \emptyset)}$$

since U_F is a subset of the set U_E. On the other hand

$$\Pr(U_F \neq \emptyset) = 1-(1-2^{-64})^{2^{32}}$$

and $\Pr(U_E \neq \emptyset)$ is given as

$$\Pr(U_F \neq \emptyset) + \Pr(U_F = \emptyset)\Pr(U_E \neq \emptyset | U_F = \emptyset).$$

Assuming that E is a random permutation when F_K has no fixed point of the form $x = (a,a)$, we have

$$\Pr(U_E \neq \emptyset | U_F = \emptyset) = 1-(1-2^{-64})^{2^{32}}.$$

Hence, we calculate $\Pr(U_E \neq \emptyset)$ as

$$1-(1-2^{-64})^{2^{32}} + (1-2^{-64})^{2^{32}}(1-(1-2^{-64})^{2^{32}}),$$

which yields to the probability

$$\Pr(S) = \frac{1-(1-2^{-64})^{2^{32}}}{(1-(1-2^{-64})^{2^{32}})(1+(1-2^{-64})^{2^{32}})}$$

concluding the proof. ■

Let us remark that the success probability given in Theorem 1 is very close to one half since the value $(1-2^{-64})^{2^{32}}$ is approximately $1-2^{32}2^{-64}$ which is almost one. One interesting result is that if the encryption function E_K is a random permutation when the function F_K has no fixed point of the form $x = (a,a)$, it is itself cannot be a random permutation in general. Because, the probability that U_E is not empty is twice as large as the probability for a random permutation. The following corollary states this phenomena formally.

Corollary 1:

$$\begin{aligned}\Pr(U_E \neq \emptyset) &= (1-(1-2^{-64})^{2^{32}})(1+(1-2^{-64})^{2^{32}}) \\ &\approx 2(1-(1-2^{-64})^{2^{32}}).\end{aligned}$$

VII. Experimental Results

We deduce the result in Theorem 1 under the assumption that the encryption function E is a random permutation when the function F_K has no fixed point of the form $x = (a,a)$. We have tested this assumption by conducting some experiments on some shrunk versions of GOST. We have verified that the success rate is indeed around one half. Also we verify that the encryption function itself is not random since the probability that U_E is not empty is twice as high as expected.

We devise 4 versions of GOST with block sizes 16, 20, 24 and 28 bit lengths. The number of rounds is fixed to 32 for any block length and we use $n \times 4$ bit key for the n bit block length. The key is divided into 8 equal parts $k_0, ..., k_7$ and incorporated into the round function as for the original GOST function. The keys are produced at random on a desktop PC. Then, they are used in the rounds in the order $k_0, ..., k_7, k_0, ..., k_7, k_0, ..., k_7, k_7, k_6, ..., k_1, k_0$.

We make $100 \times 2^{n/2+4}$ number of experiments for the block length n, and count the number of keys where there is a fixed point of the form (a,a) and the number of the weak keys, that is, the keys where the attack works successfully. The results are depicted in Table 1.

The first column in Table 1 gives the block length of the GOST version. The second column is the number of experiment done. The third column is the number of keys where there is a fixed point of the form (a,a). The last column is the number of weak keys, that is, the number of the keys where there is a fixed point of the form (a,a) for the first 8-round of the related GOST version. For each block length, we adjust the expected number of fixed points of the form (a,a) for the encryption to be 3200 and the expected number of weak keys to be 1600 in the theory given in the previous section performing different number of experiment. The number of keys used in the experiment for the 16-bit block length is selected as 100×2^{12} to reach 1600 which is the number of keys which have a fixed point for the first 8 rounds because the probability of having a fixed point for the first 8 rounds for a key is $2^{-16} \times 2^8 = 2^{-8}$ and using 100×2^{12} different keys we expect to find $100 \times 2^{12} \times 2^{-8} = 1600$ weak keys. The number of experiment for other block length are selected in a similar way. As being seen from the table, the experimental results are as expected. That is, the success ratio is around 1600/3200, which is one half.

TABLE I
THE EXPECTED NUMBER OF FIXED POINTS AND WEAK KEYS ARE 3200 AND 1600 RESPECTIVELY

Block length	Number of keys used in experiment	Number of keys which have a fixed points for E_K	Number of weak keys	Success rate
16 bits	100×2^{12}	3153	1556	0.493
20 bits	100×2^{14}	3255	1618	0.497
24 bits	100×2^{16}	3193	1598	0.501
28 bits	100×2^{18}	3229	1588	0.492

The experimental results verify that the probability that the

GOST encryption function has a fixed point of the form (a, a) is approximately twice as large as a random permutation. For a random permutation, the number of keys producing fixed points of the form (a, a) is around 1600 for each block length in the experiments.

VIII. Another Attack

We slightly improve the attack given in Section V by means of guess and determine and meet-in-the-middle techniques together. In [15], the candidate key space is reduced to 2^{192}, utilizing a guess and determine type attack. Then, the brute force attack is mounted to find the correct key among the 2^{192} key candidates. Thus, the complexity is given as approximately 2^{192} encryptions. In this attack, we reduce the size of the candidate key space to 2^{192} as in the original attack. What is more is that, we are able to cluster the candidate lists for the first 5 and last 3 rounds keys. Thus, we can reduce the brute force complexity using the clustering. The details of the attack as follows.

We first introduce a 3-round meet-in-the-middle technique used in the attack. The technique is depicted as Algorithm 1. The time complexity of Algorithm 1 is 3×2^{32} F calculations

Algorithm 1 3-round meet-in-the-middle

1: One input-output pair for 3 rounds is given and a list of candidate keys of 3 rounds will be returned.
2: **for all** Guess of 1-st round key **do**
3: Calculate the right most 32-bit of the output of 1-st round and store it into Table C.
4: **end for**
5: **for all** Guess of 3-rd round key **do**
6: Calculate the left most 32-bit of the input of 3-th round and check the value in Table C. If there is a match calculate the 2-nd round key inverting F function and store 2^{32} candidate values for the triple (k_1, k_2, k_3) into the list L.
7: **end for**
8: Output L.

and we need 2^{32} memory for Table C and L used in the algorithm.

We mount an attack on full-round GOST given in Algorithm 2.

In the Algorithm after Step 5 there will be 2^{64} key candidates under one guess of the outputs of 3-th and 5-th rounds. Because of the 64-bit sieving in Step 11 the number of survived candidate key will be 1 on the average. The probability that the survived key will not be eliminated in the checking process in Step 12 is 2^{-192}. The number of all possible guess for the outputs is 2^{128}. Thus the number of candidate keys after the execution of the attack will be 2^{-64} which means that all wrong keys are eliminated and the correct key will be recovered.

The data complexity of the attack as follows. 2^{32} chosen plaintexts having equal left and right halves are used to find a fixed point for the cipher. In the case of finding a fixed point the attack given in Algorithm 2 is executed using the fixed

Algorithm 2 Attack on full-round GOST

1: The 64-bit value x such that $F_K[1,8](x) = x$ is given.
2: **for all** Guess of the outputs of 3-rd and 5-th rounds. **do**
3: Calculate k_3 and k_4 using the output of 3-rd and 5-th rounds.
4: Apply Algorithm 1 giving x and the output of 3-rd round. Store the output of the algorithm which is a list of 2^{32} candidates for the round keys (k_0, k_1, k_2) in Table A.
5: Apply Algorithm 1 giving the output of 5-th round and x. Store the output of the algorithm which is a list of 2^{32} candidates for the round keys (k_5, k_6, k_7) in Table B.
6: For a different input-output pairs of the Encryption algorithm do the followings.
7: **for all** Values of (k_0, k_1, k_2) in Table A **do**
8: Calculate the output of the 5-th and the input of 28-th rounds making 5-round partial encryptions and 5-round partial decryptions respectively.
9: **for all** Values of (k_5, k_6, k_7) in Table B **do**
10: Calculate the output of the 16-th and the input of 17-th rounds making 11-round partial encryptions and 11-round partial decryptions respectively.
11: **if** The calculated values of the output of the 16-th round and the input of the 17-th round are equal **then**
12: Check the key using 3 different input-output pairs of the cipher.
13: **end if**
14: **end for**
15: **end for**
16: **end for**

point and arbitrary 4 input-output pairs of the cipher. Here we assume that the fixed point for the cipher is also a fixed point for first 8 rounds with a probability of $1/2$. As a result, we use 2^{32} chosen plaintext to find a fixed point and the fixed point with arbitrary 4 input-output pairs of the cipher are used in the Algorithm.

The time complexity of the attack can be computed as follows. For a guess of the outputs of 3-th and 5-th rounds we do 2^{32} operations in step 4 and 5 because the complexity of Algorithm 1 is approximately 2^{32}. We perform 2^{32} times 10-round partial encryptions in step 8 using the keys in table A and k_3 and k_4 calculated in step 3. Also, we do 2^{64} times 22-round partial encryptions using the keys in Table A and B, k_3 and k_4 in Step 10. This gives an advantage provided by the clustering of the round key candidates during the brute force. There is a 64-bit sieving in Step 11, so there will be only one key candidate for a guess of the outputs of 3-th and 5-th rounds on the average. The number of operations in Step is 3 encryptions. Thus, the number of operations is approximately $2^{64} \times 22$ F calculations which costs roughly $2^{63.46}$ encryption operations for a guess of the outputs of 3-th and 5-th rounds. The number of all possible guess for the outputs is 2^{128}. As a result, the time complexity of Algorithm 2 is around $2^{191.46}$

encryption operations. We use approximately 2^{32} memory in the attack.

IX. Conclusion

We have computed the success rate of the key recovery step of the first attack mounted on the full GOST. We have seen that the success rate is around one half. In addition, we have conducted several experiments to verify the calculations. On the other hand, we have proved that the encryption function is not random when there is a fixed point of the form (a, a). Moreover, we have mounted another attack to recover the key whenever the key is identified as a weak key.

Acknowledgment

We would like to thank the anonymous reviewers and Mehmet Sabır Kiraz for their helpful comments.

References

[1] E. Biham. New Types of Cryptanalytic Attacks Using Related Keys. *J. of Cryptology*, Vol.7, pp.229-246, 1994.
[2] E.Biham, O. Dunkelman and N. Keller. Improved Slide Attacks, In *Proc. FSE'07*, LNCS 4593, pp. 153-166, Springer, 2007.
[3] E.Biham, O. Dunkelman and N. Keller. Related-Key Boomerang and Rectangle Attacks, In *Proc. of EUROCRYPT 2005*, LNCS 3494, pp. 507-525, Springer, 2005.
[4] E.Biham, O. Dunkelman and N. Keller. New Cryptanalytic Results on IDEA, *Proc. of ASIACRYPT 2006*, LNCS 4284, pp. 412-427, Springer, 2006.
[5] E.Biham, O. Dunkelman and N. Keller. A Simple Related-Key Attack on the Full SHACAL-1. In Proc. CT-RSA'07, LNCS 4377, pp. 20-30, Springer, 2007.
[6] E.Biham, O. Dunkelman and N. Keller. A Unified Approach to Related-Key Attacks. In *Proc FSE'08*, LNCS 5086, pp73-96, Springer, 2008.
[7] A. Biryukov and D. Wagner. Slide Attacks. In *Proc. FSE'99*, LNCS 1636, pp.245-259, Springer, 1999.
[8] A. Biryukov and D. Wagner. Advanced Slide Attacks. In *Proc. EUROCRYPT 2000*, LNCS 1807, pp.589-606, Springer, 2000.
[9] N. Courtois, G.V. Bard and D.Wagner. Algebraic and Slide Attacks on KeeLoq. In *Proc FSE'08*, LNCS 5086, pp73-96, Springer, 2008.
[10] I. Dinur, O. Dunkelman, and A. Shamir. Improved Attacks on Full GOST. IACR Cryptology ePrint Archive, 2011. http://eprint.iacr.org/2011/558.
[11] O. Dunkelman, N. Keller, J. Kim. Related-Key Rectangle Attack on the Full SHACAL-1. In Proc. SAC'06 LNCS 4356, pp. 28-44, Springer, 2006.
[12] S. Furuya. Slide Attacks with a Known-Plaintext Cryptanalysis. In Proc. Information and Communication Security 2001, LNCS 2288, pp. 214-225, Springer, 2002.
[13] S. Hong, J. Kim, G. Kim, S. Lee, B. Preneel. Related-Key Rectangle Attacks on Reduced Versions of SHACAL-1 and AES-192, In *Proc. FSE'05*, LNCS 3557, pp.368-383, Springer, 2005.
[14] T. Isobe. A Single-Key Attack on the Full GOST Block Cipher. In *Proc. FSE 2011*, LNCS 6733, pp. 290-305, Springer, 2011.
[15] O. Kara. Reflection Cryptanalysis of Some Ciphers. In *Proc. Indocrypt'08*, LNCS 5365, pp. 294-307, Springer, 2008.
[16] O. Kara. Self-Similarity Analysis of Block Ciphers. In Proc. II. National Cryptology Symposium, METU Ankara 2006.
[17] O. Kara. Reflection Attacks on Product Ciphers. IACR Cryptography e-Print Archive, `http://eprint.iacr.org/2007/043`, 2007.
[18] O. Kara and C. Manap. A new class of Weak Keys for Blowfish, In *Proc. FSE'07*, LNCS 4593, pp. 167-180, Springer, 2007.
[19] B.S. Kaliski, R.L. Rivest and T. Sherman. Is DES a Pure Cipher? (Results of More Cycling Experiments on DES). In *Proc. CRYPTO'85*, LNCS 218, pp. 212-222, Springer, 1985.
[20] J. Kelsey, B. Schneier and D. Wagner. Key-Schedule Cryptanalysis of IDEA, G-DES, GOST, SAFER, and Triple-DES. In *Proc. CRYPTO'96*, LNCS 1109, pp. 237-251, 1996.
[21] J. Kim, S. Hong, B. Preneel. Related-Key Rectangle Attacks on Reduced AES-192 and AES-256. In *Proc. FSE'07*, LNCS 4593, pp. 225-241, Springer, 2007.
[22] Y. Ko, S. Hong, W. Lee, S. Lee and J. Kang. Related Key Differential Attacks on 27 Rounds of XTEA and Full-Round GOST. In *Proc. FSE'04*, LNCS 3017, pp.299-316, Springer, 2004.
[23] L. Knudsen. Cryptanalysis of LOKI91. In *Proc. of AUSCRYPT'92*, LNCS 718, pp 196-208, Springer, 1993.
[24] J.H. Moore and G.J. Simmons. Cycle Structure of the DES with Weak and Semi-Weak Keys. In *Proc. CRYPTO'86*, LNCS 263, pp.9-32, Springer, 1986.
[25] J.H. Moore and G.J. Simmons. Cycle Structure of the DES for Keys Having Palindromic (or Antipalindromic) Sequences of Round Keys. *IEEE Transactions on Software Engineering*, pp. 262-273,No 13,1987.
[26] H. Seki and T. Kaneko. Differential Cryptanalysis of Reduced Rounds of GOST. In *Proc. SAC 2000*, LNCS 9743, pp. 315-323, Springer, 2000.
[27] I.A. Zabotin, G.P. Glazkov and V.B. Isaeva. Cryptographic Protection for Information Processing Systems. Cryptographic Transformation Algorithm. In *Government Standard of the USSR, GOST 28147-89*, 1989.

CAPTCHA Metinler için YSA Tabanlı Örüntü Tanıma Yaklaşımı

Uraz Yavanoğlu, Begüm Mutlu, Esra Şahin

Özet— Bu çalışmada web sayfalarına yapılabilecek bilgisayar programlarından kaynaklı saldırıları önlemek amacıyla kullanılan "Completely Automated Public Turing Test to Tell Computers and Humans Apart" (CAPTCHA) koruma yöntemi incelenmiş, güvenli bir CAPTCHA oluşturmak için kullanılan yöntemler araştırılmış, mevcut karakter tanıma sistemleri tartışılarak karakter tanımlama bazlı bir uygulama geliştirilmiştir. Sistem geliştirilme aşamasında Görüntü İşleme ve Yapay Sinir Ağları (YSA) modelleri tasarlanmıştır. Sistem, özgün olarak hazırlanan 5 farklı tip CAPTCHA'ya duyarlı şekilde eğitilmiş ve testi için sunulan karakter öbeklerini çözmesi için test edilmiştir. Yapılan testlerde Google ve E-Devlet kapısı tarafından kullanılan CAPTCHA'ların güvenli olmadıkları gösterilmiştir. CAPTCHA için Türkçe literatüre BİAT(Bilgisayar İnsan Ayırıcı Testi) kelimesi önerilmiştir. Tasarlanan tanımlama sistemlerine ise BİATET(Bilgisayar İnsan Ayırıcı Testi Eliminasyon Teknikleri) adı önerilmiştir.

Anahtar Kelimeler—CAPTCHA, Karakter Tanıma, Yapay Sinir Ağları, Örüntü Tanıma, BIAT, BIATET

Abstract— In this study, "Completely Automated Public Turing Test to Tell Computers and Humans Apart" (CAPTCHA) are used in order to prevent web site attack based on computer programs and bots. Image processing techniques and Artificial Neural Networks (ANN) had been used in this system. The system had been taught to recognize CAPTHA's which were originally prepared with 4 different types including Google and E-Government Portal of Turkey and it had been expected that the words which was reserved for testing can have been recognized by the system. BIAT is suggested to Turkish literature response for CAPTCHA abbreviation. The Turkish word BIAT is also English translation of allegiance. In general, the proposed techniques are called BIATET in Turkish. The Turkish sentence BIATET is also English translation of "to swear allegiance to".

Index Terms—CAPTCHA, Character Recognition, Artificial Neural Networks, Pattern Recognition

I. GİRİŞ

Teknolojideki gelişmeler, kişilerin hayatlarını kolaylaştırmak için kaliteli ve yararlı çözümler sunmakla birlikte; oluşturulan sistemlerin karşı karşıya kalacağı tehlikelere de kapı açmaktadır. Özellikle, yapay öğrenme konularının çalışıldığı günümüzde insan gibi davranıp karar verebilme yeteneğini hedefleyen sistemlere saldırı yaparak onları etkisiz kılmaya çalışan robot programların sayısında ve becerilerinde büyük ölçüde artış görülmektedir [1-19]. Bu sebeple sistemlerin güvenliği için, sisteme dahil olan bireylerin insan mı yoksa program mı olduğunu anlayabilen tasarımlar geliştirmek zorunlu bir ihtiyaç haline gelmiştir. Bu ihtiyaç nedeniyle özellikle web sayfalarında yaygınca görülen CAPTCHA kullanımı ortaya çıkmıştır. Bu uygulamalarda genellikle yatay ve düşey eksenli döndürmeler ile değiştirilen sırasız karakterler bir araya getirilmekte ve sayfaya erişmeye çalışan kişilere bu harflerin neler olduğu sorularak, verilen cevaplara göre insan-makine ayırımı yapılmaya çalışılmaktadır.

Oluşturulan CAPTCHA'lar Optik Karakter Tabanlı Olan ve Optik Karakter Tabanlı Olmayan CAPTCHA'lar olarak sınıflandırılabilir [1]. Optik karakter tabanlı CAPTCHA türlerine örnek olarak Gimpy Metodu CAPTCHA'ları, Pessimal Print ve Baffle Text CAPTCHA'lar verilebilir [2-4]. Bunlardan Gimpy Metodu, Carnegie Mellon Üniversitesi tarafından geliştirilmiş kelime ve sözlük tabanlı, güvenlik düzeyi düşük bir CAPTCHA oluşturma metodudur [2]. Pessimal Print Metodu ile oluşturulan CAPTCHA'lar font ve ardışık görüntü setleri üzerinde yapılan değişimleri, Optik Karakter Tanıma araçlarının kelimeyi tanımasını zorlaştırma amaçlı kullanmaktadırlar [3]. Baffle Text CAPTCHA'lar ise kişilerde varolan Gestalt Psikolojisi'nin bir sonucu olarak oluşturulmuş olup Gimpy Metodu'na benzer yaklaşımlar sunar. Gestalt kuramcıları, kişilerin bütünü parçalar halinde değil anlamlı, örgütlenmiş bir bütün olarak algıladıklarını savunur [4]. Buna bağlı olarak yerleştirilen CAPTCHA'larda bazı parçalar, bütünü bozmayacak şekilde yok edilir ve kişilerin algılayabileceği ancak bilgisayarların optik karakter tabanlı çözümlerinin bunu algılamakta yetersiz kalacağı görüntülere yer verilir. Optik Karakter Bazlı CAPTCHA'ların sistem güvenliğini sağlamalarında önlerine çıkan engellerden birisi OCR olarak adlandırılan Optik Karakter Tanımlama (Optical Character Recognation (OCR)) metodudur. Bu yöntemin kullanımı ile CAPTCHA'ların içerisindeki karakterlerin bilgisayarın algılayabileceği formata çevrilmesi mümkündür.

OCR , karakter tanımlamada sıklıkla kullanılmakla birlikte bir araç yardımıyla, el yazısı, bilgisayar yazısı gibi kaynak dokümanları bilgisayar ortamına aktarma, bu dokümanları, bilgisayar diline sayısallaştırılarak çevirme işlemi olarak özetlenebilir. Temel olarak girdi tipine göre ikiye ayrılmaktadır [5]. Bunlar çevrimiçi tanıma ve çevrimdışı tanıma sistemleridir. Çevrimiçi tanıma sistemlerinde, girdi olarak kullanılan görüntü sistem tarafından tanımlanır. Dijital tabletler üzerine yazılmış bir yazının sistem tarafından

Uraz Yavanoğlu, Gazi Üniversitesi Mühendislik Fakültesi Bilgisayar Mühendisliği Maltepe/Ankara adresinde çalışmaktadır (uraz@gazi.edu.tr).
Begüm Mutlu, Gazi Üniversitesi Mühendislik Fakültesi Bilgisayar Mühendisliği Lisans Öğrencisidir (mutlubegumbm@gmail.com).
Esra Şahin, Gazi Üniversitesi Mühendislik Fakültesi Bilgisayar Mühendisliği Lisans Öğrencisidir (esrasahince@gmail.com).

algılanması bu yöntem ile gerçekleştirilmektedir. Çevrimdışı tanıma sistemlerinde ise girdi olarak kullanılan kaynak, bilgisayar diline çevrilmiş bir resim yada tarayıcıdan alınmış bir görüntü halinde sunulmaktadır [5].

OCR aygıtları, verileri bilgisayar diline çevirirken ışık algılama mekanizması ve lazer teknolojisini kullanmaktadır. Bu aygıtlar basit olarak daire, kare, üçgen vb. tiplerdeki şekilleri algılayabildiği gibi karmaşıklaştırılmış şekilde harf ve rakam kümelerini de okuyabilmektedir. Bazı sınavlarda cevap kayıtlarını okuyup değerlendiren optik okuyucular da OCR tekniğini kullanmaktadır [6]. Bu özellikleriyle OCR, CAPTCHA güvenliğini tehlikeye atan teknolojilerden bir tanesi olarak düşünülebilir.

OCR Tabanlı Olmayan CAPTCHA'lardan Örtülü (Implicit) CAPTCHA kullanıcıdan belirli bir noktaya tıklamasını isterken; Text-to-Speech (Metni Seslendirme) yöntemini kullananlar dijital dosyaları sese çevirip; kullanıcıdan, dinlediği ses içerisinde geçen anlamlı sözleri, belirtilen bölgeye yazmasını bekler [2]. Bunlara ek olarak Kolaj CAPTCHA'lar kolaj sanatını kullanıcıya sunduğundan bilgisayar tarafından çözümü zor olan bir tür haline gelmektedir [2].

CAPTCHA'lar, kötü amaçlı yazılımlara büyük bir engel teşkil ederler. Bu nedenle saldırgan yazılımlar, görüntü işleme ve yapay öğrenme tekniklerini kullanarak harfleri sınıflandırmaya çalışmaktadırlar. Araştırmacılar tarafından kırılan ve güven seviyesi azalan CAPTCHA'ların yerini her geçen gün yeni ve daha karmaşık CAPTCHA'lar almakta; bu durum kötü amaçlı yazılımların işini zorlaştırsa da sistemleri kullanıcı dostu olmaktan çıkardığı için geleneksel CAPTCHA türleri kadar popülerlik sağlayamamaktadır. Sonuçta bir CAPTCHA'nın kalitesi, bilgisayar tarafından algılanması ve çözülmesinin zor; insanlar tarafından ise kolay olmasına bağlıdır.

Bu çalışma, görüntü işleme teknikleri ve yapay sinir ağları yardımıyla belirlenen formlardaki CAPTCHA'ların çözülebileceğini ve sistemlerin özellikle OCR bazlı CAPTCHA'lardan ziyade, başka yaklaşımlarla korunması gerektiğini ortaya koymaktadır. İlgili dokümanın ikinci bölümünde literatürde varolan CAPTCHA, karakter tanıma ve YSA konulu çalışmalara, üçüncü bölümünde Yapay Sinir Ağları ile ilgili bilgilere ve dördüncü bölümde yapılan uygulamanın aşamaları olan görüntü işleme tekniklerine, eğitim ve test sonuçları ile uygulamanın Gmail Captcha'ları üzerindeki testine yer verilmiştir. Beşinci bölümde ise yapılan araştırmalar sonucu elde edilen bulgular tartışılmış, yapılan çalışmaların sonuçları değerlendirilmiştir.

II. YAPILAN ÇALIŞMALAR

CAPTCHA'lar web sayfalarında sıklıkla rastlanan ve sistemi bilgisayar ataklarından korumak için tasarlanmış öğelerdir. Temel amacı güvenliği sağlamak olan CAPTCHA'ların ne kadar güvenli oldukları ise günümüzün tartışma konularındandır. Luphowski tarafından yapılan bir çalışmada CAPTCHA'ların güvenlik düzeyleri incelenmiş; MSN ve Yahoo gibi portallara yapılmış saldırılar üzerinde araştırmalar yapılmıştır [7]. İnternet'te web sayfalarına sayısız saldırı olduğunun üzerinde durulmuş ve güvenlik seviyesi en düşük CAPTCHA'lar, Yahoo'nun sahip olduğu CAPTCHA'lar olarak kaydedilmiştir [7]. CAPTCHA güvenliğini arttırma amacıyla Shirali-Shahreza ve arkadaşları tarafından yapılan çalışmada Buffle Text Metodu ile oluşturulan ve içerisinde Farsça/Arapça karakterleri barındıran bir CAPTCHA yapımı önerilmiştir [8]. Ancak bu CAPTCHA'lar evrensel nitelik taşımaması sebebiyle tercih edilmemektedir. Evrensel nitelik taşımayan bu yaklaşımdan ziyade varolan CAPTCHA türlerinin güvenlik seviyesini arttırmayı hedefleyen Chellapilla ve arkadaşları tarafından yapılan araştırmada güvenli CAPTCHA'ların oluşturulması için gerekli parametreler (karakterlerin konumu, karakter sayısı, boyut, font farklılaşması, eğim) belirlenmiştir [9]. Aynı amaca yönelik farklı bir yaklaşım ise Yadava ve arkadaşlarının çalışması olarak gösterilebilir [2].

Bu çalışmada sistem güvenliğinin sağlanması için CAPTCHA resminin özellikleri ile ilgilenilmemiştir. Çalışmada, sistem saatinden bağımsız olarak değişen CAPTCHA resimleri kullanılmıştır. Bir saldırganın, sisteme girebileceği zaman dilimini kısaltması ve ona fırsat vermeden yeni resimleri ortaya çıkarması açısından, bu çalışmanın, web sayfalarının güvenlik düzeyini büyük ölçüde arttırabileceğini söylemek mümkündür [2].

CAPTCHA görüntüleri içerisindeki yazının bilgisayar tarafından anlaşılabilmesi için karakter tanıma yaklaşımı sıklıkla kullanılmaktadır. Karakter tanımlama konusunda literatürde yer alan çalışmalar incelendiğinde genel olarak 2 ana başlık üzerinde performans arttırmaya yönelik yaklaşımlar geliştirildiği görülmektedir [10]. Bu başlıklardan ilki karakterlerin görüntü içerisinde bulunması, birbirinden ayrıştırılması ve özellik çıkarımının gerçekleştirilmesidir [10]. İkincisi ise ayrıştırılan karakterin sınıflandırmaya tabi tutularak hangi karakter olduğunun bilgisayarlar tarafından algılanabilmesidir [10].

Karakteri görüntü içerisinde bulma ve birbirinden ayrıştırma işlemi genel olarak bölümleme (segmentation) olarak isimlendirilmiştir ve bu işlemin başarımını arttırmaya yönelik çalışmalar yapılmaktadır [10]. Çünkü iyi bir bölümleme aşaması sınıflandırma başarımını arttıran önemli bir etkendir. Huang ve arkadaşları, bölümleme ve gürültü ayrıştırmayı hedefleyen Chellapilla'nın Algoritması'na ekledikleri teknikle, bu algoritmanın %9'luk başarımını %14'e çıkarmış; CAPTHA'ları tanıma konusunda da %60'larda başarım elde edilmiştirdir [10].

Özellik çıkarım konulu literatür çalışmaları sınıflandırma başarımını arttırmayı hedefleyen diğer bir çalışma grubudur. Bu konuda Yang ve arkadaşları, yaptıkları çalışmada, istatistiksel özellik çıkarımının yanında yapısal özellik çıkarımı yaklaşımının, kullandıkları YSA performansını arttırdığını göstermişlerdir [11]. Benzer şekilde Onak tarafından yapılan çalışmada Fourier ve dalgacık analizine dayalı özellik çıkarım yöntemlerinin sınıflandırma başarımına etkisi konusunda bir çalışma sunulmuştur [12]. Ay ve Varol ise yaptıkları çalışmada Düzenli Özellik Çıkarma Yöntemi'ni kullanarak, Yapay Sinir Ağları ile yaptıkları sınıflandırma başarımını %100 seviyesine çıkardıklarını belirtmişlerdir[5].

Karakter tanımlamanın ikinci temel aşaması olan sınıflandırma işlemi için birçok teknik kullanılmaktadır. Bunlardan YSA, en çok tercih edilen sınıflandırma yöntemlerinden bir tanesidir. YSA konusunda, hangi algoritmanın hangi verilerle daha yüksek performansa sahip

olacağı kıyaslamasına dayalı birçok çalışma mevcuttur [13, 14, 15]. Araz tarafından gerçekleştirilen çalışmada, el yazısı karakterler için ileri beslemeli bir yapay sinir ağı üzerinde iki farklı algoritmanın (Shashank Algoritması ve Geriye Yayılım Algoritması) performansı karşılaştırılmıştır [13]. Çalışma sonucunda eğitim için kullanılan veri seti için Geriye Yayılım Algoritması'nın performansının (%83), Shashank Algoritması'nınkine (%61) nazaran daha yüksek olduğu gözlenmiştir [13]. YSA tekniklerini karakter tanımlamada kullanan başka bir çalışma da Erdem ve Uzun tarafından yapılmıştır. Uygulamada Times New Roman, Arial ve el yazısı karakterlerini tanıyabilen bir sistem geliştirilmiş; uygulamanın YSA başarımı %96 civarında kaydedilmiştir [14]. Şahin de çalışmasında Türkçe Karakter Tanıma işlemini YSA yaklaşımı ile gerçekleştirmiştir [15].

Karakter tanıma için YSA harici sınıflandırma tekniklerini kullanmak da mümkündür [16, 17]. Şekerci ve Kandemir, yaptıkları çalışmada K-En Yakın Komşu Algoritması'nı kullanarak karakter tanımlamada %100 başarı elde etmişlerdir [16]. Çalışmada en iyi başarıyı elde etmek için farklı "k" değerleri denenmiş ve o eğitim seti için "k" değeri, küçük harflerde 3, büyük harflerde 5 olarak tanımlanmıştır [16]. Demirci ise farklı fonksiyonlarını karşılaştırdığı Destek Vektör Makineleri ile çözüme gitmiş ve Radyal Tabanlı Fonksiyon ile en yüksek başarım yüzdesine ulaşmıştır [17].

Karakter tanımlama konusunda sıklıkla üzerinde durulan yöntemlerden bir tanesi OCR (Optic Character Recognation)'dır. Bu işlem bir araç yardımıyla yapılır ve karakterlerin bilgisayarca anlaşılır olmasını sağlayacak dönüşümleri gerçekleştirir. Ancak bu metot, karakterlerin yapısal özelliklerinden (font, boyut, koyu yazılıp yazılmamış olması, eğim vb.) çok fazla etkilenmektedir [18]. Bu durumun çözümü için SIFT (Scale İnvariant Feature Transform) Metodu'nu kullanarak sınıflandırma başarımını arttırmanın mümkün olduğunu savunan Zahedi ve Eslami, çalışmayı Farsça/Arapça karakterler için bir font tanıma uygulamasında deneyip %100 tanımlama başarısına ulaştıklarını belirtmişlerdir [18]. İlgili çalışma, karakter tanıma işlemini CAPTCHA kırma amaçlı incelenmiş olsa da bu konu başka problemlere de çözüm olabilecek niteliktedir [18].

Kaplan, Sağıroğlu ve Çolakoğlu tarafından yapılan çalışmada karakter tanıma işlemi YSA ile gerçekleştirilmiş ve bir Plaka Tanıma Sistemi tasarlanmıştır [19]. CAPTCHA türlerini kırmaya yönelik yapılan çalışmaları incelemek adına yapılan literatür çalışmasında, varolan CAPTCHA türlerine birçok atak yapıldığı ve bu atakların büyük başarım oranlarına sahip olduğu görülmüş; bu çalışmalardan birkaçı Tablo 1'de görselleştirilmiştir. Burada literatür çalışmasının kendisiyle ve çözülen CAPTCHA türüyle ilgili bazı bilgiler yer almakta; yapılan uygulamaya ve kullanılan tekniklere yer verilmektedir. Buna göre CAPTCHA türleri arasında basit bir karşılaştırma yapmak mümkündür. CAPTCHA türlerinden daha yüksek başarım oranlarıyla çözülebilenler Optik Karakter Tabanlı CAPTCHA'lardır. 2003 yılında Mori ve Malik; 2004 yılında ise Moy ve Jones tarafından yapılan çalışmalarda farklı teknikler kullanılarak Gimpy Metodu ile oluşturulan CAPTCHA'ların çözümünde %90'larda başarılar elde edilmiş; bu başarı oranı harf sayısı, kelime uzunluğu gibi parametrelere bağlı olarak düşmüş olsa bile bu türdeki CAPTCHA'lar için büyük tehdit oluşturmuştur [21, 22].

Resimli CAPTCHA'lar, karakter tanımlama yöntemlerinden etkilenmediğinden daha güvenilir bir yaklaşım olarak düşünülmüş ancak bu tür CAPTCHA'ların yaygınlaşmasının bir sonucu olarak bu CAPTCHA'ların güvenliğini tehdit eden çalışmalar yapılmaya başlanmıştır [1, 23]. Bunun için yapılan Resim Sözlüğü Tabanlı Ataklarla bu CAPTCHA türünün çözümü için de büyük başarım oranları elde edilmiştir [1].

Kullanıcıya bir ses dinleterek bu ses içerisindeki anlamlı karakterleri yazmasını bekleyen CAPTCHA türü olan Audio CAPTCHA'ların kırılması için ise 2008 yılında Tam ve arkadaşları tarafından Ada Boost, Destek Vektör Makineleri (SVM) ve K-En Yakın Komşu (K-NN) teknikleri ile bir çalışma gerçekleştirilmiş; bu teknikler karşılaştırılmış ve %71'e varan başarım oranları ile CAPTCHA'nın çözümünü sağlanmıştır [20].

CAPTCHA'ların mobil uygulamalarda özellikle Çoklu Dokunmatik (Multi-touch) Teknolojisi ile bütünleştirilmesi, bu CAPTCHA'ların çözümünü zorlaştırmaktadır [25]. Ancak bu uygulamanın da çözülebilir olduğunu kanıtlayan Lin ve arkadaşları 2011'de sundukları bir çalışmada bu CAPTCHA'ları %75 oranında çözdüklerini belirterek yine dokunmatik ekranlarla uyumlu olan yeni bir Mobil CAPTCHA yaklaşımını ortaya atmışlardır [25].

III. YAPAY SİNİR AĞLARI

İnsanı insan yapan en önemli özellik olan zeka; düşünme, algılama, öğrenme, karar verme, hatırlama, tecrübe edinme ve seçim yapma gibi önemli yetenekleri beraberinde getirmektedir. Bu özellikleri ile insanlar, bu yetilere hiç sahip olmayan veya sınırlı ölçüde sahip olan canlılardan üstün durumdadırlar. Teknolojinin günümüzdeki haline ulaşmasındaki en önemli etkenler; doğayı anlamak için çeşitli araştırmaların yapılması, onun çalışma şeklini taklit eden sistemler geliştirmesi ve onları doğaya sunmaya çalışmasıdır. Bu yüzden uçakların, gemi ve denizaltıların hatta uydu ve diğer uzay araçlarının tasarımında doğa motiflerine rastlanması kaçınılmazdır. Yapay Zeka teknolojisi de teknolojinin belirtilen amacının insan özelliklerini hedef alan bir sonucudur. Bilim adamları, düşünen bir makinenin tasarlanabilir olup olmadığını araştırmak adına yapay zeka bilim dalını ortaya çıkarmışlardır. Günümüzde hâlen gelişmekte olan ve Uzman Sistemler, Bulanık Mantık, Genetik Algoritma ve Yapay Sinir Ağları olarak alt dallara ayrılmış olan bu teknoloji, birçok alanda kullanılmak adına geliştiricilere sunulmuştur [26].

Bu çalışmada, Yapay Zeka çatısı altındaki tekniklerden Yapay Sinir Ağları (YSA) konusu işlenmiş ve uygulamanın geliştirilmesinde kullanılmıştır.

YSA, Elmas'ın tanımı ile, "insan beyninden esinlenerek geliştirilmiş, ağırlıklı bağlantıların birbirine bağlanan ve her biri kendi belleğine sahip işlem elemanlarından oluşan paralel ve dağıtılmış bilgi işleme yapılarıdır" [26]. Bir diğer ifadeyle YSA'nın yapısı beyindeki sinir hücrelerinin oluşturduğu ağ yapısının bilgisayar ortamına uyarlanması ile oluşmaktadır [27]. Ağ içerisinde yer alan işlem elemanları yapay sinir hücreleri olarak anılırken içerisinde yer alan elemanlar beyindeki sinir hücrelerine benzer niteliktedir [28].

TABLO 1
CAPTCHA KIRMAYA YÖNELİK BAZI ÇALIŞMALAR

Referans	Captcha Türü	Kırılma Metodu/Metotları			Destek	Kırılma Başarısı	Yılı
[1]	Naming CAPTCHA	Ratgele Tahmin Atakları	Resim Sözlüğü Bazlı Ataklar		-	98.44%	2010
	Anomally CAPTCHAs					%59,36	
	Collage CAPTCHA					%66,41	
[10]	MSN CAPTCHAs	Chellapilla'nın Algoritması	Önerilen Algoritma		-	60.57%	2008
	YAHOO CAPTCHAs					%69,90	
[20]	Audio CAPTCHA	Ada Boost	SVM	K-NN	Intel Corporation, Army Research Office, Carnegie Mellon University	71%	2008
[21]	EZ-Gimpy	Geometrik Özellikler	Maksimum Olasılık Testi		-	99%	2004
	4 Letter Gimpy					78%	
[22]	EZ-Gimpy	Algoritma A	Algoritma B		-	92%	2003
	3 Words Gimpy					33%	
[23]	Vidoop CAPTCHA	Destek Vektör Makinesi	K-En Yakın Komşu		-	%96	2009
[24]	Visual CAPTCHA	Naif Model Tanıma Algoritması			EU-funded NoE ReSIS	60%	2007
[25]	Mobil Cihazlar için Oluşturulan CAPTCHA	Erozyon Tabanlı CAPTCHA Kırma Algoritması			-	75%	2011
[Mevcut Çalışma]	GMAIL Gimpy CAPTCHA'ları	YSA Tabanlı Karakter Bazlı Yaklaşım			-	%93	2012
		YSA Tabanlı Kelime Bazlı Yaklaşım				%37	

Bir yapay sinir hücresinin girişler, girişlere ait ağırlıklar, toplama işlevi, etkinlik işlevi (transfer fonksiyonları) ve çıkış olmak üzere 5 ana öğesi bulunmaktadır. Ağ üzerinde girişler, dışarıdan (başka bir yapay sinir hücresinden veya dış dünyadan) aldığı bilgiyi sinir hücresine dahil ederken ağırlıklar bu girişlerin ağ üzerindeki etkisini ifade etmektedir. Girişlerin ağırlıkları ile çarpımlarının toplamının hesaplanıp eşik değer (€) ile işleme tabi tutulması toplama işlevinde gerçekleşmekte ve bu işlemin sonucu etkinlik işlevinden geçirilip çıkışa aktarılmaktadır [26].

Yapay Sinir Ağları'nın eğitimi, giriş değerlerinin ağırlıklarının, sonuç değerini kabul edilebilir hata değerine ulaştırıncaya kadar değiştirilmesi sürecini ifade eder. Kabul edilebilir hata değerine ulaşıldığında öğrenme işlemi tamamlanmış olur [26, 27]. Eğitimin sonlanması için dikkat edilebilecek bir diğer parametre ise iterasyon sayısıdır. Ancak bu değerin çok küçük olması, algoritmayı erken durduracağından test başarım oranını düşürebilmektedir. Bu sebeple, geliştirilen uygulamada iterasyon sayısından ziyade hata değeri kriterine dikkat edilerek eğitim sonlandırılmıştır.

Geleneksel bilgisayarların algoritmaya bağlı kalarak, matematiksel olarak ifade edilebilen problemleri çözmesi

mümkündür ancak YSA, matematiksel olarak ifadesi güç olan doğrusal olmayan problemlerin çözümü için oluşturulmuş bir teknik olduğundan özellikle veri madenciliği uygulamalarında sınıflandırmada olmak üzere; model seçimi ve sınıflandırılması, işlev tahmini gibi problemlerde başarılı sonuçlar elde edilmesini sağlamaktadır [26]. Bu özellikleri ile YSA, robotik, bankacılık ve finans, elektronik, haberleşme, tıp, trafik durum kontrolü gibi alanlarında sınıflandırma ve karar verme aşamasında kullanılabilir yaklaşımlar sunmaktadır [26, 30, 31]. YSA'nın bu özellikleri, geliştirilen uygulamada tercih edilmesinin sebebidir.

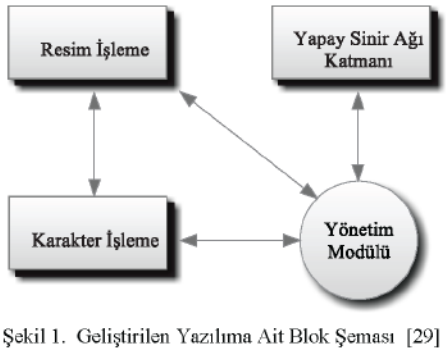
IV. GELİŞTİRİLEN UYGULAMA

İlgili çalışmada, görüntü işleme teknikleri ve YSA kullanımı ile belirli formatlarda hazırlanan CAPTCHA'ların bilgisayar destekli olarak algılanabilmesine imkan sağlayan bir sistem geliştirilmiştir. Bunun için öncelikle çok katmanlı, ileri beslemeli bir yapay sinir ağı ve diğer eğitim algoritmalarından daha başarılı sonuç vermiş olan (Tablo 2), Ölçeklendirilmiş Eşlenik Gradyand Eğitim Algoritması kullanılmıştır. Bu çalışma kapsamında yapılan işlemler, ilerleyen alt başlıklarda detaylandırılmıştır.

A. Geliştirilen Yazılıma Ait Uygulama Akışı

Problemin çözümü için bir yazılım geliştirilmiş ve deneysel test çalışmaları bu ortam üzerinden yapılmıştır. Uygulamanın blok şeması, Şekil 1'de gösterilmektedir. Buna göre sistemde resim işleme, karakter işleme modülleri etkileşimli olarak yönetim modülüne bağlıdır. Yapay Sinir Ağı Katmanı ise aynı şekilde yönetim modülünce işleme dahil edilmektedir. Şekil 2'de BİATET (Bilgisayar İnsan Ayırıcı Testi Eliminasyon Teknikleri) uygulaması akış diyagramında kullanıcının seçtiği resim dosyası okunmakta ve görüntü işleme teknikleri ile gürültüsünden arındırılmaktadır. Görüntü işleme aşamasında, resim içerisinde birden fazla karakterin olması halinde bu karakterlerin ayrıştırılması işlemi de bulunmaktadır.

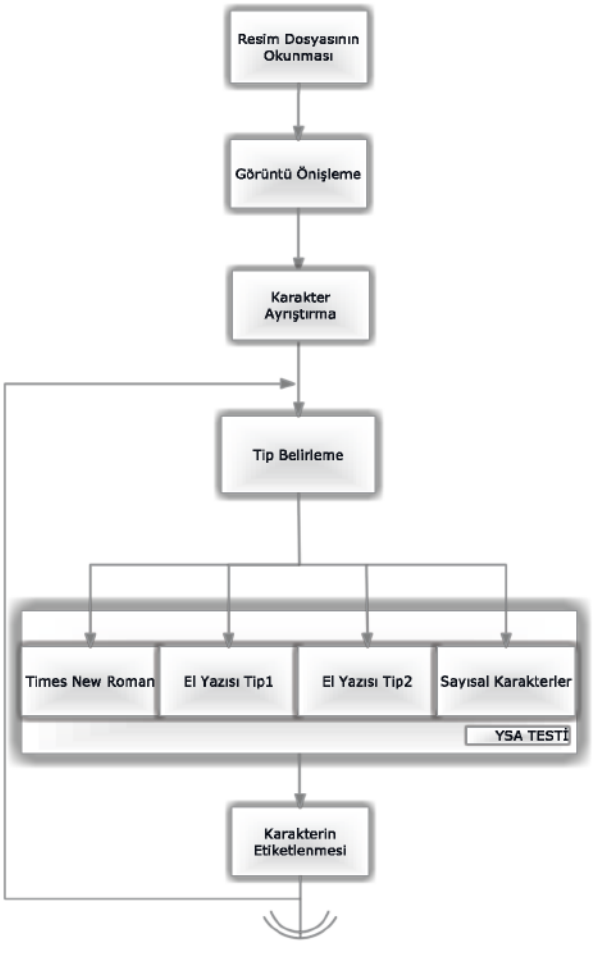
Ardından karakterler kendileri için uygun tipteki yapay sinir ağına aktarılıp çözümlenmeye çalışılmaktadır. Son aşama olarak ağdan dönen matris karakter etiketleme aşamasında kullanıcının göreceği alfabetik karakterlere dönüştürülür.



Şekil 1. Geliştirilen Yazılıma Ait Blok Şeması [29]

B. Özellik Çıkarım

YSA eğitiminin gerçekleştirilmesi için gerekli giriş değerleri içerisinde eğitimde kullanılacak karakterleri barındıran resim dosyalarının görüntü işleme teknikleri ile belirli bir formata getirilmesiyle oluşturulmuştur. Bunun için ilk olarak resim dosyalarında bulunan bilgilerin bir özellik matrisine aktarımı gerçekleştirilmiştir.



Şekil 2. BİATET (Bilgisayar İnsan Ayırıcı Testi Eliminasyon Teknikleri) Uygulama Akış Şeması

Bu özellik matrisinin YSA eğitiminde giriş matrisi olarak çalıştırılabilmesi için bazı önişlemlerden geçirilmesi ağ performansını arttıracak önemli bir kriterdir. Bu sayede özellik matrisindeki gürültülü verinin azaltılması hedeflenmiştir. İlerleyen bölümlerde özellik çıkarım aşamaları ayrıntılı olarak verilmiştir.

RGB Renk Uzayından Gri Tona Geçiş

Dosyadan okunan ve özellik matrisi çatısı altında birleştirilen veriler RGB renk uzayı formundadır. RGB Renk Uzayı bir birim küpün içerisinde belirli oranlarda karıştırılan kırmızı, yeşil ve mavi renklerinin ara renkleri oluşturabilmesi amacıyla tasarlanmıştır. Bilgisayar ekranları haricinde Katodik TV tüplerde ve tarayıcı donanımlarda da kullanılmaktadır [29]. Bu renk uzayı, üç boyutlu bir koordinat düzleminde Şekil 3'deki gibi yapılandırılmış olarak düşünülmektedir.



Şekil 3. RGB Renk Uzayı

RGB Renk Uzayı'nda oluşturulan resimlerde her piksel 3 boyutlu olarak düşünüldüğünden (Şekil 3), resim içerisinde algılanmak istenen nesnelerin belirlenmesi işlemi zorlaşmaktadır. Bu yüzden gelen resimler siyah beyaza çevrilerek her bir pikselin bir yada sıfır değerine sahip olması ve bu sayede renklerin yarattığı karmaşadan uzaklaşılması gerekmektedir.

Eşikleme (Thresholding) Evresi

Siyah beyaza çevirilen resimlerde bazı bölgeler grinin farklı tonlarında tutulmaktadır. Bu yüzden resmin içindeki gri bölgelerin daha kesin olan 1 ve 0 değerlerine yuvarlanması gerekmektedir. Otsu Eşik Belirleme Yöntemi kullanılarak gerçekleştirilen eşikleme işlemiyle, belirlenmiş eşik değerin altındaki piksel değerleri sıfıra; üstündekiler ise bire yuvarlanarak ilgili görüntüler oluşmuştur. Bu sayede resim içerisindeki tonlamalar ortadan kalktığı gibi ortam gürültüsü de büyük ölçüde azalmaktadır.

Kırpma Evresi

Gri tona çevrilip eşikleme işlemine tabi tutulan resim için yapılması gereken işlemlerden en önemlisi, içerisindeki karakteri bulup karakterin öğesi olmayan pikselleri resimden koparma işlemidir. Bunu geçekleştirmek için uygulamada resmin dört köşesinden içe doğru tarama yapılarak karakterin başladığı noktaya kadarki kısım resimden ayrıştırılmıştır.

Karakter Matrisinin Çıkarılması

Gri tona çevrim, eşikleme ve kırpma evrelerine tabi tutulan ve içerisinde tek bir karakteri barındıran resim (Şekil 4), bütün karakterler için standart olarak değerlendirilmesi açısından 50x50 olarak boyutlandırılmış matris formuna (Şekil 5) dönüştürümüştür. Daha sonra oluşan matris 2500x1 forma dönüşecek şekilde yeniden boyutlandırılmıştır.



Şekil 4. Görüntü Önişleme Aşamaları
a. Orjinal resmin görüntüsü
b. Gri tona çevrilmiş resmin görüntüsü
c. Eşikleme işleminden sonraki resmin görüntüsü
d. Kırpma işlemi sonunda resmin görüntüsü



Şekil 5. "a" Karakteri için 50x50 Boyutlu Matris Formu

Giriş Matrisinin Oluşturulması

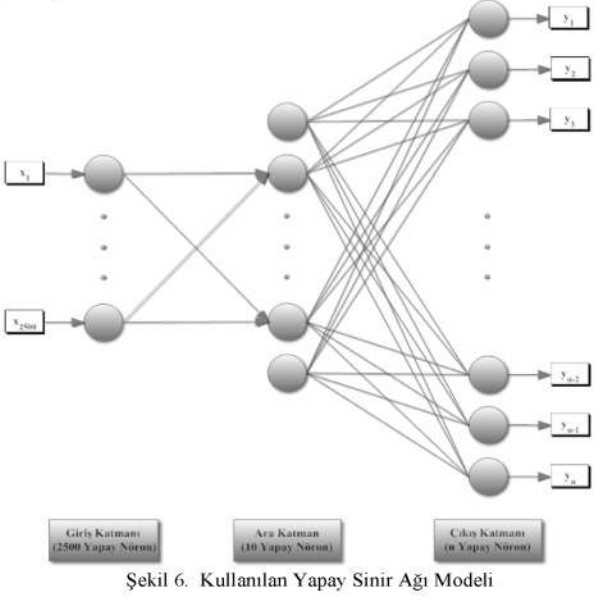
Eğitim için kullanılacak bütün karakterlerin karakter matrisleri çıkarıldıktan sonra bu matrisler kolon bazlı olacak şekilde birleştirilerek 2500x2500 boyutunda giriş matrisi oluşturulmuş ve ağ eğitiminde giriş parametresi olarak eşleştirilmiştir.

C. Yapay Sinir Ağı Eğitimi ve Performansı

Çalışmanın uygulama aşamasında özellik çıkarım işleminin ardından YSA eğitimine başlanmış; test edilen birden çok eğitim algoritmasının sonucunda ilgili eğitim seti için en başarılı yöntem olan Ölçeklendirilmiş Eşlenik Gradyand Eğitim Algoritması ile eğitilen İleri Beslemeli Ağ (Şekil 6) uygulamanın kendisine entegre edilmiştir. Giriş ve çıkış katmanlarından oluşan Şekil 6'da şematize edilmiş ağ modelinde giriş katmanında 2500, ara katmanında 10 yapay sinir hücresi bulunurken; çıkış katmandaki yapay sinir hücre sayısı dosyadan okunan karakter sayısı (n) kadardır.

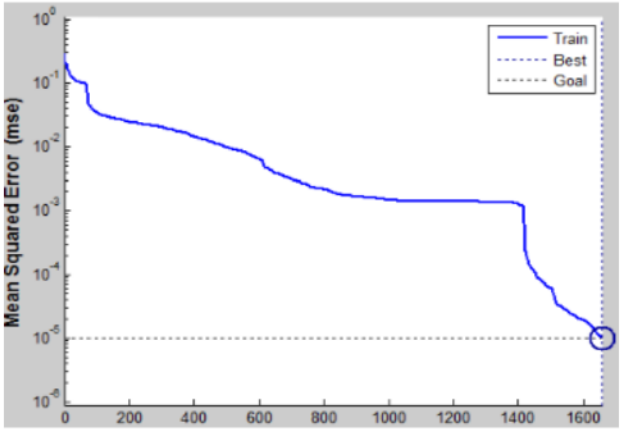
Ölçeklendirilmiş Eşlenik Gradyand Eğitim Algoritması, genel amaçlı bir eğitim algoritması olup Conjugate Algoritması'nda yapılan ve performans açısından düşüşe sebep olan "her iterasyonda arama (line search) yapma" işlemini performans ve zaman açısından geliştirecek bir boyuta geçirmiştir. Bu özelliğinin bir getirisi olarak Ölçeklendirilmiş Conjugate Algoritması olarak anılmaktadır. Bu algoritma oldukça karmaşık bir yapıya sahip olup temelde Conjugate Gradient yaklaşımının performansını arttırmayı hedeflemektedir [29].

Şekil 7'de SCG Algoritması ile yapılan eğitime ait performans grafiği bulunmaktadır. YSA eğitiminin sonlanma kriteri olarak iterasyon sayısı değil hata değeri dikkate alınmıştır.



Şekil 6. Kullanılan Yapay Sinir Ağı Modeli

Bunun için iterasyon sayısı çok yüksek (10000) tutulmuş ve uygulamanın en küçük karesel hataya (MSE) ulaştığında sonlanması sağlanmıştır. Grafiğe göre en yüksek eğitim performansına karesel hatanın $9.9213x10^{-6}$ değerinde kaydedildiği 1656. iterasyonda ulaşılmıştır.



Şekil 7. SCG Algoritması Performans-İterasyon Sayısı Grafiği

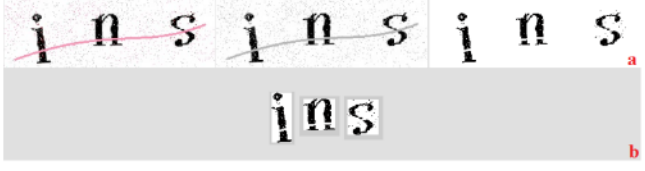
Ölçeklendirilmiş Eşlenik Gradyand Algoritması'nın ve test edilen diğer eğitim algoritmalarının performansı Tablo 2'de aktarılmıştır. Uygulama kapsamında testi yapılan diğer eğitim algoritmaları, Gradient Descent (GD), Gradient Descent with Momentum (GDM), Gradient Descent with Momentum and Adaptive Learning Rate (GDX) ve Resilient (RP) algoritmalarıdır. Eğitim başarım ölçülmesinde performans kriteri olarak MSE (Mean Squared Error) dikkate alınmış ve en küçük hata düzeyine Scaled Conjugate Gradient (SCG) Algoritması ile ulaşılmıştır.

TABLO 2
YSA EĞİTİMİ PERFORMANS DEĞERLENDİRMESİ

		Katm. Nöron Say.		Ağ Performansı	
		Giriş	Çıkış	İtr.	MSE
El Yazısı Tip 1	GD	2500	26	4443	0.16198
	GDM	2500	26	319	0.074398
	GDX	2500	26	271	0.037318
	RP	2500	26	1375	0.002267
	SCG	2500	26	5194	2.0732e-006
Times New Roman Tipi	GD	2500	23	10000	0.038101
	GDM	2500	23	10000	0.038084
	GDX	2500	23	325	0.04104
	RP	2500	23	9672	0.028147
	SCG	2500	23	1656	9.9213e-006
El Yazısı Tip 2	GD	2500	26	10000	0.078424
	GDM	2500	26	1000	0.077086
	GDX	2500	26	312	0.03707
	RP	2500	26	1522	0,03348
	SCG	2500	26	8335	3.6188e-007
Sayısal Karakterler	GD	2500	16	10000	0.033582
	GDM	2500	16	10000	0.045699
	GDX	2500	16	319	0.050996
	RP	2500	16	119	0.0096468
	SCG	2500	16	3779	6.8801e-007

D. *Uygulamanın Kelime Bazlı Test Edilmesi*

Yapılan çalışmada eğitim işleminin ardından yapılan test yazılımının ilgili CAPTCHA'larla kullanılması ardından karakter bazlı test işleminin başarım oranı %100 olarak gözlenmiştir. Ancak ortama gürültü eklenmesi, karakterin belirli bölümlerinin silinmesi, karakterin belirli açılarla döndürülmesi halinde bu başarım oranının düştüğü gözlenmiştir.



Şekil 8. Kelime bazlı karakter tanımlama
a. Resim üzerinde önişlemler
b. Karakterlerin ayrıştırılması

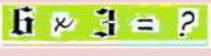
Karakter bazında yapılan test, uygulamanın bir kelimeyi algılamasında yeterli olmadığından uygulamaya test amaçlı sorulan kelimeler üzerinde de birtakım işlemler yapılmıştır. Bu işlemler özellik çıkarım aşamasında olan işlemlere benzemekle birlikte yapılan gri tona geçiş, eşikleme ve kırpma işleminin ardından oluşan resmin karakterlerine ayrıştırılması işlemi de söz konusudur (Şekil 8). Daha sonra, karakterlerine ayrıştırılan resmin bütün karakterleri tekrar kırpılarak etrafındaki beyaz bölgenin tam olarak yok olması sağlanmış; bu aşamanın da sonunda kelimeyi oluşturan karakterler teker teker YSA testine tabi tutulmuştur.

Tablo 3'te uygulama tarafından içerisindeki karakterlerin ayrıştırılabildiği bazı görüntüler bulunmaktadır. Bunların içerisinde 3 tür için karakterler bulunmaya çalışılırken; sayıların bulunduğu görüntü içerisindeki işlem bilgisayar tarafından algılanıp çözülebilmektedir.

A. *Uygulamanın E-Devlet Kapısı Captcha Karakterleri ile Testi*

Gerçekleştirilen uygulama, Şekil 9'da verilen E-Devlet Kapısı Emniyet Genel Müdürlüğü plaka Sorgulama Ekranı CAPTCHA'ları üzerinde karakter tanımlaması yapabilmektedir (Tablo 3). Bu amaçla, belirtilen CAPTCHA'lardan ayrıştırılan karakterler sisteme gönderilmiş ve sınanan 60 karakter için %83 başarım elde edilmiştir. Bu çalışmanın içerisinde yer alan sistem farklı CAPTCHA'larla eğitime tabi tutulmasına karşın E-Devlet kapısı üzerinde yer alan ve elle bölümleme yapılmış CAPTCHA'lar için yüksek başarı elde etmiştir. Saldırgan kişiler e-devlet kapısına ait CAPTCHA'lara; dolayısıyla bu CAPTCHA'ları oluşturan karakterlere erişebilmektedir. Bu kişilerin, amaçlarını gerçekleştirmek için CAPTCHA'lardan edindikleri karakterlerden geniş çaplı bir veri seti oluşturarak; bu veri seti üzerinde YSA teknikleriyle karakter analizini gerçekleştirmelerini engelleyecek bir kontrol yapılmamaktadır. Bu durum CAPTCHA güvenliğini büyük ölçüde azaltmaktadır.

TABLO 3
SİSTEM TARAFINDAN ALGILANABİLEN CAPTCHA'LAR

Görüntü				
Test Sonucu	IPJNZTUV	Gluzd	NhUWyA	3
Görüntü				
Test Sonucu	VEUHJ	Weujk	AEBC	18
Bölümlenmiş Görüntü				
Test Sonucu	bbG5P	zHzYR	FNfMH	RFZFM



Şekil 9. E-Devlet Kapısı Emniyet Genel Müdürlüğü Plaka Sorgu Ekranı

B. Uygulamanın Gmail Captcha Karakterleri ile Testi

Gerçekleştirilen uygulama, Gmail CAPTCHA'ları üzerinde karakter bazlı test edilmiştir. Bu işlem için büyük ve küçük harflerden, sayılardan ve özel karakterlerden oluşan test kümesinden yararlanılmıştır. Test kümesinin elde edilebilmesi için 114 adet Gmail CAPTCHA'sından yararlanılmış; aynı harfin farklı formatları üzerindeki başarım ölçülmüştür. Yazı tipi, test verilerindeki gürültüler ve boyut farklılıklarından dolayı %7'lık bir hata ile karakterlerin bilgisayar tarafından algılanması sağlanmıştır.

Gmail CAPTCHA'ları üzerindeki test işlemi kelime bazlı gerçekleştirildiğinde ise başarım oranı %37'ye düşmüştür. Test başarımındaki bu düşüş, oluşturulan Captcha'lar ile Gmail Captcha'larının bölümleme aşamasındaki farklılıktan doğmaktadır. Tablo 4'te yapılan test işlemine ait bazı sonuçlar görüntülenmiştir.

TABLO 4
GMAIL CAPTCHA KARAKTER BAZLI TEST İŞLEMİ

Görüntü												
YSA Test Sonucu	1	2	3	4	5	6	7	8	9	A	a	B
Görüntü												
YSA Test Sonucu	b	c	B	d	E	e	f	G	g	H	h	i
Görüntü												
YSA Test Sonucu	i	AI	K	k	L	l	M	m	P	P	P	p
Görüntü												
YSA Test Sonucu	R	r	S	s	T	t	u	V	v	A	w	x
Görüntü												
YSA Test Sonucu	Y	y	z		,	v84	V3	L2muu				

V. SONUÇ

İlgili çalışmada sistemlerin, karşılaşabilecekleri bilgisayar destekli saldırılara önlem niteliğinde olan ve Turing Testi'nin gelişmiş hali olarak düşünülebilen CAPTCHA'lar incelenmiş, literatürde, üzerinde çalışmalar yapılan bazı CAPTCHA türleri araştırılmıştır. Belirli formatta oluşturulan 5 CAPTCHA türüne uygun YSA eğitimleri yapılmış ve kelimelerle test edilmiştir.

Test edilen resim temelli CAPTCHA'ların bilgisayar tarafından analizinde, görüntü işleme teknikleri kullanılmıştır. Ardından, ileri beslemeli, Ölçeklendirilmiş Eşlenik Gradyand Algoritması ile eğitilen yapay sinir ağından elde edilen çıktılar dahilinde, oluşturulan görüntü içerisindeki karakterleri tespit eden bir test yazılımı geliştirilmiştir.

Uygulamanın asıl amacı, özellikle OCR tabanlı CAPTCHA'ların güvenlik seviyelerinin düşük olduğunu ve hedeflenen formatta bir CAPTCHA'nın görüntü işleme ve yapay zeka teknikleriyle kolaylıkla kırılabileceğini gösterebilmek; daha güvenli CAPTCHA'ların geliştirilebilmesi için gerekli parametreleri belirleyebilmektir.

Yapılan çalışmalardan elde edilen sonuçlar;

- CAPTCHA karakterlerindeki yazıların formatları insan gözüyle fark edilebilecek fakat makineler tarafından zor okunabilecek nitelikte olmalıdır. Bunu kolaylıkla sağlayacak yöntemlerden bir tanesi hemen hemen her karakter için farklı yazı tipinin kullanılmasıdır. Çünkü birbirine benzeyen karakter sayısı arttıkça CAPTCHA çözülme işlemi kolaylaşmaktadır. Yazı tipindeki farklılaşma ise saldırgan programı yanlış sınıflandırmaya sevk edebilerek, yüksek seviye güvenlik sağlanmasına yardım edeceği,
- CAPTCHA karakterlerini birbirinden farklı kılmak için her bir karakterin tip, eğim, gürültü oranı gibi özellikleri üzerinde değişiklikler yapılmalıdır. Düz karakterlerden oluşan CAPTCHA'lar eğimli karakterlere göre saldırgan sistem tarafından daha kolay okunabileceği,
- CAPTCHA çözülmesinde karakterlerin rengi makineler için büyük bir zorluk oluşturmamaktadır. Fakat renkli CAPTCHA siyah beyaz CAPTCHA'lara göre güvenlik açısından tercih edilebileceği,
- CAPTCHA'ların formatının düzenli aralıklarla değiştirilmesi ve bir sistem içerisinde birden fazla formatta CAPTCHA'nın kullanılması güvenlik düzeyini arttıracağı
- E-Devlet kapısı üzerinde yer alan CAPTCHA'ların iyileştirilmesi gerektiği,

değerlendirilmiştir.

Optik Karakter Tabanlı CAPTCHA'lar oluşturulma şekilleri ve kullandıkları karakterlerin özellikleri bakımından analiz edildikten sonra kolaylıkla çözülebilmektedir.

Çalışmada özgün olarak oluşturulan CAPTCHA yapıları üzerinde gerçekleştirilen karakter tanımlama işlemleri haricinde Gmail CAPTCHA'larını tanımlamaya yönelik bir uygulama gerçekleştirilmiştir. Bu CAPTCHA yapılarında karakter tabanlı yapılan test işleminde %93'lük başarı oranı elde edilmiştir. Aynı CAPTCHA'lar kelime bazlı test edildiğinde sistem başarısı, %37'ye düşmektedir. Bunun sebebi, Gmail CAPTCHA'ları ile çalışma başında oluşturulan özgün CAPTCHA yapılarının farklı bölümleme işlemlerine ihtiyaç duymasıdır. Bu çalışmanın konusu bölümleme olmadığı için önerilen tekniğin başarım oranlarının güncel CAPTCHA'lar için %93, elle bölümleme yapılmış E-Devlet CAPTCHA'ları üzerinde ise yapılan test işleminin başarı oranının %83 olduğu tespit edilmiştir.

İlgili çalışma sonucunda, araştırılan CAPTCHA türleri, bu CAPTCHA'ları daha güvenli hale getirmek için sunulan yaklaşımlar ve bu CAPTCHA'ları kırmaya yönelik önerilerin yer aldığı literatür taraması yapılmış ve bu taramada CAPTCHA teriminin Türkçe karşılığının olmadığı gözlenmiştir. Bu durum, birçok insanın İnternet ortamında sürekli olarak karşılaştıkları bu yapıyı tanımamalarına sebep olmaktadır. Bu yüzden bu terime uygun bir Türkçe karşılık bulunması bir ihtiyaç haline gelmiştir. CAPTCHA'ların, sisteme giren kullanıcının insan mı yoksa sisteme sızmaya çalışan bir robot mu olduğunun anlaşılmasını sağlaması, sunduğu yapılarla insan harici varlıkları yanıltabilmesi ve bu bağlamda Türkçe sözcüklerden oluşan BİAT (Bilgisayar İnsan Ayırıcı Testi) kısaltması, Türkçe karşılığı olarak kullanılmak üzere CAPTCHA ismi yerine önerilmiştir. Tasarlanan tekniklere ise BİATET (Bilgisayar İnsan Ayırıcı Testi Eliminasyon Teknikleri) adının verilmesi önerilmiştir.

Çalışmanın ilerleyen aşamalarında, karakter tanıma problemi, sıklıkla kullanılan diğer BİAT'lar için test edilecek ve internet ortamında karşılaşılan diğer BİAT 'ların çözümü için çalışmalar yapılacaktır. Yeni gelişen BİAT türlerinin bölümleme işlemi üzerinde yeni yaklaşımlar geliştirilerek BİATET'ler oluşturulacaktır.

TEŞEKKÜR

Çalışmalarımız boyunca bizleri destekleyen ve eşsiz deneyimlerini bizlerle paylaşan Gazi Üniversitesi Mühendislik Fakültesi Bilgisayar Mühendisliği Bölüm öğretim üyesi Prof. Dr. Şeref SAĞIROĞLU'na teşekkürlerimizi sunarız.

KAYNAKÇA

[1] A. Raj, A. Jain, T. Pahva, A. Jain, "Picture CAPTCHAs with Sequencing: Their Type and Analisis", ***International Journal of Digital Society***, 1(3): 208-220 (2010).

[2] P. S. Yadava, C. S. Sahu, S. K. Shukla, "Time-Varient CAPTCHA: Generating Strong CAPTCHA Security by Reducting Time to Automated Computer Programs", ***Journal of Emerging Trends in Computing and Information Sciences***, 2 (12): 701-704 (Aralık 2011).

[3] L. Coates, H. S. Baird, R. J. Fateman, "Pessimal Print: A Reverse Turing Test", ***6th International Conference on Document Analysis and Recognition***, Seattle, 1154-1158 (2001).

[4] A. Bilir, "Characteristics of Students in the First Grade of Primary School and Initial Teaching of Reading and Writing", ***Journal of Faculty of Educational Sciences***, 38(1): 87-100 (2005).

[5] S. Ay, A. Varol, "Karakter Tanıma için Düzenli Özellik Çıkarma İşleminin İncelenmesi ve Uygulanması", ***Bilimde Modern Yöntemler Sempozyumu***, Eskişehir, 1063-1070 (2008).

[6] L. D. Yalkın (Demir), "Kavramsal Çerçeve Aşamaları, Sınırları, Sorunları", Doktora Tezi, ***Ankara Üniversitesi Sosyal Bilimler Enstitüsü***, Ankara, 5-7 (2011).

[7] P. Lupkowski, R. S. Choraś, A. Zabludowski, "The Question of OCR-based CAPTCHAs Safety", ***Image Processing & Communications. Challenges Academic Publishing House EXIT***, Warszawa, 218-224 (2009).

[8] M. H. Shirali-Shahreza , M. Shirali-Shahreza, "Persian/Arabic CAPTCHA", ***International Journal on Computer Science and Information Systems (IJCSIS)***, 1(2): 63-75 (2006).

[9] K. Chellapilla, K. Larson, P. Simard, M. Czerwinski,"Computers beat Humans at Single Character Recognition in Reading based Human Insteraction Proofs (HIPs)", ***2nd Conference on Email and Anti-Spam***, California, 160-164 (2005).

[10] S. Huang, Y. Lee ve G. Bell, Ou, Z. "A Projection Based Segmentation Algorithm for Breaking MSN and Yahoo CAPTCHAs", ***World Congress on Engineering***, London, 727-730 (2008).

[11] Y. Yang, X. Lijia, C. Chen, "English Character Recognation Based on Feature Combination", ***2011 International Conference on Advances in Engineering***, Tayland, 159-164 (2011).

[12] O. N. Onak, "Comparison of OCR Algorithms Using Fourier and Wavelet Based Feature Extraction", Yüksek Lisans, ***Middle East Technical University Department of Scientific Computing***, Ankara, 3-18 (2011).

[13] P. Araz, "Bilgisayar Destekli El Yazısı Karakterlerini Tanıma Sistemi Tasarımı", Yüksek Lisans, ***İstanbul Üniversitesi Fen Bilimleri Enstitüsü***, İstanbul, 40-63 (Haziran 2006).

[14] O. A. Erdem, E. Uzun, "Yapay Sinir Ağları ile Türkçe Times New Roman, Arial ve El Yazısı Karakterleri Tanıma", ***Gazi Üniversitesi Mühendislik Mimarlık Dergisi***, 20 (1): 13-19 (2005).

[15] M. Şahin, "Karakter Tanıma", Yüksek Lisans, ***Haliç Üniversitesi Fen Bilimleri Enstitüsü***, İstanbul, 9-53 (Nisan 2007).

[16] M. Şekerci, K. Kandemir, "Sözlük Kullanarak Türkçe Elyazısı Tanıma", Yüksek Lisans, ***Trakya Üniversitesi Fen Bilimleri Enstitüsü***, Edirne, 57-84 (2009).

[17] D. A. Demirci, "Destek Vektör Makineleri ile Karakter Tanıma", Yüksek Lisans, ***Yıldız Teknik Üniversitesi Fen Bilimleri Enstitüsü***, İstanbul, 1-39 (2007).

[18] M. Zahedi, S. Eslami, "Farsi/Arabic Optical Font Recognition Using SIFT Features", ***World Congress on Information Technology***, Amsterdam, 1055-1059 (2010).

[19] Ş. Kaplan, Ş. Sağıroğlu, Ö. F. Çolakoğlu, "Araç Plaka Tanıma Sistemi", ***Elektrik-Elektronik-Bilgisayar Mühendisliği Sempozyumu***, Bursa, 355-359 (2002).

[20] J. Tam, J. Simsa, S. Hyde, L. V. Ahn, "Breaking Audio CAPTCHAs", ***Neural Information Processing Systems Foundation***, 578-586 (2008).

[21] G. Moy, N. Jones, C. Harkless, R. Potter, "Distortion Estimation Techniques in Solving Visual CAPTCHAs", ***IEEE Computer Vision and Pattern Recognition 2003 IEEE Computer Society Conference, California***, II-23 - II-28 (2004).

[22] G., Mori, J., Malik, "Recognizing Objects in Adversarial Clutter: Breaking Visual CAPTCHAs", ***IEEE Computer Vision and Pattern Recognition 2003 IEEE Computer Society Conference***, **California**, I-134 - I-141 (2003).

[23] M., Merler, J., Jacob, "Breaking an Image Based CAPTCHA", Columbia University Department of Computer Science, New York, 2-10 (2009).

[24] J, Yan, A., S., E., Ahmad, "Breaking Visual CAPTCHAs with Naïve Pattern Recognition Algorithm", ***Computer Security Applications Conference***, Miami Beach, 279 – 291 (2007).

[25] R., Lin, S., Y., Huang, G., B., Bell, Y., K., Lee, "A New CAPTCHA Interface Design for Mobile Devices", ***Australasian User Interface Conference***, Perth (2011).

[26] Elmas, Ç., "Yapay Zeka Uygulamaları 1. Baskı", ***Seçkin Yayıncılık San. Ve Tic. A.Ş.***, Ankara, 1-82 (Kasım 2007).

[27] Sağıroğlu, S., Beşdok, E., Erler, M., "Mühendislikte Yapay Zeka Uygulamaları I – Yapay Sinir Ağları 1. Baskı", ***Ufuk Kitap Kırtasiye-Yayıncılık Tic. Ltd. Şti***, Kayseri, 10-53 (Ağustos 2003)

[28] N. Baş, "Yapay Sinir Ağları Yaklaşımı ve Bir Uygulama", Yüksek Lisans, ***Mimar Sinan Güzel Sanatlar Üniversitesi Fen Bilimleri Enstitüsü***, İstanbul, 21-30 (2006).

[29] P. S. Sandhu, S. Chhabra, "A Comparative Analisis of Conjugate Gradient Algorithms & PSO Based Neural Network Approaches for Reusability Evaluation of Procedure Based Software Systems", ***Chiang Mai Journal of Science***, 38: 123-135 (2011).

[30] U., Yavanoğlu, Sağıroğlu, S., "Web Tabanlı Otomatik Dil Tanıma ve Çevirme Sistemi", ***Gazi Üniversitesi Mühendislik Mimarlık Fakülteri Dergisi***, 25 (3), 483-494 (2010).

[31] Sağıroğlu S., Yolaçan, E., N., Yavanoğlu, U., "Zeki Saldırı Tespit Sistemi Tasarımı ve Gerçekleştirilmesi", ***Gazi Üniversitesi Mühendislik Mimarlık Fakülteri Dergisi***, 26 (2), 325-340 (2011).



Uraz Yavanoğlu, Ankara doğumludur. Atılım Üniversitesi Bilgisayar Mühendisliği Bölümünden mezun olmuştur. 2009 yılında Gazi Üniversitesi Mühendislik Fakültesi Bilgisayar Mühendisliği Bölümünden yüksek lisans derecesi almıştır. Aynı bölümde Araştırma Görevlisi olarak çalışmakla birlikte Gazi Üniversitesi Elektrik Eğitimi bölümünde doktora çalışmalarına devam etmektedir. Araştırma konuları arasında yapay sinir ağları, insan bilgisayar etkileşimi ve bilgi güvenliği yer almaktadır.



Begüm Mutlu, 1990 Ankara doğumludur. Gazi Üniversitesi Mühendislik Fakültesi Bilgisayar Mühendisliği 4. sınıf, Anadolu Üniversitesi İşletme Fakültesi İşletme Bölümü 3. sınıf öğrencisidir. Araştırma konuları Veri Madenciliği, Örüntü Tanıma ve Yapay Öğrenme Teknikleri'dir.



Esra Şahin, 1990 Kayseri doğumludur. 2008 yılında Gazi Üniversitesi Bilgisayar Mühendisliği Bölümü lisans eğitimine başlamıştır. 2009 yılında Gazi Üniversitesi Elektrik-Elektronik Mühendisliği Bölümünde çift anadal eğitimine başlamıştır. İlgi alanları Yapay Sinir Ağları, Makine Öğrenmesi Görüntü İşleme, Bilgi Güvenliği, Veri Madenciliği konularıdır.

Radyo Link ve Uydu Ağları Üzerinde Gelecek Nesil Dar Bant Terminal ile Yapılan Güvenli Haberleşme Test Sonuçları ve Değerlendirilmesi

O. DİLLİ, N. AKÇAM ve M. KOYUNCU

Özet — **Haberleşme günlük hayatımızda önemli bir değere sahiptir ve her geçen gün bu değerini daha da hissettirmektedir. Bu durum haberleşmenin yapılabilmesini zorunlu hale getirmekte, hatta ve hatta söz konusu haberleşmenin uçtan uca güvenli olmasını zorlamaktadır. Söz konusu zorunluluğu önceden fark eden ülke veya ülkeler tarafından elektronik cihazların karşılıklı çalışabilirliğini gönderme ortamından bağımsız olarak sağlanmasına önemli katkı sağlayacak FNBDT (Future Narrow Band Digital Terminal) projesi başlatılmıştır. Sonraki dönemlerde bu projeye SCIP (NATO Secure Communication Interoperability Protocol) ismi verilerek uluslar arası düzeyde devam edilmiştir. Farklı haberleşme ağları üzerinde uçtan uca emniyetli haberleşmenin yapılması amacıyla geliştirilen FNBDT/SCIP protokolü, emulatör yazılımı vasıtasıyla test edilmiştir. Bu çalışmada, radyo link ve uydu ağları üzerinde yapılan testlerde elde edilen ses ve veri haberleşmelerine ait sınır değerler karşılaştırılarak yorumlanmıştır.**

Anahtar Kelimeler — **Güvenli Haberleşme, FNBDT, SCIP, Radyo Link, Uydu.**

Abstract — **As is known to all, communication plays a crucial role in our lives and it gains more and more value every other day. This fact makes the application of communication highly essential. Even, it requires communication to be fully secure from one end to the other. Countries that predicted the vitality of the issue, took on the FNBDT Project (Future Narrow Band Digital Terminal), would give great contribution to interoperability of electronic devices independent from transmission media. In later phases, the project was titled as SCIP (NATO Secure Communication Interoperability Protocol) and gained an international identity. FNBDT/SCIP protocol, which was developed for the purpose of providing secure communication from one end to the other on different communication networks, was tested through emulator software. In this study, limit values of voice and data communication on radio link and satellite network have been evaluated in comparison to the relevant standards.**

Index Terms — Secure Communication, FNBDT, SCIP, Radio Link, Satellite.

O.DİLLİ, Elekt.Elek. Müh.Böl.,Müh.Mim.Fak., Gazi Üniversitesi, Maltepe/ANKARA (e-posta: odilli@gazi.edu.tr).
N.AKÇAM, Elekt.Elek. Müh.Böl.,Müh.Mim.Fak., Gazi Üniversitesi, Maltepe/ANKARA (e-posta: ynursel@gazi.edu.tr).
M.KOYUNCU, Bil.Sis.Müh., Atılım Üniversitesi, İncek/ANKARA (e-posta: mkoyuncu@atilim.edu.tr).

I. GİRİŞ

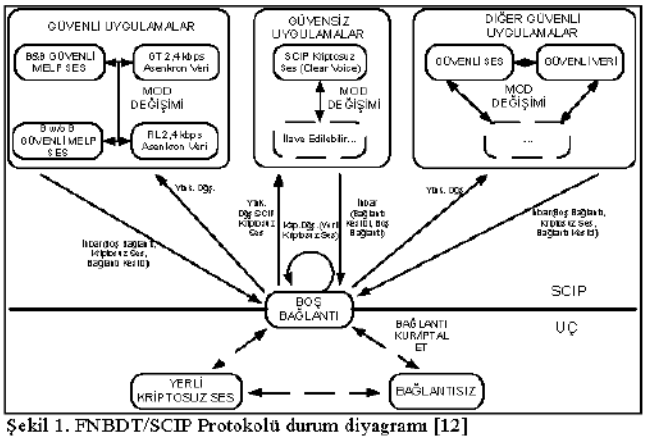
Haberleşme günlük hayatımızda önemli bir değere sahiptir ve her geçen gün bu değerini daha da hissettirmektedir. Bu durum haberleşmenin yapılabilmesini zorunlu hale getirmekte, hatta ve hatta söz konusu haberleşmenin uçtan uca güvenli olmasını zorlamaktadır. Söz konusu zorunluluğu önceden fark eden ülke veya ülkeler tarafından elektronik cihazların karşılıklı çalışabilirliğini gönderme ortamından bağımsız olarak sağlanmasına önemli katkı sağlayacak FNBDT (Future Narrow Band Digital Terminal) projesi başlatılmıştır. Sonraki dönemlerde bu projeye SCIP (NATO Secure Communication Interoperability Protocol) ismi verilerek uluslar arası düzeyde devam edilmiştir.

FNBDT veya yeni ismiyle SCIP, farklı şebekelerde haberleşme yapan cihazların birbirleri ile emniyetli iletişim ihtiyacından doğmuş bir haberleşme protokolüdür. Protokolün temel amacı iletişim sağlayan yeni nesil terminallerin farklı şebekeler üzerinden birbirleriyle dar bant kullanarak emniyetli haberleşebilmelerini sağlamaktır.

FNBDT/SCIP konusunda uluslararası [1-12] ve ulusal [13-23] alanda bugüne kadar yapılan çalışmaların genel olarak üç ana başlıkta toplandığı gözlenmiştir. Bunlar; FNBDT ile ilgili çalışmalar, SCIP ile ilgili çalışmalar ve Mixed Excitation Linear Prediction (MELP, Karışık Doğrusal Kestirim) kodlamasıyla ilgili çalışmalardır.

FNBDT/SCIP konusunda teorik çalışmaların daha yeterli düzeyde olmasına karşılık, uygulamaya yönelik çalışmaların yok denebilecek kadar az olduğu gözlenmiştir. Söz konusu uygulama eksikliğinin giderilmesine yönelik olarak tarafımızdan FNBDT/SCIP'in uydu ve radyo link üzerinde testleri yapılmıştır. Söz konusu testler ile farklı ağlar üzerinde çağrı kurma, ses ve veri haberleşmelerinin çeşitli hata ve kayıp oranları altında test edilmesi, sınır değerlerin tespit edilmesi amaçlanmıştır. Testlerde elde edilen sonuçların bir kısmı daha önce yayınlanmıştı [20, 21, 23]. Bu bildiride ise, radyo link ve uydu ağları üzerinde yapılan testlerde elde edilen ses ve veri haberleşmelerine ait sınır değerler ITU standartlarıyla da karşılaştırılarak yorumlanmıştır.

II. SCIP/FNBDT SİNYALLEŞMESİ



Şekil 1. FNBDT/SCIP Protokolü durum diyagramı [12]

Şekil 1, FNBDT/SCIP uyumlu bir terminalin uçtan-uca sinyalleşmesini kavramsal olarak göstermektedir. Terminal başlangıçta uzak uca hiç bir haberleşme bağlantısının olmadığı bağlantısız (Connection Terminated) bir durumdadır. Sinyalleşme planında tanımlanan sinyalleşme durumu gerçekleştirilmeden önce iki uç arasında FNBDT/SCIP mesajlarının karşılıklı taşınmasını temin etmek amacıyla kriptosuz bir veri yolu (clear data path) açılması şarttır. İşte uçlar arasında kriptosuz veri yolunun açıldığı ve fakat üzerinde FNBDT/SCIP uygulamalarının henüz başlatılmadığı bu duruma "Boş Bağlantı" (Connection Idle) adı verilmekte olup, FNBDT/SCIP uygulamaları bahsedilen bu boş bağlantıdan gerçekleştirilebilmektedir. Yetenekler Değişimi (Capabilities Exchange) olarak tabir edilen ilk FNBDT/SCIP çağrı kurulum değişimi standart FNBDT/SCIP kriptosuz ses uygulamaları kullanılarak yapılır. Yetenekler Değişimine ek olarak, standart güvenli FNBDT/SCIP uygulama parametrelerinden karşılıklı haberdar olabilmek için mesaj alışverişlerine ihtiyaç duyulur [12].

Aynı trafik anahtarını kullanan güvenli uygulamalar veya FNBDT/SCIP uyumlu kriptosuz uygulamaların karşılıklı görüşebilmeleri bir Mod Değişimi (Mod Exchange) işlevi ile sağlanabilmektedir. Uygulamalar arası geçişler zaman zaman Boş Bağlantı durumuna geçebilmektedir. Her hangi bir FNBDT/SCIP durumundan diğer bir duruma geçmek gerektiğinde, bu durum İhbar Mesajlarında (Notification Message) gösterilir. Tekrar FNBDT/SCIP moduna geçileceğinde bir dizi Yetenekler Mesajlaşması karşılıklı olarak yerine getirilir.

Standart bir FNBDT/SCIP durumunda çağrıyı sonlandırarak Boş Bağlantı durumuna, bilahare de kullanılan kriptosuz veri yolunu kapatarak Bağlantı Sonlandırıldı (Connection Terminated) durumuna geçmek için yine İhbar Mesajları kullanılır.

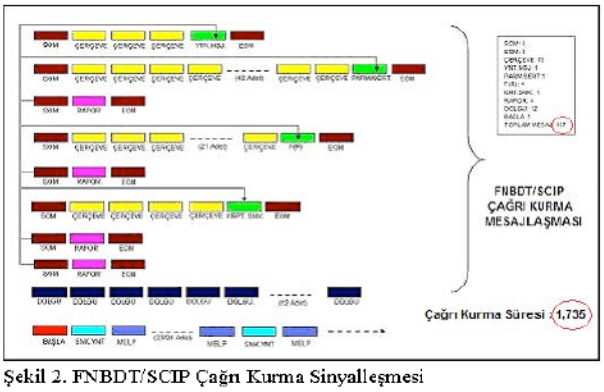
FNBDT/SCIP sinyalleşmesi esas olarak bağlantı kurma ve kontrol sinyalleşmelerinden oluşmaktadır.

Bağlantı Kurma Sinyalleşmesi; Yetenekler, Parametre/Sertifika, F(R) ve Kripto Senkronizasyon (CryptoSync),

Bağlantı Kontrol Sinyalleşmesi ise; İhbar İşlemleri (Notification), Mod Değiştirme ve Senkronizasyonu Tekrar Kurma konularını içermektedir.

FNBDT/SCIP sinyalleşmesi, Şekil 2'de görüldüğü gibi, sekiz baytlık Start of Message (SOM) ile başlayıp sekiz baytlık End of Message (EOM) ile sonlanmaktadır.

SOM ve EOM arasında gönderilen çerçeveler "çerçeve grubu (superframe)" olarak tanımlanmaktadır. Her çerçeve grubu gönderme yönünde hata düzeltimi (FEC) ve çevrimsel artıklık denetimi (CRC) ile korunan çerçevelerden meydana gelmekte; FEC ile düzeltilemeyen hataların ortadan kaldırılması içinse olumlu veya olumsuz onay verme mekanizmaları (ACK ve NACK) kullanılmaktadır.



Şekil 2. FNBDT/SCIP Çağrı Kurma Sinyalleşmesi

Her bir çerçeve, 1 çerçeve numarası, 13 mesaj, 4 FEC ve 2 CRC olmak üzere 20 bayttan oluşmaktadır. Bu çerçevelerden oluşan ve Mesaj Başlangıcı (SOM) ile başlayıp Mesaj Sonu (EOM) ile sonlanan her çerçeve grubu en az bir en çok 127 adet çerçeveden oluşmaktadır.

EOM alındığında öncelikle son alınan çerçevenin ESCAPE veya REPORT olup olmadığına bakılır, eğer değilse o ana kadar alınmış çerçeveler için rapor hazırlanır ve gönderilir. ESCAPE mesajı band genişliği kullanımı, REPORT mesajı ise gelen çerçevelerin hata oran onayları ile ilgili kavramlardır.

Benzer şekilde FNBDT/SCIP sinyalleşmesinde karşılaşılabilecek mesaj türlerinden diğer bir tanesi RESET mesajıdır ki bu mesaj gerekli durumlarda iletim katmanını yeniden senkron hale getirmek için kullanılır. RESET mesajı çerçeve numaralarını sıfırlar ve bir SOM ve EOM arasında yalnızca bir RESET mesajı gönderilir.

FNBDT/SCIP sinyalleşmesinde, bağlantı kurma sinyalleşmesinin ilk adımı olarak terminaller birbirlerine Yetenekler Mesajını (Capabilities Message) göndermektedirler. Bu mesaj sayesinde terminaller birbirleriyle uyumlu olarak ne şekilde çalışabileceklerini (açık veya kapalı modlar) belirli bir esasa bağlamakta ve güvenli modda haberleşilecek ise uygun anahtar listesinin seçilmesi de bu sayede mümkün olmaktadır. Yetenekler Mesajı gönderildiği anda ilk mesaj zamanlayıcısı başlamakta, bu zamanlayıcı karşı taraftan FNBDT/SCIP uyumlu mesaj gelmemesi halinde bağlantının zaman aşımına uğramasını temin etmektedir. Zaman aşımı sonunda Boş Bağlantı haline dönülür.

İlk mesajlaşma sonunda eğer güvenli haberleşme kararı verildiyse FNBDT/SCIP bağlantısı kurulabilmesi maksadıyla

trafik anahtarını oluşturabilmek için karşılıklı sertifikaların ve F(R)'ların değiş tokuş yapılması gerekmektedir. Bunlardan sertifikanın gönderilmesi Parametre/Sertifika mesajı ile olur.

F(R) mesajı anahtar takımı ile ilgili bir takım bilgiler (anahtarın tip, uzunluğu vb.), F(R) uzunluğu ve F(R)'ın kendisini kapsayan bir mesajdır. F(R) mesajı iletilmeden önce mutlaka parametre/sertifika mesajı iletilmiş olmalıdır.

FNBDT/SCIP bağlantısı kurmada diğer bir adım kripto senkronizasyon mesajlarının değişimidir. Değişimi yapılan sertifika ve F(R) bilgileri ile trafik anahtarı oluşturulmakta, bu anahtar ile test paketi şifrelenip Kripto Senkronizasyon Mesajı haline getirilmektedir.

Bağlantı kurma sinyalleşmesinden sonra kurulan bağlantının değişikliklere tabi tutulmasıyla ilgili bir takım sinyalleşme tanımları mevcuttur. Bağlantı kontrol sinyalleşmesinin maksadı; herhangi bir sebeple bağlantıyı sonlandırmak, mevcut uygulamayı değiştirmek, diğer terminali ikaz etmek ve/veya kripto senkronizasyonunu baştan sağlamak olabilir. Bağlantı kontrol sinyalleşmesinde dört farklı mesaj vardır. Bunlar İhbar (Notification), Mod Değişim İsteği (Mode Change Request), Mod Değişim Yanıtı (Mode Change Response) ve Kripto Senkronizasyon (CryptoSync) mesajlarıdır.

Mod değiştirme işlemi; talep ve buna verilen yanıt şeklinde iki türlüdür ve sadece her iki terminal de güvenli uygulama trafiğinde iken mümkün olabilir.

Güvenli Ses için beş farklı çağrı mevcuttur. Bunlar [2];

- Güvenli 2,4 kbps MELP kodlu Ses – Blank & Burst (DTX),
- Güvenli 2,4 kbps MELP kodlu Ses – Blank & Burst (FCT),
- Güvenli MELP kodlu Ses –Burst w/o Blank (DTX),
- Güvenli MELP kodlu Ses –Burst w/o Blank (FCT),
- Güvenli, Gelişmiş Çoklu-Band Uyarımı (AMBE).

FNBDT/SCIP' de Blank & Burst uygulamalı MELP ve Burst w/o Blank olmak üzere iki tip güvenli ses çağrısı yapılabilmektedir.

SCIP uyumlu bir terminalde, kripto senkronizasyonunun sürekliliği için belirli periyotlarla terminal tarafından 2,4 kbps'de üretilen MELP kodlu ses bilgisinin üzerine kripto senkronizasyon bilgisi yazılır. Bu işleme "B&B" (Blank and Burst) protokolü denilmekte ve bu uygulamada zaman zaman ses bilgisi silinerek yerine kripto bilgisi yazılmasından dolayı ses kalitesinde ufak çapta düşüşler yaşanmaktadır.

Blank & Burst çerçeve grubu 24 çerçeveden oluşmasına karşın, Burst w/o Blank (B w/o B) uygulaması 25 çerçeveden oluşmaktadır. Dolayısıyla Burst w/o Blank uygulaması için gerekli kanal kapasitesi 2,4 kbps'den fazla (overhead) olmaktadır. Aynı zamanda, MELP kodlanmış ses bilgilerinin üzerine kripto senkronizasyon bilgisi yazılmadığı için ses kalitesi B&B'ye göre daha iyidir.

Açık MELP ses çağrı hizmeti görüşmesinde de ortaya çıkan yapı tıpkı B&B'de olduğu gibidir. Mesaj yine, biri SM çerçevesi olmak üzere toplam 24 çerçeveden oluşan çerçeve gruplarıyla yapılır. Ancak burada kriptolama yapılmadığından SM çerçevesinin başlık kısmından sonrası sıfır ile doldurularak mesaj gönderilir.

Ayrıca ister güvenli isterse açık olarak görüşen tüm FNBDT/SCIP uyumlu terminallerin DTX ve FCT durumları desteklemesi beklenmektedir. Bunlardan DTX; bir ses çağrısı sırasında, terminalin kullanıcısı konuştuğu sürece çerçeve gruplarının oluşturularak gönderilmesi, kullanıcı sustuğunda ise gönderme yapmanın kesilmesi prensibini, FCT ise; ses çağrısı sırasında terminalin kullanıcısının sustuğu sürede de çerçeve gruplarının oluşturularak karşı terminale iletilmesi yani MELP kodlayıcı biriminin sürekli çalışmasını ifade etmektedir.

FNBDT/SCIP, veri haberleşmesinde ise iki veri hizmetini desteklemektedir. Bunlar "Güvenli Aktarım (Reliable Transport-RT)" Asenkron Veri Hizmeti ve "Garanti İş (Guaranteed Throughput-GT)" Asenkron Veri Hizmetleridir. RT Asenkron Veri hizmetinde, güvenli ses hizmetinde kullanılan sinyalizasyon mekanizmalarının aynısını kullanarak veri çağrısı başlatılır ve kanal kapasitesi %70 verimlilikle kullanılır. GT Asenkron Veri hizmeti ise kanal kapasitesinin tamamının kullanıldığı bir servistir [13, 14].

III. Uygulama Testinde Geçen Kavram ve Tanımlar

FNBDT/SCIP Emulatör: Laboratuvar ortamlarında cihazların karşılıklı çalışabilirliğini değişik senaryolar ve durumlar dahilinde test eden bir yazılım uygulamasıdır.

FNBDT/SCIP Tester: FNBDT/SCIP Emülatör Yazılımının bir parçası olup, terminaller arası FNBDT/SCIP haberleşmesinin takip ve kontrol edilmesi maksadıyla kullanılmaktadır. Modülün içerisinde test süresince haberleşmeye etki edilebilmesini (bozma, karıştırma, geciktirme vb.) sağlayan fonksiyonlar mevcuttur.

Bit Hata Oranı (Bit Error Rate-BER) : Belli bir zaman aralığında iletilen veri bitlerinden hatalı olanların, aktarılan toplam bit sayısına oranı olarak tanımlanmaktadır.

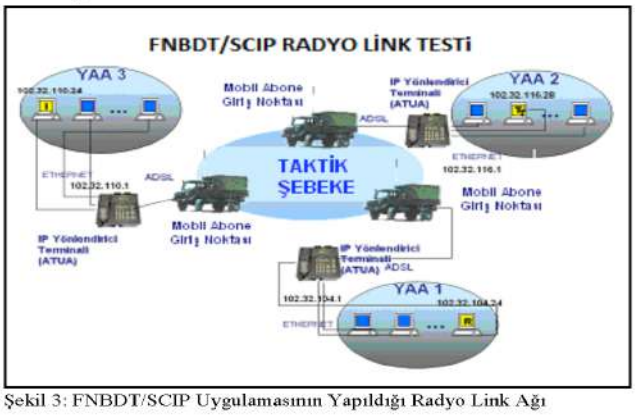
Veri Kaybı (Data Loss): Bit veya Bayt olarak hatalı aktarılan veri miktarının toplamda aktarılan veriye oranıdır. Uygulamada kanal simülatörü tarafından oluşturulan bu durumda bit kayıpları için bitler, bayt kayıpları içinse sekizli bit gruplarının rastlantısal olarak iletilmesi engellenerek veri kaybına yol açılmaktadır.

Gecikme (Delay) : Aktarılan veride yaratılan sistematik zaman kaymaları bu başlık altında tanımlanmaktadır.

IV. FNBDT/SCIP Uygulaması İçin Kurulan Ağlar

FNBDT/SCIP'in Uydu ve Radyo Link Ağları üzerinde; Çağrı Kurma, B&B Güvenli Ses Haberleşmesi, Bw/oB Güvenli Ses Haberleşmesi, RT Güvenilir Veri Haberleşmesi, GT Garantili Veri Haberleşmesi olmak üzere beş ana başlık ve her ana başlığın altında bit hata oranı ve (bayt ve bit) veri kayıpları alt başlıkları altında testler gerçekleştirilmiştir.

A. Radyo Link:



Şekil 3: FNBDT/SCIP Uygulamasının Yapıldığı Radyo Link Ağı

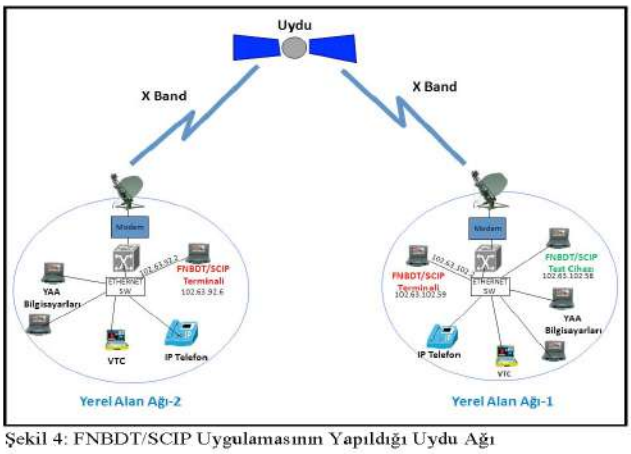
Şekil 3'de ayrıntıları görülen yapıda birbirinin aynısı üç adet yerel alan ağı oluşturulmuş, bu ağlar arasında kurulan FNBDT/SCIP haberleşmesi değişik durumlarda test edilerek sınır değerler elde edilmiştir.

Bunlardan YAA3 Başlatıcı, YAA1 Cevaplayıcı ve YAA2 ise Test Edici ortam olarak seçilmiştir. Başlatıcı üzerinden çağrı kurma, güvenli ses ve veri haberleşmesi başlatılmakta, bu haberleşme Cevaplayıcı ile karşılıklı olarak gerçekleştirilmektedir. Test Edici ortam, iki YAA arasında haberleşme sürerken değişik senaryolara göre haberleşme ortamından deneysel verilerin toplanması amacıyla kurulmuş ve kullanılmıştır. Gerektiğinde, her üç YAA da birbirinin aynı olduğundan, işlevlerinin birbirlerine aktarımı da mümkün olmuştur. Böyle bir yapılandırma kullanılan emülatör yazılımının gerekleri doğrultusunda oluşturulmuştur.

B. Uydu:

Şekil 4.'de görülen iki kullanıcı arasında uydu haberleşmesini sağlayan test düzeneği gerçek ortamda kurularak testler yapılmıştır. Şekilde görüldüğü gibi test düzeneği;

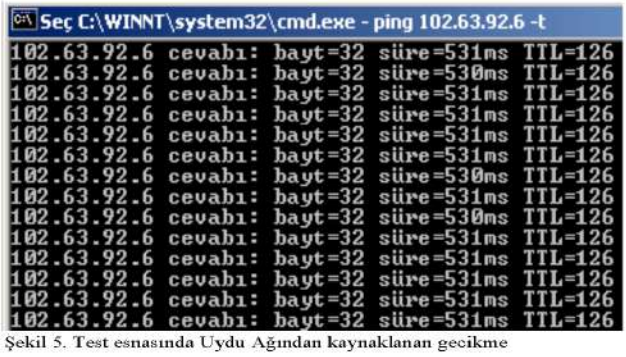
- TURKSAT-2A Uydusu,
- Çağrıyı başlatan FNBDT/SCIP Terminali,
- Haberleşme ortamını test eden FNBDT/SCIP Test Cihazı,
- Çağrıyı yanıtlayan FNBDT/SCIP Terminali,
- İki Adet Cisco Router ve Ethernet Switch ile oluşturulmuş iki adet YAA,
- 2 Adet X Bant Modemden oluşmaktadır.



Şekil 4: FNBDT/SCIP Uygulamasının Yapıldığı Uydu Ağı

Yapılan testlerde uydudan kaynaklanan gecikme nedeniyle paketlerin gidiş-dönüş süresinin, Şekil 5.'den de görüldüğü gibi, yaklaşık 530 milisaniye civarında olduğu gözlenmiştir. Bu gecikme değerinin ilgili ITU-T Standartlarında tek yönlü uydu haberleşmesinde 250 milisaniye, iki yönlü uydu haberleşmesinde 500 milisaniye olması gerektiği belirtilmiştir [24]. Testler esnasında oluşan gecikme ile ITU Standardında tavsiye edilen değerin birbirine yakın olduğu görülmektedir.

ITU-T Rec.G.1010 (11/2001) standardının performans kriterinde ise ses haberleşmesinde gecikmenin <<1 saniye olması tavsiye edilmiş [25], fakat uydunun bir kez kullanıldığı tek yönlü ses haberleşmesinde bile yaklaşık 0,25 saniye gecikmenin olabileceği yine ITU-T standartlarında yer almıştır.



Şekil 5. Test esnasında Uydu Ağından kaynaklanan gecikme

Çizelge 1. FNBDT/SCIP'in Radyo Link ve Uydu Ağlar üzerinde yapılan testler sonucunda elde edilen sınır değerler

S.Nu	Yapılan Test	Elde Edilen Sınır Değerler ve Süreler				Açıklama
		Radyo Link		Uydu		
		Sınır Değer	Süre (sn)	Sınır Değer	Süre (sn)	
1	**Çağrı Kurma**					Uydu Haberleşmesinde Çağrı Kurma Süresi Ortalama : **19,215 sn** En fazla : **56,9 sn** ITU-R S.1711-1 sf. 24-29 [26].
2	Normal Çağrı Kurma	**110 Mesaj**	3,264	**111 Mesaj**	7,182	
3	Bit Hata Oranıyla Çağrı Kurma	**% 0,05**	100,094	**% 0,05**	33,5	
4	Bayt Veri Kaybıyla Çağrı Kurma	**% 0,01**	92,687	**% 0,05**	106,953	
5	Bit Veri Kaybıyla Çağrı Kurma	**% 0,05**	156,563	**% 0,01**	74,156	
6	Diğer Tür Veri Kayıpları ile Çağrı Kurma	**SOM Mesajı**		**SOM Mesajı**		
7	**B&B/BwoB Ses Haberleşmesi**					Kabul Edilebilir Hata ve Kayıp Aralığı BER 10^{-6} - 10^{-4} Veri Kaybı 10^{-5} - 10^{-3} ETSI TR 102 157 (2003-07) sf. 57-61, ETSI TS 102 462 (2006-12) sf. 43-44, ETSI TS 102 673 (2009-11) sf. 22, ITU-R S.522-5, sf. 1-2, ITU-R S.579-6, sf. 1-2, ITU-R S.614-4, sf. 1-15 [29-34].
8	BER'in B&B Ses Haberleşmesine Etkisi	**% 0,1**		**0,1 %**		
9	Bayt Veri Kaybının B&B Ses Haberleşmesine Etkisi	**% 0,1**		**0,1 %**		
10	Bit Veri Kaybının B&B Ses Haberleşmesine Etkisi	**% 0,1**		**0,1 %**		
11	**RT Güvenilir Veri Haberleşmesi**					
12	BER'in RT **Güvenilir** Veri Haberleşmesine Etkisi	**% 0,05**	74,814	**% 0,02**	105,675	
13	Bayt Veri Kaybının RT **Güvenilir** Veri Haberleşmesine Etkisi	**% 0,02**		**% 0,03**	851,266	
14	Bit Veri Kaybının RT **Güvenilir** Veri Haberleşmesine Etkisi	**% 0,03**	670	**% 0,03**	601,625	
15	**GT Garantili Veri Haberleşmesi**					
16	BER'in GT Garantili Veri Haberleşmesine Etkisi	**% 0,1**	11,265	**% 0,1**	1,648	
17	Bayt Veri Kaybının GT Garantili Veri Haberleşmesine Etkisi	**% 0,1**		**% 0,1**		
18	Bit Veri Kaybının GT Garantili Veri Haberleşmesine Etkisi	**% 0,1**		**% 0,1**		

Farklı haberleşme ağları üzerinde uçtan uca emniyetli haberleşmenin yapılması amacıyla geliştirilen FNBDT/SCIP protokolü, emulatörler vasıtasıyla Radyo Link ve Uydu Ağları üzerinde değişik açılardan test edilmiştir. Yapılan testler sonucunda elde edilen sınır değerler ve bunlara ait süreler Çizelge 1'de verilmiştir. Çizelgede verilen sınır değer, çağrı kurulabilen veya haberleşme yapılabilen en yüksek hata/kayıp oranını ifade etmektedir. Elde edilen sınır değer ve süreleri ilgili standart değerler ile karşılaştırarak genel olarak yorumlamamız gerekirse;

Uydu haberleşmesinde normal, hata ve kayıp oluşturmadan yapılan, çağrı kurmaya ait sürenin Radyo Link ağları için belirlenen süreden fazla olduğu, her iki ağda da hata ve kayıp oranlarını arttırdıkça çağrı kurma sürelerinin de genelde arttığı gözlenmiştir.

Radyo Link ve Uydu Ağları üzerinde FNBDT/SCIP ile yapılan testler sonucunda elde edilen B&B ve BwoB Ses, RT Güvenilir ve GT Garantili Veri Haberleşmelerine ait sınır değerler standartların tavsiye ettiği alt sınır aralığında, hatta daha iyi olduğu tespit edilmiştir.

VI. SONUÇLAR

FNBDT/SCIP Protokolü Radyo Link ve Uydu Ağları üzerinde ayrı ayrı test edilerek sınır değerler elde edilmiştir. Bu çalışma ile söz konusu uygulama sonuçları karşılaştırılarak değerlendirilmiştir. Değerlendirme ile;

- Uydu Ağı üzerindeki çağrı kurma sınır değerlerinin daha küçük olduğu,
- Bit veri kaybıyla çağrı kurma testlerinden her iki ağın önemli oranda etkilendiği,
- SOM mesajı olmadığında tüm ağlar üzerinde çağrının kurulamadığı,
- B&B ve BwoB Ses Haberleşmelerine ait test sonuçlarının paralellik gösterdiği,
- RT Güvenilir Veri Haberleşme testlerinde elde edilen sınır değerlerin çağrı kurma testlerinde olduğu gibi, yakınlık gösterdiği, Uydu Ağı üzerinde elde edilen sınır değerlerin daha küçük olduğu sonuçlarına ulaşılmıştır.

Çalışma, özellikleri ve içeriği bakımından konuyla ilgili yapılan ilk çalışma sonuçlarının karşılaştırılması ve karşılaştırma sonuçlarının müteakip çalışmalara girdi oluşturma imkanı sunması nedeniyle önem arz etmektedir.

KAYNAKLAR

[1] Daniel E. J., Teague K. A., "Performance of FNBDT and Low Rate Voice (MELP) over Packet Networks", Proc.35th Asilomar Conference on Signals, Systems, and Computers, 1568–1572, Pacific Grove, California, 4-7 (2001).

[2] Daniel, E. J., Teague K. A., Sleezer R., Brewer J., Raymond W. J., Beck, J., Hershberger, "The Future Narrowband Digital Terminal", Proc. 45th IEEE Midwest Symposium on Circuits and Systems MWSCAS '2002, II-589-592, Stillwater/Tulsa, OK, (2002).

[3] Daniel E. J., Teague K. A., "Simulation of FNBDT over Internet and 3G Wireless Networks", Proc. 45th IEEE Midwest Symposium on Circuits and Systems MWSCAS '2002, 330–333, 4-7 (2002).

[4] Alvermann J. M., Kurdziel M. T., Furman W. N., "The Secure Communication Interoperability Protocol (SCIP) over An HF Radio Channel", MILCOM 2006, 1–4 (2006).

[5] Gauche F., "An Approach of the Future Narrow Band Digital Terminal Protocol", Seventh International Conference on Computer Science and Information Technologies, 457–462, Yerevan, Armenia, (28) 2 (2009).

[6] Daniel E. J.,Teague K. A., "Federal Standard 2.4 kbps MELP Over IP", Proc.43rd. IEEE Midwest Symp. On Circuits and Systems, 8 (11): 568–571 (2000).

[7] Tan E.C., Teo T.T.,"Real-Time İmplementation of MELP Vocoder", Journal of The Institution of Engineers, Singapore, Vol. 44 Issue 3, pp. 38-58, 2004.
[8] McCree A. M., III, Barnwell T. P., "A 2400 bps Mixed Excitation LPC Vocoder", Conference Record IEEE Military Communications Conference MILCOM'92, (1) 381-384 (1992).
[9] McCree A. M., III, Barnwell T. P., "Implementation and Evaluation of a 2400 bit/s Mixed Excitation LPC Vocoder", 1993 IEEE Internation Conference on Acoustics, Speech, and Signal Processing ICASSP-93, (2) 159-162 (1993).
[10] Cree A. M., Barnwell T., "A Mixed Excitation LPC Vocoder Model For Low Bit Rate Speech Coding", IEEE Transaction of Acoustics, Speech, and Signal Processing, 3 (4): 242-250 (1995).
[11] LUCK J., Details of FNBDT Signalling, SHAPE / NC3A FNBDT Workshop, The Hauge, (26) 1-41 (2003).
[12] General Dynamics Communication Systems, FNBDT Signaling Plan (Revision 1.1), Needham, Eylül (1999).
[13] Bozoklu, O., "Uyumlu ve Birlikte Çalışabilir Güvenli Muhabere Kapsamında NATO/SCIP Bünyesindeki Kripto Standartlarına Türkiye'nin Yaklaşımı", Yüksek Lisans Tezi, Kara Harp Okulu Savunma Bilimleri Enstitüsü, Ankara, 99-110, 133-139 (2007).
[14] Ören, Ö., "Geleceğin Darband Sayısal Terminali", Yüksek Lisans Tezi, Sakarya Üniversitesi Fen Bilimleri Enstitüsü, Adapazarı, 3-54, (2005).
[15] Gönen, S., "Taktik Saha Muhabere Sistemleri Arasında Müşterek Çalışabilirliğin Sağlanması: Uygulamalı Bir Araştırma", Yüksek Lisans Tezi, Kara Harp Okulu Savunma Bilimleri Enstitüsü Teknoloji Yönetimi Ana Bilim Dalı, Ankara, 1-6 (2006).
[16] Nazlıbilek, S., Bozoklu, O., Dilli, O., Koyuncu, M.ve Akçam, N., "Gelecek Nesil Terminal Cihazları İçin Farklı Şebekeler Üzerinden Uçtan Uca Emniyetli Haberleşmenin Sağlanması Üzerine Bir Uygulama", Mühendislik ve Teknoloji Ulusal Sempozyumu-1, Çankaya Üniversitesi, Ankara, Nisan (2008).
[17] Dilli, O., Nazlıbilek, S., Bozoklu, O., Koyuncu, M.ve Akçam, N., "Farklı Şebekeler Üzerinden Uçtan Uca Emniyetli Haberleşmenin Sağlanması", Ağ ve Bilgi Güvenliği Ulusal Sempozyumu-2, EMO, Girne, Mayıs 2008.
[18] Dilli, O., Nazlıbilek, S., Koyuncu, M. Akçam, N., ve Bozoklu, O., "Farklı Şebekeler Üzerinden Uçtan Uca Emniyetli Haberleşmede Sinyalleşme", Elektrik - Elektronik ve Bilgisayar Mühendisliği Sempozyumu, ELECO 2008, Bursa, Kasım (2008).
[19] Dilli, O.,Mert,M., Koyuncu, M., Nazlıbilek, S.ve Akçam, N., "SCIP (Secure Communication Interoperability Protocol)'in IP Ağları Üzerinde Uygulaması", 3. Bilgi Güvenliği ve Kriptoloji Konferansı, ISC TURKEY, Ankara, Aralık (2008).
[20] Dilli, O., Akçam, N., Koyuncu, M., Nazlıbilek, S. ve, Mert,M., "FNBDT/SCIP Protokolünün IP Ağında Uygulanması ve Çağrı Kurmaya Ait Sınır Değerlerin Elde Edilmesi", 5. Savunma Teknolojileri Kongresi, SAVTEK 2010, Ankara, 23-25 (2010).
[21] Dilli, O., Akçam, N.ve Koyuncu, M., "FNBDT/SCIP Protokolünün Yerel Alan Ağında Uygulaması ve Sınır Değerlerin Tespit Edilmesi", Gazi Üniversitesi Mühendislik ve Mimarlık Fakültesi Dergisi, 25 (2) 275-283 (2010).
[22] Dilli, O., "Gelecek Nesil Darbant Terminal Cihazlarının Farklı Şebekeler Üzerinde Testi ve Haberleşmeye Ait Sınır Değerlerin Elde Edilmesi", Doktora Tezi, Gazi Üniversitesi Fen Bilimleri Enstitüsü, Ankara, 1-18, 60-62, 118-133, (2011).
[23] Dilli, O., Akçam, N., Koyuncu, M., "Determining the Limit Values in End-to-End Secure Communication within Satellite Network with FNBDT/SCIP", Energy Education Science and Technology Part A-Energy Science and Research, Volume 29, Issue 1, 627-642, April 2012.
[24] ITU, "Performance Enhancements Of Transmission Control Protocol Over Satellite Networks", ITU, ITU-R Recommendation S.1711 (01/2010), 12-23 (2010).
[25] ITU, "End-User Multimedia Qos Categories", ITU-T Recommendation G.1010 (11/2001), 5-7 (2001).
[26] ITU, "Performance Enhancements Of Transmission Control Protocol Over Satellite Networks", ITU-R Recommendation S.1711 (01/2010), 24-29 (2010).
[27] ETSI, "Satellite Earth Stations and Systems (SES); Broadband Satellite Multimedia; IP Interworking over satellite; Performance, Availability and Quality of Service", ETSI TR 102 157 V1.1.1 (2003-07), France, 57-61 (2003).
[28] ETSI, "Satellite Earth Stations and Systems (SES); Broadband Satellite Multimedia (BSM); QoS Functional Architecture", ETSI TS 102 462 V1.1.1 (2006-12), France, 43-44 (2006).
[29] ETSI, "Satellite Earth Stations and Systems (SES); Broadband Satellite Multimedia (BSM); Performance Parameters", ETSI TS 102 673 V1.1.1 (2009-11), France, 43-44 (2009)
[30] ITU, "Allowable Bit Error Ratios at The Output of the Hypothetical Reference Digital Path for Systems in The Fixed-Satellite Service Using Pulse-Code Modulation for Telephone", ITU-R Recommendation S.522-5 1-2 (1994).
[31] ITU, "Availability objectives for hypothetical reference circuits and hypothetical reference digital paths when used for telephony using pulse code modulation, or as part of an integrated services digital network hypothetical reference connection, in the fixed-satellite service operating below 15 GHz", ITU-R Recommendation S.579-6, 1-2 (2005).
[32] ITU, "Allowable Bit Error Ratios at The Output of the Hypothetical Reference Digital Path for Systems in The Fixed-Satellite Service Using Pulse-Code Modulation for Telephon", ITU-R Recommendation S.614-4, 28-33 (2005).

O. DİLLİ, Adana'nın Kadirli ilçesinde 1971 tarihinde dünyaya geldi. İlk, orta ve lise eğitimini Adana'da tamamladı. Fırat Üniversitesi Mühendislik Fakültesi Elektrik-Elektronik Mühendisliği Ana Bilim Dalından 1992 yılında mezun oldu. Gazi Üniversitesi Mühendislik Fakültesi Elektrik-Elektronik Mühendisliği Ana Bilim Dalında Yüksek Lisansını 2004 yılında tamamladı ve Gazi Üniversitesi Mühendislik Fakültesi Elektrik-Elektronik Ana Bilim Dalında Doktora Eğitimini 2011 yılında tamamladı.

Mesleğine Hava Kuvvetler Komutanlığında 1994 yılında, mühendis subay olarak başladı. Genelkurmay MEBS Başkanlığında proje ve işletme subayı olarak çalıştı. Halen Hava Teknik Okullar Komutanlığında öğretim üyesi olarak görev yapmaktadır.

Yrd.Doç.Dr.Dilli'nin, ISDN ve Uçtan Uca Güvenli Haberleşme konusunda araştırmaları bulunmaktadır.

Kayıtlı Elektronik Posta Sistemi ve E-Posta Güvenliği

Mustafa ALKAN, Mustafa ÜNVER, Hakan TEKEDERE

ÖZET

Bu çalışmada Kayıtlı Elektronik Posta (KEP) sistemi, KEP düzenlemeleri, mimarisi, bileşenleri ve uygulamaları üzerinde durularak bu konuda yapılan çalışmalar irdelenmiştir. Ayrıca Kayıtlı Elektronik Posta Sisteminde güvenlik uygulamaları ve getirileri değerlendirilmiştir.

Anahtar Kelimeler: Kayıtlı Elektronik Posta (KEP), Standartlar, Düzenlemeler.

Registered Electronic Mail System and E-Mail Security

ABSTRACT

In this study, Registered Electronic Mail (REM) system, REM regulations, applications, architecture, components are emphasized and discussed. In addition, security practices and benefits of registered electronic mail system are evaluated.

Keywords: Registered Electronic Mail (REM), Standards, Regulations.

1.GİRİŞ

Günümüzde bilgi ve belge paylaşımının önemli bir miktarı elektronik ortamda gerçekleşmekte ve iletim ortamı olarak internet, uygulama olarak da yoğun bir şekilde elektronik posta sistemi kullanılmaktadır. Bunun yanında e-devlet uygulamalarının her geçen gün artarak devam etmesi, kamu hizmetlerinin elektronik ortamda veriliyor olması bilgi ve belge paylaşımının hukuki ve teknik alt yapısının yeniden düzenlenmesini zorunlu hale getirmiştir. Bu düzenlemenin birincisi belge paylaşımının hukuki tarafı ikincisi ise teknik ve güvenlik tarafıdır. Kayıtlı Elektronik Posta Sistemi (KEP), temelde bu iki ihtiyaçtan doğmuştur. Bu sebeple elektronik ortamda iletilen elektronik posta mesajlarının gerek hukuki geçerliliğini sağlayan gerekse teknik alt yapısını ve güvenlik unsurlarını belirleyen bir sistem olarak Kayıtlı Elektronik Posta (KEP) Sistemi ve uygulamaları geliştirilmiştir [1,2]

2.KAYITLI ELEKTRONİK POSTA SİSTEMİ DÜZENLEMELERİ

Elektronik Posta uygulamalarının gittikçe yaşamımızın bir parçası haline gelmesi ve buna paralel olarak elektronik imza (e-imza) uygulamalarının yaygınlaşması, bilgi ve belgelerin hem hukuki geçerliliği hem de güvenilir bir ortamda paylaşılmasını sağlayacak sistemlere olan ihtiyacı arttırmıştır. Günümüzde gerek iletişimde gerekse de bilgi ve belge paylaşımında elektronik posta yaygın olarak kullanılan önemli bir araçtır. Elektronik posta, kolay ve ucuz yoldan bilgi iletimini sağlaması yanında, birçok güvenlik problemleriyle de karşı karşıya kalmaktadır. Bu problemlerin belki de en önemlilerinden biri, elektronik posta mesajlarının gönderilen kaynaktan geldiğinin ve alıcıya ulaştığının garanti edilememesidir. Bu garantinin sağlanabilmesi ancak ilave güvenlik hizmetleriyle mümkün olabilmektedir. Bu konuda uluslararası kuruluşlar tarafından ilgili standartlar ve uygulamalar hızla hayata geçirilmeye çalışılmaktadır..

2.1 KEP ile İlgili Uluslararası Düzenlemeler

KEP Sistemiyle ilgili olarak yapılan en ayrıntılı çalışma Avrupa Birliği bünyesinde yer alan Avrupa Telekomünikasyon Standartları Enstitüsü (ETSI) tarafından yapılmaktadır. ETSI, Avrupa Posta ve Telekomünikasyon İdareleri Birliği (Conference of European Post and Telecommunications - CEPT) bünyesinde telekomünikasyon standartları ile ilgili görevler yürüten bağımsız bir kuruluştur. ETSI, <bilgi ve İletişim Teknolojileri (BİT) ile ilgili 60'tan fazla ülkede standartların oluşturulmasını sağlamak amacıyla çeşitli projeler yürütmektedir. ETSI bünyesinde standart çalışmaları yapan bazı çalışma grupları bulunmaktadır. Bu çalışma gruplarından birisi de *"Elektronik İmzalar ve Altyapılar (Electronic Signatures and Infrastructures - ESI)"* grubudur. Bu grup *"Özel Görev Gücü (Specialist Task Force - STF)"* adı verilen çeşitli alt gruplardan oluşmaktadır. *"Kayıtlı Elektronik Postalara Uygulanan Elektronik İmzalar: Formatlar ve Politikalar (Electronic Signatures Applied to Registered Emails: formats and policies - STF 318)"* bu alt gruplardan biridir.

ETSI'nin yayımlanmış KEP Standartları aşağıda verilmektedir.

- ETSI TS 102 640-1"KEP Mimarisi", ETSI TS 102 640-2 "Veri isterleri, Formatlar için Bilgi Güvenliği Politika İsterleri"
- ETSI TS 102 640-4 "KEP uygunluk profilleri",
- ETSI TS 102 640-5 "KEP karşılıklı işlerlik profilleri"[1].

ETSI tarafından geliştirilen KEP standartları ile ilgili yapılan çalışmalardan önce İtalya, Belçika, Fransa, İsveç, İspanya gibi değişik ülkelerde elektronik tebligatı da içerecek şekilde ülkeden ülkeye farklılık gösteren çalışmalar yapılmıştır. Bu çalışmalar belirli bir standart çerçevesinde geliştirilmemiştir. KEP ile ilgili değişik uygulamalar ve projeler hayata geçirilmiştir. İtalya, Belçika, Fransa gibi ülkelerde KEPHS'lerin işleyişlerine ilişkin yasal düzenleme yapılırken, İsveç ve İspanya gibi

ülkelerde ise herhangi bir yasal düzenlemeye gerek duyulmamış. KEP Hizmet Sağlayıcılığı (KEPHS) hizmeti kamu idareleri tarafından, noterlik fonksiyonunu da içerecek şekilde sunulmaya başlanmıştır. İtalya'da 28 Ocak 2005 tarihinde KEP hizmetini düzenleyen Kanun kabul edilmiştir. Bu kanunun ardından elektronik ortamda doküman gönderilmesinin KEP sistemi kullanılarak yapılabileceği ve bu şekilde gönderilen yazıların, fiziki ortamda postayla yapılan tebligata eşdeğer olduğu ve aynı hukuki sonuçları doğuracağı belirtilmiştir [2].

KEP konusunda önemli çalışmalar yapan bir diğer uluslararası kuruluş Dünya Posta Birliği (Universal Postal Union-UPU)'dir. Bu kuruluş tarafından da bir çok standart geliştirilmiştir. Bu standartlardan birisi de KEP ile ilgili olarak hazırlanan *"Kayıtlı Elektronik Posta İşlevsel Spesifikasyonları (Postal Registered eMail-PReM Functional Specifications)"* adıyla yayınlanmış olan standarttır. Bunun yanında *"Güvenli Elektronik Posta Hizmetleri Arayüz Spesifikasyonları"* gibi düzenlemeler de yapılmıştır. Bu konuda bir diğer önemli doküman ise Avrupa Standardizasyon Komitesi (European Committee For Standardization-CEN) tarafından yayınlanan *"Siber Kimlik: Kuruluşlar için Kimlik Doğrulama Sistemi (Cyber-Identity: Unique identification systems for organisations and parts thereof)"* dökümanıdır. Bu doküman da özetle, elektronik posta yoluyla yapılan bilgi ve belge paylaşımında gönderici ve alıcının benzersiz kimlik tanımlamalarının yapılmasının ve elektronik postanın bütünlüğünün korunarak gönderilmesinin güvenliği ve hukuki geçerliliğinin sağlanması üzerinde durulmaktadır. Bunun yanında elektronik posta yoluyla yapılan elektronik fatura uygulamalarına yönelik düzenlemeler de bulunmaktadır.

2.2. KEP ile İlgili Ulusal Düzenlemeler

Ülkemizde e-Dönüşüm Türkiye İcra Kurulu, hukuki geçerliliği olan bir bilgi doküman paylaşımının sağlanabilmesi için KEP sisteminin gerekli olduğunu benimsemiş ve bu konuda 15 Temmuz 2009 tarihli ve 28 sayılı kararı ile Bilgi Teknolojileri ve İletişim Kurumu (BTK)'nu KEP sistemi konusunda düzenleyici çalışmalar yapmak üzere görevlendirmiştir [2].

11 Mart 2010 tarihli Kamu Hizmetlerinin Hızlandırılması Amacıyla Bazı Kanun ve Kanun Hükmünde Kararnamelerde Değişiklik Yapılmasına Dair Kanun Tasarısı'nda KEP sistemine ilişkin olarak bazı düzenlemeler getirilmiştir. Bu tasarıda KEP sistemi, elektronik posta haberleşmesinin, kayıtlı elektronik posta hizmet sağlayıcıları vasıtasıyla, 5070 sayılı Elektronik İmza Kanununda tanımlanan güvenli elektronik imza ve zaman damgası kullanılarak gerçekleştirilmesini ve bu haberleşmenin göndericisinin, alıcısının ve zamanının tespit edilmesini sağlayan haberleşme sistemi olarak tanımlanmıştır [2].

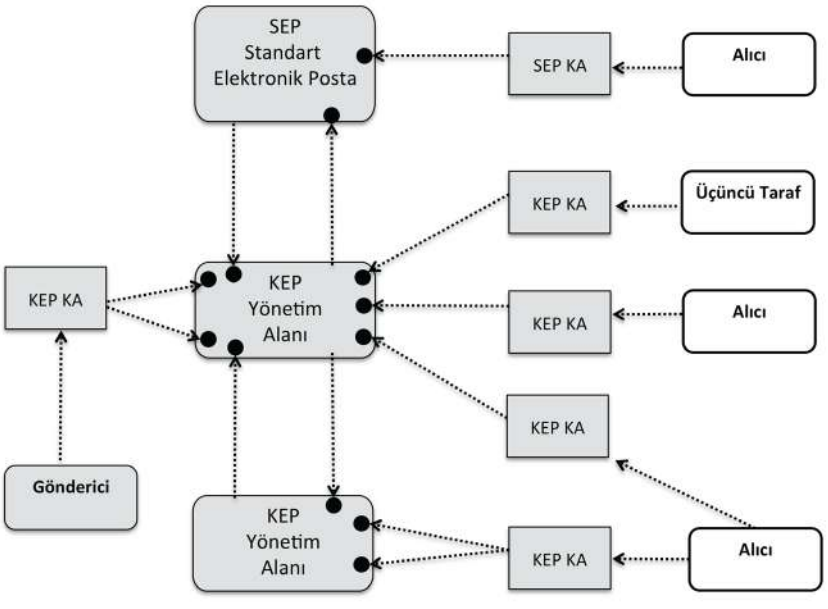
14 Şubat 2011 tarihli ve 6102 sayılı Türk Ticaret Kanunu'nun 18 inci maddesinde *"Tacirler arasında, diğer tarafı temerrüde düşürmeye, sözleşmeyi feshe, sözleşmeden dönmeye ilişkin ihbarlar veya ihtarlar noter aracılığıyla, taahhütlü mektupla, telgrafla veya güvenli elektronik imza kullanılarak kayıtlı elektronik posta sistemi ile yapılır."* ifadesi yer almaktadır. Yine bu kanunun 1525 inci maddesinde; Kayıtlı elektronik posta sistemine ilişkin usul ve esasların Bilgi Teknolojileri ve İletişim Kurumu tarafından bir yönetmelikle düzenleneceği belirtilmektedir [1,2]. Bu çerçevede BTK tarafından *"Kayıtlı Elektronik Posta Sistemine ilişkin Usul ve Esaslar Hakkında Yönetmelik"* hazırlanmış ve 25 Ağustos 2011 tarihli Resmi Gazete'de yayımlanmıştır. Yönetmelik de Türk Ticaret Kanunu gibi 1 Temmuz 2012 tarihinde yürürlüğe girmiştir. Ancak KEPHS olmak isteyen tüzel kişiler 1 Mayıs 2012 tarihinden itibaren BTK'ya bildirimde bulunabileceklerdir. KEP Rehberi ve KEP Hesabı Adreslerine ilişkin Usul ve Esaslar taslağı da 7 Mart 2012 tarihinde kamuoyu görüşü alınmak üzere BTK'nın resmi internet sitesinde yayımlanmıştır[8]. Konu ile ilgili çalışmalar devam etmektedir.

3. KEP SİSTEMİ VE UYGULAMA MODELİ

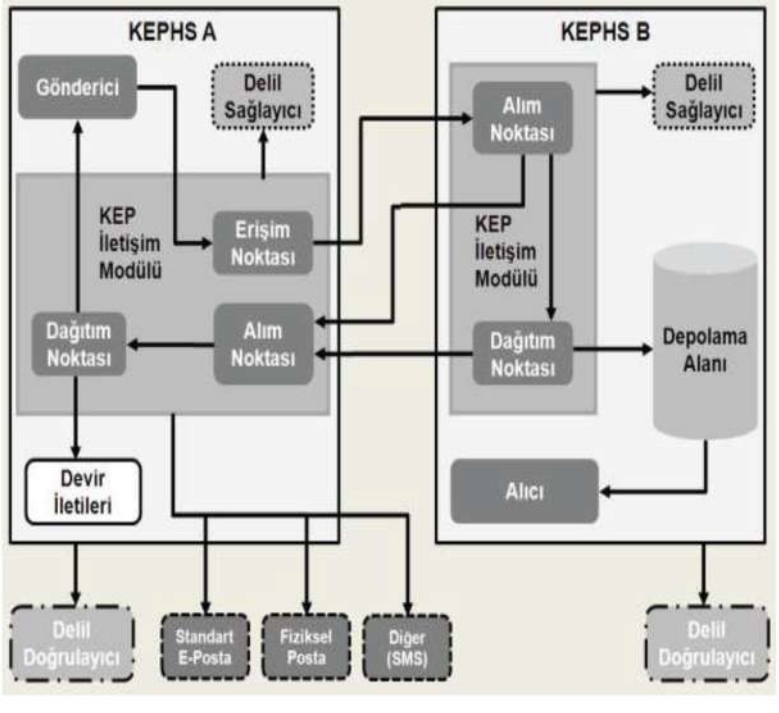
KEP; elektronik ortamda yapılan gönderilerin ne zaman yapıldığını, karşı tarafa ulaşıp ulaşmadığını, ulaşmışsa ne zaman ulaştığını kesin olarak tespit eden bir sistemdir. Klasik elektronik posta uygulamalarında güvenli olarak oluşturulan elektronik belge, teknik ve hukuki ispatının sağlanacağı şekilde gönderilememektedir. Benzer şekilde saklanması ve alınması sağlanamamaktadır. Bu konuda uluslararası standartlara ve güvenlik kriterlerine ilişkin denetlenebilir bir iletim alt yapısı bulunmamaktadır. Bu temel probleme çözüm, KEP sistemiyle getirilmiş olmaktadır. KEP sistemi ile hem uluslararası standartlara uygun hem de hukuki geçerliliği ve yeterliliği olan bir yapı oluşturulmaktadır. KEP sistemi, elektronik posta haberleşmesinin özel bir sistem üzerinden yapılması nedeniyle KEP kullanıcılarından olan gönderici elektronik iletinin kendisi tarafından gönderilmediğini, alıcı da elektronik iletinin kendisine ulaşmadığını iddia edememektedir. [3].

KEP sistemi, veri bütünlüğü, kimlik doğrulama ve inkâr edilemezlik gibi önemli unsurları yerine getirebilen elektronik imzayı, elektronik ortamdaki iş ve işlemler bilgi ve belge paylaşımında taraflar arasındaki güveni sağlamak için de kullanılabilecek önemli bir güvenlik bileşeni haline getirmektedir [1]. ETSI, AB üye ülkelerinin yetkili organları, diğer bağımsız kuruluşlar ve AB üyesi olmayan ülke kurumları arasında KEP sistemi ile ilgili uygulamalarla ilgili incelemeler yaparak bu incelemelerin sonucunda ETSI TR 102 640, Elektronik İmzalar ve Altyapılar; Kayıtlı Elektronik Posta (Electronic Signatures and Infrastructures (ESI); Registered E-Mail) standardını oluşturmuştur. Bu standart:

- Mimari
- KEP için Veri Gereksinimleri, Formatlar ve İmzalar
- KEP Yönetim Alanı için Bilgi Güvenliği Politika Gereksinimleri
- KEP Yönetim Alanı, Uyumluluk Profilleri
- KEP Yönetim Alanı, Birlikte Çalışabilirlik Profilleri alt bölümlerinden oluşmaktadır. [5,6].



Şekil 1: KEP mantıksal modeli



Şekil 2: KEP sistem bileşenleri

Şekil 1'de, noktalar KEP sisteminin kullanıcılarının KEPHS'lerin ve Standart Elektronik Posta (SEP) sunucularıyla etkileşimde bulunmak için kullandıkları ara yüzleri ifade etmektedir. KEP sisteminin kullanıcıları olan gönderici ve alıcılar KEP sistemi ile KEP kullanıcı arabirimi üzerinden, SEP kullanıcıları ise SEP kullanıcı arabirimi üzerinden haberleşmektedir. KEP kullanıcı arabirimi, kullanıcının bilgisayarında kullandığı elektronik posta istemci uygulamasına eklenmiş bir yazılım parçası olabileceği gibi KEPHS'nin sisteminde çalışan ve kullanıcının uzaktan eriştiği bir uygulama da olabilmektedir [1,2].

KEP sistemi kullanıcılarının, KEP sisteminden faydalanabilmek için herhangi bir KEPHS'den kendileri adına bir hesap açtırmaları gerekmektedir. Bu işlemden sonra kullanıcılar KEP kullanıcı arabirimini kullanarak KEP sistemine güvenli bir bağlantı üzerinden bağlanabilmektedirler. Bağlanma işleminden sonraki her bir elektronik posta gönderimi ve alımı KEPHS ile kurulan bu güvenli bağlantı üzerinden güvenli protokoller kullanılarak yapılmaktadır. KEP sisteminde birlikte çalışabilirliğin sağlanabilmesi için yetkilendirilmiş birden fazla KEPHS'nın bir denetleyici gözetiminde hizmet vermesi gerekmektedir. Bu durumda kullanıcıların, herhangi bir KEPHS'ya hesap açtırdıktan sonra bir kimlik doğrulama mekanizması ile sisteme erişimi sağlanmaktadır [1,2].

4. KEP UYGULAMA USUL VE ESASLARI

14 Şubat 2011 tarihli ve 6102 sayılı Türk Ticaret Kanunu'nda Kayıtlı elektronik posta sistemine ilişkin düzenlemelerin BTK tarafından yapılacağı belirtilmiştir. Bu kapsamda BTK, 25 Ağustos 2011 tarihli ve 28036 sayılı Resmi Gazetede yayımlanan "Kayıtlı Elektronik Posta Sistemine İlişkin Usul ve Esaslar Hakkında Yönetmelik" ile "Kayıtlı Elektronik Posta Sistemi ile ilgili süreçlere ve teknik kriterlere ilişkin tebliğ" bir yönetmelik yayımlamıştır. Bu düzenlemelerde; KEP; elektronik iletilerin, gönderimi ve teslimatı da dâhil olmak üzere kullanımına ilişkin olarak hukukî delil sağlayan, elektronik postanın nitelikli şekli olarak tanımlanmıştır.

Bahsi geçen bu düzenlemelere göre; KEP hesabı almak isteyen gerçek veya tüzel kişiler KEPHS'ye başvuruda bulunur. KEPHS başvuru sahibinin kimliğini tespit ederek KEP hesabı başvurusunu kabul eder ve KEP hesabını oluşturur. KEPHS, oluşturulan KEP hesabına ilişkin bilgileri başvuru sahibine güvenli bir şekilde teslim eder. KEPHS, başvuru sahibi ile sözleşme veya taahhütname imzalar. KEPHS, başvuru sahibinin onayını, güvenli elektronik imza ile aldıktan sonra ilgili KEP hesabını kullanıma açar. KEP sistemi, bir elektronik iletinin tarafları veya muhatapları arasında KEP hesabı vasıtasıyla hukukî ve teknik güvenliğe sahip bir şekilde gönderilip alınmasını sağlamak ve güvenli iletişimde bulunmak gibi amaçlarla kullanılır. KEP hesabının, hesap sahibi tarafından kendi nam ve hesabına kullanılması esastır. Hesap sahibinin tüzel kişi olduğu durumlarda; KEP hesabı, yetki verilmiş olan işlem yetkilisi tarafından hesap sahibinin nam ve hesabına kullanılır. KEP hesabı kullanılarak yapılabilecek işlemler ve sonuçları KEPHS ile hesap sahibi arasında imzalanan sözleşme veya taahhütname ile belirlenir. Hesap sahibi olan tüzel kişi istediği zaman işlem yetkilisini değiştirebilir. KEPHS, KEP sistemi içerisinde bir elektronik iletinin gönderilmesi ve alınması dışında elektronik belgelerin saklanması, güvenli iletişim ve elektronik ortamda güvenilir üçüncü taraf hizmetleri gibi katma değerli hizmetler sunabilir [2]..

BTK tarafından hazırlanan bu düzenlemelerde KEPHS, hesap sahibi ve Kurumun uyması gereken yükümlülükler de belirtilmiştir [7].

KEPHS'nin Yükümlülükleri

- Sakla-ilet ve sakla-bildir çalışma modellerinin biri veya her ikisi ile hizmet vermekle,
- Sunmakta olduğu hizmetler için, bu hizmetlerin gerektirdiği güvenlik seviyelerine uygun ve güvenilir bir kimlik doğrulama mekanizması tesis etmekle,
- KEP hesabının kullanıma kapatılmasına ilişkin taleplerin alınması ve derhâl gerçekleştirilebilmesi için yedi gün yirmidört saat erişilebilir bir hizmeti sunmakla,
- KEP hesabının ve bu hesap üzerinden verilen hizmetlerin güvenliğini, gizliliğini ve bütünlüğünü sağlamakla,
- Kişisel verilerin korunması için gerekli tedbirleri almakla,
- KEP sisteminin tüm süreçlerine ilişkin günlük kayıtlarını güvenliğini, gizliliğini ve bütünlüğünü sağlayarak kayıt altına almakla,
- KEP sisteminin tüm süreçlerinde oluşturulan KEP iletilerini ve KEP delillerini ilgili KEP hesabına anlaşılabilir ve okunabilir bir şekilde iletmekle, hesap sahibinin talebi hâlinde, KEP hesabına gelen iletilerin teslim alınmasına ilişkin bilgileri, alternatif iletişim kanalları üzerinden bildirmekle,
- KEP hesabına bir web ara yüzü veya elektronik posta istemci programları üzerinden güvenli bir şekilde erişilebilmesini, iletilerin okunabilmesini ve gönderilebilmesini sağlamakla,
- Hesap sahibinin önceden onayını almak kaydıyla kendisine ait bilgiler ile KEP hesabı bilgilerinden oluşan KEP rehberini tüm hesap sahipleri ve işlem yetkililerinin erişimine yedi gün yirmidört saat kesintisiz olarak açık tutmakla, kendi sistemleri üzerinde bulunan KEP hesaplarına ilişkin değişiklikleri ilgili KEP rehberine gerçek zamanlı olarak işleyerek güncellemekle ve diğer KEPHS'lerle birlikte KEP rehberini gerçek zamanlı olarak güncel tutmak için gerekli teknik altyapıyı kurmak ve işletmekle,
- KEP hesabının kullanılmasını sağlayan ara yüzleri engelli kişilerin de erişimlerini sağlayacak şekilde standartlara uygun olarak hazırlamakla,
- KEP sisteminin tüm süreçlerine ve işleyişine ilişkin bilgi, belge ve elektronik veriler ve işlemlerin yapıldığı zamana ve işlemleri yapan kişi/ kişilere ait bilgileri içeren kayıtları gizliliğini, bütünlüğünü ve erişilebilirliğini koruyarak en az yirmi yıl süreyle saklamakla,
- KEP hesabının ilk kullanımından önce hesap sahibini ve varsa işlem yetkilisini KEP sistemine ilişkin tüm süreçler hakkında bilgilendirmekle,
- Sözleşmenin veya taahhütnamenin yenilenmemesi durumunda KEP hesabının kullanıma kapatılacağına ilişkin hesap sahibini ve işlem yetkilisini sözleşme veya taahhütname süresinin sona ermesinden üç ay önce uygun

iletişim kanallarından en az birisi ile bilgilendirmekle,
- KEP hesabının kapatılması sürecinde, herhangi bir mağduriyetin yaşanmaması için gerekli tedbirleri almakla,
- KEP sistemine ilişkin ana ve yedek sistemlerini Türkiye Cumhuriyeti sınırları içerisinde bulundurmakla,
- KEP sistemindeki tüm imzalama süreçlerinde ESHS (Elektronik Sertifika Hizmet Sağlayıcısı)'lar tarafından KEPHS için oluşturulan işlem sertifikasını kullanmakla,
- Hesap sahibinin veya işlem yetkilisinin talep etmesi hâlinde KEP delillerinin gerçek zamanlı olarak doğrulanması hizmetini sunmakla yükümlüdür.

Hesap sahibinin yükümlülükleri

- KEP hesabı başvurusu için gerekli olan bilgi ve belgeleri tam ve doğru olarak KEPHS'ye vermekle,
- Başvurusunda KEP hesabını sadece alıcı veya hem alıcı hem gönderici olarak kullanacağını KEPHS'ye açıkça belirtmekle,
- Başvurusunda sakla-ilet ve sakla-bildir çalışma modellerinden hangisi ile hizmet alacağını açıkça KEPHS'ye belirtmekle,
- KEP hesabı bilgilerinde olan değişiklikleri, KEPHS'ye derhâl bildirmekle,
- KEPHS ile imzaladığı sözleşmede veya taahhütnamede belirtilen hüküm ve koşullara uygun hareket etmekle,
- Kimlik doğrulama amacıyla kendisine verilen bilgileri korumakla, üçüncü kişilerle paylaşmamakla ve başkasına kullandırmamakla yükümlüdür.

SONUÇ ve YORUMLAR

Sonuç olarak KEP Sistemi, yapısı itibariyle elektronik ortamda paylaşılan bilgi ve belgelerin elektronik posta yoluyla ileri mesajlaşma teknikleri ve yüksek güvenlik mekanizmalarıyla gerçekleştirildiği bir sistem olarak önemli bir alt yapı ve ortam sunmaktadır. İletilen ve paylaşılan bilgi ve belgelerin hukuki geçerliliği yanında zaman damgası, kimlik doğrulama, inkar edilemezlik ve veri bütünlüğü gibi temel güvenlik kriterlerini de beraberinde getirmektedir. Bu sistem sayesinde başta e-devlet uygulamaları olmak üzere, e-ticaret e-fatura e-belge vb. tüm e-uygulamalar standartları belirlenmiş teknik bir alt yapıya ve hukuki bir zemine oturmuş olacaktır. Benzer şekilde başta e-imza uygulamaları ve zaman damgası gibi uygulamalar olmak üzere yeni servislerin ve hizmetlerin yaygınlaşmasının da önemli ölçüde önünü açacaktır.

KAYNAKLAR

[1] ETSI TS 102 640-1,Electronic Signatures and Infrastructures (ESI); Registered Electronic Mail (REM); Part 1: Architecture, 2010-01.
[2] Alkan, M., Ünver, M., Kabasakal, D., Günaydın, Y. (2011). Kayıtlı Elektronik Posta Sistemi Teknik Yapısı, Özellikleri ve İşleyişi. ISBN: 978-9944-0189-7-5.
[3] Kayıtlı E-Posta ve Hizmet Sağlayıcılığı. http://www.eventbrite.com/event/2157176172
[4] UPU, Postal Registered eMail (PReM) Functional Specification.
[5] CEN, Cyber-Identity: Unique identification systems for organisations and parts thereof||, s. 5-6-7
[6] CEN, e-Invoicing Compliance Guidelines Commentary to Compliance Matrix||, s. 41
[7] BTK. (2011). Kayıtlı Elektronik Posta Sistemine İlişkin Usul ve Esaslar Hakkında Yönetmelik. 25 Ağustos 2011, Resmî Gazete, Sayı:28036.
[8] KEP Rehberi ve KEP Hesabı Adreslerine ilişkin Usul ve Esaslar taslağı http://www.btk.gov.tr/kamuoyu_gorusleri/kog.php?ID=47

Mustafa ALKAN
1962 yılında Kayseri'de doğdu. Erciyes Üniversitesi Mühendislik Fakültesi, Elektronik Mühendisliği Bölümünde lisans eğitimini tamamladı. Yüksel lisans ve doktora eğitimini Erciyes Üniversitesi Mühendislik Fakültesi, Elektronik Mühendisliği Bölümü Elektronik Ana Bilim Dalında yaptı. Niğde Üniversitesi Mühendislik Fakültesi Elektrik-Elektronik kurucu bölüm başkanlığı, Niğde MYO Müdürlüğü, Bilgi Teknolojileri ve İletişim Kurumu Başkan Yardımcılığı görevlerinde bulundu. Halen Gazi Üniversitesi Teknoloji Fakültesi Elektronik Anabilim dalında öğretim üyesi ve Bilgi Güvenliği Derneği Başkanlığını yürütmektedir.

Hakan TEKEDERE
1975 yılında Malatya'da doğdu. 1997 yılında Fırat Üniversitesi Teknik Eğitim Fakültesi Elektronik-Bilgisayar Eğitimi Bölümü'nden mezun oldu. 2001 yılında Niğde Üniversitesi'nde yüksek lisansını, 2009 yılında Gazi Üniversitesi'nde doktorasını tamamladı. 2010 yılında yardımcı doçent unvanını aldı. Bilgisayar, iletişim teknolojileri, eğitim teknolojileri alanlarında çalışmaları bulunmaktadır

Kuantum Anahtar Dağıtımında (KAD) Gizli Anahtar Uzlaştırma: CASCADE Protokolü ve LDPC Kodları

Burcu A. Korkmaz, Mustafa Toyran, Thomas B. Pedersen,
A. S. Atilla Hasekioğlu, Pars Mutaf, M. Ali Can

Özetçe—**Bu çalışmada kuantum anahtar dağıtımında (KAD) karşılaşılan bilgi uzlaştırma problemi tanıtılacaktır. Ayrıca, bu probleme çözüm olarak sunulan en yaygın iki hata sezme ve düzeltme tekniğine yer verilecektir. Bu iki teknik, güvenlikleri ve güvenilirlikleri yönünden de karşılaştırılacaktır.**

Anahtar Kelimeler—**Kuantum anahtar dağıtımı, gizli anahtar uzlaştırma, hata düzeltme, CASCADE, LDPC**

Abstract—**This work introduces the secret key reconciliation problem in quantum key distribution (QKD). Then, the two most common error detection and correction techniques as solutions to this problem are given. These two techniques are also compared in terms of their security and reliability.**

Index Terms—**Quantum key distribution, secret key reconciliation, error correction, CASCADE, LDPC**

I. GİRİŞ

MODERN kriptografi [1], **gizli anahtar** adı verilen bir parametrenin **varlığı**na ve **gizliliğ**ine dayanmaktadır. Gizli anahtar, sadece sahibinin ya da yetkili kimselerin bilmesi gereken çok değerli bir varlıktır. Çünkü, mesajlar gönderici tarafta **açık/gizli** anahtarla şifrelenmekte ve şifreli mesaj da alıcı tarafta ancak doğru gizli anahtarla çözülebilmektedir. Modern kriptoda kullanılan **güçlü** algoritmalar ve protokoller herkese açık olduğundan gizliliğin bağlı olduğu tek parametre gizli anahtardır. Gizli anahtarla ilgili en önemli konular ise üretimi, **dağıtım**ı ve doğumundan ölümüne kadar doğru yönetimidir. Bu döngüde doğru kullanım için her aşamanın **güvenli** ve **güvenilir** bir şekilde yerine getirilmesi gerekir.

Anahtar dağıtımı, kriptografide önemli ve çözülmesi zor problemlerden [2] birisi olarak tarihteki yerini almıştır. **Anahtar dağıtım problemi**, üretilen gizli anahtarın başka hiçbir kimsenin eline geçmeden alıcıya ulaştırılmasıdır. Çünkü, dağıtım esnasında gizli anahtarın ele geçmesi demek, mesajın içeriğinin de ele geçmesi demektir. Tarih boyunca insanlar bizzat mesajın kendisini ya da sadece gizli anahtarları alıcıya ulaştırabilmek için kuş, ulak gibi geleneksel veya telli ya da telsiz modern iletişim yöntemleri kullanmışlardır. Kurye kullanımı bugün de güvenli kabul edilip tercih edilen temel anahtar dağıtım yöntemlerinden birisidir. Ancak, klasik anahtar dağıtım yöntemlerinin en büyük problemi dağıtılan anahtarların gizliliğinin **garanti** edilememesidir. Örneğin, güvenilir kurye yolda giderken yetkisiz kişiler anahtarın bir kopyasını bir şekilde ellerine geçirebilir. Klasik tekniklerin hiçbirisi bize bunu anlamamızı sağlayacak bir araç sunmaz (**iletişimin dinlenip dinlenmediği anlaşılamaz**). Bunun yanında, güvenlikleri verimli çözülebilirliği henüz **ispatlanmamış** birtakım zor matematiksel problemlere (**asal çarpanlara ayırma**, **ayrık logaritma alma** gibi) dayanan açık anahtarlı dağıtım sistemleri de tam olarak güvenli kabul edilemezler. Çünkü, belki kimseyle paylaşmak istemeyen birileri bu problemleri de kolayca çözüyor olabilir. Mesela, kuantum bilgisayarların böylesi problemleri çok verimli bir şekilde çözebileceği öngörülmektedir [3]. Dolayısıyla, güvenliğin şansa bırakılmadığı, birtakım **varsayım**lara dayanmadığı; aksine, **ispat**lanabildiği, **garanti** edilebildiği daha güvenilir ve güvenli başka anahtar dağıtım yöntemlerine ihtiyaç vardır. Bir çözüm, **kuantum anahtar dağıtımı**dır.

Çalışmamızın sonraki kısımlarında sırasıyla şu bölümler yer almaktadır. Kısım II'de kuantum anahtar dağıtımı (KAD) ve bilgi uzlaştırma problemi kısaca tanıtılmaktadır. Kısım III'te CASCADE hata düzeltme protokolü, Kısım IV'te LDPC hata düzeltme kodları, Kısım V'te bu iki farklı hata düzeltme tekniğinin güvenlik (*sızdırılan bilgi miktarı*) ve güvenilirlik (*hata düzeltme performansı*, vb.) yönünden karşılaştırmaları, analizleri, Kısım VI'da ise sonuçlar yer almaktadır.

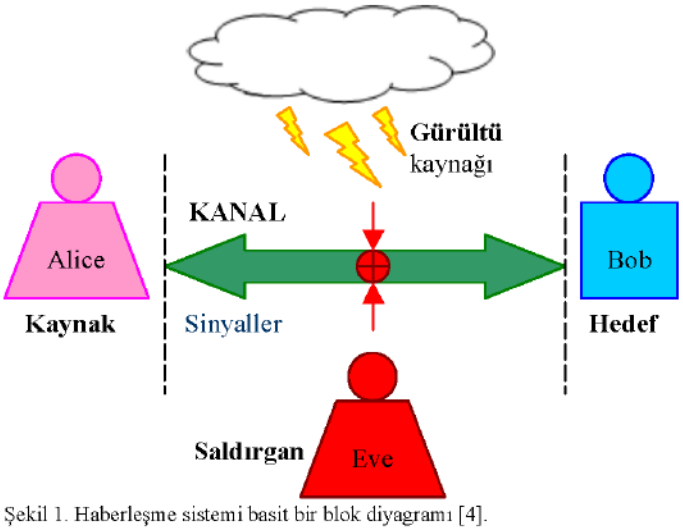
B. A. Korkmaz,
Ege Üniversitesi, Uluslararası Bilgisayar Enstitüsü, Bornova, İzmir.
burcuakmankorkmaz@gmail.com
M. Toyran. MS.
UEKAE, BİLGEM, TÜBİTAK, P.K.: 74, 41470, Gebze/KOCAELİ.
mustafa.toyran@uekae.tubitak.gov.tr
T. B. Pedersen. Ph.D.
UEKAE, BİLGEM, TÜBİTAK, P.K.: 74, 41470, Gebze/KOCAELİ.
pedersen@uekae.tubitak.gov.tr
A. S. A. Hasekioğlu. Ph.D.
UEKAE, BİLGEM, TÜBİTAK, P.K.: 74, 41470, Gebze/KOCAELİ.
atilla@uekae.tubitak.gov.tr
P. Mutaf. Yrd. Doç. Dr.
Ege Üniversitesi, Uluslararası Bilgisayar Enstitüsü, Bornova, İzmir.
pars.mutaf@gmail.com
M. A. Can. Ph.D.
UEKAE, BİLGEM, TÜBİTAK, P.K.: 74, 41470, Gebze/KOCAELİ.
can@uekae.tubitak.gov.tr

II. KUANTUM ANAHTAR DAĞITIMI (KAD)

Haberleşme sistemlerinin temel amaçlarından ikisi, bilgiyi bir **KANAL** (iletim/taşıma ortamı) aracılığıyla **Kaynak** (bilgi kaynağı, gönderici, verici, 1. kişi, Alice) adı verilen bir uçtan **Hedef** (alıcı, 2. kişi, Bob) adı verilen başka bir uca/noktaya **güvenilir** ve **güvenli** bir şekilde taşımaktır. Burada,

- **güvenilirlik** ile gizli (mahrem, hassas) bilginin içeriğinin dosdoğru, bozulmasız bir şekilde iletilmesi,
- **güvenlik** ile de gizli bilginin içeriğinin 3. kişilerin (Eve, düşman, saldırgan, meraklı) eline asla geçmemesi

kastedilmektedir. Haberleşme sistemlerinin diğer amaçlarına örnek olarak ise verimlilik, hız, maliyet, vb. de verilebilir.



Şekil 1. Haberleşme sistemi basit bir blok diyagramı [4].

Şekil 1'de, pratik bir haberleşme sistemi modellenmektedir. Burada, kanal olarak CD/DVD, sabit disk, RAM, vs. bellek ortamları kullanılırsa yapılan iş depolama adını alır. Depolama işlemi de bir tür haberleşme olarak düşünülebilir.

Bizler kullanıcılar olarak bir iletişimde ya da depolama işleminde güvenilirlik ve güvenlik konularından tam olarak emin olmak isteriz. Ancak, uygulamada bu amaçlara ulaşmak hiç de kolay değildir. Şekil 1'de de gösterilmeye çalışıldığı gibi, sisteme 2 olumsuz bileşen daha dahil olmaktadır:

- **Gürültü**: Mevcut bütün iletim ortamları gürültülüdür. Gürültü, hatalara, bozulmalara neden olur.
- **Saldırgan** (Eve, rakip, kriptanalizci, hain, vb.): Mevcut bütün (klasik) iletim ortamları pasif saldırganlarca dinlenebilir ve iletişimin dinlendiği anlaşılamaz.

Pratikte, amaçlarımıza ulaşabilmek için bu olumsuzluklara karşılık biz de sisteme 2 yeni olumlu bileşen ekleriz:

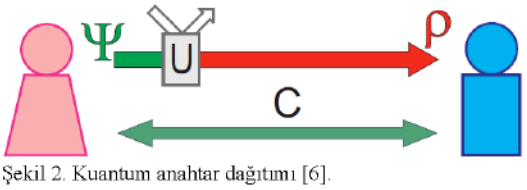
- **Hata sezme ve düzeltme teknikleri**: Kodlama servisi ile bilgiyi kodlarız, bozulursa anlayıp düzeltebilelim diye.
- **Kriptografik teknikler**: Şifreleme servisi ile bilgiyi şifreleriz, içeriğini başkaları asla anlayamasın diye.

Her iki teknikte de bilgi, kesin olarak kanıtlanmamış çeşitli Matematiksel yöntemlerle korunmaya çalışılır.

- Mevcut klasik hata düzeltme tekniklerinin bütün hataları düzeltebileceklerinin bir garantisi yoktur.
- Klasik/Modern kriptografide güvenlik, gizli anahtarlara dayanmaktadır. Ancak, en büyük problem de bu "gizli anahtar"ların gizliliğinin hiçbir zaman tam olarak garanti edilememesidir. Mevcut tüm anahtar dağıtım yöntemleri matematiksel ispattan yoksundur.

Kuantum kriptografi [5], tüm bu sorunların çözülebildiği bir Kriptografi tekniğidir. Yine "gizli anahtar"ların varlığına ve gizliliğine dayanılır, güvenilir. Ancak, burada anahtar dağıtımı (kuantum) Fizik yasaları ile güvenli hale getirilir. Dolayısıyla, bilgi de Fizik yasaları ile korunmuş olmaktadır:

- **Güvenlik ispatlıdır**, evrensel fizik kanunlarına dayanır.
- **İletişimin dinlendiği de anlaşılabilir.**

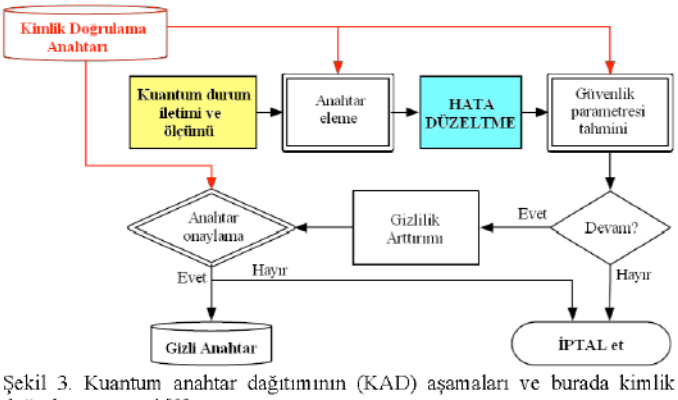


Şekil 2. Kuantum anahtar dağıtımı [6].

Kuantum anahtar dağıtımında (KAD) [7], gizli anahtar bitlerini taşıyıcı çok güvenilir kuryeler olarak tek tek fotonlar kullanılmaktadır. Şekil 2'den de görüldüğü gibi protokol iki aşamadan oluşur: *i*) Kuantum kanal üzerinden gerçekleştirilen kuantum kısım ve *ii*) Klasik kanal üzerinden gerçekleşen klasik kısım. Protokol, özetle, şu şekilde çalışmaktadır:

- Alice rasgele bir A bit dizisi üretir ve herbir bitini tek tek fotonlarla kuantum kanaldan Bob'a gönderir. Kuantum kanaldaki bozulmalar ve diğer kuantum bileşenlerdeki kusurlar nedeniyle Bob'daki dizi $B = A + e$ şeklinde olur.
- Sonraki aşama klasik bir kanal üzerinden hata sezme ve düzeltme teknikleri kullanarak B'deki tüm hatalı bitleri bulup düzeltmek yoluyla $B = A$ yapmaya çalışmaktır.

Güvenlik için klasik kanal üzerinden gerçekleştirilen tüm iletişimlerin **kimlik doğrulamalı** olması gerekir. Aksi halde, KAD protokolü saldırganlarca yapılacak bir **ortadaki adam saldırısına** karşı tamamen savunmasız olmaktadır.



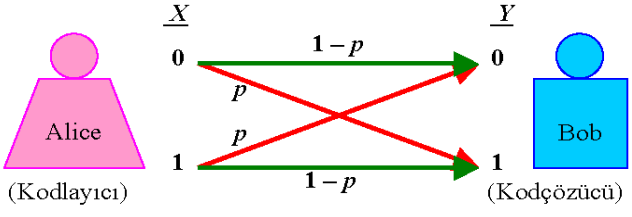
Şekil 3. Kuantum anahtar dağıtımının (KAD) aşamaları ve burada kimlik doğrulamanın yeri [8].

Şekil 3'te görüldüğü gibi KAD'da kimlik doğrulamanın yeri ve önemi büyüktür. KAD protokollerinin güvenliği için kimlik doğrulama **koşulsuz güvenlikte** olmalıdır.

Kuantum kriptografi, KAD, güvenliği ve ispatları hakkında daha fazla bilgi için [9]-[17]'ye de başvurulabilir.

III. CASCADE HATA DÜZELTME PROTOKOLÜ

İletişim kanalı, simgelerin (0, 1'ler) alıcıya aktığı bir yol veya ortamdır. Analizlerde kuantum kanal, istatistiksel kanal modellerinden **BSC** (binary symmetric channel, ikili simetrik kanal) ile modellenmektedir (bkz. Şekil 4).



Şekil 4. BSC (binary symmetric channel, ikili simetrik kanal) kanalın diyagramı [18]-[20].

En geniş anlamda modern iletişim sistemleri, elektrik ya da optik sinyaller kullanarak mesajı (içerdiği enformasyonu) bir noktadan (kaynak) diğer bir noktaya (hedef) yüksek bir **verim**le ve **güvenilir**likle iletmeye çalışırlar.

Enformasyon teorisi, bizlere mesaj sinyallerinin içerdiği **enformasyon** miktarını belirlemek için nicel bir ölçü sağlar ve bu enformasyonun kaynaktan hedefe gönderilebilmesi için gerekli iletişim sistemi kapasitesinin hesaplanmasına izin verir. BSC kanal için **kanal kapasitesi** şu şekildedir:

$$C = 1 + p\log_2 p + (1-p)\log_2(1-p) \qquad (1)$$

Enformasyon teorisinin başlıca konularından biri olan **kodlama**nın kullanılmasıyla mesaj sinyallerindeki **gereksizlik** azaltılabilir ve böylece kanallar çok daha ***verimli*** bir biçimde kullanılabilir (kaynak kodlama). Ek olarak, iletilen sinyale **sistematik fazlalık** eklenebilir ve böylece kanallar çok daha ***güvenilir*** olarak da kullanılabilir (kanal kodlama).

Pratikte, KAD'da en çok tercih edilen iki hata sezme ve düzeltme tekniği, CASCADE ve LDPC'dir.

CASCADE protokolü:

Cascade protokolü, ilk defa [21]'de verilmiştir. Protokolün ana fikri, mesajı küçük bloklara bölmek ve blok paritelerini karşılaştırmak/sağlatmak suretiyle hataları bulmaktır. Cascade tüm blokların bir kaydını da tutarak verimliliği iyileştirir.

Protokol birkaç çevrimde ilerler. Çevrimlerin sayısı Alice ve Bob tarafından protokolü çalıştırmadan önce belirlenir. Bu seçim tamamen kuantum (optik) kanalın hata olasılığı olan p parametresi ile ilgilidir. Alice ve Bob'un dizileri sırasıyla,

$A = A_1, A_2, \ldots, A_n$,

$B = B_1, B_2, \ldots, B_n$, ($A_i, B_i \in \{0, 1\}$) olsun.

Çevrim 1: Alice ve Bob, k_1 çevrim 1 blok uzunluğunu seçer ve dizilerini k_1 bitlik bloklara böler. Pozisyonları

$$K_v^1 = \{l \mid (v-1)k_1 < l \le vk_1\}$$

olan tüm bitler 1. çevrimin v. bloğunu oluştururlar. Alice, tüm bloklarının paritelerini Bob'a gönderir. Aşağıda açıklanacak olan BINARY adlı süreç kullanılarak Bob, paritesi Alice'te karşı gelen bloğun paritesinden farklı olan her bloktaki bir bitlik hatayı düzeltir. Çevrim sonunda, Bob'un bloklarının tümü çift sayıda (yada sıfır) bir hataya sahiptir.

Çevrim $i > 1$: Herbir $i > 1$ çevriminde Alice ve Bob bir k_i çevrim i blok uzunluğu ve bir $f_i : [1..n] \to \left[1..\left\lceil \frac{n}{k_i} \right\rceil\right]$ rasgele sıkıştırma (özetleme) fonksiyonu belirler. Pozisyonları $K_j^i = \{l \mid f_i(l) = j\}$ olan tüm bitler i. çevrimin j. bloğunu oluştururlar. Ve Alice, herbir $1 \le j \le \left\lceil \frac{n}{k_i} \right\rceil$ mesaj bloğu için, $a_j = \bigoplus_{l \in K_j^i} A_l$ parite değerini hesaplar ve tümünü Bob'a yollar. Bob da kendi b_j paritelerini aynı şekilde hesaplar ve onları Alice'ten gelen a_j'lerle karşılaştırır. Herbir $b_j \neq a_j$ için K_j^i ile tanımlanan blok üzerinde BINARY metodunu çalıştırırlar. Bob, $B_l \neq A_l$ olan bir $l \in K_j^i$ bulacaktır ve onu düzeltecektir. Sonra, Alice ve Bob geriye-iz-sürme-prosedürünü başlatırlar.

Geriye iz sürme prosedürü: $l \in K_j^i$ durumunda, $1 \le u < i$ olan tüm eski u çevrimleri için $l \in K_v^u$ olan tüm geçmiş K_v^u blokları artık tek sayıda hataya sahip olacaktır. Bu blokların kümesi κ olmuş olsun. Şimdi Alice ve Bob, κ'daki *en küçük* blokları seçebilir ve başka bir hatayı daha bulmak için BINARY metodunu kullanabilir. A ve B dizilerinde bu yeni hatanın pozisyonu l' olsun. $B_{l'}$ biti de düzeltildikten sonra, Bob herbir u çevriminde $B_{l'}$ bitini içeren bloklardan oluşan θ kümesini de belirleyebilir. Ayrıca, $\kappa' = (\theta \cup \kappa) \setminus (\theta \cap \kappa)$ değerini hesaplayarak tek sayıda hata içeren blokların kümesi olan κ' kümesini de elde edebilir. Eğer $\kappa' \neq \phi$ (tek sayıda hata içeren blok var anlamında, ϕ: boş küme) ise, Bob aynı şekilde bir başka hata çiftini daha bulur ve düzeltir. Bu süreç, $\kappa' = \phi$ (tek sayıda hatalı blok yok) olana kadar tekrarlanır.

Geriye doğru iz sürme prosedürü bittikten sonra, Alice ve Bob i. çevrimdeki pariteleri karşılaştırmaya devam eder. Bir parite farklı olduğunda/sağlanmadığında yeni bir geriye doğru iz sürme süreci başlatırlar. Tüm pariteler kontrol edildikten sonra, i. çevrim sona erer. Bu noktada, 1. çevrimden i. çevrime kadar tüm bloklar çift sayıda (belki 0) hata içerir.

BINARY metodu: Alice'teki X ve Bob'daki $Y = X + \varepsilon$ dizileri tek sayıda (1, 3, 5, …) bit hatasına sahip olduklarında,

(1) Alice X'i iki parçaya böler ve X'in ilk parçasının paritesini Bob'a gönderir.

(2) Bob aynı şekilde Y'yi iki parçaya böler ve tek sayıda hatayı hangi parçanın içerdiğini tespit etmek için gelen pariteyi Alice'inki ile karşılaştırır.

(3) Bir hatalı bit bulunana kadar ilk iki adım defalarca tekrarlanır. Bulunan 1-bitlik hata Bob'da düzeltilir.

Cascade, p parametresine göre farklı blok uzunluğu ve çevrim sayısı seçer. [21]'de verilen protokolde 1. çevrim blok uzunluğu $k_1 \approx 0.73/p$, sonraki çevrimlerde ise $k_i = 2k_{i-1}$ olarak seçilmiş ve 4 çevrimde de gerçekleştirilmiştir.

IV. LDPC HATA DÜZELTME KODLARI

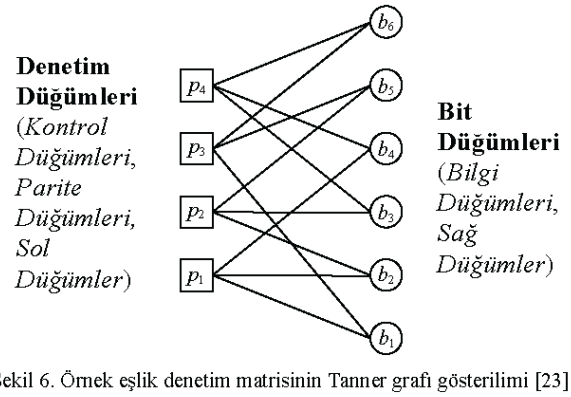
LDPC (low density parity check, düşük yoğunluklu eşlik denetim) kodları ilk olarak [22]'de önerilmiş parite kontrolüne dayanan lineer blok kodlardır. Yoğunluk terimi, eşlik denetim matrisindeki sıfır harici elemanların sayısının tüm matris elemanlarının sayısına oranı olarak tanımlanır. Genel olarak diğer tüm doğrusal kodlara ait eşlik denetim matrislerinde sıfırların ve birlerin sayısı yaklaşık olarak aynı olmaktadır. 1'lerin sayısı, tüm matris elemanlarının sayısının yanında çok seyrek kalıyorsa, bu eşlik denetim matrisinin oluşturduğu koda düşük yoğunluklu eşlik denetim kodu adı verilir.

n kod uzunluklu bir doğrusal eşlik denetim kodu, kod sözcükleri $(n - k)$ adet doğrusal parite kontrol kısıtlamasını sağlayan bir (n, k) lineer blok koddur: k bit bilgi sözcük uzunluğuna ve n bit kod sözcük uzunluğuna sahiptir. 2^k adet bilgi sözcüğü ve 2^k adet de kod sözcüğü bulunmaktadır. Geleneksel olarak, $(n - k)$ x n boyutundaki bir eşlik denetim matrisi H_{MxN} ile tanımlanır (bkz. Şekil 5). Bu matristeki $N = n$ adet sütun, her bitin hangi kısıtlamalarda kullanıldığını belirtir. $M = n - k$ adet satır ise $n - k$ adet kısıtlamayı ifade eder. Dolayısıyla, 2^{n-k} adet de kısıtlama/denklem/eşitlik sözcüğü vardır. Eşlik denetim kodu, sadece $c.H^T = 0$ koşulunu sağlayan (yani, sendrom = 0 olan) n uzunluklu c kod sözcüklerinin kümesinden oluşmaktadır, $c_{1xn} = (c_1, c_2, ..., c_n)$.

$$H_{4x6} = \begin{bmatrix} 1 & 1 & 0 & 1 & 0 & 0 \\ 0 & 1 & 1 & 0 & 1 & 0 \\ 1 & 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 1 & 0 & 1 \end{bmatrix} \quad (2)$$

Şekil 5. Örnek bir eşlik denetim matrisi [23].

Herhangi bir eşlik/parite denetim kodunu, LDPC kod dahil, görselleştirmek ve grafiksel olarak temsil etmek amacıyla Tanner grafı kullanılmaktadır. Şekil 5'teki örnek matrisin grafı Şekil 6'daki gibidir. Bu graf, kod çözme algoritmalarının kolaylıkla geliştirilebilmesine olanak sağlamaktadır.



Şekil 6. Örnek eşlik denetim matrisinin Tanner grafı gösterilimi [23].

Tanner graflarında bir bit düğümünden (bilgi düğümü de denir) başlayıp aynı bit düğümünde sona eren yola çevrim (cycle) adı verilmektedir. Graf iki yönlü olduğundan dolayı bir çevrimin minimum uzunluğu dört (4) olmaktadır. Rastgele bir biçimde üretilen bir eşlik denetim matrisine ait Tanner grafında 4 uzunluklu çevrimlerin olma olasılığı çok yüksektir. Ancak, performansı çok olumsuz etkiledikleri için 4, 6, 8, ... gibi çok kısa uzunluklu çevrimlerin olması pek istenmez.

LDPC kodlarını, ifade etmenin bir yolu da Mackay ve diğerlerince önerilen "alist" formatıdır [24]. Şekil 5'teki H_{4x6} matrisinin alist formatı gösterilimi Şekil 7'deki gibidir. alist formatında çeşitli matrislere [25] linkinden ulaşılabilir.

6 4	(*1. SATIR*)
3 2	(*2. SATIR*)
3 3 3 3	(*3. SATIR*)
2 2 2 2 2 2	(*4. SATIR*)
1 2 4	(*5. SATIR*)
2 3 5	⋮
1 5 6	
3 4 6	(*8. SATIR*)
1 3	(*9. SATIR*)
1 2	
2 4	⋮
1 4	
2 3	
5 6	(*14. SATIR*)

Şekil 7. Örnek eşlik denetim matrisinin alist formatı gösterilimi.

Yukardaki örnek alist içeriğinde:

1. SATIR: Matrisin boyutlarını ifade eder. Büyük olanı N, küçük olanı M değeridir.

2. SATIR: Matrisin satırlarının ve sütunlarının maksimum ağırlıklarını ifade eder. Büyük olanı satırlara, küçük olanı ise sütunlara ilişkin olandır.

3. SATIR: Matrisin satırlarının ağırlıklarını, yani 1'lerinin sayısını, ifade eder. Bu satır daha kısadır.

4. SATIR: Matrisin sütunlarının ağırlıklarını, yani 1'lerinin sayısını, ifade eder. Bu satır ise daha uzundur.

5. - 8. SATIRLAR: Matrisin satırlarının değeri 1 olan elemanlarının indexlerini vermektedir. Aralık daha dardır.

9. - 14. SATIRLAR: Matrisin sütunlarının değeri 1 olan elemanlarının indexlerini vermektedir. Aralık daha geniştir.

Eğer bir kod için bit düğümlerinin dereceleri birbirine eşit ve denetim düğümlerinin dereceleri de birbirine eşit ise bu koda düzenli LDPC kod denir. Düzensiz LDPC kodlar için ise her bir düğüm için farklı dereceler geçerli olabilmektedir. Karşılaştırma yapmak gerekirse rasgele üretilen ve düzensiz olan kodlar düzenli kodlara göre çok daha iyi bir bit hata başarımı sunmaktadır. Düzensiz LDPC kodların kod uzunluğu yeterince uzun ise kanal kapasitesine daha fazla yaklaşılır.

LDPC kodlar, iyi bir başarım ve düşük kod çözme karmaşıklığı sunarlar. Bununla birlikte, pratik kullanımda gönderici tarafındaki kodlama işleminin karmaşıklığı LDPC kodları için bir dezavantaj olabilmektedir.

LDPC kodları, tasarım, kodlama ve kodçözme yöntemleri hakkında detaylı bilgi için [26]-[30]'a başvurulabilir.

CASCADE ve LDPC'de parite/eşlik bitleri/bilgisi alıcıya **bozulmasız** klasik kanaldan gönderilmektedir.

V. ANALIZLER

Bu çalışmada, CASCADE ve LDPC teknikleri için istemci-sunumcu tarzında uygulamalar hazırlanarak birbirine 100 Mbps Ethernet ağı ile bağlı iki farklı kişisel bilgisayar üzerinden simülasyonlar gerçekleştirilmiştir. Her iki teknikte de Alice sunumcu, Bob ise istemci olarak kabul edilmiştir. Benzetim ortamına ilişkin temel parametreler şu şekildedir:

- LDPC kodu olarak, D.J.C. MacKay'in "alist" formatında [25] verilen **273.82.3.353** H matrisi kullanılmıştır. Bu matris için minimum uzaklık değeri d_{min} = 10'dur. Dolayısıyla, 273 bitlik bir blok uzunluğu için teorik hata düzeltme kapasitesi yaklaşık %1.6 olmasına rağmen simulasyonlarda %4 hata oranına kadar da yüksek başarı gözlenmiştir.
- BSC kanalının çıkışındaki bozulmuş veriyi düzeltmek için LDPC kod çözme tekniği olarak mesaj aktarma algoritması (message passing algorithm) kullanılmıştır. Bu algoritma, Tanner grafındaki dallar boyunca bir düğümden diğer düğüme mesajlar aktaran bir kod çözme tekniğidir. Kanı yayılımı (belief propagation) algoritması ya da toplam–çarpım (sum–product) algoritması olarak da adlandırılmaktadır. Bu teknik hakkındaki detaylar için [23]'e başvurulabilir.
- CASCADE tekniğinde, çevrim 1 blok uzunluğu olan k_1 değeri BSC kanalın hata oranına göre

  $$k_1 = \text{mesaj_uzunluk} / \text{farklı_bit_sayısı}$$

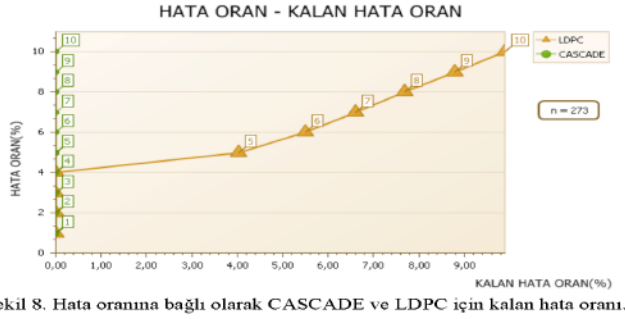
  uyarınca hesaplanmıştır. Örneğin, %10 hata varsa, 20 bitte 2 bitte hata vardır ve k_1 =20/2=10 elde edilir. Sonraki çevrimlerin blok uzunluğu ise

  $$k_i = 2 \cdot k_{i-1}, \quad 2 \le i \le 4$$

  formülü uyarınca hesaplanmıştır.

CASCADE ve LDPC teknikleri ile ilgili olarak aşağıdaki benzetimler gerçeklenmiştir:

- Hata düzeltme performans karşılaştırma (bkz. şekil 8),
- Sızdırılan bilgi (açıklanan parite) miktarı karşılaştırma (bkz. Tablo I),
- Hata Oranı-Toplam Süre karşılaştırması (bkz. şekil 9),
- Değişik hata oranları için gizli anahtar üretme hızı karşılaştırması (bkz. Tablo II).



Şekil 8. Hata oranına bağlı olarak CASCADE ve LDPC için kalan hata oranı.

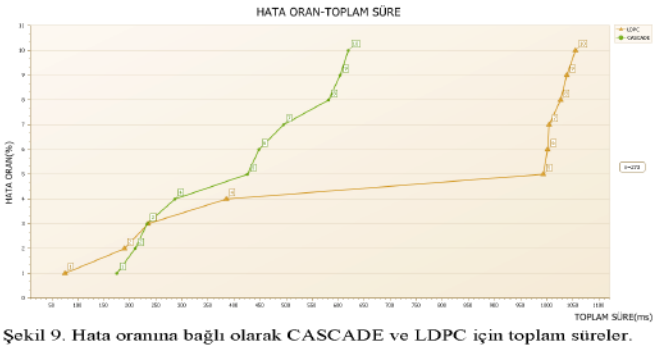
Şekil 8'de n = 273 bit uzunluklu diziler için başlangıç hata oranına göre düzeltme sonunda kalan hata oranları görülmektedir. %10'a kadar bit hata oranları verildiğinde CASCADE'in tüm hatalı bitleri başarıyla düzelttiği görülmüştür. Benzer şekilde, LDPC kodu da teorik olarak düzeltebileceği %1.6 hata oranının üzerinde yaklaşık %4'e kadar hatalı bitleri başarıyla düzeltmiştir. Bu oranlardan daha yüksek başlangıç değerlerinde ise hata bırakmıştır. Bu analiz için CASCADE protokolü 4 iterasyon, LDPC kodu ise ortalama 10 iterasyonda düzeltme işlemini sonlandırmıştır.

LDPC kodu hata düzeltirken ağı sadece bir kez kullanmakta

TABLO I
HATA ORANINA GÖRE AÇIKLANAN PARİTE MİKTARLARI

Hata oranı (%)	Bit uzunluk	CASCADE Açıklanan parite miktarı	LDPC Açıklanan parite miktarı
1	273	28	82
2	273	33	82
3	273	42	82
4	273	47	82
5	273	75	82
6	273	83	82
7	273	89	82
8	273	94	82
9	273	99	82
10	273	105	82

ve klasik kanaldan açıklanan parite miktarı kullanılan kodun özelliklerine bağlı sabit bir değer olmaktadır. Hata oranını arttırdıkça CASCADE'de daha fazla iletişim (parite alış-verişi) yapıldığından (bkz. Tablo I) ağ kullanım süresi ile birlikte açıklanan parite miktarı da artmaktadır.



Şekil 9. Hata oranına bağlı olarak CASCADE ve LDPC için toplam süreler.

Şekil 9, değişik hata oranlarına göre düzeltme işlemi için harcanan toplam süreleri göstermektedir. %3 hata oranına kadar LDPC kodu kullanmak süre avantajı sağlarken daha yüksek hata oranlarında CASCADE protokolü kullanmak daha avantajlı olmaktadır. LDPC için %4 hata oranından sonra toplam sürenin anormal artışı, kullandığımız LDPC kodunun hata düzeltme özelliğini kaybetmesinden ve toplam iterasyon sayısına ulaşıp hataları düzeltemeden sonlanmasından kaynaklanmaktadır.

Tablo II'de %4'e kadar olan hataların düzeltilmesi sonunda

TABLO II
HATA ORANINA GÖRE ANAHTAR ÜRETİM HIZI

	CASCADE		LDPC	
Hata oranı (%)	Başarı İhtimali (%)	Anahtar Üretim Hızı (bit/s)	Başarı İhtimali (%)	Anahtar Üretim Hızı (bit/s)
1	100	1400	100	2547
2	100	1143	100	1005
3	100	991	100	813
4	100	790	94	491

elde edilen gizli anahtarın üretim hızı verilmiştir. Düşük hata oranlarında LDPC kodunun CASCADE'e göre daha hızlı anahtar ürettiği rahatlıkla görülebilmektedir. Daha yüksek kapasiteli ve blok uzunluklu LDPC kodu kullanılırsa bu farkın çok daha fazla olacağı öngörülmektedir. Hata oranı kullanılan LDPC kodun kapasitesinin üzerine çıktığında anahtar üretme hızı dramatik bir şekilde düşmekte ve CASCADE çok daha avantajlı hale gelmektedir. Bütün bunların yanında CASCADE için Alice ile Bob arasındaki fiziksel mesafe uzadıkça ve ağ üzerinden parite paylaşımı gereksinimi arttıkça (yüksek hata oranlarında) anahtar üretim hızının o oranda düşeceği de göz önünde bulundurulması gerekmektedir.

VI. SONUÇ

KAD'da *bilgi uzlaştırma problemi* ya da *gizli anahtar uzlaştırma problemi* olarak da adlandırılan *hata düzeltme* problemine çözüm olarak sunulan iki önemli teknik CASCADE protokolü ile LDPC kodlarıdır. Benzetimlerden de görülebildiği üzere her iki tekniğin de başarılı olmalarının yanında avantajları ve dezavantajları bulunmaktadır:

- CASCADE protokolü çok iyi bir hata sezme ve düzeltme performansı sunmasına karşılık gönderici ile alıcı arasında çok fazla mesaj alış-verişi gerektirir. Bu kadar fazla iletişim hızlı ağlarda bir sorun yaratmıyor olsa da mesafe arttıkça gecikmenin artması (latency) ya da düşük bağlantı hızları dezavantaj olmaktadır.
- Üstün hata düzeltme performansları ile LDPC kodları, CASCADE tekniğine karşı çok iyi bir alternatif olarak görülmektedir. Özellikle düşük bağlantı hızlarında (veya uzun fiziksel mesafelerde) CASCADE protokolünün yerine tercih edilebilecek niteliktedir.

KAD'de bilgi uzlaştırma probleminin *güvenilir* ve *güvenli* bir çözümü için kullanılacak hata sezme ve düzeltme yöntemi:

- Bütün hataları düzeltebilmelidir. KAD protokolleri en fazla 15% hata oranları ile çalışabilmektedir.
- Gönderilen parite değerlerinin miktarı orjinal veriyi asla ele vermeyecek miktarda olmalıdır.

CASCADE protokolü ve LDPC kodları yukarıda verilen her iki şartı da başarıyla yerine getirmektedir.

Çalışmamızın bu konularla ilgilenen araştırmacılar için iyi bir başlangıç olmasını ümit ediyoruz.

KAYNAKLAR

[1] B. Schneier, *Applied Cryptography: Protocols, Algorithms and Source Code in C, 2nd Edition*. John Wiley & Sons, Inc, 1996, ch. 1.
[2] R. Thomas, 2002, "Safety in numbers", +plus magazine, Issue 21, Link: http://plus.maths.org/content/safety-numbers. Erişim: Ocak 2012.
[3] P. W. Shor, 1994, "Algoritms for quantum computation: discrete logarithms and factoring", Proceedings of the 35th Symposium on Foundations of Computer Science, Los Alamitos, edited by Shafi Goldwasser (IEEE Computer Society Press), 124-134.
[4] W. Trappe, L. C. Washington, *Introduction to Cryptography with Coding Theory*, Prentice-Hall, Inc. 2002.
[5] N. Gisin, G. Ribordy, W. Tittel, H. Zbinden, 2002, "Quantum Cryptography", 57 pages, 32 figures, submitted to Reviews of Modern Physics, quant-ph/0101098. DOI: 10.1103/RevModPhys.74.145.
[6] V. Scarani, H. Bechmann-Pasquinucci, N. J. Cerf, M. Dusek, N. Lutkenhaus, M. Peev, 2009, "The Security of Practical Quantum Key Distribution", 50 pages, 9 figures, submitted to Reviews of Modern Physics, arXiv:0802.4155. DOI: 10.1103/RevModPhys.81.1301.
[7] C. H. Bennet, G. Brassard, "Quantum Cryptography: Public Key Distribution and Coin Tossing", Proc. Int'l Conf. Computers, Systems & Signal Processing, CS Press, 1984, pp. 175–179.
[8] D. Stebila, M. Mosca, N. Lütkenhaus, "The Case for Quantum Key Distribution", Lecture Notes of the Institute for Computer Sciences, Social Informatics and Telecommunications Engineering, volume 36, page 283--296. Springer, 2010. DOI: 10.1007/978-3-642-11731-2_35.
[9] C. Kollmitzer, M. Pivk, *Applied Quantum Cryptography*, Lect. Notes Phys. 797 (Springer-Verlag, Berlin Heidelberg 2010).
[10] M. A. Nielsen, I. L. Chuang, *Quantum Computation and Quantum Information*, Cambridge University Press, 2000.
[11] C. P. Williams, S. H. Clearwater, *Explorations in QUANTUM COMPUTING*, Springer-Verlag NewYork, Inc. TELOS,1998.
[12] M. Toyran, "Kuantum Kriptografi, Benzetimi ve Analizleri", 15. İstatistik Araştırma Sempozyumu (İAS'2006), 2006.
[13] M. Toyran, T. B. Pedersen, A. S. A. Hasekioğlu, M. A. Can, S. Berber, "Bilgi Güvenliğinde Kuantum Teknikler", IV. Ağ ve Bilgi Güvenliği Sempozyumu, 25-26 Kasım 2011, sh. 98-107.
[14] Kuantum kriptografi, http://tr.wikipedia.org/wiki/Kuantum_kriptografi, Vikipedi, özgür ansiklopedi, Erişim: Ocak 2012.
[15] P. W. Shor, J. Preskill, "Simple Proof of Security of the BB84 Quantum Key Distribution Protocol", Phys. Rev. Lett., vol. 85, July. 2000, pp. 441-444, doi:10.1103/PhysRevLett.85.441.
[16] R. Renner, N. Gisin, and B. Kraus, "Information-theoretic security proof for quantum-key-distribution protocols", Phys. Rev. A, vol. 72, July. 2005, p. 012332, doi: 10.1103/PhysRevA.72.012332.
[17] Search or Article-id: "quantum cryptography", http://arxiv.org/.
[18] Binary symmetric channel, Wikipedia, the free encyclopedia, http://en.wikipedia.org/wiki/Binary_symmetric_channel.
[19] E. Afacan, *Analog ve Sayısal İletişim Teori ve Problemlerle*, Nobel Yayın Dağıtım Ltd. Şti., 2003.
[20] H. P. Hsu, *Analog and Digital Communications Schaum's Outlines*, McGraw-Hill, 1993.
[21] G. Brassard, L. Salvail, "Secret-key reconciliation by public discussion", EUROCRYPT, pp. 410–423 (1993).
[22] R. G. Gallager, "Low - Density Parity - Check Codes", IRE Trans. Inform. Theory, 1962.
[23] S. J. Johnson, "Introducing Low-Density Parity-Check Codes". http://materias.fi.uba.ar/6624/index_files/outline_archivos/SJohnsonLDPCintro.pdf. Erişim: Ocak 2012.
[24] alist format, David J. C. MacKay, Matthew Davey, and John Lafferty, http://www.inference.phy.cam.ac.uk/mackay/codes/alist.html.
[25] Encyclopedia of Sparse Graph Codes, David J. C. MacKay, http://www.inference.phy.cam.ac.uk/mackay/codes/data.html.
[26] R. G. Gallager, *Low-Density Parity-Check Codes*. Cambridge, MA:MIT Press, 1963.
[27] T. Richardson, R. Urbanke, *Modern Coding Theory*, Cambridge University Press, 2008.
[28] T. Mataracıoğlu, *Düşük Yoğunluklu Eşlik Denetim Kodları İçin Kodlayıcı Ve Kod Çözücü Tasarım Teknikleri*, Yüksek Lisans Tezi, İstanbul Teknik Üniversitesi Fen Bilimleri Enstitüsü, Haziran 2006.
[29] The Art of Error Correcting Coding, http://the-art-of-ecc.com/.
[30] LDPC Codes, http://sigpromu.org/ldpc/.

A True Random Number Generator and Test Platform Built in FPGA

Salih YILDIRIM and Cüneyt F. BAZLAMAÇCI

Abstract - **This paper demonstrates an implementation of an embedded true random number generator (TRNG) and its test platform on Xilinx Virtex–5 Field Programmable Gate Array (FPGA). The implemented TRNG uses only primitive resources of FPGA that are common for all kind of FPGAs. The randomness source of TRNG is jitter on ring oscillator clocks. Randomness is extracted from jitter with a self-failure detecting and sampling logic. The statistical quality of generated random bits is confirmed by NIST random number test suite (SP800-22), which runs on the embedded microprocessor of FPGA. The implemented TRNG produces random bits with a throughput up to 0.4 Mbps and it occupies only 25 slices of FPGA. This design shows us the possibility of generating and confirming true random bit sequences by using only the internal resources of FPGAs instead of using separate IC solutions.**

Index Terms - **FPGA, NIST Test Suite, TRNG, Ring Oscillators**

I. Introduction

Random numbers are essential necessity for cryptographic applications because various cryptographic processes use random numbers for functions such as key generation, authentication, padding, password generation, etc. The security of a cryptographic system depends on the true randomness of these numbers. Hence random numbers that are used in cryptographic systems should meet stringent requirements. These numbers should first be unpredictable (unbiased and independent) and irreproducible and also should have good statistical features.

Random numbers that have good statistical properties can be generated by deterministic processes. Such generators are called pseudo random number generators (PRNG). The PRNGs are implementations of deterministic polynomial time algorithms that expand a short seed value into uniformly distributed long bit sequences having good statistical features. The output of PRNG is not unpredictable because input ("seed") deterministically governs the output. Secondly PRNGs can generate a fixed number of bits so they repeat themselves in long sequences. Because of these obvious drawbacks of PRNGs, they are not suitable for cryptographic applications [9].

On the other hand, some generators use uncontrollable and unpredictable physical processes as source of randomness. This type of RNGs is called true random number generators (TRNG). The statistical properties and features of the generated random numbers by TRNGs are based on the randomness of the physical process and the extraction method employed. If the underlying physical process cannot be controlled, the generator output also becomes unpredictable and/or uncontrollable.

The digital devices are produced for implementing deterministic processes and any non-deterministic behavior can cause failures on these devices. On the other hand unpredictable and uncontrollable events due to underlying physical processes are unavoidable for such devices while device vendors aim to minimize them. These underlying physical processes and impurities in a deterministic system can provide a source of randomness for our case. In general, one can utilize three kinds of randomness in an FPGA. These are *i*) variation of logic gates, *ii*) transient behavior of logic gates between two states (meta-stability), and *iii*) thermal noise in FPGA [10].

There are several proposals in literature about true random number generation using FPGA resources. These methods differ from each other by the source of randomness and/or the extraction method that is employed. Some of these proposals are briefly reviewed in the following paragraphs.

The TRNGs proposed in [12] and [13] are based on sampling phase jitter in ring oscillators. A ring oscillator contains delay elements (logic gates) and an odd number of inverters in order to produce an oscillation. The jitter on a ring oscillator arises from the variation of the signal propagation delay in logic gates. The main principle in this method is sampling the outputs of a huge number of ring oscillators that are XORed together by D-FF and finally post processing this by a resilient function.

The true random number generation principle proposed in [14], [15] and [16] uses two ring oscillators with linear feedback that have been inspired from generalized LFSRs (Fibonacci and Galois LFSR) while using inverters instead of delay elements in the shift registers.

The method in [17] uses a chain of n delay elements (delay line). The delay of each delay element in the delay line has to be smaller than the standard deviation of the jitter of the clock signal. The clock signal is delayed linearly by a small amount in the each line element. The outputs of all delay elements are XORed to get one random bit per n bits.

Manuscript received March 1, 2012.

S. Yıldırım is with Aselsan, Inc., Yenimahalle, Ankara, TURKEY. (phone: 312-592-1586; fax: 312-354-1679; e-mail: sayildirim@aselsan.com.tr).

C.F. Bazlamaçcı is with Middle East Technical University, Ankara 06800 Turkey (e-mail: cuneytb@metu.edu.tr).

The basic principle behind the TRNGs in [18] and [19] is to extract the randomness by sampling reference clock jitter with a rationally related (clock) signal synthesized in the embedded analog PLLs.

The method proposed in [20] uses the write collisions in dual port block RAMs in FPGAs as an entropy source for true random number generation.

The true random number generation methods mentioned above have their own pros and cons. The TRNG in [1] extracts the randomness from the ring oscillator's clock jitter with self-failure detection and sampling logic. We preferred to implement [1] because the generator is suitable to be implemented in all FPGA families. It uses very few logic resources and it is expect that power consumption is relatively small.

Random numbers that are generated by a TRNG can be biased and can have bad statistical properties even if they are extracted correctly. Therefore post processing is needed in most TRNG outputs in order to get good statistical properties. This post processing brings the risk of being unaware of TRNG failure since post processing may hide the impurity of the outputs. Because of this risk TRNG tests should be run in real time and in a continuous manner for detecting any possible failure in the random number generator [3]. Embedded tests that run concurrently with TRNG are explained in FIPS-140-1 [11].

Besides such embedded tests, the evaluation of TRNG should also be done using statistical tests such as NIST SP800-22 [2] or Die Hard Test Suite.

The major contribution of our paper is implementing the TRNG and its statistical testing mechanism within the same FPGA with a very small footprint. The built-in testing mechanism enables testing of the statistical quality of the generated random numbers that are used by the cryptographic application running on the same FPGA chip. The generation, testing and use of true random numbers all in the same chip overall enhance the security and reliability of a cryptographic application.

In this paper, we present the implementation details of a TRNG and its associated testing mechanism, which uses only available FPGA sources. The rest of the paper is organized as follows: In section 2 we explain the details of our TRNG implementation, which is originally proposed in [1]. The associated test platform design, relevant statistical tests and the results obtained are all presented in section 3. Section 4 discusses possible improvements for the implemented system and in section 5 we conclude our paper.

II. TRUE RANDOM NUMBER GENERATOR DESIGN

This section presents the implementation details and discusses the engineering challenges encountered in implementing the true random number generator proposed in [1].

A. Overall System Design

The source of randomness in our TRNG implementation is the ring oscillator's clock jitter. As the TRNG core, we construct two separate ring oscillators, one sampler and one controller logic. Block diagram of the overall TRNG system core is illustrated in Fig 1- Block diagram of TRNG core.

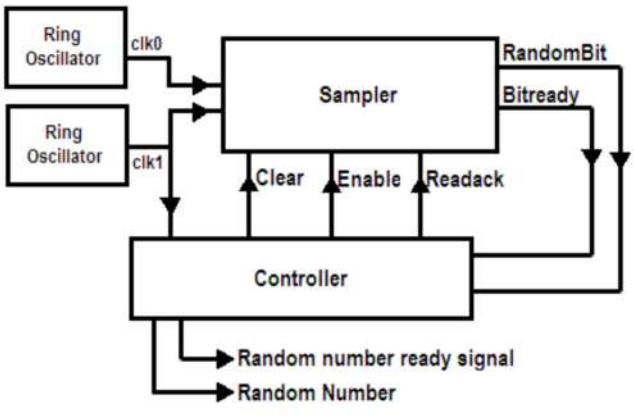


Fig 1- Block diagram of TRNG core

Two separate ring oscillators are implemented, which have close but non-identical oscillation frequencies. We use these two ring oscillators to supply streams of pulses to the sampler logic. The sampler logic extracts the random bit by the help of the controller and produces the *bitready* signal for every random bit. The controller module drives the sampler module to get true random bits. The controller also pushes these random bits into a 32 bit register and produces random number ready pulse for every new random number (one for every 32 pushes) composed of 32 bits. The operation and implementation details of each module are explained below. The whole TRNG system core has been implemented using only 25 slices of Xilinx Virtex-5 FPGA.

B. Ring Oscillators

The ring oscillator we have implemented on FPGA has three stages of delay elements and one inverter. Oscillating output of the inverter toggles a flip flop. The output of the flip flop is then used as the clock output of the ring oscillator. The VHDL implementation of the ring oscillator is not an ordinary VHDL code because the vendor's synthesizing tool or the mapper can prune the delay elements automatically. In order to prevent this, we construct the ring oscillator by using primitive entities[5] of Xilinx with "KEEP" attribute[4]. For every FPGA, a similar design technique can be applied. It is possible to place all components of the ring oscillator into a single slice of Virtex-5 FPGA. The schematic diagram of the ring oscillator is shown in Fig 2 – Ring oscillator.

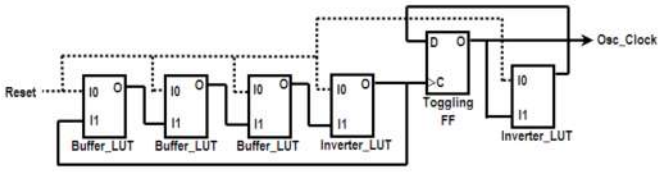


Fig 2 – Ring oscillator

The frequencies of the two ring oscillator instances used for TRNG directly determine the throughput of the TRNG. In order to get a high throughput, the ring oscillators' frequencies should be high enough. The frequency of the ring oscillator is proportional to the number of delay elements used in the ring oscillator [1]. The equation for the nominal frequency (f) of the ring oscillator is

$$f = \frac{1}{2\sum_{i=1}^{k} p^i}$$

where k is the number of delay elements and p is the time delay of each delay element.

The entropy of the ring oscillator's clock jitter is also related to the number of delay elements of the ring oscillator. Considering these relations and multiple experiments conducted, we use three delay elements and one inverter for the construction of the ring oscillator. This configuration of one ring oscillator fits into a single slice of Virtex-5.

The frequencies of two ring oscillators can't be made exactly the same. For our purpose they should be close but not identical. This can be achieved by placing each oscillator into individual but close slices. The frequencies of our ring oscillators are around 195 MHz as shown in Fig 3 – Ring Oscillator's clock scheme.

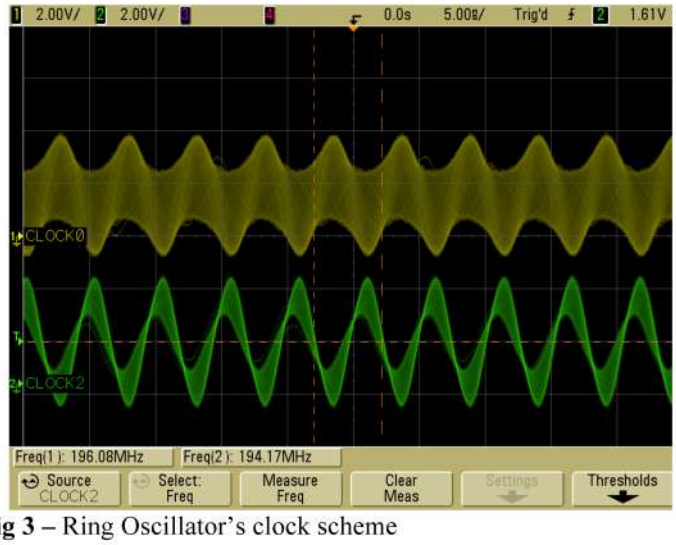


Fig 3 – Ring Oscillator's clock scheme

C. Sampler

The sampler circuit extracts a single random bit from the jitter noise on the input ring oscillator clocks. The input clocks have close but non-identical frequencies. So if we sample one of them with the rising edge of the other one, the sampled output will have long sequences of 1s or 0s because of period drifting of the clocks. The count of cycles that the sampled output is not changing will be random because of jitter on the ring oscillator clocks. The sampler circuit counts the number of cycles that the sampler flip-flop output is not changing using a counter (single flip flop). The output of the counter flip flop has a random bit for each state change (rising edge) of the sampling flip flop's output. The schematic logic diagram of the sampler is shown in Fig 4 – Sampler logic diagram.

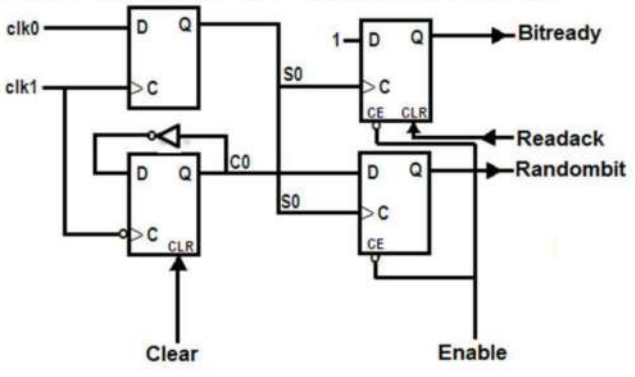


Fig 4 – Sampler logic diagram

Reset input of sampler clears the one bit counter. For each bit generation, this counter should be cleared in order to eliminate the correlation between successive bits.

The enable input of the sampler circuit is then used to keep the random bit unchanged after the first rising edge of the S0 signal. After each rising or falling edge of the S0 signal, S0 signal has many state changes with short cycles because of jitter noise. So after the first rising edge of S0, enable signal drops to low. The controller circuit then keeps the enable signal low for a predetermined period in order to wait for S0 signal to settle up.

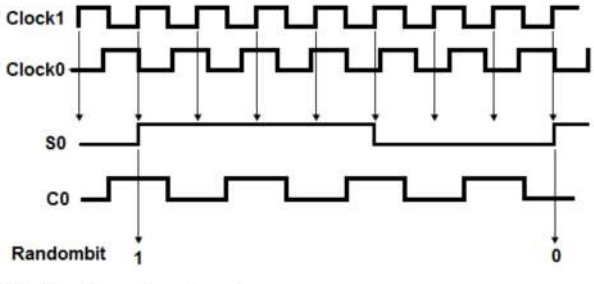


Fig 5 – Sampler signals

For every rising edge of the S0 signal *bitready* flip flop goes high. After *bitready* gets high, the controller circuit disables the *bitready* and *randombit* flip flops as shown in Fig 5 – Sampler signals. Then the controller samples the *randombit* and clears the *bitready* flip flop. Then the controller waits S0 signal to settle up for re-enabling the sampler.

D. Controller

The controller circuit of the TRNG drives the sampler circuit in order to have a correct operation for every random bit. The controller manages enabling or disabling of the sampler and clears the counter flip flop for each run. In order to generate a single random bit, the controller enables the sampler and waits for *bitready* signal. As soon as *bitready* signal gets high, it disables the sampler and then reads the random bit. After reading the random bit, controller waits for a predetermined amount of time in order to give some time to S0 signal to settle up, then it enables the sampler for the next random bit. Meanwhile the controller uses XOR corrector in order to

prevent the bias on the output. It pushes the output of the XOR corrector into a 32 bit register and produces ready signal for every new random 32 bit number. XOR corrector halves the throughput of the generator but increases its statistical properties.

III. TEST PLATFORM OF TRNG

The output of the implemented TRNG has to be confirmed by statistical tests. Most of the statistical tests are infeasible and difficult to implement using VHDL. Hence we designed an embedded test platform that provides an environment to run the test codes while our TRNG is producing the outputs. The schematic block diagram of our test platform is shown in Fig 6 – Block diagram of the test platform. Details of its implementation and operation of each module are explained in this section.

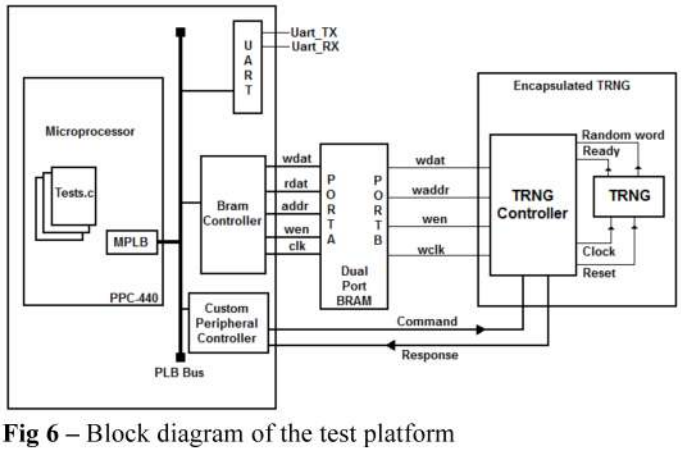


Fig 6 – Block diagram of the test platform

A. Test Platform Design

The test platform is basically composed of a microprocessor that one can run the test codes on, a dual port block RAM and the encapsulated TRNG and all modules are embedded in the same FPGA. In our design we used the embedded Power PC (PPC) of Virtex-5 as the microprocessor. This microprocessor communicates with the peripheral devices through peripheral local bus (PLB). Using the software part of this system one can read/write from/to RAM by using BRAM controller. And we can also send commands and read responses from the encapsulated TRNG by using our custom peripheral controller.

The user interface of the test platform is the HyperTerminal console of any personnel computer (PC) that is connected to the FPGA board via RS232 port. When the microprocessor boots up, it waits a command from UART in order to send the start command to TRNG. After sending start command, TRNG starts to generate the random numbers and writes them to the shared BRAM. As soon as it completes number generation, it sends a ready command to PPC through custom peripheral controller. After TRNG finishes its job, one can read all random numbers that are written into shared BRAM area by the software of the system. We integrated the source code of all NIST test suite into the embedded software project of the test platform. The original test suite code gets random numbers from a file system and writes the results of the tests to a file. But in our case the test code reads the random number from shared BRAM and writes the results back to UART. By using our test platform, we can test the statistical characteristics of random numbers that are generated by our embedded TRNG on FPGA.

B. Encapsulation of TRNG

Our TRNG core generates random bits and packs them into a 32 bit register with every clock input. For every new 32-bit random number, it generates a ready signal in order to inform the higher layer driver modules. On the other hand, encapsulated TRNG employs a TRNG core, which generates random numbers after the start command arrives. After start, the TRNG controller allows TRNG core to generate the required number of random numbers by providing clock and then releasing the reset input of TRNG. The controller keeps the TRNG core on reset if it is not needed for generating random numbers. While TRNG core is generating random numbers the controller writes these numbers to the shared BRAM starting with the starting first field of the BRAM. Whenever the required amount of random numbers is written to the BRAM area, the controller sends ready command to microprocessor.

C. NIST Test suite

The Information Technology Laboratory (ITL) is a major research component of the National Institute of Standards and Technology (NIST) of the Technology Administration, U.S. Department of Commerce. ITL develops tests and measurement methods, reference data and technical analysis that help to advance the development and to use new information technology [7]. ITL published a statistical test suite for random and pseudorandom number generators for cryptographic applications with the name NIST SP800-22. This publication provides some recommended statistical tests. These tests may be useful as a first step in determining whether or not a generator is suitable for a particular cryptographic application. NIST believes that these procedures are useful in detecting deviations of a binary sequence from randomness. However, a tester should note that apparent deviations from randomness may be due to either a poorly designed generator or to anomalies that appear in the binary sequence that is tested (i.e., a certain number of failures is expected in random sequences produced by a particular generator). It is up to the tester to determine the correct interpretation of the test results.

D. Test Results

Randomness is a probabilistic property. So the judgment of being random or not can be described in probabilistic terms. The statistical tests that are included in NIST test suite give probabilistic results of randomness. NIST test suite includes fifteen different statistical tests that are listed below.

1. The Frequency (Monobit) Test,
2. Frequency Test within a Block,
3. The Runs Test,
4. Tests for the Longest-Run-of-Ones in a Block,
5. The Binary Matrix Rank Test,
6. The Discrete Fourier Transform (Spectral) Test,

7. The Non-overlapping Template Matching Test,
8. The Overlapping Template Matching Test,
9. Maurer's "Universal Statistical" Test,
10. The Linear Complexity Test,
11. The Serial Test,
12. The Approximate Entropy Test,
13. The Cumulative Sums (Cusums) Test,
14. The Random Excursions Test, and
15. The Random Excursions Variant Test.

The test suite produces a p-value for each test. The p-value is the probability that a perfect random number generator would have produced a sequence less random than the sequence that was tested, given the kind of non-randomness assessed by the test. If a p-value for a test is determined to be equal to 1, then the sequence appears to have perfect randomness. A p-value of zero indicates that the sequence appears to be completely non-random.

When tested data is truly random, test results may conclude as being non-random with a small percentage. The probability of this kind of conclusion is called level of significance of the tests. The level of significance (α) of random number should be about 0.01 – 0.001 in cryptography. In order to decide whether the test is successful or not, p-value and the level of significance are used. If p-value is greater than or equal to the level of significance then the tested data is passed meaning that it is truly random.

The NIST test suite prepares a final analysis report for all tests that are run on the data set. This report includes results for the uniformity of p-values and the proportion of successful sequences.

Ten mega bits of random data that is generated by our TRNG is tested by our integrated NIST test suite with a level of significance of 0.01 and passed all test suites. The final analysis result for our test data is shown in Table 1 – NIST Test Suite Test Results.

Statistical Tests	Passing Rate	P-value
Frequency	10/10	0.911413
Block Frequency	9/10	0.739918
Cumulative Sums	10/10	0.350485
Cumulative Sums	10/10	0.739918
Runs	10/10	0.122325
Longest Run	10/10	0.534146
Rank	10/10	0.739918
FFT	10/10	0.534146
Non-overlapping Template	10/10	0.911413
Overlapping Template	10/10	0.534146
Approximate Entropy	10/10	0.739918
Serial	9/10	0.066882
Serial	10/10	0.534146
Linear Complexity	10/10	0.99146

Table 1 – NIST Test Suite Test Results

IV. FUTURE WORK

Other random number generation methods found in the literature should be implemented and tested with the same platform in order to compare those with the already implemented one.

The tests that are explained in FIPS-140-1 can be implemented in VHDL as a hardware testing core. We can increase the security of TRNG by using this hard testing core in order to detect any failure or attack on the TRNG[3]. We can also create alarm conditions for any impurity of the true number generator output before post processing.

We can run the test codes of other test suites such as diehard battery of tests or test of BSI (Bundesamt für Sicherheit in der Informationstechnik) on the microprocessor.

V. CONCLUSION

This paper explains the details and challenges of implementing and testing a TRNG by using only FPGA resources. Considering the prevalence of FPGAs in cryptographic systems, a TRNG built in FPGA may improve the security and quality of the system. The footprint of the implemented TRNG is negligible even for a low volume FPGA. The throughput of the implemented TRNG for a single core is 0.4Mbits/s. This throughput can be sufficient for many cryptographic applications and can also be upgraded by employing more TRNG cores easily. Meanwhile using embedded TRNG in FPGA is more advantageous than using separate IC such as RPG100 [8] for true random number generation. This approach decreases vendor dependency and cost of the complete design. Besides, security of the whole system also increases with embedded TRNG against external attacks.

REFERENCES

[1] P. Kohlbrenner and K. Gaj, "An embedded true random number generator for FPGAs," in Proc. of the ACM/SIGDA 12th Int. Symp. on Field Programmable Gate Arrays (FPGA 2004), ser. ACM, R. Tessier and H. Schmit, Eds. Monterey, California, USA, 2004, pp. 71-78.

[2] A. Rukhin, J. Soto, J. Nechvatal, M. Smid, E. Barker, S. Leigh, M. Levenson, M. Vangel, D. Banks, A. Heckert, J. Dray, S. Vo, A Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications, NIST Special Publication SP800-22 rev 1a. (Revised: April 2010)

[3] M. Varchola and M. Drutarovsky, "Embedded platform for automatic testing and optimizing of FPGA based cryptographic true random number generators" Radioengineering, Vol. 18, No. 4, 2009, pp.2-3.

[4] Xilinx Virtex – 5 User guide
\ www.xilinx.com/support/documentation/user_guides/ug190.pdf

[5] Xilinx Virtex-5 Libraries Guide for Schematic Designs
\http://www.xilinx.com/support/documentation/sw_manuals/xilinx12_4/virtex5_scm.pdf

[6] NIST. Federal Information Processing Standards Publication 140-2 – Security Requirements for Cryptographic Modules, March 2002. Online. http://csrc.nist.gov/publications/fips/fips140-2/fips1402.pdf.

[7] A Statistical Test Suite For Random And Pseudorandom Number Generators For Cryptographic Applications - ITL Security Bulletin http://csrc.nist.gov/publications/nistbul/12-00.pdf

[8] FDK corporation / True Random Number Generator (TRNG) RPG100 / http://www.fdk.com/cyber-e/pdf/HM-RAE106.pdf

[9] C.K. Koc and B. Sunar, Cryptographic Engineering Book, Chapter 4 - True Random Number Generator for Cryptography,

[10] B. Sunar and D. Schellekens, Secure Integrated Circuits and Systems Book, Chapter 6 - Random Number Generators for Integrated Circuits and FPGAs.

[11] Federal Information Processing Standard 140-1. Online http://csrc.nist.gov/publications/fips/fips1401.htm

[12] D. Schellekens, B. Preneel, and I. Verbauwhede. FPGA vendor agnostic true random number generator. Proc. 16th Int. Conf. Field Programmable Logic and Applications-FPL, 2006.

[13] B. Sunar, W.J. Martin, and D.R. Stinson. A Provably Secure True Random Number Generator with Built-In Tolerance to Active Attacks. IEEE TRANSACTIONS ON COMPUTERS, pages 109–119, 2007.
[14] J.D. Golic. New Methods for Digital Generation and Postprocessing of Random Data. IEEE TRANSACTIONS ON COMPUTERS, pages 1217–1229, 2006.
[15] J.D. Golic. New paradigms for digital generation and post-processing of random data. Technical report, Cryptology ePrint Archive, Report 2004/254, 2004.Online. Available: http://eprint.iacr.org/2004/254.ps, 2004.
[16] M. Dichtl and J.D. Golic. High-Speed True Random Number Generation with Logic Gates Only. In Cryptographic Hardware and Embedded Systems - CHES 2007, volume 4727 of LNCS, pages 45–61. Vienna, Austria, Springer Verlag, 2007.
[17] J.-L. Danger, S. Guilley, and P. Hoogvorts, "High speed true random number generator based on loop structures in FPGAs," Microelectronics Journal. Microelectronics Journal Volume 40, Issue 11, November 2009, Pages 1650–1656.
[18] V. Fischer, M. Drutarovsky, M. Simka, and N. Bochard. High performance True Random Number Generator in Altera Stratix FPLDs. Lecture notes in computer science, FPL'04, pages 555–564, 2004.
[19] V. Fischer and M. Drutarovsky. True Random Number Generator Embedded in Reconfigurable Hardware. In Cryptographic Hardware and Embedded Systems - CHES 2002, volume 2523 of LNCS, pages 415–430. Redwood Shores, CA, USA, Springer Verlag, 2002.
[20] Tamas Györfi, Octavian Cret, Alin Suciu. High performance true random number generator based on FPGA block RAMs. IEEE International Symposium on 23-29 May 2009
[21] Güneysu, T. True Random Number Generation in Block Memories of Reconfigurable Devices. Field-Programmable Technology (FPT), 2010 International Conference on 8-10 Dec. 2010

Quantum Random Number Generators

Muhammet Ali Can, Fikret Hacızade, Atilla Hasekioğlu, Thomas Pedersen, and Mustafa Toyran
TÜBİTAK, BİLGEM

***Abstract*—The aim of this position paper is to argue that quantum random number generators are the appropriate choice for critical cryptographic systems. We also discuss some important issues in the design of quantum random number generators.**

***Index Terms*—Quantum cryptography, random number generators, random extractors**

I. Introduction

The ability to make random choices is fundamental in many fields of science and engineering. In cryptography, random bits are used to create cryptographic keys and nonces. In some numerical methods, such as Monte-Carlo algorithms, randomness is used. In simulation, random numbers are used to imitate stochastic processes from the simulated system. In this paper we give a brief overview of some of the techniques used to create and extract randomness.

Random number generators are divided into three categories: pseudo-random number generators (PRNGs), "true" random number generators (TRNGs), and quantum random number generators (QRNGs). PRNGs are deterministic processes whose output is difficult to predict. Strictly speaking it is thus wrong to say that they generate random numbers. However, in many applications using unpredictable numbers suffice. In contrast, TRNGs extract randomness from unpredictable noise of a physical system (stochastic processes). QRNGs are special cases of TRNGs where the source of randomness is intrinsic randomness from a quantum system. Whereas noise can, at least in principle, be predicted or estimated, quantum randomness is intrinsic, and can never be predicted. In this paper, we will always use TRNG to denote hardware random number generators based on noise sources. In Section II, we discuss some details about commonly used sources of randomness, and give a brief discussion of some of the drawbacks and benefits of each. In Section III, we go into more details with different approaches to create randomness from quantum phenomena, which, as we argue, provides the most suitable random number generators for critical security systems, and in Section VI we compare some of the state-of-the-art techniques from all three categories of random number generators.

The typical requirements of a random number generator is that the output be independent and uniformly distributed bits. However, when using a physical system as the source of randomness, the generated randomness may not be uniform. The well-studied field of *randomness extractors*[1] addresses this issues. The task of randomness extractors, first explicitly defined by Nisan and Zuckerman in [18], is to extract independent uniformly distributed bits from an imperfect (non-uniform, low entropy) source of randomness. Randomness extractors are commonly used in "true" and quantum random number generators, where the source of randomness may not always be uniform. We give a brief overview of randomness extraction in Section IV.

When using a random number generator in a critical security system, where unpredictability of the generated number is essential, it is also important to consider the robustness of the generator against attacks. The simplest form of attack is to attempt to predict the future output of the generator by observing past outputs. This is particularly effective against PRNGs, where future output only depend on the current internal state (which is correlated with past outputs). For "true" and quantum random number generators another concern is the tamper resistance of the generator. If not designed properly, the output of these generators can be affected by external manipulation such as heat, power surges, or radiation.

II. Sources of Randomness

A. Pseudo RNG

PRNGs are *deterministic* algorithms which produce a sequence of bits which are, in practice, hard to predict when given only a limited number of previously generated bits.

PRNGs consist of an internal state and a (deterministic) generator function which maps the internal state to a short (typically 32 or 64 bits) sequence of random looking bits, and a new state. Initially the internal state is set to a, supposedly, random value — the so called *seed* of the generator. By successively applying the generator function, an arbitrarily long sequence of bits can then be generated. Since the internal state has a finite size, it is clear that any PRNG will, after some time, repeat itself. The number of bits which are generated before the generator returns to its original internal state is called the *period* of the generator.

The output of a good PRNG will have a lot of the same statistical properties as a sequence of bits chosen independently at random. As a minimum, the frequency of zero and one must be close to 1/2. Standardized tests (such as [6], [16], [4]) are commonly used to verify bit-frequency and many other statistical properties which let us believe that the sequence shares as many statistical features as possible with a uniformly distributed sequence of bits. However, it is important to remember that any PRNG generates a *deterministic* sequence of bits. Anyone who learns the internal state of a PRNG can predict any future output of that generator.

The major advantages of PRNGs is that they can be implemented in software, and that the bit generation rate is very high.

[1] In some papers the term noise widening is used synonymously to random extractor.

B. True RNG

TRNGs avoid the main problems of PRNGs: the finite period and deterministic behavior. TRNGs extract randomness from a source of noise. The noise source is some physical phenomena which is hard to predict, such as thermal noise.

TRNGs have some disadvantages. If the noise source is sampled faster than the noise frequency, the measurement outputs, and thus the random bits, will be correlated. TRNGs are, therefore, typically limited in speed.

Strictly speaking, TRNGs cannot be said to be truly random. We can mainly divide TRNGs into two categories, depending on the source of noise they use: Generators using thermal noise, and generators using chaotic systems. The "randomness" of chaotic systems comes from the impracticality of determining the exact state of the system. Any error in estimating the state of a chaotic system will make it difficult to predict the evolution of that system. Even thermal noise is, at least in principle, deterministic. The "randomness" in thermal noise comes from the statistical approximation of a large, complicated, but essentially deterministic, physical system. Even though TRNGs are not random in the real sense, it is, however, very unlikely that anyone can predict a well-designed TRNG. It is a matter of choice whether one will accept TRNGs as providing sufficiently trustworthy randomness.

The noise source used in a TRNG may not produce uniformly distributed bits, and may, indeed, have a bias. The bias may even change over time depending on influences from the surrounding environment, such as applied voltage, temperature, and radiation. To prevent this bias from influencing the quality of the output, a random extraction algorithm is applied. The random extraction algorithm takes a number of "low-quality" random bits as input, and produces a smaller amount of "good-quality" random bits as output.

C. Quantum RNG

Quantum mechanics states that some physical phenomena are intrinsically random. There is no way — even in principle — to predict, for instance, the exact decaying time of a radioactive nuclei. Furthermore, these phenomena are not sensitive to changes in the environment. This makes quantum randomness ideal for random number generation.

A typical example of a QRNG can be seen in Fig. 1. A source of laser light (LD) emits photons, which are shot at a semi-transparent mirror (BS). A photon which is reflected by the mirror will be detected by a single-photon detector (The APD labeled 0), while a photon which is transmitted through the mirror will be detected by the other detector (The APD labeled 1). Whether a photon is reflected or transmitted is, by the laws of quantum mechanics, a random process — it can never be predicted. The probability of reflection, p, is not very sensitive to changes in the environment, so if the digital logic (DL) of the generator outputs 0 when one detector detects a photon, and 1 when the other detector detects a photon we are guaranteed that the result is a Bernoulli process with parameter p (under the assumption that the detectors are perfect).

Just as for TRNGs, QRNGs will need a random extractor to generate uniformly distributed bits from the output distribution of the process (Bernoulli in the above example).

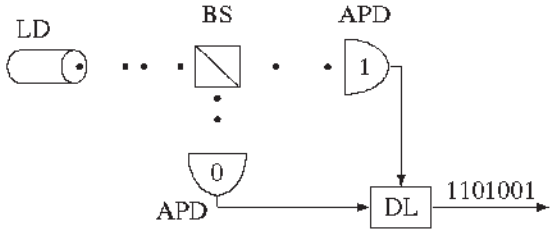


Fig. 1. A simple quantum random number generator

While the underlying randomness is unquestionable in QRNGs, the detection system is subject to influences from noise from the environment. However, where TRNGs uniquely rely on thermal and other sources of noise, QRNGs can be designed to avoid noise as much as possible.

III. Quantum Random Number Generators

A great advantage of basing random number generation on quantum mechanics is that quantum mechanics is intrinsically random. Quantum mechanics guarantees that the outcome of measurements of certain quantum mechanical phenomena are random by nature. No improved measurement apparatus or refined knowledge of the underlying physical system will allow an observer to predict the outcomes of the next measurement. This is in contrast to TRNGs which rely on noise arising from imperfect measurements and/or limited knowledge about the physical system.

One of the first methods proposed for QRNGs was based on radioactive decay. The main disadvantage of this system is that it is slow.

Most current QRNGs are based on the quantum behavior of photons. There are basically two properties of photons which can be used to extract randomness: the uncertainty in the emission time of photons, and the uncertainty in the location of a photon. Fig. 1 is an example of the latter, where the randomness comes from the uncertainty about whether the photon is transmitted or reflected by the semi-transparent mirror. The photon generation of a laser source is Poisson distributed — or, equivalently, the time between generation of two successive photons is exponentially distributed. This uncertainty of photon generation is commonly used in high-speed QRNGs.

The first widely available commercial QRNG was Quantis by ID Quantique[27]. Quantis is based on the principle described in Fig. 1, and has an output bit-rate of 4 Mbps. The Quantis generator also has a more cost-effective 16 Mbps version, where four QRNG components are placed on the same board.

One drawback of using location uncertainty as the source of randomness is that the spatial resolution is directly proportional to the number of detection elements used in the system. This limits the number of output bits per detection by a detection element, thus increasing the overall cost of the generator. When using uncertainty in time, on the other hand, the amount of randomness per detection is only limited by the accuracy and speed of the detection timing. Typically systems based in time uncertainty use only one detection element.

In [25] a QRNG based on the randomness of photon generation time is presented. The QRNG has an output rate of more than 110 Mbps. In order to extract more than one bit of randomness from each detected photon, time is split into equal-size buckets, and the number of the bucket (in binary) in which a photon arrives is used as random sample. The probability of a photon occurring in each bucket is made almost uniform by changing the applied voltage to the laser in such a way that the exponentially distributed generation times become almost uniform up to a certain time interval. A random extractor (SHA256) is applied to the random sample to improve the quality of the randomness.

Another QRNG based on generation time uncertainty is presented in [9]. As in [25], the authors propose a sampling method which guarantees almost uniform bits, thus avoiding any post-processing. Their prototype reaches an output rate of 50 Mbps, and is the basis of the commercial quRNG QRNG[28].

In both location and time based QRNGs single photon detectors are used. The speed of these detectors are the bottleneck for these systems. The commercially available APD single photon detectors typically have a time resolution in the order of tenths of nano seconds[12], [10].

A recent QRNG which is neither based on location nor time uncertainty is presented in [26]. The source of randomness in their proposal is the phase noise of laser light. A benefit of this approach is that phase noise is not measured by slow single photon detectors, but by fast continuous detectors. The speed of their system is limited by electrical noise induced in the detectors which becomes apparent when sampling the noise too fast. The raw output of their randomness source is 1 Gbps, however, due to inefficient randomness extraction, the final output rate of their prototype is 500 Mbps.

Even though the source of randomness in QRNGs is guaranteed by quantum mechanics, any system build to harvest that randomness will be subject to noise which is non-quantum in nature. The number of photons generated per second depends, to some extend, on the voltage applied to the laser. And the efficiency by which a detector detects individual photons is affected by both voltage and heat. In a carefully designed system, however, it is possible to make the effects of noise very small.

To distinguish quantum randomness from noise, so called certifiable QRNGs have been proposed[19]. In quantum mechanics stochastic processes can show correlations which are not possible in classical (non-quantum) physics[3], [8]. This phenomena can be used to certify that a stochastic process is indeed quantum. This provides the user of the QRNG with a guarantee of the genuine randomness of the system.

IV. Randomness Extraction

In TRNGs and QRNGs we often have sources of randomness which are not uniformly distributed, but still have some amount of randomness. The process of turning this "low quality randomness" into "good quality randomness" is the topic of randomness extraction.

The first random extraction algorithm was proposed by von Neumann[24], and provides a good example: Suppose that we have a sequence of independent Bernoulli trials with identical parameter p. To turn this into a sequence of independent uniform bits, we can pair the input bits and output 0 if the input is 01, and 1 if the input is 10. If the input is either 00 or 11 we do not produce any output, but continue to the next input pair. Since the probability for the events 01 and 10 are both equal to $p(1-p)$ the output will be 0 and 1 with identical probability.

The problem with von Neumann's extractor is that the output sequence is less than half the size of the input sequence. Modern extractors perform much better than that.

It is easy to prove that the largest number of uniformly distributed bits that can be extracted from a stochastic variable, X, equals the min-entropy of X (See for instance [11]). The min-entropy of an n-bit binary random variable is defined as

$$H_\infty(X) = \min_{x \in \{0,1\}^n} -\log_2(\Pr[X = x]). \quad (1)$$

On the other hand, it has also be proven that *no deterministic extractor* can extract even one bit of uniform randomness from a stochastic variable of which only the min entropy is known[22]. Any randomness extractor must be randomized, which seems to defy the purpose. The good news is that the extractor can use a relatively small amount of uniform randomness to extract a large amount of uniform randomness from a stochastic variable with high min-entropy.

A random extractor is thus a function, $E : \{0,1\}^n \times \{0,1\}^d \rightarrow \{0,1\}^m$, which takes a sample from an n-bit stochastic variable, X, with min entropy at least k, and d uniformly random bits, such that the variational distance:

$$\|E(X, U_d) - U_m\| < \epsilon, \quad (2)$$

for an appropriately small ϵ, where U_m is the uniform distribution over d-bit strings[18]. We want m to be as large as possible, and d to be as small as possible.

An obvious problem with randomness extractors is to get the bits for the uniformly distributed seed. Fortunately, there are constructions which will convert an extractor, which uses uniform seed, into an extractor which uses another min-entropy source as seed. The only requirement is that the two weak randomness sources should be independent of each other[2]. While independence may be difficult to guarantee in practice, it provides a good heuristic method.

A common approach used in the literature of "true" and quantum random number generators for extracting randomness is to apply a cryptographic hash function to the output of the physical generator. Besides being overly complex, this approach has only recently been proven to guarantee that the output is uniformly random[7]. Much simpler and more efficient random extractors exists. Currently, the best random extractor for many scenarios is Trevisans extractor[23] which can extract almost $H_\infty(X)$ bits by using a random seed which is only poly-logarithmic in n. There are several surveys going into more depth with randomness extractors, such as [15], [17], [21].

One side-effect of using a randomness extractor, is that it becomes very difficult to find systematic errors in the hardware by applying statistical tests to the output of the random number generator. The randomness extractor effectively

masks systematic errors. A common way to overcome this problem used, for instance, in [25], [9] is to try to make the output of the randomness sampling as close to uniform as possible, and then apply statistical tests to the output of the randomness sampling. In those cases randomness extractors are either entirely omitted, or only used to make give extra robust. However, this approach may not always allow for the highest possible throughput: to maximize throughput one should maximize min-entropy per second generated by the source and not the number of bits close to uniform. It is important to realize that the output of the randomness sampling does not need to be close to uniform in order to be useful for a random generator.

V. Verifying Randomness

Any proposed random number generator must be tested to verify that the output looks random. There are a wide range of standardized tests available [16], [4], [6], etc. Essentially a randomness test is a function which takes n bits as input, and produces some (real) value as output. The test is said to be passed if the probability that n truly uniform random bits would give a value at least as extreme (deviating from the expected value by at least the same amount) is below a given threshold. See [16] for a more elaborate explanation of the design of randomness tests.

A very important point about randomness tests is that *no test can verify randomness*. The only thing a randomness can do is to reject the hypothesis that a sequence of bits comes from a uniformly random process. Passing a randomness tests gives no conclusion about the quality of the randomness. Randomness test should therefore only be used to detect problems with an RNG design. The tests cannot be used as a qualitative measure of "how random" the output of a generator is.

Randomness extraction, most often used by "true" and quantum random number generators, have the ability to make most binary sequences look random to a statistical test — in some sense they are, themselves, pseudo random number generators. This means that testing the final output of a TRNG or QRNG which applies a good randomness extractor is very unlikely to reveal problems with the generator. Instead of analyzing the final output of the generator, the output of the sampling method should be tested. If the sampling output is expected to be uniform, this is easy, and indeed this approach is used in many designs. However, in some designs the sampling method does not give uniform output. In these cases specialized tests needs to be performed.

VI. State-of-the-art Random Number Generators

The Mersenne twister PRNG[13] is one of the most popular PRNGs today, preferred for it's efficient implementation and very large period of $2^{19937} - 1$ bits. The Mersenne twister, however, is not considered secure for cryptographic usage, since the stream can be predicted after observing a small amount of output[13]. To amend this, a modified version of the Mersenne twister has been proposed[14]. In cryptography, however, a general construction introduced by Blum, Blum, and Shup[1] is often preferred. It has been proven impossible to distinguish the output of the BBS PRNG from a uniform distribution in polynomial time under the assumption that the quadratic residuosity problem is difficult.

TABLE I
List of some state-of-the-art random number generators.

	Generator	Throughput	Price
PRNG	Mersenne Twister	–	$0
	Blum Blum Shup	–	$0
TRNG	Protego SG100[20]	0.128 Mbps	$325
	Comscire R2000KU[5]	2 Mbps	$895
QRNG	Quantis[27]	4 Mbps	$1500
	QRBG121	12 Mbps	?
	quRNG[9]	50 Mbps	?

The Comscire R2000KU TRNG uses a combination of thermal and transistor noise to generate randomness at a rate of 2 Mbps.

We have already mentioned the state-of-the-art QRNGs in the previous section. Here it suffices to emphasize that during the last couple of years we have seen a surge in the speed of QRNGs.

Table I shows a few of the most widely available random number generators. We have not included the fastest QRNGs, since they are not commercially available yet. The PRNGs are freely available, so no cost is involved in their use. The throughput of PRNGs depends on the implementation and on the underlying hardware, so throughput is not listed. In general, though, PRNGs are much faster than both QRNGs and TRNGs.

VII. Conclusion

In this paper, we have presented evidence to support our claim that quantum random number generators should be the generator of choice for critical security systems. We have also pointed out some of the techniques that we believe are the most promising when creating QRNGs: We believe that QRNGs based on time uncertainty are likely to provide the most cost effective and fast systems. We have also pointed out the importance of choosing the appropriate randomness extraction method[2]. Finally, we gave a warning about some pitfalls when verifying true and quantum random number generators: Some researchers design the randomness sampling such that it passes the statistical tests, wheres the randomness sampling should aim at maximizing the min-entropy output per second. Secondly, we mentioned that passing a statistical test does *not* guarantee good randomness. Statistical tests can only be used to detect poor quality randomness.

References

[1] L. Blum, M. Blum, M. Shub, *A simple unpredictable pseudo random number generator*, In SIAM J. Comput., 15(2):364–383 May 1986.
[2] B. Barak, R. Impagliazzo, and A. Wigderson, *Extracting randomness using few independent sources*, In Proc. IEEE 45th Annu. IEEE Symp. Foundations of Computer Science (FOCS04), 2004, pp. 384–393.
[3] J. Bell, *On the Einstein Podolsky Rosen Paradox*, In Physics 1 (3):195–200, 1964.

[2]Currently we recommend using Trevisans extractor[23] for most cases.

[4] *Ais 20: Functionality classes and evaluation methodology for deterministic random number generators, v2.0, bsi*, https://www.bsi.bund.de/cae/servlet/contentblob/478150/publicationFile/30276/ais20 pdf, 1999.
[5] Comscire, http://comscire.com
[6] http://www.stat.fsu.edu/pub/diehard/
[7] Y. Dodis, R. Gennaro, J. Håstad, H. Krawczyk, and T. Rabin, *Randomness Extraction and Key Derivation Using the CBC, Cascade and HMAC Modes*, In Advances in Cryptology - CRYPTO 2004, 24th Annual International Cryptology Conference, 494–510, 2004.
[8] A. Einstein, B. Podolsky, N. Rosen, *Can Quantum-Mechanical Description of Physical Reality Be Considered Complete?*, Physical Review 47(10):777, 1935.
[9] M. Furst, H, Weier, S. Nauerth, D. G. Marangon, C. Kurtsiefer, and H. Weinfurter, *High speed optical quantum random number generation*, In Optics Express, 18(12), June 2010.
[10] Hamamatsu APDs: http://sales.hamamatsu.com/index.php?id=13166473
[11] J. Håstad, R. Impagliazzo, L. A. Levin, and M. Luby, *A Pseudorandom Generator from any One-way Function*, SIAM Journal on Computing, 28(4): 1364–1396, 1999.
[12] ID100 series of APDs from ID Quantique: http://www.idquantique.com/scientific-instrumentation/id100-silicon-apd-single-photon-detector.html
[13] M. Matsumoto and T. Nishimura, *Mersenne twister: a 623-dimensionally equidistributed uniform pseudo-random number generator*, In ACM Trans. Model. Comput. Simul., 8(1):3–30, January 1998.
[14] M. Matsumoto, T. Nishimura, M. Hagita, and M. Saito, *Cryptographic Mersenne Twister and Fubuki Stream/Block Cipher*, http://eprint.iacr.org/2005/165.
[15] N. Nisan, *Extracting randomness: How and why: A survey*, In Proceedings of the Eleventh Annual IEEE Conference on Computational Complexity, pages 44–58, Philadelphia, Pennsylvania, 24–27 May 1996. IEEE Computer Society Press.
[16] National Institute of Standards and Technology, *A Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications*, Available online: http://csrc.nist.gov/publications/nistpubs/800-22-rev1/SP800-22rev1.pdf, April 2009.
[17] N. Nisan and A. Ta-Shma, *Extracting randomness: A survey and new constructions*, JCSS: Journal of Computer and System Sciences, 58, 1999.
[18] N. Nisan and D. Zuckerman, *Randomness is linear in space*, in Journal of Computer and System Sciences, 52(1):43–52, February 1996.
[19] S. Pironio, A. Acín, S. Massar, A. Boyer De La Giroday, D. N. Matsukevich, P. Maunz, S. Olmschenk, D. Hayes, L. Luo, T. A. Manning, and C. Monroe, *Random numbers certified by Bell's theorem.*, In Nature, 464(7291):10, 2010.
[20] Protego, http://protego.se
[21] R. Shaltiel, *Recent developments in explicit constructions of extractors*, Bulletin of the EATCS 77:67–95, 2002.
[22] M. Santha and U. V. Vazirani, *Generating quasi-random sequences from semi-random sources*, Journal of Computer and System Sciences, 33:75–87, 1986.
[23] L. Trevisan, *Construction of extractors using pseudorandom generators.* In Proceedings of the 31st ACM Symposium on Theory of Computing, 1999.
[24] J. von Neumann, *Various techniques used in connection with random digits*, In Applied Math Series, 12:36–38, 1951.
[25] M. A. Wayne and P. G. Kwiat, *Low-bias high-speed quantum random number generator via shaped optical pulses*, In Optics Express, 18(8), 12 April 2010.
[26] B. Qi, Y-M. Chi, H-K. Lo, and L. Qian, *High-speed quantum random number generation by measuring phase noise of a single-mode laser*, In Optical letters, 35(3), February 2010.
[27] The Quantis QRNG by ID Quantique. More information available at http://www.idquantique.com/images/stories/PDF/quantis-random-generator/quantis-whitepaper.pdf.
[28] quRNG by quTools, http://www.qutools.com/products/quRNG/

On the Random Oracle Model and the Game Hopping Technique

Murat Ak, Turgut Hanoymak

Abstract—**In modern cryptography, provable security gained much attention because it provides theoretical evidence about the security of public key schemes. Provable security is achieved via a reduction technique which relates the security of a scheme to a mathematically hard problem. Typically, a reduction from a mathematically hard problem to the cryptographic scheme is given and it is argued that if there exists an adversary that can break the scheme, one may construct an algorithm solving the underlying hard problem using the adversary as a subroutine. There are several techniques used in such proofs two of which are random oracles and game hopping. In this paper, we discuss the random oracle model (ROM) which has been proposed as an alternative to the standard model. In ROM, basically, hash functions are modeled as random oracles, which is a hypothetical black box that gives truly random outputs to distinct inputs. We also discuss two major objections on the validity ROM and we point out that one of these objections is not indeed sound. Then we give the game hopping technique since sometimes security proofs in cryptography may be constructed as sequence of games. In particular, we give some concrete illustrations of public key encryption schemes and their security proofs that utilize random oracles and game hopping.**

Index Terms—**Provable Security, Public Key Encryption, Random Oracle Model, Game Hopping**

I. Introduction

SECURITY of the cryptographic schemes in the public key setting typically depends on the mathmatical problems that are believed to be hard to solve such as integer factorization and discrete logarithms.

Anyone who proposes a new public key encryption scheme must first take potantial security proofs into consideration because otherwise the resulting scheme becomes most probably vulnurable. Currently, there are two models for proving security :

- The standard model is the default security model which assumes nothing but well established mathmatically hard problems. However, the problem with this model is that the schemes which can be proven secure turns out to be inefficient. There exist schemes that are both secure and efficient such as [4]
- The random oracle model which was proposed by Bellare and Rogaway [3] is an alternative to the standard counterpart. In this model, hash functions are modeled as random oracles which are not actually possible in the real world however, due to this relaxation, one may construct more efficient schemes. As a matter of fact, random oracle proofs are not considered to be rigorous mathematical proofs and indeed it is shown that there exist schemes which can be proven in the random oracle model but completely insecure in real world such as [8]. Probably, this is why the use of ROM is objected by a number of cryptographers such as Menezes and Koblitz [1]. But this does not make ROM completely useless because at least it guarantees that there are no inherent design flaws and this is certainly better than providing no proof at all.

We stress that, it is still preferable to use a scheme secure in the standard model even if it is slightly less efficient as opposed to the random oracle counterpart.

Random oracle is a hypothetical "magic" box that is assumed to have the following two properties:

- It produces truly random outputs
- For each input it gives the same output

The objections on ROM comes from that fact that random oracles do not exist in the real world, and the simulator needs to see the queries of the adversary which is not so realistic. Also it is assumed that the simulator can set the output of the random oracle as it wishes. This is called *programmability* yet it is not realistic, neither.

One of the most popular techniques used in security proofs is game hopping. In this method, we construct different versions of the security game played between the adversary and the challenger. Typically, the first game is the original security game. And the last game is a game in which the adversary gains no information, theoretically. Finally, the basic argument of game hopping methods is that since the views of the adversary in successive versions of the game are indistinguishable, the success probability in the original attack game is related to the success probability in the last game which acts like a one-time pad, thus must be negligible due to transitivity.

In this paper, we will present the random oracle methodology in detail and give three example proofs. Then, we will present two proofs that use game hopping techniques.

II. Preliminaries and Notation

A. Reduction Proofs

Most of the security proofs in the literature are in the form of a reduction. Typically, a mathematically hard problem M is reduced to breaking the scheme S that is wanted to be proven secure. Existence of such a reduction implies that the problem of breaking the scheme S is as hard as M. This implication stems from the following contraction argument: If there exist a

M. Ak is with the Department Computer Engineering, Bilkent University, Ankara, 06800, Turkey. e-mail: muratak@cs.bilkent.edu.tr
T. Hanoymak is with the Institute of Applied Mathematics, Middle East Technical University, Ankara, 06531, Turkey. He is also affiliated with Yüzüncü Yıl University, Van, Turkey. e-mail: hturgut@metu.edu.tr

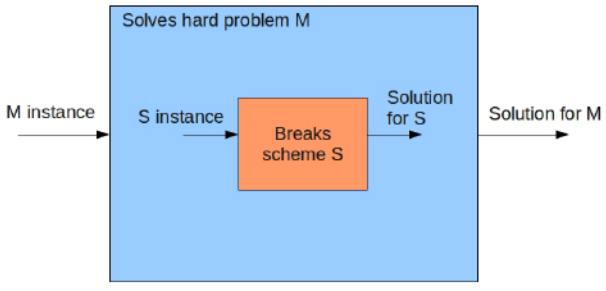


Fig. 1. The idea of reduction illustrated. Given an instance of M, one needs to form an instance of the scheme S and use the breaker to break S and this result is used to solve M instance.

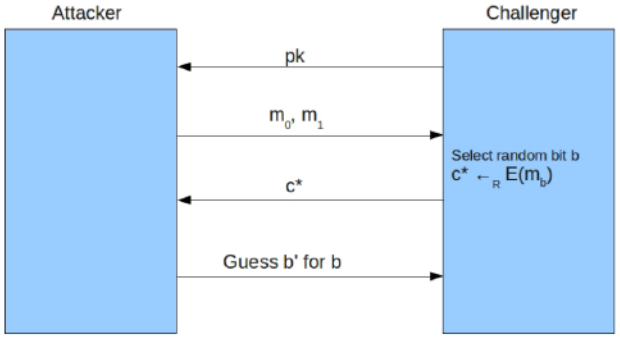


Fig. 2. The chosen plaintext attack (CPA) game is illustrated.

polynomial time algorithm A that breaks the scheme S, then due to this reduction, one may construct a polynomial time algorithm B which uses A as a subroutine to solve M which is assumed to be impossible. See Figure 1.

B. Security Models

When we talk about the security of a cryptographic scheme, we need to define the goal and the capabilities of the adversary. As the goal becomes more difficult or as the capabilities are more limited the security proof becomes easier. In the cryptography literature, several goals and capabilities are discussed so far. The most popular adversarial goal is to distinguish between the plaintext of a given ciphertext. When we prove that such an adversary cannot exist, this is called indistinguishability. Note that indistinguishability means that a ciphertext gives semantically no information about the plaintext. So, it is also called semantic security.

There are several possible capabilities of an attacker in the public key setting depending on the availability of the decryption oracle which is a hypothetical black box that is presented to the attacker so that it can make decryption queries of its own choice and gets the corresponding plaintexts. This captures the possible real life attacks that consist of attackers that has gained temporary access to the decryption oracle. In this respect, there are three types of decryption oracle access:

- CPA (Chosen plaintext attack): if there is no decryption oracle access at all, we call this a chosen plaintext attack.
- CCA1 (Non-adaptive chosen ciphertext attack, or lunchtime attack): adversary can access the decrpytion oracle until it sees the ciphertext it needs to break.
- CCA2 (Adaptive chosen ciphertext attack): adversary always has access to the decryption oracle but querying the ciphertext it needs to break is prohibited.

The most widely accepted level of security is CCA2 security. However, in CCA security proofs, there is a difficulty of providing decryption oracles. Because usually, the decryption key is not in the control of the simulator but it rather inherently depends on the instance of the hard problem. In this paper, we focus on CPA security, since it is enough to present the main idea of random oracle proofs and game hopping methods.

C. Semantic Security

The notion of semantic security captures the following: Even if the adversary chooses two messages m_0, m_1 and gets the ciphertext of one of them c^*, it cannot distinguish whether $c^* = E(m_0)$ or $c^* = E(m_1)$. This means that the ciphertext gives *no information* about the plaintext. Note that semantic security requires the encryption algorithm to be randomized. Otherwise, the adversary can always encrypt both the messages and check with the challenge ciphertext c^*.

In order to prove semantic security we consider a hypothetical game between an adversary and a challenger. There are three steps:

1) Adversary chooses two messages of its own choice and sends them to the challenger.
2) Challenger selects one of these messages randomly, encrypts it and sends back the ciphertext as the challenge.
3) In the final step, the adversary tries to guess the message that is used in the challenge.

These steps are also shown in Figure 2.

Then the success of the adversary is measured with its advantage in this game defined as $Pr[b' = b] - 1/2$.

D. Cryptographic Hardness Assumptions

In this section, we recall four popular hardness assumptions that the security proofs we will discuss later depend on. Namely, the RSA assumption, the discrete log assumption, and decisional and computational versions of the Diffie-Hellman assumption.

RSA assumption Let N be the product of two large primes p and q, and let e and d be two integers such that

$$ed = 1 \mod \phi(N)$$

Given N, e, y it is computationally hard to find an $x \in \mathbb{Z}_N^*$ such that $x^e = y \mod N$.

Discrete logarithm assumption Let $\mathbb{G}$ be a group of primer order q. Given a generator g and an element of $\mathbb{G}$, h, finding x such that $g^x = h$ is computationally hard.

Computational Diffie-Hellman assumption Let $\mathbb{G}$ be a group of primer order q. Given a generator g and two elements of $\mathbb{G}$, g^a, g^b, finding g^{ab} is computationally hard.

Decisional Diffie-Hellman assumption Let $\mathbb{G}$ be a group of primer order q. Given a generator g and three elements of $\mathbb{G}$, g^a, g^b, g^c, finding whether $ab = c \mod q$ is computationally hard. This assumption can also be represented in terms of

probabilities as follows: Let D be a polynomial time algorithm that is designed for deciding whether a three-tuple is a DDH tuple, and let

$$Pr[D(g^a, g^b, g^{ab}) = 1] - Pr[D(g^a, g^b, g^c) = 1]$$

where a, b, and c are selected randomly from $\mathbb{Z}_q$ is defined as the advantage of D in distinguishing a DDH tuple distribution from a random one. The DDH assumption assumes that this advantage is negligible.

III. Random Oracle Model and Security Proofs

As we mentioned previously, random oracle model is well accepted as a method for proving security of public key encryption schemes, because the schemes that can be proven in the standard model require more complex operations whereas, the use of hash functions is usually sufficient to obtain schemes that can be proven in the random oracle model. The core idea of the random oracle model is that we assume hash functions are truly random functions. In fact, it is tricky to use random oracle idea in a rigorous proof since hash functions are not truly random. In random oracle proofs, basically, the adversary claims to perform a successful attack even if the challenger simulates and provides a truly random function of its choice. This is indeed a very strong claim and it is not very surprising that an attack of this kind can be proven to be impossible. But, random oracle model still draws a good deal of attention because usually, efficient schemes can be proven secure only in this model. In the random oracle model proofs, hash functions are thought as random oracles and are provided for the attacker by the challenger (simulator) who has full control over this oracle. The main assumptions of the random oracle model are the following:

- When the attacker needs to use the hash function, it has to submit a query to the random oracle simulated by the challenger.
- The challenger can set the output of the random oracle query to any value of its choice which is called programmability.

In order to make this idea more clear, we now present different random oracle proofs from the literature.

A. CPA Secure RSA Encryption in the ROM

The first scheme we will discuss is an IND-CPA secure version of RSA based encryption scheme. The scheme is defined by the following three algorithms:

- **Setup**: Let N be an RSA number and e, d is an RSA key pair. Let $H : \mathbb{Z}_N^* \to \{0,1\}^\ell$ be a hash function.
- **Encrypt**(m): Given a message $m \in \{0,1\}^\ell$, a random $r \in \mathbb{Z}_N^*$ is chosen and m is encrypted as:

$$c = r^e \mod N, H(r) \oplus m$$

- **Decrypt**(c): Given a ciphertext $c = (c_1, c_2)$,

$$m = H(c_1^d) \oplus c_2$$

Theorem III.1 *If the RSA problem is hard, then the scheme above is IND-CPA secure in the random oracle model.*

Proof: The proof will proceed as follows: a reduction from breaking the scheme to solve the RSA problem is presented. Suppose there exists an adversarial algorithm A that can break the scheme. We will construct another algorithm B that solves the RSA problem using A as a subroutine. Algorithm B will simulate an attack game for the successful attacker A given. We construct B as follows:

Algorithm 1 $B(N, e, y)$

1: Choose $s \in_R \mathbb{Z}_N^*$. Consider $t = y^{1/e}$ which we do not actually know, and due to programmability, let $H(t) = s$.
2: Simulate IND-CPA game for A as follows:
3: Provide the public key (N, e) to A.
4: Maintain an initially empty table T for random oracle queries and set $t = \perp$.
5: Whenver A makes a random oracle query q:
6: Check whether $q^e = y$ if so, set $t = q$ return s.
7: Otherwise, randomly choose $H(q)$, save $(q, H(q))$ to table T and return $H(q)$ to A (provided that q is not queried before, in that case return the same value from the table).
8: A outputs two messages m_0, m_1.
9: Randomly select a bit b and give the challenge ciphertext $c = (c_1, c_2) = (y, s \oplus m_b)$
10: Whenever A makes a random oracle query q it proceeds same as Line 5.
11: After the game is over return t.

The core idea of the proof is as follows: If t is not queried, then $H(t)$ is considered to be truly random, hence, c_2 is like a one-time pad encryption. If it is queried, then t must be the answer we are looking for, i.e. the answer of the RSA problem. So we can argue that Algorithm B solves the RSA problem if A can break the scheme. This contradicts with the RSA assumption, so the scheme is IND-CPA secure. ■

B. Security of Hashed El Gamal under CDH Assumption

Now, we will look at a similar but slightly more complicated example random oracle proof. The reduction will be similar to that of the previous section but there will be a probabilistic argument. This time, the encryption scheme is as follows:

- **Setup**: Let g be a generator of some prime order group $\mathbb{G}$. Let x be the private key and $h = g^x$ be the public key. Let $H : \mathbb{G} \to \{0,1\}^\ell$ be a hash function.
- **Encrypt**(m): Given a message $m \in \{0,1\}^\ell$, a random $r \in \mathbb{G}$ is chosen and m is encrypted as:

$$c = (g^r,\ H(h^r) \oplus m)$$

- **Decrypt**(c): Given a ciphertext $c = (c_1, c_2)$,

$$m = H(c_1^x) \oplus c_2$$

Theorem III.2 *If the computational Diffie-Hellman (CDH) problem is hard, then the scheme above is IND-CPA secure in the random oracle model.*

Proof: In order to prove this theorem, a reduction from breaking the scheme to solve the CDH problem will be given.

Similar to the previous proof, we will assume that we have an adversarial algorithm A that can break the scheme above and construct another algorithm B that solves the CDH problem using A as a subroutine. Algorithm B will be similar to that of the previous proof except that we cannot check the queries whether they correspond directly to the answer of the CDH problem we are looking for. However, note that when we set the parameters g^a and g^r to the input of the CDH problem g^a and g^b respectively, if the attacker is successful in breaking the scheme this means that it must have queried the oracle with g^{ab} somewhere in its execution. So, one of the queries consists of the answer of the CDH problem. Because otherwise, the ciphertext part c_2 is like a one-time pad due to the truly randomness assumption of random oracles. Hence, at the end of the game simulation, algorihtm B selects one of the queries randomly and returns it as the output. The probability of this output to be correct is $(1/q)\epsilon$ where q is the number of queries performed, and ϵ is the success probability of the adversary. Since the number of queries is polynomially bounded, the probability is divided into polynomial factor which is still non-negligible. Hence, the scheme is IND-CPA secure. ■

Note that in the proof of the IND-CPA RSA scheme, the success probability is preserved since we can explicitly test whether a random oracle query is the one that consists of the answer of the RSA problem, but we cannot do the same check in the proof of IND-CPA El Gamal scheme, but fortunately returning one of the queries still works since it decreases the success probability only in polynomial factor.

C. Existentially Unforgeable RSA Signature Scheme

In this section we will present an example proof in the random oracle model for a signature scheme. First, let us consider the plain RSA signature scheme:

- **Setup**: Let N be an RSA number and (e, d) is an RSA key pair.
- **Sign**(m): Given a message $m \in \mathbb{Z}_N^*$, m is signed as: $s = m^d \mod N$.
- **Verify**(s): Given a signature (m, s), verification equation is: $m = s^e \mod N$.

Unfortunately, this is not considered as a secure signature scheme because one can forge a message-signature pair by simply choosing a signature s randomly and computing the corresponding message m as $s^e \mod N$

Indeed, the most widely accepted security definition for signature schemes is as follows:

Existential unforgeability: A signature scheme is existentially unforgeable under an adaptive chosen message attack if there exists no polynomial time algorithm that can output a valid message-signature pair given access to a signature oracle.

So, according to this definition, the scheme above is not existentially unforgeable. However, it is possible to construct a secure signature scheme that is a modified version of the basic RSA signature scheme using a hash function as follows:

- **Setup**: Let N be an RSA number and (e, d) is an RSA key pair. Let $H : \mathbb{Z}_N^* \to \{0,1\}^\ell$ be a hash function.
- **Sign**(m): Given a message $m \in \{0,1\}^\ell$, m is signed as: $$s = H(m)^d \mod N$$
- **Verify**(s): Given a signature (m, s), verification equation is: $$H(m) = s^e \mod N$$

Recall that for signature schemes, in a *no-message attack*, adversary needs to find a valid message-signature pair without having access to a signature oracle.

Theorem III.3 *If the RSA problem is hard then the modified RSA signature scheme above is existentially unforgeable under a no-message attack in the random oracle model.*

Proof: The proof proceeds similar to the proof of the RSA encryption scheme of Section III-A. We construct an algorithm B for solving the RSA problem assuming that we have an algorithm A that can forge a signature pair. Algorithm B is constructed as follows: Given an RSA problem instance (N, e, y), it gives A the public key (N, e). Whenever A makes random oracle queries, B responds with random values. Except that for a randomly selected query, it responds with y instead of a random value. So, when the simulation is over, and A outputs a forgery (m, s), B outputs s. Note that s is the correct answer of the RSA problem, i.e. $y = s^e \mod N$ with a probability $(1/q)\epsilon$ where q is the number of random oracle queries and ϵ is the success probability of algorithm A. Because A must have queried m to the random oracle since otherwise $H(m)$ remains truly random and s cannot be determined thus cannot be included in a forgery. So, since a polynomially many random oracle queries are allowed, and ϵ is assumed to be non-negligible, the success probability of algorithm B is also non-negligible which contradicts the RSA assumption. So the scheme is existentially unforgeable under a no-message attack in the random oracle model. ■

Now we will present the same scheme is indeed existentially unforgeable under an adaptive chosen message attack in the random oracle model.

Theorem III.4 *If the RSA problem is hard then the modified RSA signature scheme above is existentially unforgeable under an adaptive chosen message attack in the random oracle model.*

Proof: The proof proceeds same as the proof of the no-message case except that the adversary must be provided with a signature oracle. This signature oracle can be simulated by using the programmability feature of the random oracle. When the adversary A requests a signature on message m, B sets $H(m)$ to be $s^e \mod N$ for a randomly selected s and returns s to A. Note that here, B does not have to know d explicitly, and since it sets $H(m)$ it can respond to later random oracle queries consistently with the previous ones. Together with the previous construction, this addition is sufficient to complete the proof. ■

An Important Remark on the Validity of the Random Oracle Model: In the cryptography literature, there are two major objections about the validity of the random oracle

model originating from the usage of hash functions to simulate random oracles:

- Programmability property is not possible in the real world:
  Since in the real world it is impossible to set the output of an hash function to a specific value, this is indeed a sound objection. Because most of the time, a concrete hash function (e.g. SHA-1) is used and the result is immediately set as soon as the input is given. Some sort of programmability would be possible in a highly hypothetical environment where hash families could be used instead of a concrete hash function.
- In the real world, it should be impossible for any other entity to see the hash evaluations that the adversary makes:
  Unlike the previous one, this objection may not be correct. Note that by arguing such an impossibility, one imposes that the hard problem being reduced cannot be broken by the same breaker as the scheme security of which is being proved. To make this point clear, suppose that we are proving the security of a scheme S by reducing a mathematically hard problem P to S. In such a reduction, we need to provide a breaker B_P for P assuming that we have a breaker B_S for S. If we do not allow B_P to see the hash evaluations that B_S makes, this implies the restriction that B_P cannot be designed by the same entity who designed B_S. However, this is an unnecessary restriction because it must be sufficient to show that if S can be broken so can P, no matter who designs the breaker algorithms B_S and B_P. So, since B_S and B_P can possibly be designed by the same entity (at least we cannot prohibit this), the hash evaluations of B_S should be visible to B_P.

IV. Game Hopping Techniques

In this section, we will look at another security proof technique, which is called game hopping. The idea is to start with the original attack game, usually called G_0, and slightly modify into a number of games satisfying the following:

- Successive games are indistinguishable from the view of the adversary and this indistinguishability is shown by relating them to the usual underlying mathematically hard problems.
- Adversary gains no information in the last game, meaning that its success probability is $1/2$.

By showing these two properties, one proves that the view of the adversary in the original game and the last game are indistinguishable which means that the success probability of the adversary in the original game is negligible.

In order to illustrate this idea, we present two different examples which are CPA-secure in the standard model.

A. Security Analysis of El Gamal Encryption Scheme under DDH Assumption

First we briefly recall the El Gamal encryption scheme.

- **Setup**: Let g be a generator of some prime order group $\mathbb{G}$. Let x be the private key and $h = g^x$ be the public key.
- **Encrypt**(m): Given a message $m \in \mathbb{G}$, a random $r \in \mathbb{G}$ is chosen and m is encrypted as:
$$c = (g^r, h^r \cdot m)$$
- **Decrypt**(c): Given a ciphertext $c = (c_1, c_2)$,
$$m = c_2 / c_1^x$$

Now, we will briefly explain the game hopping proof of the CPA-security of the El Gamal encryption scheme in the standard model.

Theorem IV.1 *If the Decisional Diffie-Hellman (DDH) problem is hard, then the El Gamal encryption scheme is IND-CPA secure in the standard model.*

Proof: We will first consider the original CPA attack game Game 0 between an adversary A and a challenger C. Game 0 proceeds as follows:

Game 0 :

1) *First, C runs the Setup algorithm and provides the public key to A.*
2) Find Stage: *A chooses two messages m_0, m_1 and sends them to C.*
3) Challenge: *C selects a random bit b and encrypts m_b as $c^* = (g^r, h^r \cdot m_b)$.*
4) Guess: *A guesses b' for b.*

Next, with a small change, we define a new game Game 1 same as Game 0 except in the challenge ciphertext C sends $c^* = (g^r, g^z \cdot m_b)$ where z is randomly chosen from $\mathbb{Z}_q$. Now, we argue that the adversary cannot distinguish its view in games Game 0 and Game 1 depending on the DDH assumption. Because note that knowing g^r and $h = g^x$ the adversary needs to distinguish $h^r = g^{xr}$ and the random value g^z which corresponds exactly the DDH decision problem. What remains is that the success probability of the attacker in Game 1 is information theoretically $1/2$ since g^z is randomly selected from a uniform distribution over $\mathbb{G}$ which makes it like a one-time pad. This concludes the proof. ■

B. Security Analysis of Hashed El Gamal under DDH Assumpiton and Entropy Smoothing

In this section we will discuss the hashed version of the El Gamal encryption scheme which we already defined in Section III-B. However, this time, the security of the scheme will be proved in the standard model under the DDH and entropy smoothing assumptions. First we define entropy smoothing.

Entropy smoothing: Let $\mathcal{H} = \{H_k\}_{k \in K}$ be a family of hash functions where each $H_k : \mathbb{G} \to \{0,1\}^\ell$. $\mathcal{H}$ is called entropy smoothing if there exists no polynomial time adversary that can effectively distinguish between the pairs $(k, H_k(x))$ and (k, h), where $k \in_R K$, $x \in_R \mathbb{G}$ and $h \in_R \{0,1\}^\ell$.

The intution behind entropy smoothness is that the range of an arbitrary hash function from the hash family is uniformly distributed.

Now we present the semantic security of hashed El Gamal encryption scheme in the standard model using game hopping techniques.

Theorem IV.2 *Under the DDH assumption and entropy smoothing property of the hash family, hashed El Gamal encryption scheme is CPA-secure in the standard model.*

Proof: Let Game 0 be the original CPA attack game.

Game 0 :

1) *First, C runs the Setup algorithm and provides the public key to A.*
2) Find Stage: *A chooses two messages m_0, m_1 and sends them to C.*
3) Challenge: *C selects a random bit b and encrypts m_b as $c^* = (g^r, H(h^r) \oplus m_b)$.*
4) Guess: *A guesses b' for b.*

Let Game 1 be the same as Game 0 except a small change in the challenge, $c_2 = H(g^z) \oplus m_b$ instead of $H(h^r) \oplus m_b$ where z is randomly chosen from $\mathbb{Z}_q$. Note if a polynomial time adversary can distinguish its views in Game 0 and Game 1 with a non-negligible success probability, one can construct an efficient algorithm that can decide DDH problem which contradicts the hardness assumption of DDH.

Now, let Game 2 be the same as Game 1, except that in the challenge, $c_2 = r \oplus m_b$ instead of $H(g^z) \oplus m_b$ where r is a random element of $\{0,1\}^\ell$. Note that due to the entropy smoothing property of the hash family used in the scheme, no efficient adversary can distinguish between its views in Game 1 and Game 2.

Finally, the success probability of the adversary in Game 2 is information theoretically 1/2, i.e. it behaves like a one-time pad and this concludes the proof. ■

V. Conclusion

In this paper, we have briefly discussed several security proofs that utilize the random oracle model and the game hopping technique. We hope that the ideas presented here will help the readers having a better understanding about security proofs in modern cryptography. Here, we confined ourselves to rather simple constructions and proofs, however, random oracle and game hopping techniques are two of the main building blocks of most security proofs in the public key setting.

Acknowledgment

We would like to thank Ali Aydın Selçuk and Ersan Akyıldız for useful discussions.

References

[1] N. Koblitz and A. Menezes, *Another Look at Provable Security*. J. Cryptology 20(1): pages 3-37, 2007.
[2] M. Bellare, A. Desai, D. Pointcheval and P. Rogaway, *Relations among notions of security for public-key encryption schemes*. Advances in Cryptology, CRYPTO'98.
[3] M. Bellare and P. Rogaway, *Random Oracles are practical:a paradigm for designing efficient protocols*. In First ACM Conference on Computer and Communications Security, pages 62-73, 1993
[4] R. Cramer and V. Shoup, *A practical public key cryptosystem provably secure against adaptive chosen ciphertext attack*. In Proceedings of Crypto 1998, LNCS 1462
[5] D. Pointcheval, *Contemporary Cryptology: Provable Security for Public Key Schemes*, Advanced Courses CRM Barcelona, pages 133-189, 2005.
[6] S. Goldwasser and S. Micali, *Probabilistic encryption and how to play mental poker keeping secret all partial information*, Proc. 14th Symposium on Theory of Computing, pages 365-377, 1982
[7] S. Golwasser and S. Micali, *Probabilistic encryption*, Journal of Computer and System Sciences, pages 270-299, 1984
[8] R. Canetti, O. Goldreich and S. Halevi, *The random oracle methodology, revisited*, In proceedings of the 30thAnnual ACM Symposium on the Theory of Computing, 1998

Burke Shaw Kaotik Sisteminin Güvenli Haberleşme İçin Elektronik Devre Gerçeklemesi ve Senkronizasyon Uygulaması

İsmail Koyuncu, Yılmaz Uyaroğlu, İhsan Pehlivan

Abstract— **In this paper, Simulink and Pspice modeling of the Burke-Shaw chaotic system are introduced. Synchronization studies of the modeled chaotic systems were performed using Pecora-Carroll (P-C) method. Usability of the Burke-Shaw chaotic system for signal masking and secure communication applications was showed as a result of the synchronization of modeled Burke-Shaw attractors. Burke-Shaw oscillators having different initial conditions are synchronized completely in a very short time in performed synchronization. Chaotic oscillator of the Burke-Shaw system designed with analog electronics elements is first time introduced by this paper. Different signal masking applications having an other methods would be realized using electronic circuit modeling of the Burke-Shaw system given in this paper,**

Index Terms— **Chaos, Chaotic system, Burke Shaw chaotic oscillator, chaotic synchronization**

Özet— **Bu çalışmada, Burke Shaw kaotik sisteminin Simulink ve Pspice programları ile yapılan modellemesi tanıtılmaktadır. Modellenen kaotik sistemlerin Pecora-Carroll (P-C) metodu ile senkronizasyon çalışması yapılmıştır. Modellenen Burke Shaw çekicilerinin senkronizasyonu ile, sinyal gizleme ve güvenli haberleşme uygulamaları için Burke-Shaw sistemin kullanılabileceği gösterilmiştir. Gerçekleştirilen senkronizasyonda farklı başlangıç şartlarında çalıştırılan Burke Shaw osilatörleri çok kısa bir sürede tam olarak senkronize olmaktadır. Burke-Shaw sisteminin analog elektronik elemanlar ile tasarlanan kaotik osilatörü ilk defa bu makale ile tanıtılmıştır. Burke-Shaw sisteminin bu makalede verilen elektronik devre modellemesi kullanılarak, farklı yöntemler kullanan değişik sinyal gizleme uygulamaları yapılabilir.**

Anahtar Kelimeler—**Kaos, Kaotik sistem, Burke Shaw kaotik osilatör, kaotik senkronizasyon**

İ. Koyuncu, Düzce University, Department of Control and Automation, Duzce Vocational High School, Uzun Mustafa Mh, 81010 Duzce, Turkey, +90 0 380 5240099, ismailkoyuncu@duzce.edu.tr.

Y. Uyaroğlu, Sakarya University, Engineering Faculty, Electrical Electronics Engineering, 54050, Esentepe Campus, Sakarya, Turkey, uyaroglu@sakarya.edu.tr.

İ. Pehlivan, Sakarya University, Faculty of Technology, Electrical and Electronics Engineering Department, , 54187, Esentepe Campus, Sakarya, Turkey, ipehlivan@sakarya.edu.tr.

I. Introduction

Kaos, düzensiz görünümlü davranışlar sergileyen ancak kendine has bir düzene sahip olan dinamik sistemlerde bilinen en karmaşık kararlı hal davranışıdır. Kaos, doğrusal olmayan, zamanla değişen sistemlerde ortaya çıkan bir durum olmakla birlikte bu tür sistemler literatürde kelebek etkisi olarakta adlandırılmaktadır. Kaosun ve kaotik işaretlerin başlıca önemli özellikleri; zaman boyutunda düzensizliği, sınırsız sayıda değişik periyodik salınımlar içermesi, gürültü benzeri geniş güç spektrumuna sahip olması, limit kümesinin parçalı (fraktal) boyutlu olması, genliği ve frekansı tespit edilemeyen, ancak sınırlı bir alanda değişen işaretler içermesidir. Kaotik sistemlerin en büyük özelliği başlangıç koşullarına hassas bağlı olmalarıdır. Kaos tabanlı sistemlerde genel olarak sisteme ilk bakıldığında işaretler karmaşık bir görünüm sergilediklerinden dolayı sistemde herhangi bir periyodiklik veya düzen gözlemlenememektedir [1, 2].

Literatürde en çok çalışma yapılan ve kaotik dinamikleri en iyi bilinen otonom sistemler Chua osilatörü, Rösler osilatörü ve Lorenz sistemidir [3, 4, 5]. Chua devresi [6], basit bir devre yapısına sahip olmasına rağmen kompleks dallanma ve kaos sergilemesi dolayısıyla elektronikteki kaos olayının açıklanmasında model devre olmuştur.

Günümüzde kaos tabanlı uygulamalar, kriptoloji [7], elektronik ve güvenli haberleşme [8 ve 9], kontrol ve sürücü sistemleri [10], hava durumu tahminleri [5] gibi pekçok alanda uygulanabilirliğini kanıtlamıştır. Ayrıca kaotik sistemler, tahmin edilemez özelliklere ve gürültü benzeri geniş bir spektruma sahip olmalarından dolayı, kriptoloji ve güvenli haberleşme uygulamalarında oldukça yaygın bir biçimde kullanılmaya başlanmıştır.

Kaos tabanlı güvenilir haberleşme sistemleri, iletilecek bilgi işaretlerinin spektrumunu geniş bir sahaya yayabilmeleri, eşzamanlı olarak bildiri işaretlerini kodlayabilmeleri ve bu işlemleri basit ve pahalı olmayan kaotik devre düzenekleriyle gerçekleştirebilmeleri sebebiyle, literatürdeki standart geniş spektrumlu haberleşme sistemlerine alternatif olmuşlardır. Bir diğer önemli nokta ise kaotik sistemler başlangıç değerlerine üstel olarak duyarlı sistemler olup, bunların çözümlerinin uzun zaman aralıkları için öngörülmesi mümkün olmamaktadır. Bunun yanında kaotik işaretlerin periyodik olmamaları nedeniyle, frekans spektrumları sürekli ve geniştir. Bu gibi özellikler taşımalarından dolayı yaygın bir biçimde kriptoloji

ve güvenli haberleşmede Lorenz, Chua, Chen, Rossler, Lü, Duffing gibi kaotik tabanlı sistemler kullanılmaktadır [11-16].

Bu çalışmada birinci bölümde kaos ve kaotik sinyaller hakkında genel bilgiler verilmiştir. İkinci bölümde Matlab-Simulink ile Burke Shaw kaotik sisteminin modellenmesi ve simülasyonu gerçekleştirilmiştir. Modelin analog elektronik devre elemanları ile gerçeklenebilirliğini göstermek için Orcad-Pspice programında elektronik devre tasarımı yapılmıştır. Üçüncü bölümde, Burke Shaw kaotik sisteminin Matlab-Simulink ve Orcad Pspice üzerinde senkronizasyon çalışmaları gerçekleştirilmiş ve başarılı sonuçlar elde edilmiştir. Son bölüm sonuçlar ve değerlendirmeleri içermektedir.

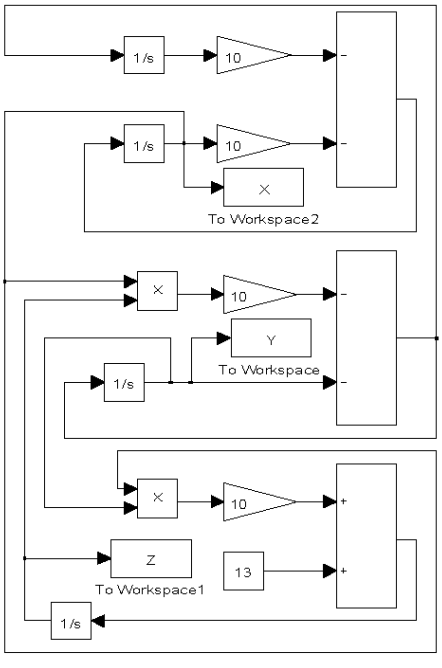
II. BURKE SHAW KAOTIK SISTEMININ MATLAB-SIMULINK VE ELEKTRONIK DEVRE MODELLEMESI

Burke-Shaw nonlineer otonom kaotik sistemi için denklem takımları aşağıda (1) verilmektedir.

$$\begin{aligned} dx/dt &= -\alpha \cdot x - \alpha \cdot y \\ dy/dt &= -\alpha \cdot x \cdot z - y \\ dz/dt &= \alpha \cdot x \cdot y + \beta \end{aligned} \qquad (1)$$

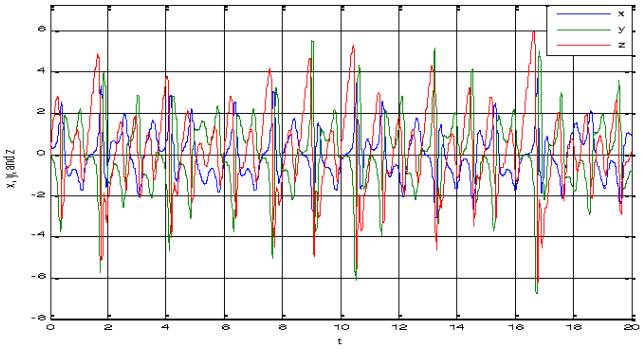
Bu denklem takımlarındaki α ve β parametrelerinin değişimi kaotik sistemin dinamik davranışını değiştirmektedir. Bu nedenle bu parametrelerin değeri oldukça önemlidir. Yapılan çalışmada α parametresi 10.0 ve β parametresi ise 13.0 olarak seçilmiştir. Kaotik sistem başlangıç koşulları x_0=0.6, y_0=0.0 ve z_0=0.0' tir.

İlk olarak yukarıda verilen Burke Shaw kaotik sistemi, yapılan elektronik devre tasarımı sonuçlarını doğrulamak amacıyla Matlab-Simulink programında modellenmiştir. Şekil 1'de Burke Shaw kaotik sisteminin Matlab-Simulink'de yapılan modellemesi görülmektedir.

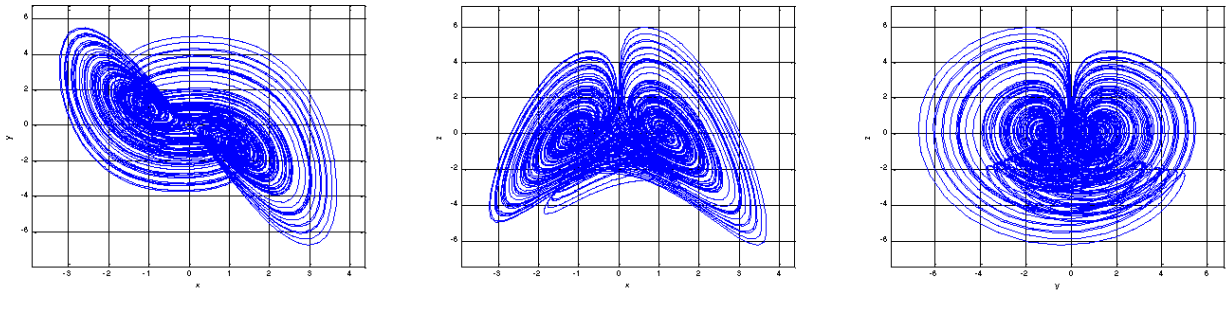


Şekil 1. Burke Shaw kaotik sistemi Matlab-Simulink modeli

Şekil 2'de ve Şekil 3 (a), (b) ve (c)'de Burke Shaw kaotik sistemi Matlab-Simulink programı modelleme sonuçlarından elde edilen çıkış grafikleri verilmiştir. Şekil 3 (a) Burke Shaw kaotik sisteminin x çıkışının y çıkışına göre, Şekil 3 (b) x çıkışının z çıkışına göre ve Şekil 3 (c) y çıkışının z çıkışına göre değişimini göstermektedir.



Şekil 2. Burke Shaw kaotik sistemi x, y, ve z çıkış grafikleri.

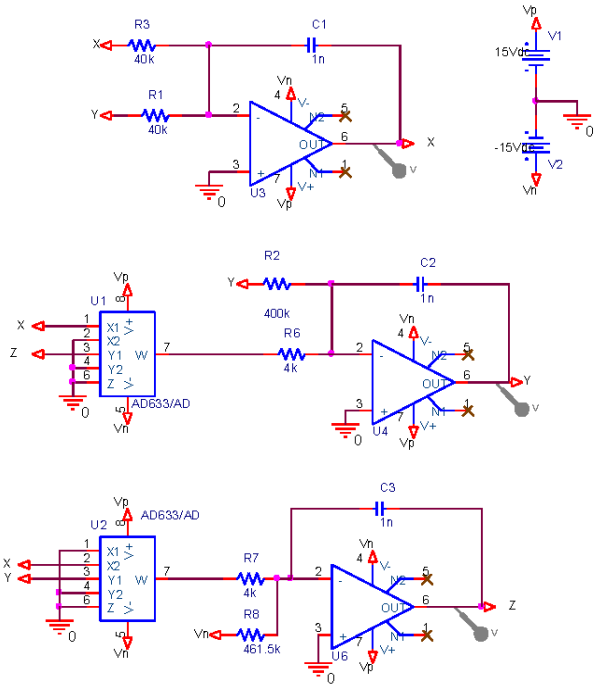


Şekil 3. Matlab-Simulink programı modelleme sonuçlarından elde edilen çıkış grafikleri
(a) x sinyalinin y sinyaline gore değişimi (b) x sinyalinin z sinyaline gore değişimi (c) y sinyalinin z sinyaline gore değişimi

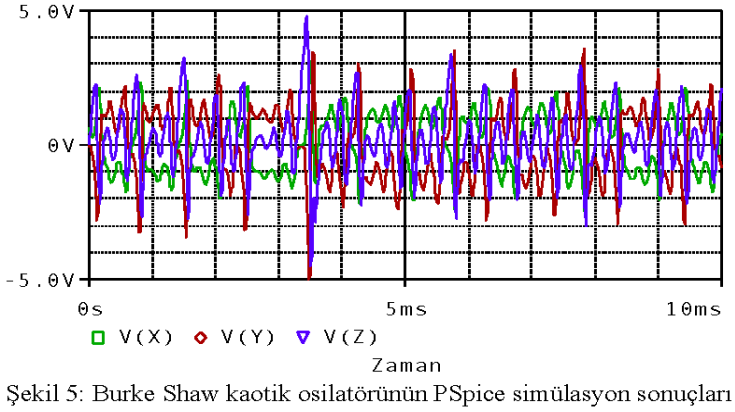
Burke Shaw kaotik osilatörünün denklemleri ORCAD-Pspice elektronik tasarım programı ile analog elemanlar kullanılarak modellenmiştir. Sistemde üç adet TL081 op-amp, iki adet AD633 çarpıcı, üç kapasitör ve değişik değerlere sahip altı adet direnç elemanı kullanılmıştır. Devre bağlantılarının karmaşık görünümden kurtarılması amacıyla bazı sinyaller sadece isimleri kullanılarak verilmiştir. Devrede kullanılan işlemsel yükselteçler (opamp) ve çarpıcı üniteleri simetrik 15V güç kaynağı ile beslenmiştir. Bu analog elektronik elemanlar kullanılarak Burke Shaw kaotik sistemi modellendiğinde diferansiyel denklem eşitlikleri (2) aşağıdaki gibi olmaktadır.

$$\begin{aligned} dx/dt &= -\left(\frac{1}{R_3C_1}\right)\cdot x - \left(\frac{1}{R_1C_1}\right)\cdot y \\ dy/dt &= -\left(\frac{1}{R_2C_2}\right)\cdot x\cdot z - \left(\frac{1}{R_2C_2}\right)\cdot y \\ dz/dt &= \left(\frac{1}{R_7C_3}\right)\cdot x\cdot y + \left(\frac{1}{R_8C_3}\right)\cdot V_n \end{aligned} \qquad (2)$$

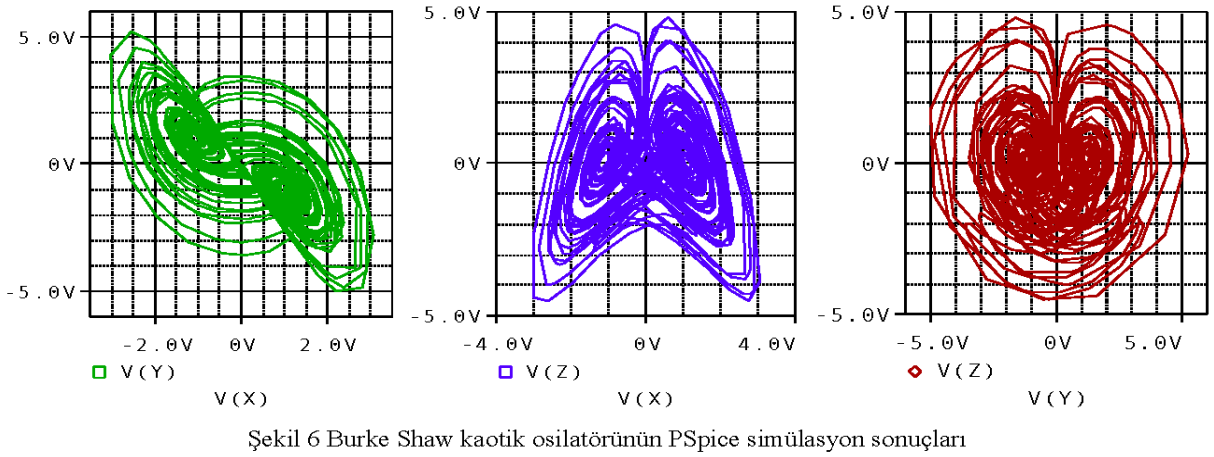
Şekil 4'te ORCAD-Pspice programında tasarımı yapılan Burke-Shaw kaotik sistemin elektronik devre şeması görülmektedir. Şekil 5 ve 6'da ise kaotik sistemin elektronik devresine ait simülasyon sonuçları verilmiştir.



Şekil 4: Burke Shaw kaotik sisteminin elektronik devre şeması.



Şekil 5: Burke Shaw kaotik osilatörünün PSpice simülasyon sonuçları



Şekil 6 Burke Shaw kaotik osilatörünün PSpice simülasyon sonuçları
(a) x sinyalinin y sinyaline göre değişimi (b) x sinyalinin z sinyaline göre değişimi (c) y sinyalinin z sinyaline göre değişimi

III. BURKE SHAW KAOTIK OSILATÖRLERININ SENKRONIZASYON UYGULAMALARI

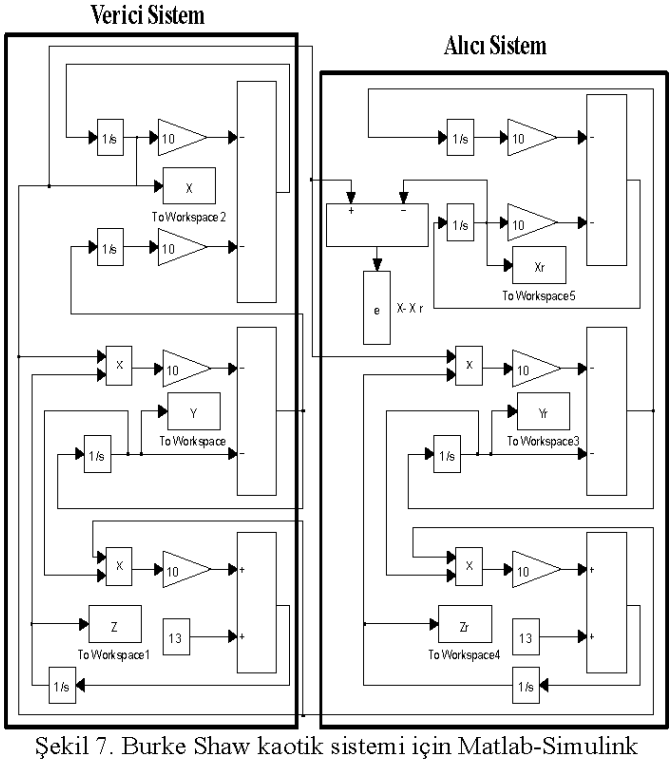
Kaos tabanlı osilatörler kullanılarak yapılan senkronizasyon çalışmaları güvenli haberleşme uygulamalarında oldukça fazla ilgi çekmektedir. Çünkü kaos tabanlı senkronizasyon sistemleri güvenli bir haberleşme ve sinyal işleme için potansiyel uygulamalar sağlamaktadır. İki kaos tabanlı sistemin sonkronize edilmesi için temelde tek-yönlü kuplaj yöntemi ve peş peşe bağlama yöntemi olarak tanımlanan Pecora-Carroll (P-C) yöntemi [17, 18] kullanılmaktadır. Bu iki metodun temel çalışma biçimi bir mesaj sinyalinin, verici tarafından, senkronizasyonda bulunan bir kaotik sinyalin güdümü altında, alıcıda yeniden oluşturulabilecek şekilde gönderilmesi şeklindedir.

Bu bölümde Matlab-Simulink ve Orcad-Pspice programları kullanılarak iki adet Burke Shaw kaotik sisteminin senkronizasyon modellemeleri ve bu sistemlerden elde edilen simülasyon sonuçlarını sunulmaktadır.

Pecora-Carroll senkronizasyon metodunun Burke Shaw kaotik sistemine uygulanabilmesi amacıyla ilk olarak Verici Burke Shaw ve Alıcı Burke Shaw yapıları oluşturulmalıdır. Verici Burke Shaw (3) ve Alıcı Burke Shaw (4) yapılarının oluşturulması için gerekli denklemler aşağıda verilmiştir.

$$\begin{aligned} dx/dt &= -\alpha \cdot x - \alpha \cdot y \\ dy/dt &= -\alpha \cdot x \cdot z - y \\ dz/dt &= \alpha \cdot x \cdot y + \beta \end{aligned} \tag{3}$$

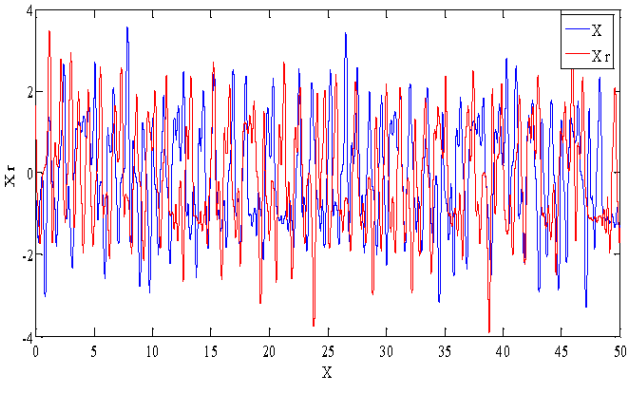
$$\begin{aligned} dx_r/dt &= -\alpha \cdot x_r - \alpha \cdot y_r \\ dy_r/dt &= -\alpha \cdot x \cdot z_r - y_r \\ dz_r/dt &= \alpha \cdot x \cdot y_r + \beta \end{aligned} \tag{4}$$



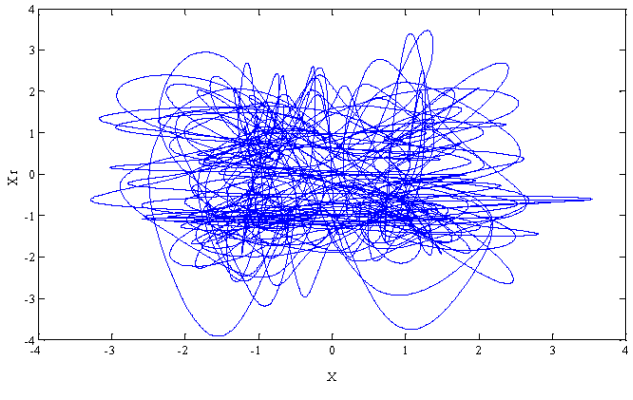
Şekil 7. Burke Shaw kaotik sistemi için Matlab-Simulink programı ile modellenen senkronizasyon sistemi

Şekil 7'de bu denklemlere ait kaotik sistemi için Matlab-Simulink programı ile modellenen Verici ve Alıcı Burke Shaw osilatörleri ile elde edilen senkronizasyon sistemi verilmektedir. Burada Sürücü (Verici) devrenin başlangıç şartları x_0=0.6, y_0=0.0 ve z_0=0.0 ve alıcı devrenin başlangıç şartları ise x_0=1.0, y_0=0.0 ve z_0=0.0 olarak alınmıştır.

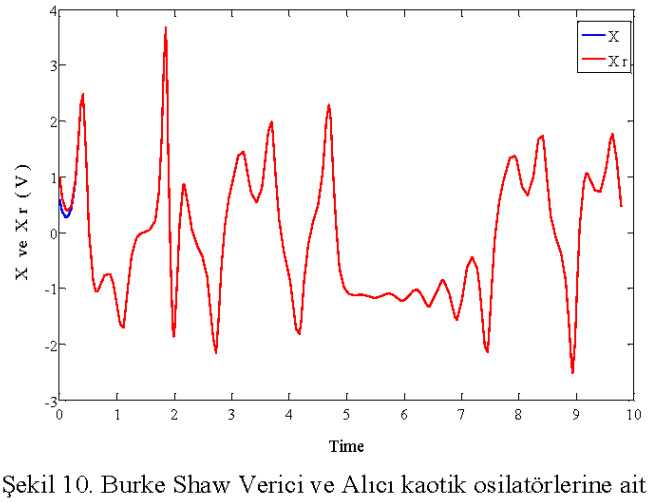
Senkronizasyon öncesi, Verici ve Alıcı Burke-Shaw osilatörlerine ait kaotik X ve Xr sinyallerinin zaman gore değişimi Şekil 8'de, bu sinyallere ait faz portresi ise Şekil 9'da verilmiştir.



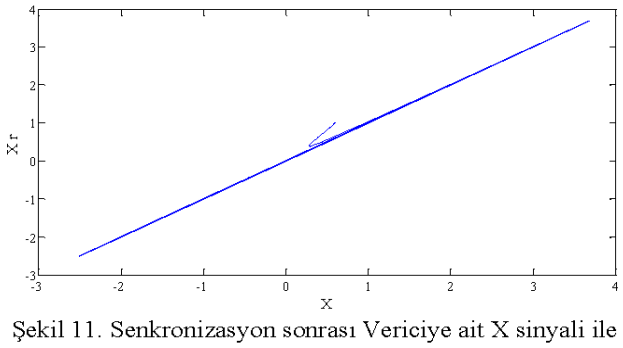
Şekil 8. Burke Shaw Verici ve Alıcı kaotik osilatörlerine ait senkronizasyon öncesi X ve Xr sinyalleri.



Şekil 9. Senkronizasyon öncesi Vericiye ait X sinyali ile Alıcıya ait Xr sinyaline ait faz portresi

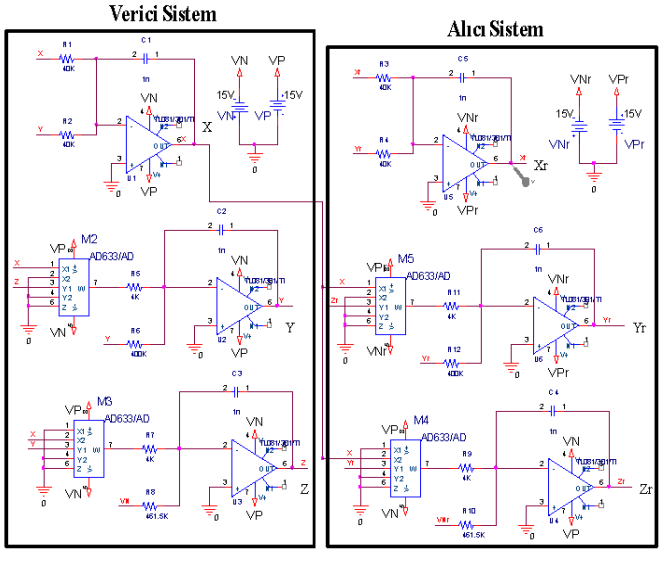


Şekil 10. Burke Shaw Verici ve Alıcı kaotik osilatörlerine ait senkronizasyon sonrası X ve Xr sinyalleri.



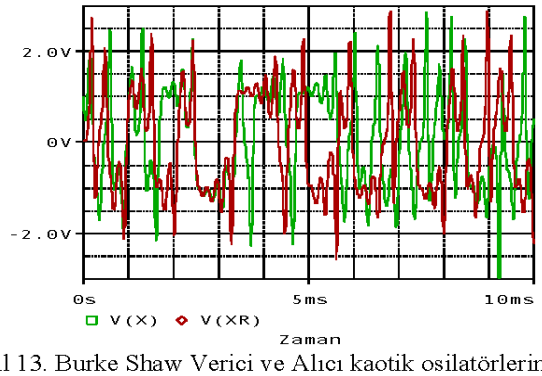
Şekil 11. Senkronizasyon sonrası Vericiye ait X sinyali ile Alıcıya ait Xr sinyaline ait faz portresi

P-C yöntemi ile yapılan senkronizasyon işleminde sürücü (verici) devrenin başlançış şartları x_0=0.6, y_0=0.0 ve z_0=0.0 ve alıcı devrenin başlangıç şartları ise x_0=1.0, y_0=0.0 ve z_0=0.0 olarak alınmıştır. Senkronizasyon öncesi başlangıç şartları farklı alındığında kaotik sistemler arasında senkronizasyon bulunmamakta idi. Senkronizasyon işlemi sonunda başlangıç şartları farklı olmasına rağmen Sürücü ve Alıcı sistemler 0,876ms gibi çok kısa bir sürede senkronize olmuştur. Yapılan modelleme ve simülasyon işlemlerinin doğruluğunun gösterilmesi hem de gerçek elektronik devre tabanlı uygulamalar için gerçeklenebilirliğinin kanıtlanması bakımından aynı işlemler Orcad Pspice tasarım programında da gerçekleştirilmiştir. Şekil 12'de Orcad PSpice ile modellenen Burke Shaw senkronizasyon sisteminin elektronik devre modeli verilmiştir. Senkronizasyon metodu olarak Pecora-Carroll (P-C) yöntemi seçilmiştir. Bu yöntemde iki adet Burke Shaw kaotik sistemi kullanılarak senkronize işlemi yapılmıştır. Bu sistemlerden ilki Verici system, ikincisi ise Alıcı sistem olarak tanımlanmaktadır. Sürücü sistemin senkronizasyonu X, Y, veya Z sinyal çıkışlarından birisi kullanılarak gerçekleştirilebilir. Bu yapıda Sürücü sisteminden alınan X sinyal çıkışı, Alıcı sistemin ikinci ve üçüncü denklemlerindeki Xr sinyalleri yerine kullanılmaktadır.

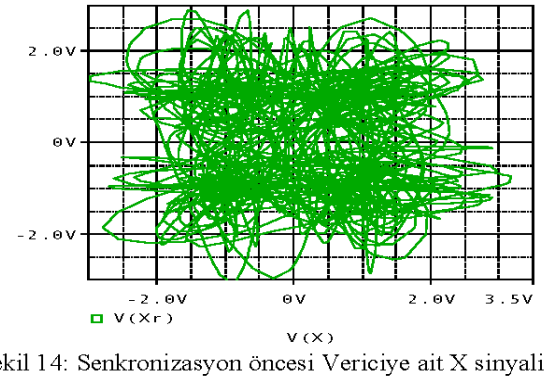


Şekil 12. Burke-Shaw kaotik sistemlerinin OrCAD-PSpice ile modellenen senkronizasyon devresi

OrCAD-PSpice elektronik devre tasarım program kullanılarak gerçekleştirilen Burke Shaw kaotik sistemi senkronizasyon modelinin senkronizasyon öncesi Verici ve Alıcı osilatörlerine ait kaotik X ve Xr sinyallerinin zamana göre değişimi Şekil 13'te ve bu sinyallere ait faz portresi ise Şekil 14'te verilmiştir. Buradaki grafiklerden elde edilen sonuçlar ile nümerik yöntem kullanılarak modellemesi yapılan kaotik senkronizasyon sisteminin sonuçları birbirini doğrulamaktadır.

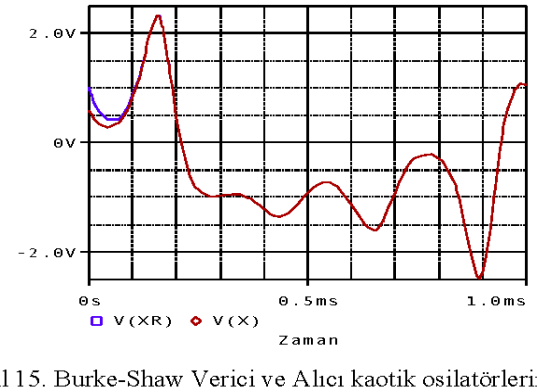


Şekil 13. Burke Shaw Verici ve Alıcı kaotik osilatörlerine ait senkronizasyon öncesi X ve Xr sinyalleri.

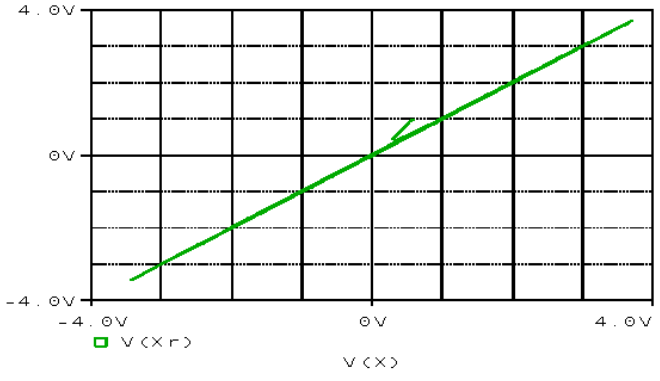


Şekil 14: Senkronizasyon öncesi Vericiye ait X sinyali ile Alıcıya ait Xr sinyali arasındaki faz portresi

Şekil 15'te senkronizasyon sonrası elektornik devre çıkışları verilmiştir. Sürücü sistemin başlangıç şartları x_0=0.6, y_0=0.0 ve z_0=0.0 ve alıcı devrenin x_0=1.0, y_0=0.0 ve z_0=0.0'dır. Farklı başlangıç değerlerine sahip kaotik çıkış değişikenleri, 1ms'den az bir sure içerisinde senkronize olmuştur.



Şekil 15. Burke-Shaw Verici ve Alıcı kaotik osilatörlerine ait senkronizasyon sonrası X ve Xr sinyalleri.



Şekil 16. Senkronizasyon sonrası Vericiye ait X sinyali ile Alıcıya ait Xr sinyalinin faz portresi

IV. SONUÇLAR

Bu çalışmada, Burke Shaw kaotik sisteminin Simulink ve OrCAD-PSpice programları ile kaotik sistem modellemesi gerçekleştirilmiştir. Bu kaotik sistemler kullanılarak senkronizasyon çalışması yapılmış ve senkronizasyon yöntemi olarak Pecora-Carroll (P-C) metodu seçilmiştir. P-C yöntemi kullanılarak yapılan Burke Shaw çekicisinin senkronizasyonunu ile güvenli haberleşme uygulamaları için kullanılabileceği gösterilmiştir. Simülasyon sonuçlarından görüleceği gibi farklı başlangıç şartlarında çalıştırılan Burke Shaw osilatörleri 0,876ms gibi çok kısa bir sürede tam olarak senkronize olmaktadır. Burke Shaw kaotik sisteminin senkronize olduğunun görülmesi sinyal gizleme amaçlı uygulamalar için uygun olabileceğini göstermektedir. Bu bildiri ile ilk defa elektronik devresi sunulan Burke Shaw kaotik osilatörü kullanılarak değişik metotlarla sinyal gizleme amaçlı yeni devreler tasarlanabilir.

Ayrıca gerçekleştirilen senkronizasyon çalışmalarının doğruluğunu ve yapılan modellemelerin elektronik devre tabanlı gerçeklenebilirliğini göstermek amacıyla aynı kaotik sistem Orcad Pspice program kullanılarak modellenmiştir. Böylece kaotik sistem yapılarının analog elektronik elemanlar kullanılarak gerçeklenebilirliği ortaya konulmuştur.

Kaotik işaretlerin elektronik mühendisliğindeki önemli araştırma ve uygulama alanları arasında şifreleme, güvenli haberleşme düzenekleri oluşturma, gürültü üreteçleri, ikili-kodlu rasgele sayı üreteçleri bulunmaktadır. Bu uygulamalarda kullanılması gereken temel yapı, gerekli kaotik işareti üreten bir kaos üretecidir. Yeni ve farklı özelliklere sahip kaotik işaret üreteçlerinin literatüre kazandırılması gerekliliği de her zaman bulunmaktadır. Bu çalışma ile yeni ve farklı dinamik özelliklere sahip bir kaotik işaret üreteci literatüre kazandırılmıştır.

İleriki çalışmalarda Burke Shaw kaotik sisteminin analog devre elemanları ile gerçeklenmesi düşünülmektedir. Ayrıca kaotik sistemin FPGA (Field Programmable Gate Array-Alanda Programlanabilir Kapı Dizileri) tabanlı modellemesi ve senkronizasyon çalışmasının yapılması planlanmaktadır. Bu çalışma ile dijital tabanlı kaotik işeret üreten çipler ile analog elektronik malzemelerin önemli bir dezavantajı olan sıcaklık ve kullanım ömrü ile değerlerinin değişmesi gibi sistem dinamiklerini doğrudan etkileyen olumsuz yönleri giderilmiş olacaktır.

REFERENCES

[1] İ. Pehlivan, Y. Uyaroğlu, "*Simplified Chaotic Diffusionless Lorentz Attractor and its Application to Secure Communication Systems*", IET Communications, 1, 5, 1015-1022, (2007).
[2] F.Umut, "*Kaotik Zaman Serilerinin YSA ile Kestirimi: Deprem Verisi Durumu*". Yıldız Teknik Üniv., Yüksek Lisans Tezi, İstanbul, 2006.
[3] L.O. Chua, C.W. Wu, A. Huang, G. Zhong, "*A Universal Circuit for Studying and Generating Chaos-Part I: Routes to Chaos*", IEEE Trans. Circuits&Systems-I, 40, 732-761, 1993.
[4] O.E. Rössler, "*An equation for continuous chaos*", Phys. Lett. A, 57, 397–398, 1976.
[5] E.N. Lorenz, "*Deterministic nonperiodic flow*", J. Atmos. Sci., 20, 130–141, 1963.
[6] T. Matsumoto, L.O. Chua, S. Tanama, "*Simplest Chaotic Nonautonomous Circuit*", Physical Rev. A, 30, 1155-1157, 1984.
[7] O. Fındık, "*Şifrelemede Kaotik Sistemin Kullanılması*". Selçuk Üniversitesi, Yüksek Lisans Tezi, Konya, 2004.
[8] A. Khadra, X. Liu, X. Shen, "*Application of Impulsive Synchronization to Communication Security*", IEEE Transactions on Circuits and Systems I, 50(3), 341-351, 2003.
[9] İ. Pehlivan, Y. Uyaroğlu, "*Rikitake Attractor and its synchronization application for secure communication system*", Journal of Applied Sciences, 7(2), 232-236, 2007.
[10] T.C. Lin, C.H. Kuo, V.E. Balas, "*Uncertain Fractional Order Chaotic Systems Tracking Design via Adaptive Hybrid Fuzzy Sliding Mode Control*". International Journal of Computers, Communications & Control, Vol. 4, No. 3 (September), pp. 418-427, 2011.
[11] G. Chen., T Ueta, "Yet another chaotic attractor", Int. J. Bifurc. and Chaos, 9:1465-1466, 1999.
[12] J. Lü, G. Chen, "*A new chaotic attractor coined*", Int. J. Bifurc. & Chaos, 12:659-661, 2002.
[13] J. Lü, G. Chen, D. Cheng and S. Celikovsky, "*Bridge the gap between the Lorenz system and the Chen system*", Int. J. Bifurc. and Chaos, 12:2917-2926, 2002.
[14] G. Qi, S. Du and G. Chen, "*On a four-dimensional chaotic system*", *Chaos*, Solitons and Fractals, 23:1671- 1682, 2005.
[15] Y.Ohmori, N. Nakagawa, T. Saito, "*Mutual Coupling of Oscillators with Chaos and Period Doubling Bifurcation*", ISCAS'85 International Conference on Circuits and Systems, 61-64, 1985.
[16] T. Saito, "*A Chaos Generator Based on a Quasi-Harmonic Oscillator*", IEEE Trans. Circuits&Systems, CAS-32, 320-331, 1985.
[17] L.M. Pecora, T.L. Carroll , "*Synchronization in Chaotic Systems*", Phys. Rev. Lett., 64:821-824., 1990.
[18] L.M. Pecora, T.L. Carroll, "*Driving systems with chaotic signals*", Physical Rev. A , 44:2374-2383, 1991.



Ismail Koyuncu has a M.S. Degree from University of Abant Izzet Baysal, Bolu-Turkey. He is currently conducting his doctoral research in the Department of Electrical and Electronics Engineering, Sakarya University Sakarya-Turkey. He is a instructor in Control and Automation Technology Program of Duzce Vocational High School, Duzce University. His main research interests are digital system design, chaos and FPGA systems.

Oyun Teorisi Kullanılarak Bulut Bilişimde Ölçeklendirebilir Güvenlik Değerlendirmesi

Evrim Furuncu, İbrahim Soğukpınar

Özet—**"Bulut Bilişim" günümüz Internet dünyasında ön plana çıkan kavramların başında gelmektedir. Bulut bilişim alt yapısında bulunan hizmet modellerinde uygulanan güvenlik, hizmet modellerine göre farklılıklar göstermektedir. Bir modelde uygulanan güvenlik diğer modelde farklı kişi veya kuruluşlara aktarılmakta, bu yüzden bir karmaşa yaşanmaktadır. Ayrıca bulut bilişim sistemi içindeki her varlık farklı güvenlik önlemi gerektirebilecektir. Bu husus, önemsiz bilgilerin yüksek güvenlik seviyesi ile saklanmasına neden olmakta ve bulut sağlayıcı gereksiz masraf yaşamaktadır. Bu çalışmada, ölçeklendirilebilir bulut bilişim güvenliği bu sorunlara çözüm olarak önerilmiştir. Bu çözüm günümüzde yaygın olan oyun teorisi ile dinamik olarak modellenmiştir.**

Anahtar Kelimeler — **Bulut Bilişim Güvenliği, Ölçeklendirebilir Güvenlik, Oyun Teorisi**

Abstract —**The term "Cloud Computing" is one of the most popular concepts of the today's IT world. The security of the service models in cloud computing is different from each other because of the infrastructure needed for each of the service models. The security implemented in a model is transferred to other persons or entities in a different model. This makes a mess about the security. Each asset in cloud computing may need the different security level as the other assets. This state causes unimportant information to have more security than needed and results in unnecessary expense. In this work scalable security in cloud computing has been proposed as a solution for this problem. This solution is presented by using one of the hot topics in today's dynamic security modeling, namely game theory. The game that is played in this problem is dynamic game with incomplete information, namely a Bayesian game.**

Keywords— Cloud Computing Security, Scalable Security, Game Theory Security Modeling

I. GİRİŞ

Gelişen bağlantı hızları sayesinde uzaktaki güçlü sunucuların kaynaklarını verimli bir şekilde kullanarak işlerin yapılması, günümüzde bulut bilişim kavramını ortaya çıkarmıştır. İşletmeler bulut bilişimi kullanarak, bilgisayar kaynaklarının maliyetlerinde tasarruf ve esneklik elde edebilmektedirler. Talep üzerine kapasite ekleyerek, işletmeler bulut bilişimi kendi altyapılarını genişletme amacıyla kullanabilmektedirler.

Birden fazla kullanıcının ortak altyapı kullanması bu sistemin güvenliğini önemli kılmaktadır. Bulut bilişimin hizmet modelleri olan; SoY (Servis olarak Yazılım), SoP (Servis olarak Platform) ve SoA (Servis olarak Altyapı) modellerinin her birisinde farklı hizmetler belli bir kademeye kadar çalıştırılmaktadır. Mevcut hizmet modellerinde ihtiyaç duyulan farklı kaynaklar nedeniyle alınan güvenlik önlemleri de farklılık göstermektedir. Güvenlik önlemleri Bazı modellerde mutlaka alınması gerekirken, bazılarında alınması zorunlu olmamakta veya kullanıcının alması gerekmektedir. Bu önlemlerin servis modellerine göre değişiklik göstermesinin yanı sıra, bulut servis sağlayıcılar ile kullanıcılar arasında yapılan hizmet seviyesi anlaşmasına (SLA - Service-level agreement) göre de değişebilmektedir.

Tablo-1'de NIST tarafından bulut bilişim tanımında kullanılan [1] bulut servis modellerindeki güvenlik ihtiyaçları verilmiştir. Burada dikkat edilmesi gereken bir konu, bulut servis modellerinin sadece bu tanımdaki gibi üç modelden oluşmamasıdır. SoY, SoA ve SoP gibi modellerin yanında günümüzde hareketli operatörlerin kullandığı SoaA (Servis olarak ağ), yedekleme veya tekil kişilerin kullandığı SoDA (Servis olarak Depolama Alanı) ve işyerlerinin elemanlarının bilgisayarlarını buluta aktaran SoM (Servis Olarak Masaüstü) gibi modellerde gelişmektedir. Bu modellerin güvenlik gereksinimleri ihtiyaç duydukları kaynaklara göre değişmektedir. Örneğin SoaA'da mevcut olma gereksinimi diğer bütün gereksinimlere göre daha önemlidir. Bunun nedeni bu sistemin asıl kullanım amacı kullanıcıya ağı sunmak yani bant genişliği sağlamaktadır. Üzerinden geçen bilginin gizliliği, bütünlüğünün sağlanması servis sağlayıcıya ait değildir. Fakat servis olarak yazılım hizmetinde yapılan tüm işler bulut sağlayıcı tarafından yapıldığından dolayı, bulut sağlayıcı Tablo-1'de gösterilen her güvenlik özelliğini düşünmek ve uygulamak zorundadır.

Bilgi Güvenliği Gereksinimleri	Bulut Kurulum Modelleri					
	Genel			Özel		
	Bulut Servis Modelleri					
	IaaS	PaaS	SaaS	IaaS	PaaS	SaaS
Mevcut Olma	X	X	*	X	X	X
Yetkilendirme	X	X	X	*	*	X
Gizlilik	*	*	X	*	X	X
Bütünlük	X	*	X	*	X	X
Kimlik Doğrulama	X	*	X	X	*	X

X Gerekli ihtiyaçlar * Opsiyonel ihtiyaçlar

Tablo 1- Bulut bilişim güvenlik gereksinimleri

Evrim FURUNCU, Gebze Yüksek Teknoloji Enstitüsü Bilgisayar Mühendisliği, Gebze Yüksek Teknoloji Enstitüsü İstanbul Caddesi, P.K. 141,Gebze, 41400– Kocaeli, TÜRKİYE, Ttel: +90 262 605 22 32Fax: +90 262653 84 90 E-mail: efuruncu@bilmuh.gyte.edu.tr

İbrahim SOĞUKPINAR, Gebze Yüksek Teknoloji Enstitüsü Bilgisayar Mühendisliği, Gebze Yüksek Teknoloji Enstitüsü İstanbul Caddesi, P.K. 141, Gebze, 41400 – Kocaeli, TÜRKİYE, Ttel: +90 262 605 22 01Fax: +90 262653 84 90 E-mail: ispinar@bilmuh.gyte.edu.tr

Genel olarak ağ saldırganları zeki ve mantıklı insanlardır. Yapacakları saldırıların masraflarını ve kazançlarını göz önünde bulundururlar. Savunanlar ise saldırıyı engelleyerek bir kazanç sağlamakta, fakat herhangi bir saldırı olmadığı zamanda aldıkları güvenlik önlemlerinin bir maliyeti olmaktadır. Belirtilen özellikler bu durumun oyun teorisi tarafından modellemesini uygun kılmaktadır. Bulut bilişimde, ağ güvenliğinde olduğu gibi, saldırganlar ve savunanlar arasında çok önemli bir oyun bağlantısı bulunmaktadır. Savunanın ideal savunma stratejisi ve saldırganın saldırı stratejileri birbirleri ile bağlılık göstermektedir.

Bu çalışmada, saldırganların ve savunanların bu özellikleri kullanılıp, yapılan saldırılar ve alınabilecek güvenlik önlemleri göz önüne alınarak saldırgan ve savunan için ideal stratejilerin belirlenebilmesi için bir model önerilmiştir. Yöntemin kullanılmasıyla ortaya çıkan sonuca göre saldırgan veya savunanın kendi kârını artırarak veya kendine en az zararı verdiren stratejiler ilgili oyuncuların önüne sunulmaktadır. Sonuçta bulut bilişim güvenlik elemanları kazançlarına ve kayıplarına göre karar vererek, gerekli güvenlik önlemlerini geliştirebileceklerdir.

Makalenin organizasyonu aşağıdaki şekildedir: İkinci bölümde oyun teorisinin temelleri ve ilgili çalışmalar verilmiştir. Üçüncü bölümde önerilen oyun teorisi modeli açıklanmıştır. Dördüncü bölümde çalışmayı örneklemek için bir vaka ve analiz sunulmuştur. Sonuç bölümünde yapılan çalışma değerlendirilip, gelecekte yapılacaklar ve geliştirilmesi gereken noktalar aktarılmıştır.

II. BİLGİ GÜVENLİĞİNDE OYUN TEORİSİ VE İLGİLİ ÇALIŞMALAR?

Bilişim teknolojisi güvenliğinde saldırı, saldırgan ile hedef alınan sistemi güvenli yapan savunma sistemi arasındaki etkileşimdir. Savunma sistemleri ve saldırgan aktif oyuncular olmakta iken, hedef alınan sistem ise bütünün basit bir parçası olarak kalmaktadır. Etkileşimli sistemleri inceleyen çalışma oyun teorisidir. Bilişim teknolojisinde güvenlik bir oyunun özelliklerini taşımaktadır. Ekonomi, Biyoloji, Hukuk ve Psikoloji gibi bilimler oyun teorisi tekniklerini kullanmaktadırlar. Bilişim dünyasında ise nüfuz tespit sistemleri ve oyun teorisi çok çalışma yapılan konular arasındadır. Son yıllarda oyun teorisi, ekonomi teori ve bilgisayar bilimleri arasında yapılan çalışmalar Algoritmik Oyun Teorisi [10] alanına yön vermiştir.

Oyun teorisi modellemesinin amacı insanların neden belirli bir şekilde davrandığı ve bu davranışlara göre gelecekte yapacakları davranışlarını açıklamaktır. Bu teorinin arkasında bulunan basit varsayımlar; oyuncular başkaları hakkında inanç oluştururlar, bu varsayımlara göre en iyi cevabı verirler ve oyuncular arasında ortak bir bilgidir. Dolayısıyla, bir oyunda her oyuncu karşısındakinin uygulayacağı stratejiye göre kendi için ideal stratejiyi seçer.

Güvenlik konusunda ise oyun teorisi, savunanın ve saldırganın belirli olasılıklarla seçeceği stratejilere göre, ideal savunma veya saldırı stratejisi seçilmesinde yardım etmektedir. Oyun teorisi, her bir oyuncu için oyunun kıstaslarına göre bir karakteristik fonksiyon oluşturarak, farklı seçeneklerde her bir oyuncunun ne kadar bedel ödediğine veya kazandığını gösterir. Bu bedeller hesaplandıktan sonra bir oyuncunun seçtiği eylem, diğer oyuncuların seçtikleri eylemlere bakıldığında oynanabilecek en iyi seçenek ise, bu eylemin o oyuncu tarafından seçildiği var sayılır. Eğer bu tüm oyuncular için geçerli ise, kısacası, hiçbir oyuncu, rakip oyuncunun stratejisi sabit kaldığı sürece kendi eylemini değiştirerek kazanç sağlayamamakta ise, bu oyunun dengede olduğunu belirtir ve bu dengeye Nash dengesi denmektedir.

Bulut bilişimde güvenlik değerlendirmesi yeni bir konu olduğundan dolayı bu konuda yapılan çalışmalar nispeten yenidir. Yapılan çalışmaların büyük bir kısmı ise sadece bilgisayar kümeleri teknoloji düşünülerek yapıldığından dolayı, bulut bilişimin en önemli yanı olan depolama güvenliği arka planda kalmakta ve genelde statik bir güvenlik değerlendirmesi önerilmektedir.

Kupsch, Miller, Heymann ve César önerdikleri modelde [5], bulut bilişimden daha çok ızgara hesaplama yapan sistemlerde program ile donanım arasında çalışan katmana uygulanmaktadır. Temel olarak bulut bilişimle benzer olsa da, bulut bilişimde, özellikle SoA ve SoP hizmetinde, verilen altyapının üzerine kullanıcılar kendi hizmetlerini kurduklarından dolayı, bu yöntem yetersiz kalmaktadır. Temel olarak bu yöntemde, ilk önce verilen işlerin hangi varlıklarla ilişkiye girdiği ile alakalı bir ağaç çıkarılmaktadır. Sonrasında bu ağaç içindeki her düğümün birbirleri ile ilişkisi incelenmekte ve burada oluşabilecek açıklıklar bulunmaktadır. Daha sonra bu kısımların kodları daha önceden ağaç yönetiminden çıkabilecek açıklıklar göz önüne alınarak uzmanlar tarafından elle incelemektedir. Bu yöntemin en büyük sorunu bulut bilişimde kullanılan uygulama programı arabirimlerinin çok büyük olması ve özellikle SoA ve SoP hizmetlerinde incelemenin kısıtlı olmasının yanı sıra elle inceleme işleminin çok uzun sürmesidir. Ayrıca ızgara hesaplama ile bulut bilişim teknolojileri bazı kısımlarda aynı görevi görse de, riskleri birbirinden farklıdır.

Peiyu ve Dong bulut bilişim için üç katmanlı risk değerlendirme modeli önermişlerdir[3]:

- Katman 1: İlk aşamada problem hiyerarşik bir düzende formülleştirilmektedir. En üst katman ulaşılacak amacı belirtmektedir. Bu modelde ilk katman bütün olarak bulut bilişim platformunu karşılık gelmektedir.
- Katman 2: Bu katman, birinci katmanın değerlendirilmesi için 8 adet özellik içermektedir.
- Katman 3: Karar çerçevesinde somut değerlendirmenin yapıldığı son bölümdür. Üsteki katmanlarla ve özel durumlarla ilgili 39 farklı faktör belirlenmiştir.

AHP gerçekleştirilmesi 3 prensibe bağlıdır: Ayrıştırma, birbirleri ile karşılaştırma ve ağırlık sentezi. AHP yönteminin bulut bilişim mimarisi üzerinde bazı avantajları bulunmaktadır. Bunlar:

- Problemi hiyerarşik parçalara bölebilmek,
- Nitelikli veri bulunmayan durumlarda karar vericinin

deneyimlerinden faydalına bilmek.

Karar vericiye (uzman) bağlı olarak katman 3'deki faktörlere göre değerlendirme yapılır ve hepsine bir ağırlık verilerek bir matriste toplanıp bir ağırlık vektörü elde edilir.

Burada bulunan sorun karar veren kişilerin yaptığı değerlendirmeler tutarlılık doğrulamasından geçmediği sürece, karar verenlerin formlarını tutarlılıktan geçene kadar elle bu vektörleri değiştirmek zorunda kalmalıdır.

III. BULUT BİLİŞİM GÜVENLİĞİNİN OYUN TEORİSİ MODELİ(BBGOTM)

Güvenlik modellemesi yapılırken tehditlerin hesaplanması güvenlik değerlendirmesinin en önemli parçasıdır. Bu ihtiyaçlara göre aşağıdaki varsayımlar yapılmıştır.

- Savunan ve saldırgan bu oyunda birer oyuncu olmaktadır. Birden çok saldırgan var ise bunlar işbirliği yaparak saldırının oluşturulduğu, birden çok savunan var ise işbirliği yaparak savunma oluşturulduğu var sayılmaktadır.
- Her saldırganın saldırı kabiliyeti ortak sayılmaktadır. Böylece tipik saldırılarda her saldırganın eşit saldırı olasılığı bulunmakta ve her tehdit her bir sunucu (veya servis) üzerinde önemli bir risk oluşturmaktadır.
- Yapılan bütün saldırılar eğer bir güvenlik önlemi yok ise başarılı sayılmaktadır.
- Yapılan saldırılar güvenlik cihazları tarafından gerçek zamanlı tespit edilip, durdurulabilecektir.

Oynanan oyunun modeli statik eksik bilgili işbirliksiz sıfır toplam olmayan tipindedir. Saldırgan ve savunan ortaklaşa çalışmayacaklarından dolayı işbirliksiz bir oyundur. Saldırgan ve savunan kendi hareketlerini yaptıklarında, saldırı ve savunma stratejilerinin bir genel maliyeti olacak, bu yüzden karakteristik fonksiyonu sadece kazançları hesaplayarak bir sonuç gösteremeyecektir. Kısacası birinin karı her zaman diğerinin %100 kazancı olmamaktadır. Bu yüzden oyun sıfır olmayan toplam tipli bir oyundur.

Saldırganın kazancı, sistemin kaybettiği değerin belli bir yüzdesi kadar olmaktadır. Bu modelin asıl amacı, bulut sağlayıcıdan alınan kaynakların içinde bulunan veya içine kurulan sistemlere karşı oluşturabilecek bir saldırı sonucunda savunana seçebileceği savunma stratejileri sunmaktır.

Tanım1: $G: (P, S, U)$

a) $P = (1,2,\dots,n)$ saldıran ve savunan tarafındaki oyuncuları göstermektedir.

b) $S = (s_1, s_2, \dots, s_n)$ strateji uzayını göstermektedir ve $\forall x \in P$, $S_x \neq \emptyset$, $S_x = (s_1^x, s_2^x, \dots, s_m^x)$ x oyuncusunun strateji kümesidir.

c) $U = (U_1, U_2, \dots, U_n)$ oyuncuların karakteristik fonksiyonlarıdır.

Tanım2: Önerilen model iki oyunculu statik sonlu işbirliksiz sıfır olmayan toplam tipinde olmaktadır:

$$\text{BBGOTM} = (\{a, d\}, \{S_a, S_d\}, \{U_a, U_d\})$$

Burada a saldırganı, d ise savunanı göstermektedir. $S_a = (s_1^a, s_2^a, \dots, s_n^a)$ saldırganın strateji uzayı, s_i^a bir saldırı stratejisi olmaktadır. $S_d = (s_1^d, s_2^d, \dots, s_n^d)$ savunanın strateji uzayı, s_i^d ise savunanın bir stratejisi olmaktadır. U_a ve U_d ise saldırgan ve savunanın karakteristik fonksiyonlarını belirtmektedir.

A. Saldırı ve Savunmanın Modellenmesi

Ağ güvenliği alanında yapılan çalışmalarda (MIT Lincoln Laboratuvarı Saldırıları) saldırıların sunucular üstündeki etkileri tam olarak bir parametre ile ifade edilememektedir. Bu etkileri belirlemek için günümüz güvenlik dünyasından temel olarak bilinen GBE (Gizlilik, Bütünlük, Elde edilebilirlik) kavramı kullanılacaktır. Bir saldırı sonucunda sunucunun üstündeki etki bu kavramlar ile hesaplanabilir. Saldırıların sınıflandırılmasında temel olarak yapılan saldırının tipi ile ne elde edilmek istendiği ve saldırının stratejik hedefleri değerlendirilmiş ve buna göre her özelliğe 0 ile 1 arasında puan verilmiştir.

Kategori	Tanım	G	B	E
DoS	Dağıtık hizmet engelleme	0	0	1
Kullanıcı	Kullanıcı yetkisi kazanma	0,5	0,1	0,05
Veri	İzinsiz veri yazma ve okuma	1	1	0,2
Yönetimsel	Yönetici yetkisi edinme	1	0,1	0,05
Tarama	Tarama saldırısı	0,3	0	0,2

Tablo 2 - Örnek Saldırı Sınıflandırması

Savunma metotlarını ise savunma işleminin harcadığı zamana ve yapılan işlemin sisteme etkisine göre Tablo 3'de gösterildiği şekilde üçe ayrılmıştır.

Kategori	Tanım	Özellikler
Basit	Sanal makine ayarlarının değiştirilmesi	Gerekli işlem için harcanan zaman az ve sistemin durdurulmasına gerek yok
Orta Seviye	Yeniden başlatma, yönetici yetkisi kullanılarak ayar değiştirilmesi, politika değiştirilmesi, güvenlik güçlendirmesi	Gerekli işlem için harcanan zaman daha uzun, profesyonel bilgi gerekli, sistem gerekirse durdurulabilir
İleri Seviye	Sistem yedeği alma, sanal güvenlik ürünleri kurma veya güncelleme, sistem güncellemesi, virüs taraması	İşlem çok uzun sürmekte, profesyonel bakım gerektirir ve sistem tamamıyla kapatılabilir.

Tablo 3 - Örnek Savunma Sınıflandırması

B. Kazanç Tablosu Hesaplaması

U_{kl}^{a} 'yi saldırganın karakteristik fonksiyonu olarak kabul edersek, B_{kl}^{a} saldırganın saldırıdan kazandığı kazanç, C_{kl}^{a} ise saldırının maliyeti olmaktadır. k ve l simgeleri ise saldırganın k stratejisini ve savunanında l stratejisini seçtiğini gösterir. Aynı şekilde U_{kl}^{d} savunanın karakteristik fonksiyonunu, B_{kl}^{d} savunanın kazancını, C_{kl}^{d} ise savunanın maliyetini belirtmektedir. k ve l simgeleri ise saldırganın k stratejisini ve savunanında l stratejisini seçtiğini gösterir.

Tanım 3: Katılan oyuncuların karakteristik fonksiyonları:

$$U = B - C \quad (1)$$

Yani, saldırganın karakteristik fonksiyonu

$$U_{kl}^{a} = B_{kl}^{a} - C_{kl}^{a} \quad (2)$$

olmaktadır. Savunanın ise

$$U_{kl}^{d} = B_{kl}^{d} - C_{kl}^{d} \quad (3)$$

olmaktadır.

C. Savunanın Kazancı

Saldırı sınıflandırmasına göre bir sunucunun gizlilik, bütünlük ve elde edilebilirlik özellikleri hasar görmektedir. Bu

Strateji	Kazanç
s_k^a, s_l^d	$B_{kl}^{d} = (R_c - L_c) * V_c + (R_I - L_I) * V_I + (R_A - L_A) * V_A$
$s_k^a, -s_l^d$	$B_{kl}^{d} = -((L_C * V_C) + (L_I * V_I) + (L_A * V_A))$
$-s_k^a, s_l^d$	$B_{kl}^{d} = 0$
$-s_k^a, -s_l^d$	$B_{kl}^{d} = 0$

Tablo 4 - Savunanın Kazancı

sunucuya verilen hasarın seviyesi L_C, L_I, L_A şeklinde ve bu sunucunun değeri de aynı cinsten V_C, V_I, V_A şeklinde belirtilirse, bu değerlerin çarpımı sunucunun kaybettiği değer olmaktadır.

Eğer sunucu geri kurtarılır ise, R sunucu kurtarıldığında CIA sınıflandırmasında geri kazanılan değer olarak kabul edilmektedir.

Geri Kazanılan Sunucu Değeri

$$= (R_C * V_C) + (R_I * V_I) + (R_A * V_A) \quad (4)$$

Tablo 4'te gösterilen $s_l^d s_k^a$ saldırı stratejisine karşı başarılı savunma strateji olmaktadır. $-s_l^d$ ise s_k^a saldırı stratejisine göre başarısız savunma stratejisi olmaktadır. $-s_k^a$ ise saldırının uygulanmadığı belirtmektedir.

D. Savunanın Maliyeti

Savunanın aldığı güvenlik önlemlerinin maliyeti olacaktır. Bu maliyetler yapılan sınıflandırmaya göre farklı değerler almaktadır.

Temel olarak maliyetler üç adettir:

- Operasyon Maliyeti (C_O): Harcanan zaman ve hesaplama kaynakları

Strateji	Masraflar
s_k^a, s_l^d	$C_{kl}^{d} = C_O + C_R + C_A$
$s_k^a, -s_l^d$	$C_{kl}^{d} = 0$
$-s_k^a, s_l^d$	$C_{kl}^{d} = C_O + C_R + C_A$
$-s_k^a, -s_l^d$	$C_{kl}^{d} = 0$

Tablo 5 - Savunanın Maliyeti

- Sunucu Geri Kazanım (C_R): İşlem için harcanan masraflar (maddi maliyet)

- Sistem kullanılabilirliği (C_A): Sistemin kapatılmasından doğan masraflar (zararlar)

E. Saldırganın Kazancı

Saldırganın kazancı savunma sisteminin kaybı olmaktadır. Yani sunucu veya sistemin değer kaybıdır. Fakat GBE değerlendirmesinde kaybedilen her değer, tam olarak saldırgan tarafından kazanılmayabilir. Bu yüzden $z \in [0,1]$ kaybedilen değerin ne kadarının saldırgan tarafından kazanıldığı gösteren bir değer olarak tanımlar isek, saldırganın kazancı

Strateji	Kazanç
s_k^a, s_l^d	$B_{kl}^{a} = k((R_c - L_c) * V_c + (R_I - L_I) * V_I + (R_A - L_A) * V_A)$
$s_k^a, -s_l^d$	$B_{kl}^{a} = k((L_C * V_C) + (L_I * V_I) + (L_A * V_A))$
$-s_k^a, s_l^d$	$B_{kl}^{a} = 0$
$-s_k^a, -s_l^d$	$B_{kl}^{a} = 0$

Tablo 6 - Saldırganın Kazancı

$B^a = -k * B^D$ olmaktadır.

F. Saldırganın Masrafı

Saldırgan saldırıyı yapabilmesi için gerekli aletlere sahip olması ve saldırı için ihtiyaç duyulan zaman saldırının operasyon maliyetini belirtir. Ayrıca saldırı savunan tarafından tespit edilirse, saldırgan kendini ifşa ettiğinden dolayı bir ceza

Strateji	Masraflar
s_k^a, s_l^d	$C_{kl}^{a} = C_{AO} + C_D$
$s_k^a, -s_l^d$	$C_{kl}^{a} = C_{AO}$
$-s_k^a, s_l^d$	$C_{kl}^{a} = 0$
$-s_k^a, -s_l^d$	$C_{kl}^{a} = 0$

Tablo 7 - Saldırganın Maliyeti

bedeli ödemektedir.

IV. UYGULAMA ÖRNEĞİ VE DEĞERLENDİRME

Güvenlik değerlendirmesi yöntemini tanıtmak için bir senaryo oluşturulmuştur. Bu senaryoda farklı iki modelde hizmet veren bulut sağlayıcıların içinde bulunan bir veri tabanı sunucu değerlendirilmiştir.

Bu deneyde bulut içinde bulunan veri tabanı sunucularının değerleri Tablo-8'deki gibi alınmıştır.

Servis olarak yazılım modeli içinde bulunan veri tabanı sunucusunda, bulut sağlayıcı sunucunun bütünün

güvenliğinden sorumlu iken (bknz. Tablo-1), servis olarak altyapı sağlayan bulut sağlayıcı ise sadece sunucunun mevcut olma güvenlik özelliğinden sorumlu olmaktadır. Bu yüzden dolayı iki farklı hizmet modelinde aynı sunucu farklı varlık değerlerine sahiptir. Burada unutulmaması gereken önemli bir nokta ise, bir SoA sistemin üstüne SoY sistem kurulabilmesidir. Yani bir SoY firması gerekli altyapıyı SoA hizmeti veren bir bulut sağlayıcısından alabilmektedir. Bu durumda güvenliğin büyük kısmı SoY hizmeti veren firma veya SoA hizmetini satın alan kullanıcı üzerine düşmektedir.

	Gizlilik	Bütünlük	Mevcut Olma
SoY VT	100	100	60
SoA VT	20	80	100

Tablo 8 - Farklı Servis Modellerindeki Sunucuların Varlık Değerleri

Sunucular üstünde CVE-2012-0116 [12] açıklığı bulunduğu varsayılmıştır. Bu açıklığa uygun saldırı modeli Tablo-2'de yer alan veri kategorisinde bulunan izinsiz veri yazma ve okuma olarak seçilmiştir. Bu saldırının vereceği hasar seviyeleri sırayla $L_C = 1$, $L_I = 1$, $L_A = 0{,}2$olmaktadır. Bazı parametreler deneyimlere bağlı olarak verilmiştir: $R_C = 1$, $R_I = 1$, $R_A = 0{,}4$.

Açıklığı gidermek için gereken işlemin maliyeti ise sırayla $C_O = 60$, $C_R = 70$, $C_A = 50$ olmaktadır. Saldırının işlem maliyeti ise $C_{AO} = 30$ olmakta ve saldırgan tespit edildiği zaman ise $C_D = 50$ ceza ödemektedir.

	Savun	Önlem Alma
Saldırı Yap	$-92, -168$	$194, -224$
Saldırma	$0, -180$	0,0

Tablo 9 - SoY VT Sunucusu Çözüm Matrisi

Saldırganın ve savunanın karakteristik fonksiyonları hesaplandıktan sonra ortaya çıkan sonuç matrisleri Tablo 9 ve Tablo 10'da gösterilmiştir.

Nash dengesine göre, her sonlu oyunda en az bir denge noktası bulunmaktadır. Tablo 10'da gösterilen SoA matrisinin tanımladığı oyunu oyuncuların birbirlerinin oynadığı hareketlere verebilecekleri en iyi cevapları göstererek çözebiliriz. Eğer saldırgan saldırıyı gerçekleştirir ise, savunanın önlem almaması kendi çıkarı açısından daha iyi sonuç vermektedir. Eğer savunan önlem almaz ise, saldırganın kendi çıkarı açısından saldırması saldırmamasına göre daha iyi sonuç vermektedir. Bu yüzden dolayı matrisin sağ üst kısmı Nash dengesidir.

	Savun	Önlem Alma
Saldırı Yap	$-100, -160$	$110, -140$
Saldırma	$0, -180$	0,0

Tablo 10 - SoA VT Sunucusu Çözüm Matrisi

Bu tip oyunlarda ya katkısız strateji Nash dengesi veya karma Nash dengesi bulunmaktadır. SoY çözüm matrisinde ise SoA çözüm matrisindeki gibi katkısız strateji Nash dengesi bulunmamaktadır. Karma Nash dengesi SoY matrisi uygulandığında, savunanın 0,68 olasılıkla savun seçeneğini seçmesi saldırganın saldırı yap ve saldırma seçeneklerinin bedelleri eşitlemektedir. Bu yüzden saldırgan saldırsa da saldırmasa da aynı bedeli almaktadır. Aynı şekilde saldırgan 0,79 olasılıkla saldırı gerçekleştirir ise, savunanın güvenlik önlemi alması ve alamaması arasında bir bedel farkı bulunmamaktadır.

Kısacası eğer savunan kişi elindeki sistemlerin %68'inin üzerinde güvenlik önlemi aldığı takdirde, saldırgan saldırmadığı takdirdeki bedeli saldırdığı takdirdeki ödediği bedelden fazla olmaktadır. Elde edilen bu sonuç savunmanın güvenlik önlemlerini planlamasında kullanılabilecektir.

Önerilen modelin diğer yöntemlere göre üstün yanı, varlığa verilen değere göre ve varlığın vereceği hizmete göre güvenlik önlemleri alınabilmesidir. Böylece bulut bilişimde farklı hizmet modellerinde, o sistemin güvenliğinden sorumlu şahıs veya kuruluşlar sorumlu oldukları alan kadarı ile güvenlik önlemi almaktadır. Kısaca, bulut bilişimde hizmet modellerinin gerektirdiği ihtiyaçlara göre ve kullanan şahıs veya kurumların isteklerine göre ölçeklendirebilir güvenlik sağlanmaktadır. Bütün sistem üzerinde uygulanacak ve uzun sürecek ve güvenlik değerlendirme yöntemi kısaltılmakta ve dinamikleştirilmektedir.

V. SONUÇ VE ÖNERİLER

Günümüz yöntemleri bulut bilişimde saldırgan ve savunanın kazançlarını ve masraflarını ön plana çıkarmamaktadır. Bu çalışma, bulut bilişim kullanılması durumda ideal güvenlik önlemlerinin bulunmasında yardım etmektedir. Önerilen modelde ekonomide çok sık kullanılan oyun teorisini kullanarak saldırgan ve savunanın çıkar modellemesi yapılmıştır. Savunanın ideal güvenlik stratejisi sunucu değerlerine ve sunucu üstündeki saldırı risklerine bakılarak hesaplanmıştır. Bu model, sabit olarak sadece bulut bilişimdeki objelerin birbirleri ilişkilerine bakarak, aralarında oluşabilecek riskleri bulut bilişimin altyapısını oluşturan devasa kod üzerinde aramaktan daha hızlı ve verimli olmaktadır.

Saldırganın yapacağı farklı tipteki saldırıları çözüm matrisinde farklı satırlara konarak ve buna karşı savunanın uygulayabileceği güvenlik önlemler de farklı sütunlara konarak çözüm matrisi büyütülmesi gelecekte yapılacak çalışmalar arasındadır. Bu şekilde ortaya çıkan matriste, saldırganın saldırılarından cayması için savunanın hangi güvenlik önlemini hangi sistemin en azından ne kadarına uygulaması gerektiği hesaplanacaktır. Karakteristik fonksiyonun oluşturan değişkenlerin bulut sağlayıcının geçmişinden öğrenerek, bulut sağlayıcının verdiği hizmet modeline uygun sonuçlar verebilmesi de gelecekte yapılacak çalışmalar arasındadır.

KAYNAKLAR

[1] P. Mell and Timothy Grance, "The NIST definition of cloud computing" National Institute of Standards and Technology Special Publication 800-145, Sept. 2011

[2] S. and Eloff, M.M. and Smith, E. Ramgovind, "The management of security in Cloud computing," Information Security for South Africa (ISSA), 2010, vol. 1-7, 2010.

[3] LIU Peiyu, LIU Dong, The New Risk Assessment Model for Information System in Cloud Computing Environment, Procedia Engineering, Volume 15, 2011, Pages 3200-3204, ISSN 1877-7058,

[4] Sajjan Shiva, Sankardas Roy, and Dipankar Dasgupta. 2010. Game theory for cyber security. In Proceedings of the Sixth Annual Workshop on Cyber Security and Information Intelligence Research (CSIIRW '10), Frederick T. Sheldon, Stacy Prowell, Robert K. Abercrombie, and Axel Krings (Eds.). ACM, New York, NY, USA, , Article 34 , 4 pages

[5] James A. Kupsch, Barton P. Miller, Elisa Heymann, and Eduardo César. 2010. First principles vulnerability assessment. In Proceedings of the 2010 ACM workshop on Cloud computing security workshop (CCSW '10). ACM, New York, NY, USA, 87-92

[6] European Network and information Security Agency, "Cloud Computing Security Risk Assessment".

[7] P.G. Dorey, A. Leite, Commentary : Cloud computing – A security problem or solution?, Information Security Technical Report, Volume 16, Issues 3–4, August–November 2011, Pages 89-96, ISSN 1363-4127

[8] Cloud Security Alliance, "Security Guidance for Critical Areas of Focus in Cloud Computing 3.0".

[9] Armando Fox, Rean Griffith, Anthony D. Joseph, Randy Katz, Andy Konwinski, Gunho Lee, David Patterson, Ariel Rabkin, Ion Stoica, and MateiZaharia Michael Armbrust, "Above the Clouds: A Berkeley View of Cloud Computing," Commun. ACM 53, 4 , pp. 50-80, April 2010.

[10] Nisan N, Roughgarden T, Tardos E, Vazirani V, editors. Algorithmic game theory. Cambridge University Press, 2007

[11] Dan Svantesson, Roger Clarke, Privacy and consumer risks in cloud computing, Computer Law & Security Review, Volume 26, Issue 4, July 2010, Pages 391-397, ISSN 0267-3649

[12] http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-0116

[13] DimitriosZissis, DimitriosLekkas, Addressing cloud computing security issues, Future Generation Computer Systems, Volume 28, Issue 3, March 2012, Pages 583-592, ISSN 0167-739X

[14] S. Chen, B. Mulgrew, and P. M. Grant, "A clustering technique for digital communications channel equalization using radial basis function networks," *IEEE Trans. Neural Networks*, vol. 4, pp. 570–578, Jul. 1993.

DSAB – An Efficient Approach for Security in MANET

Gulshan Kumar, Rahul Saha, Mritunjay Kumar Rai

Department of Computer Science and Engineering

Lovely Professional University, Phagwara, Punjab, India

gulshan_acet@yahoo.com , rsahaaot@yahoo.com, raimritunjay@gmail.com

Abstract- **With the increasing demand of mobile usage, it is highly recommended to ensure the security of the data transmission. As security factors have a great impact in performance analysis of the wireless network, it is necessary to use proper security mechanism with each wireless network applications. For this reason it is a concern to generate such a security mechanism which will be easy to implement, energy efficient, and robust enough against the malicious attack. In our following paper we have introduced our novel security approach by using digital signature with Blowfish algorithm (DSAB) and compared its performance with existing encryption techniques like AES, DES.**

Keywords- **DSAB, DSA, Blowfish, efficiency, energy, encryption.**

I. INTRODUCTION

In this present era, mobility is a main issue of our life. Day by day the increasing rate of mobile users and other mobile entities creates a great concern on the issue of security. MANET or Mobile Ad hoc Networks is a unstructured dynamic network comprises of mobile nodes that can join or walk out any time in the network. So, MANET is likely to be vulnerable to the malicious activities of intruders. But with the growth of this kind of network, it is necessary to provide a security mechanism for MANET in such a way which can provide strong authorization property and security [1, 3] too along with other constraints like energy-efficient, low-cost, easy implementable etc. So, we have chosen DSA (digital signature algorithm) for authorization and verification of identity and Blowfish algorithm for encryption purpose.

A. *Security Attacks in MANET*

The present attacks on MANET highly concentrated around DoS. The different types of attacks are listed below.

TABLE I

Attacks in MANET

Layer	Attacks
Application layer	Repudiation, data corruption
Transport layer	Flooding
Network layer	Worm hole , Black hole
Data link layer	Traffic analysis
Physical layer	Eavesdropping, Jamming
Multilayer	DoS

Repudiation

Non-repudiation refers to the fact of denying transmission of a message or a data packet. It is a kind of passive attack.

Data corruption

Data corruption occurs due to some modification, fabrication operation by the intruders in the transmitted data. Intruders actively take part in this kind of attacks and therefore it is an active attack.

Flooding Attack

The malicious node which is may be or may not be a part of a MANET may send huge number of request packets to a node which is part of the network and thus may disrupt the availability of the service of the victim node. This attack is

a form of denial of service attack. Fig.1 represents flooding attack.

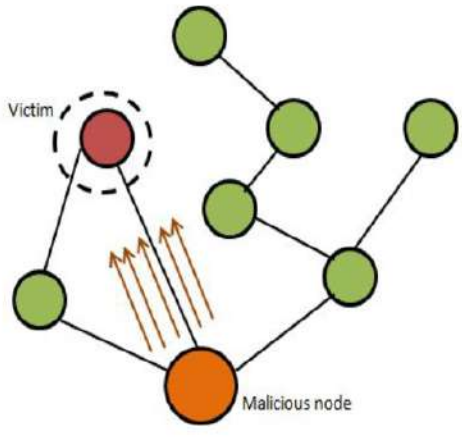


Fig.1.Flooding Attack

Worm hole

In this attack intruders are more than one with a high speed link in use. Requests go through the attacker zone to the destination using the high speed link. Destination confirms this false high speed link as an optimum route and replies back. As a result, all data transmission is open to the malicious nodes. Fig.2 represents a schematic diagram for worm hole attack.

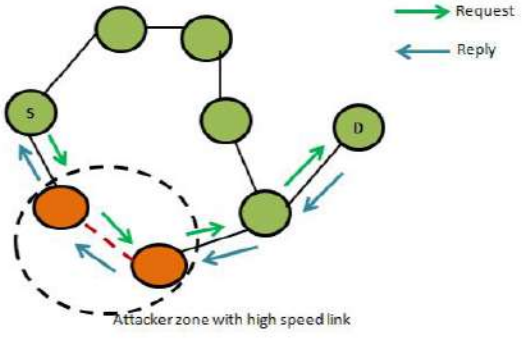


Fig.2. Wormhole attack

Black hole

The entire data pass through the malicious node as it claims itself to be the optimum route by fabricating the sequence number in packets higher than the other nodes and sends fake reply to the source. Fig.3 represents black hole attack.

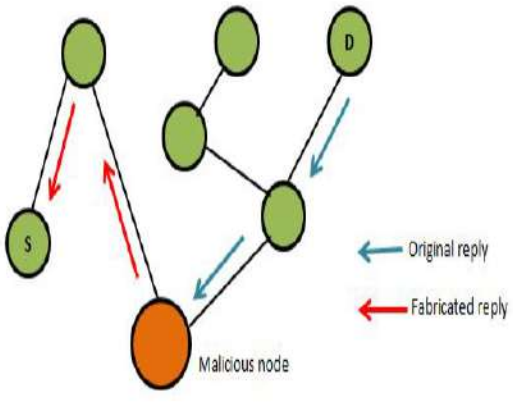


Fig.3. Black hole attack

Traffic analysis

The intruder attempts to guess the traffic being transmitted between the sender and receiver. It is a passive attack which is difficult to detect but easy to defense by implementing required encryption technique. Fig.4 represents traffic analysis scheme.

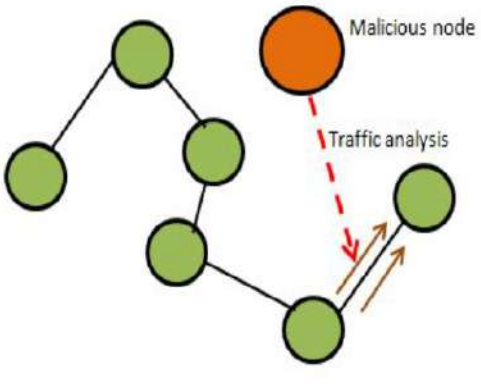


Fig.4.Traffic analysis

Eavesdropping

Eavesdropping attack in MANET shares the wireless medium, as wireless medium make it more vulnerable for MANET malicious nodes to intercept. The attacker node intercepts the transmission as every MANET node is equipped with transceiver in range of the communication which can be decode by means of malicious node to target the authorized node on the network, malicious node can obtain the sensitive information etc. modify the routing route or poison the routing table.

Jamming

Jamming is one of many exploits used compromise the wireless environment like MANET. It works by denying service to authorized users as legitimate traffic is jammed by the overwhelming frequencies of illegitimate traffic. Jamming can result in denial of service attack.

Denial of Service

It is an extended version of jamming attack. It can occur in any layer. Denial of Service refers to the situation where a service is made unavailable to the legitimate users by sending huge number of requests to the service at a time.

B. *Security Services*

Authentication refers to the confirmation and verification of the identity of the communicating parties. Peer-to-peer authentication is confirmed at the establishment or at the run time of a data transmission. Data origin authentication confirms the source identity.

Confidentiality refers to the maintenance of the privacy of the message being transferred from source to destination so that the message content is not revealed to a third party.

Integrity is defined in the term of originality of the message i.e. the message must be transmitted from source to destination without any alteration (in the same way as created and sent by the sender).

Non-repudiation deals with storing the proof of data transmission by both sender and the receiver so that neither of them can deny its responsibility later.

Availability ensures the presence of network services despite of security attacks.

II. DSAB (DSA with Blowfish)

From the discussion of the security attacks, we can say that MANET is vulnerable to the malicious activities. Using a strong authentication algorithm along with an encryption technique can overcome the security problems. Therefore, we have chosen DSA (Digital Signature Algorithm) for authentication purpose and Blowfish algorithm for encryption.

A. *Digital Signature Algorithm (DSA)*

Digital Signature Algorithm (DSA) [2] is based on logarithmic computations and therefore hard to break in. The requirements for DSA are classified into four categories and are listed Table II.

TABLE II
Requirements for DSA

Global Public key components (p, q, g)	p is a prime number ranging $2^{L-1} < p < 2^{L}$ where L is the bit length of p ranging from $512 \le L \le 1024$ and integer multiple of 64 q is a prime divisor of (p-1) where $2^{139} < q < 2^{160}$ g is a generator of the subgroup of the order q mod p such that $1 < g < p$
Users' private key (x)	x is a random or pseudorandom integer ranging $0 < x < q$
Users' public key (y)	$y = g^{x} \bmod p$
Users' per message secret number (k)	k is a random or pseudorandom integer ranging $0 < k < q$
Global Public key components (p, q, g)	p is a prime number ranging $2^{L-1} < p < 2^{L}$ where L is the bit length of p ranging from $512 \le L \le 1024$ and integer multiple of 64 q is a prime divisor of (p-1) where $2^{139} < q < 2^{160}$ g is a generator of the subgroup of the order q mod p such that $1 < g < p$
Users' private key (x)	x is a random or pseudorandom integer ranging $0 < x < q$
Users' public key (y)	$y = g^{x} \bmod p$
Users' per message secret number (k)	k is a random or pseudorandom integer ranging $0 < k < q$

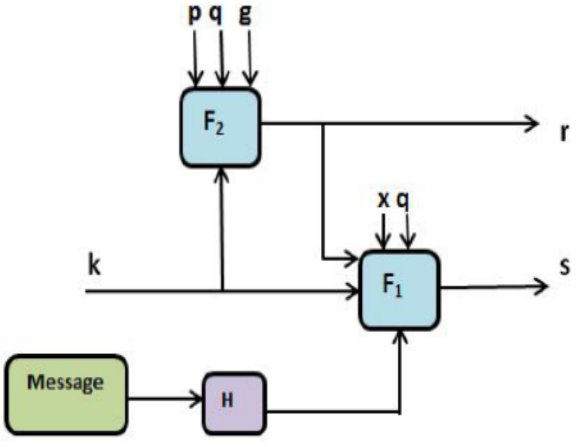


Fig.5 Signing in DSA (sender)

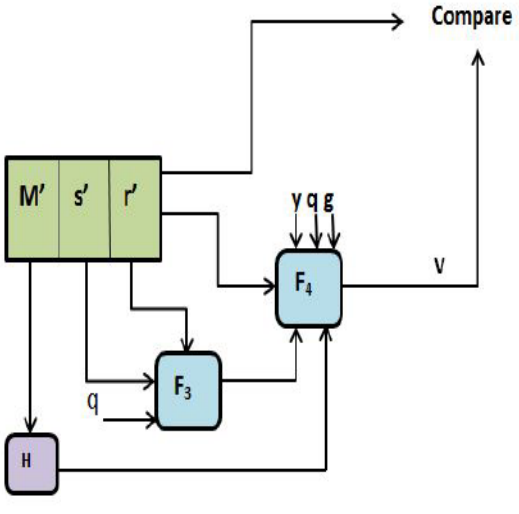


Fig. 6. Verification Process (receiver side)

DSA algorithm has two stages. In the first stage, message is signed by the sender. Fig.5 represents the signature process and functions in DSA in sender side. This signature (r, s) along with the message (M) is transmitted to the receiver. The receiver receives a triplet of { M', r', s'} where M', r', s' are the received versions of M, r and s respectively. The second stage occurs at receiver side by verifying the signature of the message shown in Fig.6. The different functions used in different stages are shown in Table III.

Table III
Functions used in DSA

Signing	$r = F_2(k, p, q, g) = (g^k \bmod p) \bmod q$ $s = F_1(H(M), x, r, q, k) = (k^{-1}(H(M) + xr)) \bmod q$ Signature= (r, s)
Verification	$w = F3(s', q) = (s')^{-1} \bmod q$ $v = F4(y, p, g, w, r', H(M')) = [(g^{[H(M')w] \bmod q} y^{(r')w \bmod q}) \bmod p] \bmod q$ Test v = r'

B. *Blowfish Algorithm*

Blowfish a symmetric key block cipher using 64 bits of data blocks and a variable size key maximum up to 448 bits. It comprises of Feistel Network having 16 times iterative operations of a simple encryption function. The prime characteristics of Blowfish algorithm is that it includes key dependent S-boxes and has a complex key schedule which makes the algorithm stronger.

Encryption

The data block of 64 bits are first divided into two halves of 32 bits each. Each line in the diagram of the Blowfish algorithm represents 32 bit data. It uses two sub key arrays 18-entry P-array and 256-entry S-boxes. The S-boxes convert the 8 bit input into 32 bits output. One entry of P-array is compulsory for each of 16 rounds as shown in the Fig.7. The remaining two P-array entries are used after the final round to separately XOR the outputs of each of the halves of the data block of 32 bits. In the function F, four S-boxes and two types of bit operations: XOR and addition of modulo 2^{32} are used. The function F first divides the input of 32 bits into four S-boxes of consisting 8 bits each. The outputs of first and second S-boxes are first added to modulo 2^{32} and the output is XOR ed with the third S-box output. The result of XOR operation and the output of fourth S-box is finally added to modulo 2^{32} and we get the final 32 bit output from the function F. The round function operation is shown in Fig.8.

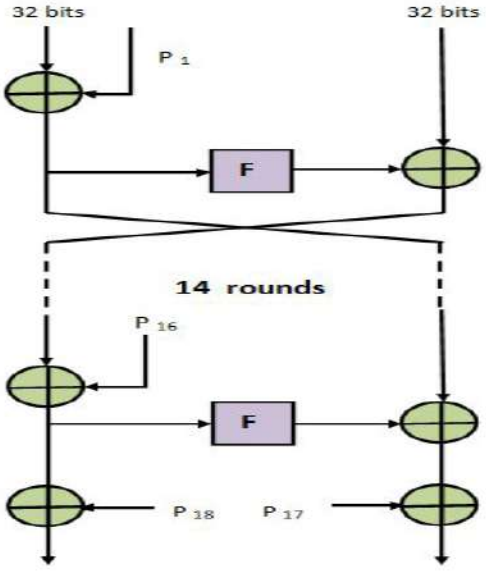


Fig.7 Blowfish Algorithm

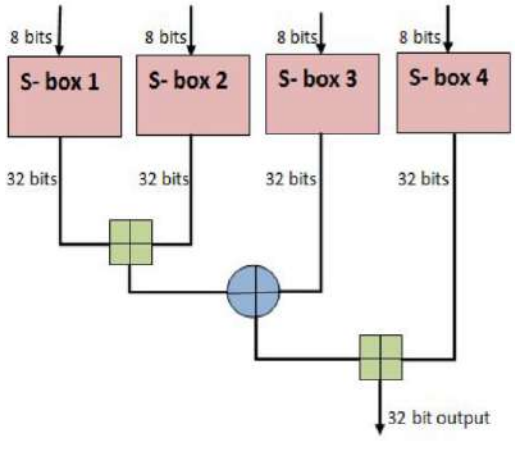


Fig.8 Round function F in Blowfish

The key schedule of Blowfish algorithm starts by initializing the P-array and S-boxes with values derived from the hexadecimal value of pi (∏). The secret key is then byte wise XOR-ed with all the P-entries in order. Many implementations may support 576 bit key size as the P-array is 576 bits long (18 * 32 bits) and the bytes are XOR-ed with all these bits.

Decryption

Decryption is exactly the same as encryption technique except the P1, P2 …… P18 are used in reverse order.

C. Merging of Blowfish and DSA

In wireless network environment messages or data are transmitted in form of packets. The attacks in the MANET environment are due to basically fabrication or modification in data and unauthorized mobile node interception. So, it is needed to utilize the both authentication and encryption. The sender creates a data packet and encrypts with Blowfish Algorithm. The encrypted data is then digitally signature by the sender where a random number is generated per message and keep secret. So, any other third party cannot break through it as the secret number is unknown to the third party. To gain access to the message the third party must need the secret number. So, authentication and encryption both are utilized to make the transmission secure enough.

III. RESULTS

For the purpose of simulation we have used NS-2. While simulating we had a network of 100 nodes on 1500 X 1000 area size where the radio range is 200 m and simulation time is 60 seconds considering Constant Bit Rate (CBR). The packet size is considered of 512 bytes. We also considered Taking Random Way Point Mobility Model and varying speed to 10, 20, 30, 40, 50 m/s where Pause time is 5 m/s. We have analyzed the performance of DSAB based on the efficiency in terms of robustness to the attacks, the speed of the algorithm, energy consumption. For this we have considered the packet size of 64 bits, key size of 64 bits and 16 rounds of operation. We have also compared our algorithm with other encryption algorithm like AES and DES. The results are shown below.

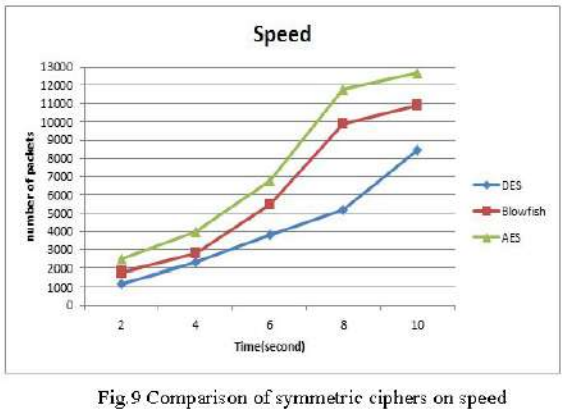


Fig.9 Comparison of symmetric ciphers on speed

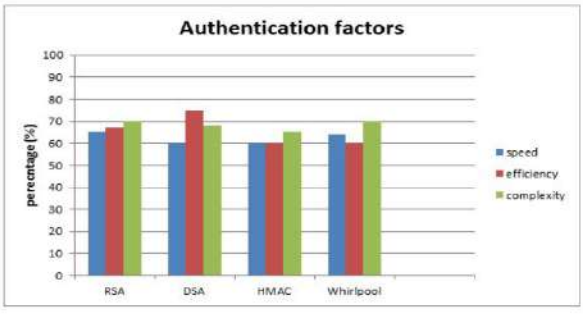


Fig.10 Comparison of authentication protocols

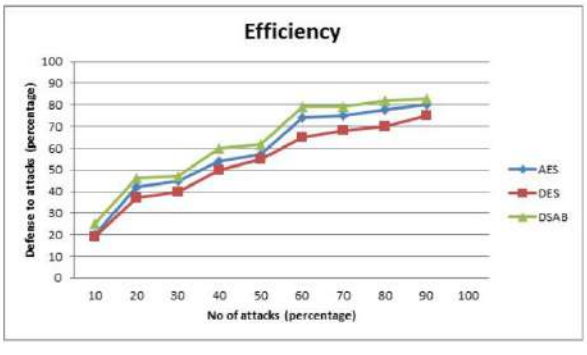


Fig.11 Comparison of DSAB with AES and DES

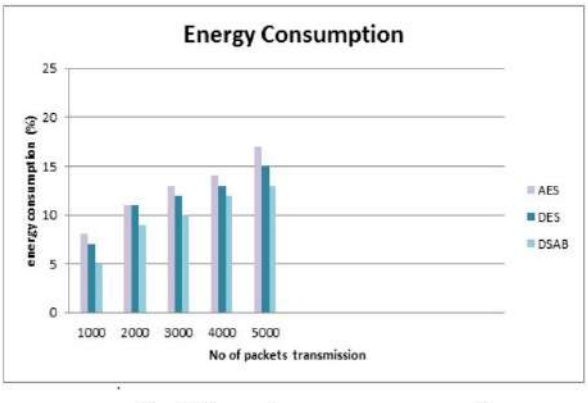


Fig.12 Comparison on energy consumption

According to the statistical analysis of the results found during the experiment and simulation of the work, DSAB is near about 15 % more efficient than the other approaches compared here. It is also observed that power consumption of DSAB is near about 25 % less than AES or DES. From the above results of our work, we can easily say that our approach of DSAB is quite efficient to defense the security attacks along with low energy consumption.

IV. CONCLUSION

From the above discussion, we can state that our DSAB approach can provide security, confidentiality and authentication. Though the speed of AES is higher than the Blowfish, still we are using it as the energy consumption is low for Blowfish and it can provide same level of security as like AES and with DSA its performance gets better as we have seen above. In future, we would like to work on the complexity levels of the algorithms used here.

REFERENCES

[1]H.M. Kader and M.M. Hadhoud, "Performance Evaluation of Symmetric Encryption Algorithms," Performance Evaluation, pp. 58-64, 2009.

[2] W. Stallings, "Cryptography and Network Security 4th Ed," Prentice Hall , 2005,PP. 58-309 .

[3] M.N. Islam, M. Mia, M. Chowdhury, M.A.Matin, "Effect of Security Increment to Symmetric Data Encryption through AES Methodology"Ninth ACIS International Conference on Software Engineering, Artificial Intelligence, Networking, and Parallel/Distributed Computing, 2008(SNPD '08). 6-8 Aug. 2008,PP.291 – 294, Phuket, Thailand.

[4] Wander, A.S., Gura, N., Eberle, H., Gupta, V., and Shantz, S.C., "Energy Analysis of Public-Key Cryptography for Wireless Sensor Networks", In proceedings of PerCom pp. 324-328, 2005.

[5] S. Hirani, "Energy Consumption of Encryption Schemes in Wireless Devices Thesis," university of Pittsburgh, April 9, 2003. Retrieved October 1,2008.

[6] Gulshan Kumar, Mritunjay Kumar Rai, "An Approach to provide Security in Mobile Ad Hoc Networks using Counter Mode of Encryption on MAC Layer", International Journal of Network Security & Its Applications (IJNSA), Vol.3, No.4, July 2011

BIBLIOGRAPHY



Gulshan Kumar is pursuing his M.Tech degree in Computer Science and Engineering from Lovely Professional University, Jalandhar, India. His research interest includes Cryptography and Mobile Ad hoc Networks.



Rahul Saha is pursuing his M.Tech from Lovely Professional University, Punjab, India in the department of Computer Science and Engineering. His research interest includes Software Engineering, Network Security and Cryptography.



Mritunjay Kumar Rai received his Ph.D. Degree from ABV-Indian Institute of Information Technology and Management, Gwalior, India. Currently he is working as an Assistant Professor in Lovely Professional University. His research interest area is Mobile Ad hoc Networks and Wireless Sensor Networks.

Siber Güvenlik ve Savunma
Cyber Security and Defence

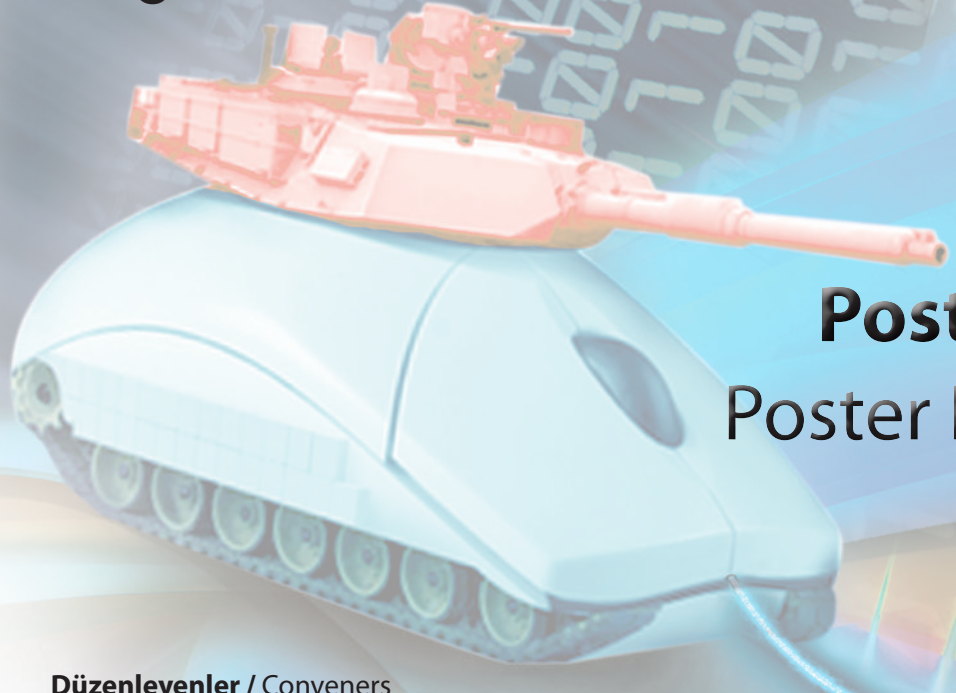
BİLGİ GÜVENLİĞİ VE KRİPTOLOJİ KONFERANSI
ISC Turkey

5. Uluslararası Bilgi Güvenliği ve Kriptoloji Konferansı

5th International Conference on Information Security & Cryptology

17-18 Mayıs
May 2012

ODTÜ Kültür ve Kongre Merkezi
METU Culture and Congress Center
Ankara-TURKEY



Poster Bildiriler
Poster Presentation

Düzenleyenler / Conveners

T.C. ULAŞTIRMA DENİZCİLİK VE HABERLEŞME BAKANLIĞI

BİLGİ GÜVENLİĞİ DERNEĞİ

Destekleyenler / In Collaboration with

IPv6 Security Vulnerabilities

Harith A. Dawood[1]

Abstract*--Internet Protocol version 6 (IPv6) is the newest version of the protocol that is used for communications on the Internet. And it has been in existence for many years. But, currently many organizations have slowed their migration to IPv6 because they realize that the security considerations and products for IPv6 might be insufficient, despite the fact that the network infrastructure is ready to support IPv6 transport. They realize that they cannot deploy IPv6 without first considering the security of this protocol. IPv6 security vulnerabilities currently exist, and as the popularity of the IPv6 protocol increases, so do the number of threats. This paper covers and reviews some of the fundamental vulnerabilities topics of IPv6 security, considerations, issues and threats. At the end, it concludes summarizing some of the most common security concerns the new suite of protocols creates.

Index Terms -- IPv6, IPsec, Network Security, Security Vulnerabilities.

1. INTRODUCTION

IPv6 defined in the mid-1990s in Request for Comments (**RFC**) 2460 "Internet Protocol, Version 6 (**IPv6**) Specification" and a host of other more recent RFCs, is an "improved, streamlined, successor version" of IP version 4 (**IPv4**).

IPv6 offers the potential of achieving increased scalability, reach ability, end-to-end interworking, Quality of Service (**QoS**), and commercial-grade robustness for data communication, mobile connectivity, and for Voice over IP (**VoIP**). The current version of the Internet Protocol, IPv4, has been in use successfully for almost 30 years and exhibits some challenges in supporting emerging demands for address space cardinality, high-density mobility, multimedia, and strong security.

IPv6 is an improved version of IP that is designed to coexist with IPv4 while providing better internetworking capabilities than IPv4, and resolving unanticipated IPv4 design issues and takes the Internet into the 21st Century [2],[3].

IPv6 was initially developed because of the anticipated need for more end system addresses based on anticipated Internet growth, encompassing mobile phone deployment, smart home appliances, and billions of new users in developing countries.

IPv6 features include the following [4], [11], [14]:

1. Expanded Addressing Capabilities. IPv6 increases the IP address size from 32 bits to 128 bits.
2. Header Format Simplification.
3. Authentication and Privacy Capabilities. In IPv6, security is built in as part of the protocol suite: extensions to support authentication, data integrity (encryption), and (optional) data confidentiality are specified for Internet Protocol Security (**IPsec**). IPsec is a set of protocols and was originally developed as part of the IPv6 specification. IPsec is mandated as required in IPv6 while it is optional in IPv4, which means, "IPv6 is more secure."
4. Flow Labeling Capability.
5. Improved Support for Extensions and Options (with greater flexibility for introducing new options in the future).

Additionally, there are many others IPv6 features [12], [13], [15]:

- Stateless auto-configuration: The ability for nodes to determine their own address.
- Multicast: Increased use of efficient one-to-many communications.
- Jumbograms: The ability to have very large packet payloads for greater efficiency.
- Mobility: Simpler handling of mobile or roaming nodes.

IPv6 is a technology now being deployed in various parts of the world that will allow truly explicit end-to-end device addressability. IPv6 becomes an institutional imperative in the final analysis. But the security considerations continue to be critically important.

2. IPv6 SECURITY VULNERABILITIES

The security features of IPv6 are described in the Security Architecture for the Internet Protocol (RFC 2401, RFC 2402, and RFC 2406), but we will describe the real IPv6 security issues:

2.1 TRACKING THE IDENTITY OF THE USER

Traditional interface identifiers for network adapters use a 48-bit address called an IEEE 802 address. It consists of a 24-bit company ID (also called the manufacturer ID), and a 24-bit extension ID (also called the board ID). The combination of the company ID, which is uniquely assigned to each manufacturer of network adapters, and the board ID, which is uniquely assigned to each network adapter at the time of assembly, produces a globally unique 48-bit address. This 48-bit address is also called the Media Access Control (**MAC**) address.

In today's IPv4-based Internet, a typical Internet user connects to an Internet Service Provider (**ISP**) and obtains an IPv4 address using the Point-to-Point Protocol (**PPP**) and the Internet Protocol Control Protocol (**IPCP**). Each time the user connects, a different IPv4 address might be

[1] Manuscript received March 1, 2012

Harith A. Dawood, I.T. Department, British Royal University for Science and Technology, Erbil, IRAQ. *Harith.dawood@hotmail.com*.

obtained. Because of this, the identity of users on the Internet is often unknown. So, it is difficult to track a dial-up user's traffic on the Internet on the basis of IP address [6]. And this has created an environment where attackers can easily operate, without their targets knowing much about the source of the messages.

Also, the use of Network Address Translation (**NAT**) is often misunderstood as a security protection measure because it hides the internal addresses and thus secures the internal network topology. NAT breaks the use of the full end-to-end communication model that IP Security (**IPsec**) needs to be fully effective.

For IPv6-based dial-up connections, the user is assigned a 64-bit prefix after the connection is made through router discovery and stateless address auto-configuration. If the interface identifier is always based on the EUI-64 address (as derived from the static IEEE 802 address) as shown in figure 1, it is possible to identify the traffic of a specific node regardless of the prefix, making it easy to track a specific user and their use of the Internet.

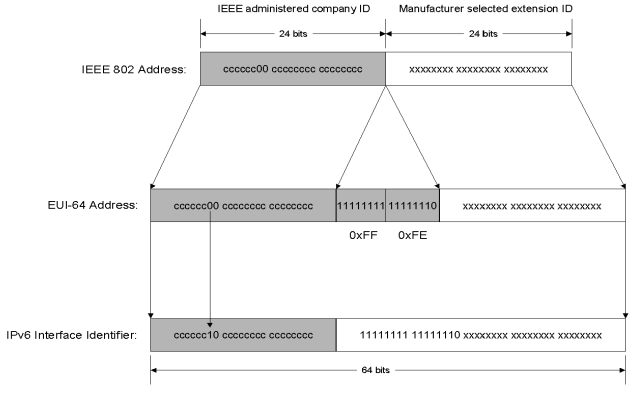


Figure 1: The conversion of a universally administered, unicast IEEE 802 address to an IPv6 interface identifier.

2.2 IPv6 Address Spoofing (MAC Address Spoofing) Vulnerability

Because of IPv6 address depends on MAC address which in a sense the MAC address is a computer's true name on a LAN. A person might want to change the MAC address of a NIC for many reasons:

1. To get past MAC address filtering on a router.
2. Sniffing other connections on the network.
3. To keep their burned in MAC address out of IDS and security logs.
4. To pull off a denial of service attack.

Therefore, many people changing their MAC address in different operating systems (Window XP/Vista, Linux and Mac OS X) either manually or by software. Unfortunately, this is privacy risk, because anyone who has your MAC address also has your IP address!

2.3 Large Address Space

Port scanning is one of the most common techniques in use today. Port scanning allows "black-hats" to listen to specific services (ports) that could be associated to well-known vulnerabilities. In IPv6 networks, IPv6 subnets use 64 bits for allocating host addresses. Scanning such a large address space (2^{64}) is not absolutely impossible [8].

The hacker community has started exploring IPv6, and they are constructing tools that leverage weaknesses, back doors and bypass firewalls in the protocol. In fact, IPv6 capabilities have started to be added to several popular hacker tools. Many of these IPv6 attack tools are already available and relatively easy to install and operate. Tools such as Scapy6 and the Hacker's Choice IPv6 Toolkit come to mind.

2.4 Multiple Addresses Vulnerability

IPv6 assigns multiple addresses to an interface which challenges the filtering rules in the firewalls and access control lists [10]. In such cases, a firewall will need to learn all the addresses dynamically and the filtering rules will need to be automatically generate-able using sophisticated policy rule sets. And such capabilities are not available.

2.5 Multicast Security Vulnerability

IPv6 has no broadcast method of packet forwarding and instead uses multicast for all one-to-many communications. IPv6 uses multicast for neighbor discovery, Dynamic Host Configuration Protocol (**DHCP**), and traditional multimedia applications.

If an attacker could send traffic to these multicast groups and all the systems that are part of these groups respond, that would give the attacker information that could be used for further attacks. The attacker would have information about all the routers within the IPv6 network and all the DHCPv6 hosts. These are critically important nodes for aiding an attacker in determining what other computers are contained within the network, either through neighbor caches, binding updates, or DHCPv6 logs. We can even argue that the reconnaissance phase is no longer required with IPv6. To launch a blind attack (no return traffic) against all DHCPv6 servers, the attacker has only to send his packet to FF05::1:3.[5].

Multicast could not only be used for reconnaissance but also as a way to amplify traffic volumes for DoS attacks. A spoofed source address in a packet destined to a multicast address could result in amplification of the return traffic toward the target spoofed source address. Securing multicast has historically been a challenge. The nature of multicast is that there is a single source sending to many receivers.

2.6 Extension Header Vulnerability

Because the protocol specifications have not constrained the usage of extension headers as shown in figure 2, they could potentially cause problems if used maliciously [5].

Figure 2 shows the structure of an extension header and describes how they form a linked list of headers before the

packet payload. There are many more types of extension headers available for use in IPv6 packets, but this figure shows how they are arranged in the packet.

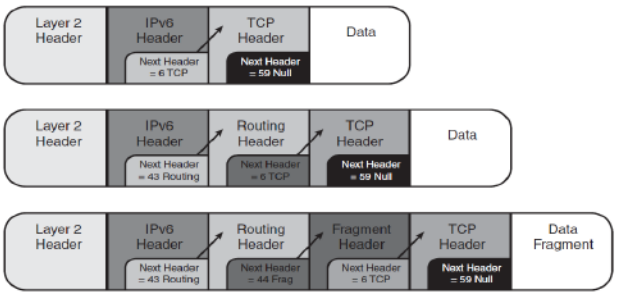


Figure 2: Example of the Extension Headers.

An attacker could perform header manipulation on the extension headers to create attacks. Someone could create an IPv6 packet that meets the protocol specification and has an unlimited number of extension headers linked together in a big list. A packet like this might cause a DoS of intermediary systems along the transmission path or the destination systems. The crafted packet might also pass through the network without causing any problems. Chaining lots of extension headers together is a way for attackers to avoid firewalls and Intrusion Prevention Systems (**IPS**).

Packets that have a large chain of extension headers could be dangerous. Numerous extension headers in a single packet could spread the payload into a second fragmented packet that would not be checked by a firewall that is only looking at the initial fragment.

2.7 Fragmentation Security Vulnerability

Fragmentation is the process of dissecting an IP packet into smaller packets to be easily carried across a data network that cannot transmit large packets, as shown in figure 3 below:

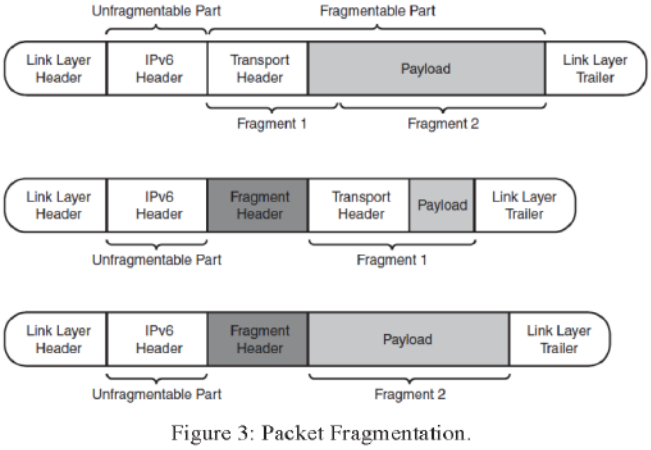


Figure 3: Packet Fragmentation.

In IPv6, fragmentation is never performed by the intermediary routers but by the end nodes themselves. So, only the end hosts are allowed to create and reassemble fragments. This process can be used by attackers to either hide their attacks or to attack a node. By putting the attack into many small fragments, the attacker can try to bypass filtering or detection. Attackers can also create fragments in such a way as to exploit weaknesses in the method an end host uses to reassemble the fragments. Examples of this would be overlapping fragments, where there is an overlap in the offset and out-of-order fragments where the fragments IDs do not match correctly with the data. Another type of fragment attack involves an attacker sending an incomplete set of fragments to force the receiving node to wait for the final fragment in the set. Fragmentation attacks can also involve nested fragments or fragments within fragments, where the IPv6 packet has multiple fragmentation headers. Fragmentation attacks are typically used by hackers with tools such as Whisker, Fragrouter, Teardrop, and Bonk [5].

3. SOME COMMON ATTACKS

When you consider the ways that an IPv4 or IPv6 network can be compromised, there are many similarities. Attacks against networks typically fall within one of the following common attack vectors [5], [7], [9], [16]:

- Internet (DMZ, web pages, pop-ups).
- Sniffing, header manipulation, session hijacking, man-in-the middle.
- Buffer overflows, SQL injection, cross-site scripting.
- Email (attachments, phishing, hoaxes)
- Worms, viruses, distributed denial of service (**DDoS**)
- Macros, Trojan horses, spyware, malware, key loggers
- VPN, business-to-business (**B2B**)
- Chat, peer-to-peer (**P2P**)
- Malicious insider, physical security, rogue devices, dumpster diving.

As noticed above, it is important for considering that IPv6 is not necessarily more secure than IPv4 [1]. In fact, IPv6 approach to security is only slightly better than IPv4 but not fundamentally new.

Finally, many groups are performing extensive testing of IPv6, so they hopefully can find many of the issues before it is time to deploy IPv6. However, all the major vendors of IT equipment and software have published vulnerabilities in their IPv6 implementations, (such as: Microsoft, Linux, Sun, and Cisco) all have published vulnerabilities in their software. As IPv6 has been adopted, it is evident that these major vendors have drawn the attention of the hackers.

4. CONCLUSION

Defiantly, before deploying IPv6 you should be aware of the following aspects of security for IPv6 traffic:

- Protection host from scanning and attacking
- Protection of IPv6 packets
- Protecting & Controlling of what traffic is exchanged with the Internet.
- Authorization for automatically assigned addresses and configurations
- Prevention systems (Firewalls and intrusion detection)

However, because IPv6 and IPv4 are both network layer protocols, many of the network layer vulnerabilities are therefore similar.

Therefore, you must connect to IPv6 natively. By itself IPv6 is not a panacea for IP-layer/network-layer security concerns.

ACKNOWLEDGEMENTS

At first I must thank my lovely wife for her support.
I would like to thank Dr. Moa'aml A. Ibrahim for encouragement.
I would also like to thank Mr. Alaa Al-Din Al-Radhi for providing me such good guidance.

REFERENCES

[1] Al-Radhi, A, A. 2011. *IPv6 Promised Role in Mitigating Cyber Attacks: Really it's Time!*. Swiss Cyber Storm-International IT Security Conference, Switzerland.
[2] Khaldoun, B. Khaled, B. Amer, A. 2011. *THE NEED FOR IPv6*. International Journal of Academic Research, Vol. 3. No. 3. May 2011, II Part. PP.431-448, Azerbaijan. http://www.ijar.lit.az
[3] Minoli, D. Kouns, J. 2009. *Security in an IPv6 Environment.* CRC Press, USA.
[4] Davies, J. 2008. *Understanding IPv6.* Microsoft Press, USA. 2nd edition.
[5] Hogg, S. Vyncke, E. 2009. *IPv6 Security*, Cisco Press, USA.
[6] White Paper, (Published: September 2003 & Updated: January 2008). *Microsoft Windows Server 2008, Introduction to IP Version 6*, Microsoft Corporation, USA.
[7] White paper 2004. *IPv6 and IPv4 Threat Comparison and Best Practice Evaluation(v1.0)* , Cisco Press, USA.
[8] Szigeti, S.; Risztics, P. 2004. *Will IPv6 bring better security?. Proceedings 30th Euromicro Conference*, vol., 532- 537, 31 Aug.-3 Sept.
[9] Sotillo, S. 2006. *IPv6 Security Issues.* East Carolina University, USA.
[10] Choudhary, A. R. Sekelsky, A. 2010. *Securing IPv6 Network Infrastructure: a New Security Model. IEEE Conference,* USA.
[11] Blanchet, M. 2006. Migrating to IPv6. *John Wiley & Sons Ltd, England.*
[12] Hagen, S. 2006. *IPv6 Essentials*, O'Reilly Media, USA, 2nd edition.
[13] Popoviciu, C. Abegnoli, E. L. Grossetete, P. 2006. *Deploying IPv6 Networks.* Cisco Press, USA.
[14] Karlsson, B. 2003. *Cisco Self-Study: Implementing IPv6 Networks (IPV6).* Cisco Press, USA.
[15] Li, Q. Jinmei, T. Shima, K. 2009. *Mobile IPv6: Protocols and Implementation,* Elsevier Inc. USA.
[16] Hauser, V. 2008, *Attacking the IPv6 Protocol Suite*, The Hacker's Choice, http://www.thc.org/thc-ipv6.

Harith A. Dawood. He has B.Sc. and M.Sc. degree in Computer Science, University of Technology (UOT), Baghdad, IRAQ. The author became a Member of the Iraqi Computer Science Society in 1990. And he was a lecturer in many Iraqi colleges; recently, he is IPv6 researcher and trainer.

Digital Watermarking Enhancement for Satellite Images Using a DCT Algorithm

Mustafa B. Abugharsa, Mohamed A. Sullabi and Alhusain M. Taher
Faculty of Information Technology, Misurata University, Misurata, Libya

Abstract— **The rapid growth of communication networks allows the widespread distribution of multimedia data in various ways. Since digital productions are easily duplicated, discouraging unauthorized cloning and illegal distribution of electronic documents are issues that have to be resolved. This paper investigates a technique for digital watermarking using the Discrete Cosine Transform (DCT) Domain and introduces the use of pseudo random noise in watermarking to hide information for the purpose of authentication. The underlying system is based on Code Division multiple Access (CDMA), which is a form of spread spectrum communication. The objectives include the development of a watermark embedding strategy and the analysis of the results. A compression method was considered as an image attack to perform the implemented approach. The proposed technique has been successfully tested on a simple satellite image and it provided a robust watermark extraction.**

Index Terms—**Digital Watermarking, Satellite Image, Discrete Cosine Transform, Image attack.**

I. Introduction

THE Digital watermarking is the process that embeds data called a watermark into a digital media such that the watermark can be detected or extracted later to make an assertion concerning the object [1]. Each watermarking system has two main stages: the embedding stage in which the watermark is stored in the cover image and the extraction stage in which the watermark is retrieved from the cover image. In most cases the extraction is the reverse operation of the embedding stage [2]. Furthermore, according to their resilience, watermarks can be fragile or robust.

Saxena [3] defined Digital watermarking as a technique used to hide data or identifying information within digital multimedia. However, Genov [4] defined digital watermarking as data embedded into the original object to be watermarked. The embedding should be done in a way that ensures later detection or extraction of the watermark for making certain assertions. Perceptible marks of ownership or authenticity have been around for centuries in the form of stamps, seals and signatures but given current data manipulation technologies, imperceptible digital watermarks are mandatory in most applications. The digital watermark is a digital code irremovably, robustly, and imperceptibly embedded in the host data and typically contains information about the origin, status, and destination of the data [5].

Fragile watermarks are used for authentication and localization of modifications. Similar to digital signatures, their goal is to detect the slightest change to the document. In contrast, robust watermarks are designed to survive (remain detectable) through most attacks. While an attack of sufficient magnitude could erase the watermark, the hope is that an attacker would have to significantly degrade the document in order to destroy the watermark.

General image watermarking methods can be divided into two groups according to the domain of application of the watermarking. In the spatial domain method the pixel values of the cover image are altered in the original image. In the transform domain, the image pixels are altered after applying a certain transform on the image, such as a watermark via DCT, Fourier, wavelets, etc.

With the Internet revolution, sharing multimedia such video, audio and images has never been easier. However, protecting them from illegal use on the Internet has become a great challenge for the multimedia industry. This has led to a new problem in terms of copyright, since anybody can select, modify and distribute protected media. For that reason, developing and providing technologies that will allow sharing of multimedia safely and securely has been a field of great interest.

This paper aims to investigate a robust watermark domain-frequency composite scheme under the framework of the Joint Photographic Experts Group (JPEG) still image compression standard. JPEG is the most widely used image compression. Baseline JPEG uses a DCT (Discrete Cosine Transform). This analysis is done using MATLAB programming code for the DCT and GUI (Graphical User Interface) model.

II. Discrete Cosine Transformation (DCT)

Among frequency domain techniques, the Discrete Cosine Transform (DCT) is one of the most popular domains for digital content processing. 2D DCT is defined as using the reparability property transform on the rows and on the columns, applied separately as shown in Equation 1:

$$F_{(u,v)} = D_y\{ D_x\{f_{(x,y)}\}\} \quad (1)$$

The discrete cosine transform DCT is a transform function which transforms an image from the spatial domain to the frequency domain which allows the analysis of a signal.

Manuscript received on February 29, 2012.
Mustafa B. Abugharsa, Mohamed A. Sullabi and Alhusain M. Taher are with the Faculty of Information Technology, Misurata University, Misurata, Libya.

Simple watermarking in the DCT domain is usually performed on the lower or the mid-band frequencies, as the higher frequencies are lost during image compression [6].

One of the advantages of DCT is the fact that it is a real transform; this implies lower computational complexity, which is sometimes important for real-time applications. DCT is used in some loss compression algorithms, including JPEG. (The JPEG standard codec is more complicated, for it includes quantizing for the DCT coefficients and the DPCM statistical prediction scheme. The output of the codec is a prediction error, which is encoded using a lossless entropy code). In the transform image, DC is the matrix element (1, 1), corresponding to the transform value X (0, 0). High spatial X and Y frequencies correspond to high column and row indexes, respectively.

The DCT breaks a digital media into different frequency bands. Lower frequencies are in general the most visually exposed therefore these are the important parts of a digital media. Higher frequencies on the other hand are the most vulnerable parts of a digital media due to the likelihood of being removed due to compression and noise attacks. Therefore, the middle frequency bands are the safest zone for embedding a watermark [7].

III. PROCESS MODELLING

An overview of the work flow for the satellite image watermarking is shown in Figure 1. A digital watermarking process typically involves three entities. These are the original data (image, audio, or video), a watermark, and an optional Key. Watermark embedding is a process to insert or embed the watermark into the original data that results in a watermarked set of data. In watermark extraction the watermark is detected or extracted from the watermarked data. Generally the watermarking process starts with selecting the original data to be watermarked and the watermark itself. The second step is embedding the watermark into the original data using a secret key. The same key must be provided to the watermark extractor. Then, the watermarked data is distributed at which point it could be vulnerable to attacks that could destroy the watermark inserted in the data. Subsequently, the watermark is extracted and it is important to note that it is possible to do watermark insertion without necessarily doing watermark extraction since it is possible that the watermark encoder is different from the watermark decoder.

IV. IMPLEMENTATION

In order to evaluate the proposed method in this research, different DCT coefficients were used on the test image. A method of image quality measurement is the Peak Signal to Noise Ratio (PSNR), which estimates the quality of a reconstructed image compared with the original image. Once the PSNR for each image is determined, images with a high PSNR may not necessarily look better than those with a low PSNR. This proves particularly true in the DCT domain techniques.

V. SIMULATION RESULTS

The digital image watermarking system is made to be simple with as little complexity as possible as the users may be new to the usage of a digital image watermarking system. The whole system is divided into three main parts, namely embedding, extracting and attacks. One image will be used in this test as the original image. Moreover, a 64 x 64 pixel binary image is chosen to be tested as a watermark sign.

The Gain Factor (GF) is an integer number that determine the levels of the watermark robustness. A higher GF means a more robust watermark which introduces more distortion into the original image, and vice versa. On the other hand, increasing the gain value will increase the distortion average on the pixels that are hosting the watermark. JPEG compression was considered as an image attack process.

This showed how the threshold affects the watermark robustness against JPEG compression. To perform this test, a satellite image was watermarked by the binary image with different GF values. The threshold values were 5, 18, 25, and 40. After that, each of these images has been compressed to JPEG images with the same compression level.

The watermarking algorithm embeds the watermark in the luminance component, keeping the chromatic component constant. Hence, the two standard colour images are compressed by a quality factor of 75 %. Table I shows the watermarked image as a JPEG compressed by a quality factor. It is almost impossible to perceive the difference between the original image and the watermarked image with a gain factor of 5. However, comparing the original image with an image watermarked with a gain factor of 18, the watermark is less perceptible compared to a watermarked image with a gain factor of 40 but it is still hard to notice any difference between the original and either of the two watermarked images. The watermark distortion starts to be noticeable when the gain factor is increased to 60.

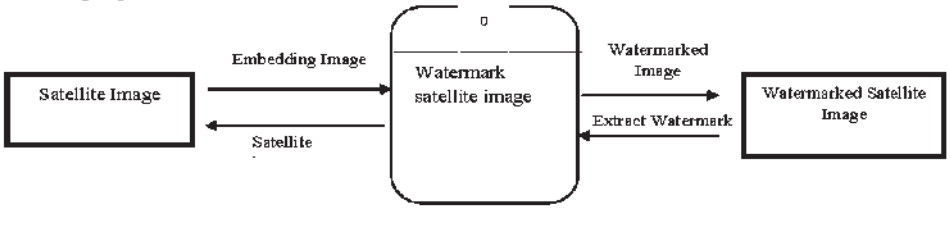
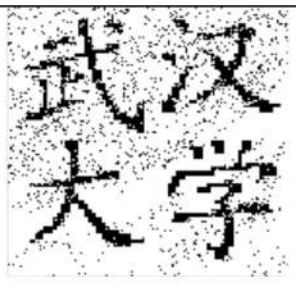
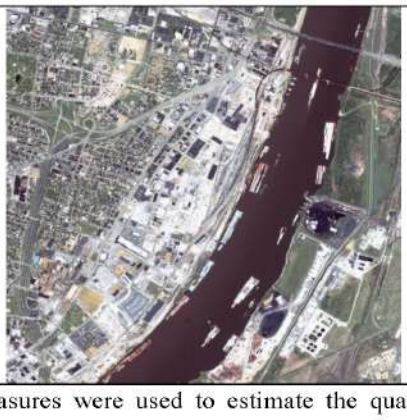


Figure 1. An overview of the digital watermarking model.

TABLE I
EXTRACTED IMAGE AFTER JPEG COMPRESSION ATTACK

	Original Image	Recovered message
Gain factor = 5		
Gain factor = 18		
Gain factor = 25		
Gain factor = 40		

PSNR measures were used to estimate the quality of the reconstructed image compared with the original image. The

fundamental image was compared with the original image to compute a value that reflected the quality of the reconstructed image. Reconstructed images with a higher metric are referred to as having a better quality. The *PSNR* is one of the most commonly used measures for image quality as described by Equation 2.

$$PSNR = 20\log_{10}\left(\frac{255}{\sqrt{MSE}}\right) \quad (2)$$

where,

$$MSE = \left(\frac{\sum[f(i,j) - F(i,j)]}{N^2}\right) \quad (3)$$

and *f(i ,j), F(i, j)* denote the source image and the reconstructed image respectively, $0 \le i \le N$, and $0 \le j \le N$.

The PSNR of this particular image cannot be compared with the PSNR of another image, even if both values are same. One image with a 20 dB PSNR may look much better than another image with 30 dB PSNR. Typically, the PSNR value ranges from 20 dB to 40 dB. Usually, any image with a *PSNR* of more than 32 dB is considered to be good. Table II, shows that an increasing gain factor will give better quality.

TABLE II
PSNR FOR THE IMAGE USING DIFFERENT GAIN FACTORS.

Gain Factor (GF)	PSNR
5	1.8803e+004
18	1.4508e+003
25	1.5508e+003
40	293.7897

It can be observed that the technique works perfectly for un-altered images, with a good visual quality of the watermarked image. The block-size for each of the DCT-based techniques was kept constant at 8x8, in anticipation of JPEG compression. Better results could be obtained using larger block sizes at the expense of message capacity.

The DCT watermarking method proved to be both moderately robust against Gaussian noise, and extremely robust against JPEG compression. The most interesting result is that the recovered image after JPEG compression with a quality factor of 75 is actually better than the watermark recovered from a pristine cover. This would tend to indicate that embedding the watermark in the same domain as expected transformations is clearly advantageous. By predicting which DCT coefficients would be altered using JPEG, an extremely high level of JPEG robustness was achieved.

I. CONCLUSION

Digital watermarking in the work presented was undertaken especially on a satellite image using the DCT algorithm after JPEG compression. By anticipating which coefficients will be modified by the subsequent transforms, it is possible to produce a watermarking technique with moderate robustness, good capacity and low visual impact. This holds particularly true in the case of compression techniques, were the compression algorithms are well known. Further work can be applied as an enhancement of the single watermark to embed more than one watermark in a satellite image.

REFERENCES

[1] R. B. Wolfgang, C. I. Podilchuk, and E. J. Delp, "Perceptual watermarks for digital images and video," *Proceedings of the IEEE*, vol. 87, no. 7, pp. 1108-1126, 1999.

[2] I. Cox, M. Miller, J. Bloom *et al.*, "Digital watermarking," *Journal of Electronic Imaging*, vol. 11, pp. 414, 2002.

[3] V. Saxena, "Digital image watermarking," Department of Computer Science and Engineering, Jaypee Institute of Information Technology, NOIDA, INDIA, 2008.

[4] E. P. Genov, "Digital watermarking of bitmap images," in Proceedings of the 2007 international conference on Computer systems and technologies, NY, USA, 2007, pp. 37.

[5] J. K. Su, F. Hartung, and B. Girod, "Digital watermarking of text, image, and video documents," *Computers & Graphics*, vol. 22, no. 6, pp. 687-695, 1998.

[6] J. Xiao, and Y. Wang, "Toward a better understanding of DCT coefficients in watermarking," in Pacific-Asia Workshop on Computational Intelligence and Industrial Application, Wuhan 2008, pp. 206-209.

[7] C. Shoemaker, *Hidden bits: A survey of techniques for digital watermarking*, 2002.

Sazan Avlama* (Phishing): Kullanılan Teknikler ve Bunlardan Korunma Yöntemleri

Ali ŞENOL, Hacer KARACAN

***Özet*—İnternet dolandırıcılığı, hızla gelişen ve milyonlarca kişiyi mağdur eden, milyarlarca dolarlık da bir pazar haline gelen bir suç ortamıdır. İnternet ortamı, saldırganın çok kolay bir şekilde ve arkada hemen hemen hiç iz bırakmadan kaybolabilmesini sağlayan bir ortam olduğu için bu ortamda gerçekleşen saldırılar günden güne artmaktadır. Bu saldırıların başında da sazan avlama olarak adlandırılan internet dolandırıcılığı yöntemi gelmektedir. Saldırgan kişi veya sistem, kurbanı tuzağa düşürebilecek türlü araç ve yollar kullanabileceği için, sazan avlama yönteminde pek çok farklı teknik veya dolandırıcılık metodundan bahsedilebilir. Bu çalışmada sazan avlamanın tanımı, hangi argümanları kullandığı ve hangi aşamalardan oluştuğu belirtilerek korunma yöntemleri üzerine bazı öneriler sunulmuştur.**

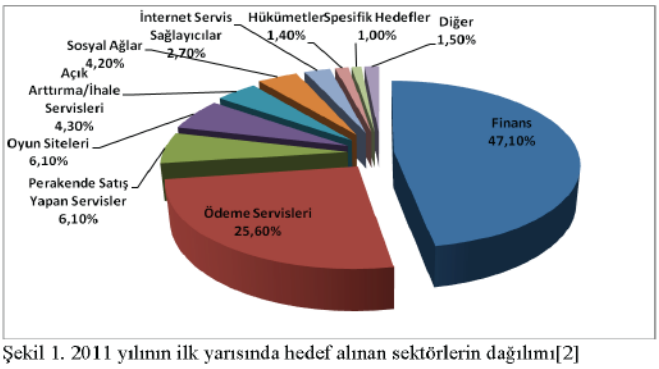
***Anahtar Kelimeler*—Sazan Avlama, İnternet Dolandırıcılığı, Sahte E-Posta, Korunma Yöntemleri.**

***Abstract*—Internet scams are the most popular scam type which have billion dollars of market scale and aggrieve millions of people with its fast growth rate. Since, an attacker has the chance to destroy all evidences, Internet fraud is the easiest way for him/her to disappear after defrauding the victim. The most important of these attacks is phishing which is a term combining the words "password" and "fishing". As internet fraud methods, we can talk about lots of techniques. The reason for this many methods is the usage of a variety of tools and ways by computer hackers or attacker systems to trap their victims. In this work, the definition of phishing and its arguments which are used as attack materials and its stages are described while also explaining several ways to prevent ourselves from these attacks.**

***Anahtar Kelimeler*—Phishing, Internet Scams, Fake E-mail, Protection Methods.**

I. GİRİŞ

BİLGİSAYAR ve internet hayatımızın her alanına girerek bize sayısız kolaylıklar sağlamaktadır. İnternet, bilgiye ulaşmayı çok kolay hale getirmiş; eğitim, sosyal, iş ve özel hayatımızı doğrudan etkiler duruma gelmiştir. Bugün pek çok işi internet üzerinden çok kısa zamanda halledebilmekteyiz. Fatura ödeme, alış-veriş yapma, para transfer etme ve daha pek çok işlemi gerçekleştirmek dakikalarımızı hatta bazen saniyelerimizi almaktadır. Türkiye Bankalar Birliği'nin (TBB) Ekim-Aralık 2011 dönemi verilerine göre 7,8 milyon bireysel müşteri en az bir kez internet bankacılığı giriş işlemi yapmıştır. Bu miktar, toplam kayıtlı bireysel müşteri sayısının yüzde 43'ünü oluşturmaktadır. Ekim-Aralık 2011 döneminde, aktif bireysel müşteri sayısında bir önceki yılın aynı dönemine göre 1 milyon 765 bin kişi, bir önceki üç aylık döneme göre ise 738 bin kişi artış olmuştur. Ayrıca, Ekim-Aralık 2011 döneminde internet bankacılığı ile gerçekleştirilen 11,4 milyon adet yatırım işleminin hacminin 89,9 milyar TL olduğu belirtilmektedir [1]. TBB tarafından açıklanan veriler, İnternet bankacılığının saldırıların odağı olmasındaki mali boyutunun öğrenilmesi açısından önem taşımaktadır. Şüphesiz internet sayısız kolaylıklar sağlamaktadır. Ancak, internetin bu kadar popüler olması ve bu denli büyük bir parasal işlem hacmini barındırması kötü niyetli kişilerin bu bilgileri ele geçirerek haksız kazanç sağlamaları açısından iştah kabartıcıdır. Haksız kazanç sağlamak amacıyla yapılan İnternet saldırılarının önde gelenlerinden biri, kullanıcılarının internet sitelerine girişte kullandıkları kullanıcı adı ve şifre gibi özel bilgilerini ele geçirmeyi ve bu bilgilerle maddi açıdan kazanç sağlamayı amaçlayan sazan avlama (phishing) saldırılarıdır. Sazan avlamada en çok hedef alınan sektör ise %47'lik bir oranla finans sektörüdür[2].

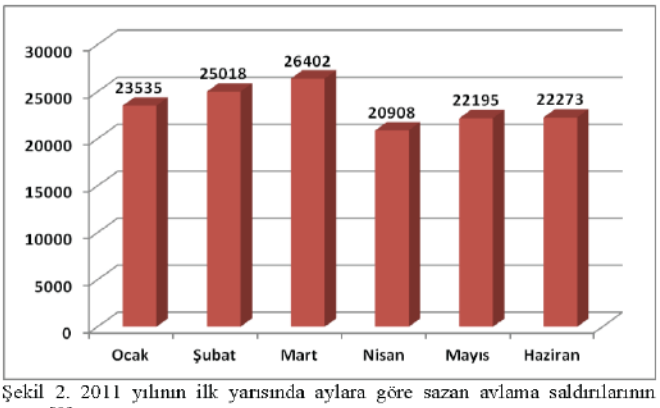


Şekil 1. 2011 yılının ilk yarısında hedef alınan sektörlerin dağılımı[2]

Aylık bazda yaklaşık 20.000 ile 25.000 sazan avlama saldırısının yapıldığı ve bazen yüzbinlerce bazen de milyonlarca kişiyi mağdur ettiği belirtilmiştir[2].

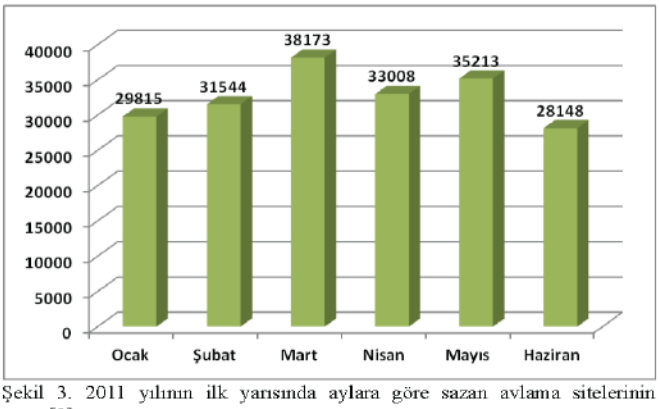
Ali ŞENOL, Gazi Üniversitesi, Mühendislik Fakültesi, Bilgisayar Mühendisliği Bölümü, Eti Mah. Yükseliş Sok. 06570 Ankara/Türkiye. alisenol@gazi.edu.tr
Hacer KARACAN, Gazi Üniversitesi, Mühendislik Fakültesi, Bilgisayar Mühendisliği Bölümü, Eti Mah. Yükseliş Sok. 06570 Ankara/Türkiye. hkaracan@gazi.edu.tr

· Terimin Türkçe çevirisinin elde edildiği kaynak: *Canbek, G., Sağıroğlu, Ş., Bilgi ve Bilgisayar Güvenliği: Casus Yazılımlar ve Korunma Yöntemleri, Ankara, 2006.*



Şekil 2. 2011 yılının ilk yarısında aylara göre sazan avlama saldırılarının sayısı[2]

2011 yılının ilk yarısı için, sazan avlama saldırılarının en yaygın yapıldığı metod olarak dikkat çeken sahte web sitesi yöntemiyle hazırlanmış olan, 28.000 ila 38.000 adet farklı sazan avlama sitesi rapor edilmiştir[2].



Şekil 3. 2011 yılının ilk yarısında aylara göre sazan avlama sitelerinin sayısı[2]

Her geçen gün İnternet dolandırıcılığı yöntemlerinde ve sayısında çok büyük bir artış oluşmaktadır. İnternetin sahip olduğu geniş kullanıcı yelpazesi sebebiyle, bu alanda yapılan dolandırıcılık günden güne yeni bir yöntemle kurbanlarını maddi veya manevi açıdan zarara uğratmaktadır.

II. SAZAN AVLAMA

Sazan avlama yöntemi internet kullanıcılarının internet sitelerine girişte kullandıkları kullanıcı adı ve şifre gibi özel bilgilerini ele geçirmeyi ve bu bilgilerle maddi açıdan kazanç sağlamayı amaçlayan bir internet dolandırıcılığı türüdür. Password(Şifre) ve Fhishing(balık avlama) kelimelerinin birleştirilmesiyle oluşturulduğu düşünülmektedir[3]. İnternet dolandırıcılığı yöntemleri arasında en tehlikelisi olarak göze çarpan phishing Türkçeye sazan avlama veya yemleme olarak çevrilmiştir[4].

Sazan avlama yöntemi balık avlamaya benzetilmektedir. Saldırgan kurbana bir bankadan gönderiliyormuş gibi ve bilgilerini güncellemesi gerektiğini bildiren sahte bir siteye yönlendirilmiş link içeren sahte bir e-posta (Bkz. Şekil 4) gönderir. Kurban, linki tıkladığında tasarım olarak aynı ancak arkaplanda işlev olarak farklı sahte siteye yönlendirilir. Kurban bilgilerini girip güncellemeye çalıştığında bu bilgiler saldırgana ulaştırılır[5].


TÜRKİYE CUMHURİYET MERKEZ BANKASI

Sayın müşterimiz;
Ağustos ayından itibaren T.C Merkez Bankası'nın aldığı karara dayanarak tüm internet bankacılığı sistemlerinde TCMB'ye bağlı tüm bankaların (AKBANK, ANADOLU BANK, ASYA BANK, GARANTİ BANKASI, FORTIS BANK, FİNANSBANK, HSBC BANK, ŞEKERBANK, T.C İŞ BANKASI, TURKEYFINANS, TEB, TEKFENBANK, TEKSTILBANK, KOÇBANK, KUVEYTTÜRK, YAPI VE KREDİ BANKASI, VAKIFBANK) SSL yazılımları ve internet bankacılığına hizmet eden bilgisayarlar güncellenmektedir. Bu güncelleme nedeniyle sistemler yenileneceğinden, hem aktif internet bankacılığı kullanıcılarını tespit etmek, hem de güvenlik açısından sizlere daha iyi bir hizmet verebilmek için bilgilerinizi teyit etmeniz gerekecek ve yeni veritabanımıza kaydedilecektir. Bilgilerinizin teyidi ve yeni veritabanına eklenmesi zorunludur. Teyit işlemi yapılmadığı taktirde Ağustos ayından sonra internet bankacılığını kullanabilmeniz için TCMB Ankara Şubesi'nden bilgilerinizi teyit edip yeni veritabanına kaydettirmeniz gerekecektir. Aşağıdaki linkten bilgilerinizi internet üzerinden teyit edebilir, ya da TCMB Ankara Şubesi'nden bilgilerinizi teyit edebilirsiniz.

İnternet üzerinden teyit işlemini yapmak için aşağıdaki linke tıklayın;
http://tcmb.gov.tr.teyit.merkezbanka.org/guncelleme.php?sid=d3fd99df91df76df8

DİKKAT: Lütfen TCMB üzerinden gelmeyen mailleri dikkate almayınız. TCMB üzerinden gelmeyen mailleri güvenliğiniz için bize bildirin. Teyit işlemleriyle hiçbir banka doğrudan ilgilenmemektedir. Bütün teyit işlemleri TCMB tarafından organize edilmektedir. Teşekkürler.

Adres: İstiklal Cad. 10 Ulus 06100 Ankara, Türkiye
Telefon : (312)510 3640
©TCMB 2006

Şekil-4: TCMB'ından Gönderilmiş Gibi Gösterilen Sahte E-posta

Sazan avlamada saldırganların en çok faydalandıkları yöntem sosyal mühendislik tekniklerdir[6]. Sosyal mühendislik teknikleri veri ve sistem güvenliği için çok önemli bir tehdittir[7]. Literatürde sosyal mühendislik "insanların istediğiniz gibi davranmasını sağlamaya çalışma sanat ve bilimi" olarak tanımlanmaktadır[8].

Sazan avlama yönteminde bir senaryo ve bu senaryoya göre oluşturulan bir teknolojik yapı söz konusudur. Bu yöntemde çeşitli yöntemlerden bahsedilebilir anacak büyün yöntemlerde kurbanın zaaflarından faydalanma vardır. FBI'ın en çok arananlar listesine giren ilk "hacker" olan Kevin Mitnick'e göre "güvenlik zincirindeki en zayıf halka insan"dır[9]. Çünkü her bilgisayar sistemi bir insan tarafından kullanılır veya kontrol edilir. Bu da insani değerlerden olan dalgınlık, yanılma, dikkatsizlik gibi etkenler sonucu yanlış işlemlerin yapılması sonucu sistemin zarar görmesine neden olacak eylemlerin ortaya çıkması anlamına gelmektedir.

Bir sazan avlama saldırısının başarılı olabilesi için sahte site tasarımının gerçek gibi görünmesi, gönderilen e-potanın inandırıcı olması ve saldırıdan sonra tüm izlerin yok edilmesi gerekir[10].

A. Sazan Avlamanın Tarihsel Gelişimi

"Phishing" kavramı, bir görüşe göre, 1980 yılında ilk kez psikolojik teknikler kullanarak kredi kartı bilgilerini ele geçiren Brien Phish'e bir atıf olarak ortaya çıkmıştır[11]. İlk sazan avlama örneğine 2 Haziran 1996 yılında ABD'de faaliyet gösteren AOL(America On-Line) firmasına ait haber grubunda rastlanmıştır[12]. 2003 yılına kadar sazan avlama yöntemi konusunda çok fazla gelişme olmamıştır. 2003 yılından sonra çok hızlı ve çeşitli sazan avlama yöntemleri ortaya çıkmıştır. Bunun nedeni de dinamik sitelerin yaygınlaşması ve bedava alan veren sunucuların sayısının artması olarak düşünülmektedir. Türkiye'de bu yöntemin kullanılmaya başlanması 2004 yılını bulmaktadır. İlk zamanlar çok da inandırıcı olmayan bir şekilde kullanılmaya başlanan bu yöntem zaman içinde farklılaşmış ve birçok insanı etkileyecek duruma gelmiştir.

B. Sazan Avlamada Ön Plana Çıkan Yöntemler

Sazan avlama dolandırıcılığı konusunda pek çok yöntemden söz edilebilir. Bu yöntemlerde en çok faydalanılan argümanlar e-posta ve sosyal mühendislik teknikleridir[13]. Çevrimiçi alışveriş sağlayan e-ticaret firmaları veya bankaların belli aralıklarla güvenliği arttırmak amacıyla şifre değiştirme isteğiyle gönderdikleri e-postalar suistimal edilir. Söz konusu kuruluşlar bazen uzun zaman hesapta bir hareketlilik görmedikleri zaman bazen de güvenliği arttırmak amacıyla bu e-postaları göndererek, müşterilerin sistemlerini daha aktif ve daha güvenli bir şekilde kullanmalarını amaçlamaktadır. Saldırganlar bu tür e-postaları taklit ederek kurbanlarını hazırladıkları sahte sitelere yönlendirmektedirler. Bu yöntem en çok karşılaşılan yöntem olmasına rağmen saldırganlar bazen sistemsel bazen de insan kaynaklı açıkları da değerlendirerek ve sosyal mühendislik teknikleri ile inandırıcılık katarak kurbanlarını tuzağa düşürmeye çalışmaktadırlar.

Saldırganlar kurbanların kullandıkları veya kurbanların hizmet aldıkları sistemlerin güvenlik önlemlerini atlatmak için çeşitli yöntemler kullanırlar. Saldırgan gönderdiği e-postanın spam filtrelerini atlatmak için mesaj içeriklerini gizler. Ayrıca kurbana e-posta servisini sunan çoğu e-posta yazılımı kullanıcıya başlık bilgilerinin tamamını göstermez. Bu durumda görünen isim ve gerçek gönderen farklı olmasına rağmen kullanıcı bunun farkına varamamaktadır[14].

Sahte Web Sitesi Yöntemi

Sahte web sitesi yöntemi, sazan avlamada en yaygın kullanılan yöntemdir. Bu yöntemde saldırgan, kurbana çeşitli senaryolara göre güvendiği bir sistemden veya kişiden gönderiliyormuş gibi sahte bir e-posta gönderir[15]. E-postanın içeriğinde kurbanın bilgililerini güncellemesi gerektiği belirtilir. Gönderici e-posta adresinin aynı olması gibi yöntemlerle ilgili sistemden gönderiliyormuş gibi gösterilen bu e-postalarda sahte web sitesine yönlendirilmiş bir link verilir. Saldırgan çeşitli yöntemlerle söz konusu linkin sahte siteye yönlendirildiğinin anlaşılmamasını sağlamaya çalışır. Kurban bunu anlamaması durumunda, sistemin birebir kopyası olan sahte siteye yönlendirilir. Bu durumda kullanıcı karşısına gelen formun sahte bir form olduğunu anlamadan doldurmaya başlar ve bilgilerinin saldırganın eline geçmesine olanak sağlar. Kurbanın bilgileri bazen sahte web sitesi üzerinden e-posta ile gönderilirken bazen de sahte web sitesinde örneğin bir text dosyasında tutulur[16].

Link Manipulasyonu

Link manipulasyonu yöntemi sazan avlamanın bir diğer etkin yöntemidir. Saldırganlar sahte web sayfalarını hazırlarken alan adını mümkün olduğunca taklit ettikleri sitenin alan adına benzetmeye çalışır (www.akbank.sahteadres.com gibi) [17]. Saldırgan gönderdiği e-postada da kullandığı linki mümkün olduğunca gerçek siteye yönlendirilmiş adrese benzetme çalışır. Bunu sağlamak için öncelikle bedava web alanı veren sitelerden en yakın alan adını alır. Bunun yanında verdiği linkte linkin sahte durumunun anlaşılmaması için ASCII karakterlerin hexadecimal karşılıklarını kullanarak da kurbanları tuzağa düşürmektedir. Çünkü tarayıcılar karakterlerin hexadecimal karşılıklarını da kabul etmektedirler[18]. Ayrıca tarayıcıların adres çubuğunda kullanılan '@' işaretine karşı gösterdikleri hassasiyeti de suistimal etmektedirler. Tarayıcılar adres çubuğunda '@' işareti kullanıldığında bu işaretten önce yazılanları ihmal eder ve sonra yazılanı kabul etmektedirler. Eğer saldırgan, kurbana http://www.twitter.com@www.sahtesayfa.com linkini içeren bir e-posta gönderirse kurban twitter yerine sahtesayfaya yönlendirilecektir. Örneğin, adres satırına www.twitter.com@%77%77%77%2E%73%61%68%74%65%73%61%79%66%61%2E%63%6F%6D/ girildiğinde Twitter yerine sahte sayfaya yönlendirme gerçekleşecektir.

SMisShing Yöntemi

Bir diğer sazan avlama tekniği sosyal mühendislik tekniklerinden faydalanan SMS Phishing ya da SMiShing adı verilen yöntemdir[19]. Bu yöntemde kurbana bir kampanyadan ödül kazandığına ve belirtilen numarayı araması gerektiğine dair bilgi içeren bir SMS gönderilir. Kurban söz konusu numarayı aradığında kişisel bilgileri istenir. Bu yöntem bedava SMS servisleri ve internet üzerinden SMS gönderilebilmesi nedeniyle son yıllarda çok sayıda kişiyi etkilemiş bir yöntemdir[20].

Telefonla Arayarak Sazan Avlama

SMS phishing'in yanında saldırganların kurbanları telefonla arayarak ve sosyal mühendislik teknikleri kullanarak bilgilerini ele geçirmeye çalıştıkları yöntemden de bahsetmek gerekir. Bu yöntemde saldırgan bir bankadan arıyormuş gibi davranarak kurbanın bilgilerini ele geçirmeye çalışır [17].

Açılır Pencere Yardımıyla Phishing

Bu yöntemde kurbana gerçek siteye yönlendirilmiş bir link gönderilir. Kurban gerçek siteye girdikten sonra bilgilerini girmesini isteyen bir açılır pencere sayfanın üzerinde belirir. Kurban bu açılır pencerenin gerçek siteye ait olduğunu düşünür. Ancak bu pencere saldırganın bilgileri ele geçirmek için kullandığı sahte bir sayfadır[17].

Oturum Bilgilerini Çalma Yöntemiyle Sazan Avlama

Bu yöntemde saldırgan çevrimiçi sistemlerde oturum açma mantığından faydalanır. Kurban oturum açtığı bir sitede gezinirken saldırgan oturumunu sona erdirerek tekrar giriş yapmasını sağlamaya çalışır. Saldırgan JavaScript yardımıyla giriş yapması için bir açılır pencere açar. Kurban giriş yapmaya çalıştığında bilgileri saldırganın eline geçer. Oturum bilgilerini çalma yönteminin bir diğer yolu ise kurbanın bir sistemde oturum açtığında bilgisayarında tutulan oturum bilgilerini çalması yöntemidir[21]. Bu yöntemde XSS açığından faydalanılmaktadır.

Tıpkısının Aynısı Pencere Yönemiyle Sazan Avlama

Bir diğer yöntem dilimize tıpkısının aynısı pencere olarak bir karşılık önerilen "doppelganger window" yöntemidir[22]. Bu yöntemde kullanıcı SSL gibi bir güvenlik sertifikasına

sahip bir sitede de olsa bilgiler çalınabilmektedir. Kurbanın giriş ekranından girdiği giriş bilgileri bir klavye kaydedici sayesinde saldırganın eline geçebilmektedir.

Ortadaki Adam Saldırıları

Bu yöntemde saldırgan kurban ve gerçek site arasındaki bağlantıyı yönlendirir. Bu yöntemde kurban SSL bağlantılı bir siteye de bağlantı sağlasa saldırgan tüm trafiği dinlediğinden kurbanın bilgilerini ele geçirebilmektedir[23].

DNS Ayarlarını Değiştirme Yöntemi

İnternet kullanıcıları bazen yasaklanmış sitelere girebilmek için DNS ayarlarını değiştirmektedirler. Bu durumu değerlendirmek isteyen saldırganlar forumlara güvenli olmayan DNS adresleri yükleyerek kurbanları sahte sitelere yönlendirmektedirler[17].

"ClickJacking" ile Sazan Avlama

Bu yöntem web sitelerinde bir web sitesinin bir diğerinin içine gömülmesi yönteminden faydalanır. Kurban bir yere tıkladığında bilgilerini çalmaya yönelik bir programın indirilmesine neden olabilir[24].

Sistem Ayarlarını Değiştirme Yöntemiyle Sazan Avlama

Bu yöntemde saldırgan çeşitli yollarla sisteme sızar ve sistemde değişiklik yaparak kurbanın bilgilerini ele geçirir. Kurbanın internet tarayıcısında kayıtlı kısa yolları değiştirmek bunlardan biri olarak sayılabilir.

Bu yöntemlerin yanı sıra saldırgan sahte yazılım veya zararlı yazılımlarla sisteme sızmak suretiyle kurbanı sahte sitelere yönlendirerek dolandırmaktadır.

C. Sazan Avlamadan Korunmak İçin Yapılan Çalışmalar

Sazan avlamadan korunmak için yazılan saldırı tespit sistemlerinin yanında bu tür saldırılarla mücadele ve bir farkındalığın oluşturulabilmesi için sivil toplum kuruluşları da kurulmuştur. Bunların başında uluslararası bir kuruluş olan Anti-Phishing Çalışma Grubu (APWG) gelmektedir. Bu kuruluş söz konusu saldırılarla ilgili istatistikî bilgileri belli aralıklarla paylaşmakta ve çeşitli eğitimler vermektedir[25].

Saldırganlar pek çok yöntem ve araç kullandıklarından tüm saldırılara karşı koyacak ve internet kullanıcılarını koruyacak bir savunma sisteminden veya yazılımından söz etmek mümkün değildir. Ancak bu tür saldırılardan korunmak için çeşitli akademik çalışmalar yapılmaktadır.

Kullanıcıları sazan avlama saldırılarına karşı korumak adına üç temel stratejiden söz edilebilir. Bunlar: zararlı içeriklerin kullanıcılara ulaşmasına engel olmak, kullanıcıları sazan avlama içerikli sayfalar hakkında bilgilendiren arayüzler geliştirmek ve kullanıcıları sazan avlama saldırılarından korumaya yönelik etkili eğitim[26].

Yapılan çalışmalardan biri veri madenciliği teknikleri kullanarak sazan avlama sitelerini tespit etmeye yarayacak sistemler geliştirmek üzerinedir. Bu çalışmaya göre veri madenciliği yöntemlerinden sınıflandırma ve ilişkilendirme yöntemleri ile beraber PSO (Particle Swarm Optimization) algoritmasının kullanılmasında kayda değer sonuçlar alınmıştır[27]. Ancak bu çalışmanın performansını arttıracak çalışmalar da yapılmaktadır. Bu çalışmalardan birinde MBAT (Modified Bat Algorithm) denilen ve metasezgisel temele dayanan algoritma kullanılmıştır. Bu algoritma ile PSO algoritmalarının karşılaştırılması sonucunda, MBAT algoritmasının daha az hata oranı ile sonuç ürettiği tespit edilmiştir.

Sazan avlama ile mücadele anlamında yapılan bir diğer çalışma sazan avlama tehlikesi içerdiği düşünülen web sitelerini tespit eden ve kullanıcıyı uyaran AntiPhish denilen yazılımdır. Bu yazılım Mozilla web tarayıcısına bir eklenti olarak geliştirilmiş ve diğer internet tarayıcılarına eklenti olarak eklenmesi için de çalışmalar devam etmektedir. Bu yazılım, internet kullanıcısı internette gezinirken güvenli olmayan sitelere giriş yapıldığı ve kişisel bilgilerin paylaşılması durumunda kullanıcıyı güvenli olmayan bir siteye giriş yapıldığına dair uyaran bir yazılımdır [11].

AntiPhish yapısı itibariyle bazen yanlış alarm verebilen bir yazılım olduğundan bu eksikliği gidermek adına bir çalışma yapılmıştır. Bu amaçla AntiPhish yazılımının eksikliklerini gidermek adına DOMAntiPhish geliştirilmiştir. DOMAntiPhish kötü niyetli web sayfalarının gerçek web siteleri ile olan benzerliklerine dayanarak kötü niyetli web sitelerini ayırt etme temeline dayanan bir yaklaşımdır. Yapılan testler sonucunda da DOMAntiPhish'in AntiPhish'e göre daha başarılı olduğu tespit edilmiştir [28].

İnternet kullanıcılarını, girdikleri site hakkında bilgilendiren yazılımlardan bir diğeri de iTrustPage'dir. Bu yazılım, kullanıcı şüpheli bir internet sayfasına girdiğinde kullanıcıdan yapmak istediği işlemi tanımlamasını ister. Kullanıcı istenen bilgiyi girdiği zaman, yazılım girilen bilgilere göre bir arama yapar, eğer girilen bilgilere göre dönen sonuçlar içinde söz konusu site ilk sıralarda değilse kullanıcıyı şüpheli bir siteye girildiği konusunda uyarır [29].

Bahsi geçen web tarayıcılarına ait eklentilerin yanında SpoofGuard, SpoofStick, Cloudmark, Fraud Eliminator, eBay Toolbar, Site Safe, PwdHash, Petname gibi dolandırıcılık amaçlı kullanılan siteleri tespit ederek kullanıcıları bu konuda uyaran eklentiler de geliştirilmiştir[30].

Sazan avlama ile mücadelede kötü niyetli web sayfalarını ifşa eden kara liste yaklaşımı kuşkusuz kullanıcıları bilinçlendirmek adına önemlidir. Ancak sürekli yeni sahtecilik amaçlı web sayfalarının üretildiğini düşünürsek bu yaklaşım internet kullanıcılarını korumak için yeterli değildir. Bu nedenle dolandırıcılık amaçlı kullanılan e-posta adreslerini sınıflandırma(Dynamic Markov Chains Class-Topic Models) mantığına dayanarak tespit etmeye çalışan bir yaklaşım ortaya atılmıştır. Bu çalışmada önemli sonuçlar alınmış ve bu yaklaşımın daha fazla geliştirilmesiyle daha iyi sonuçların alınabileceği düşünülmektedir [31].

Sazan avlama ile mücadelede en önemli noktalardan biri de internet kullanıcılarının bilinçlendirilmesidir. Yapılan bir çalışmaya göre öğrencilere bir sazan avlama saldırısının ne şekilde çalıştığının ve kurbanları nasıl tuzağa düşürdüğünün anlaşılması için çeşitli uygulamaların yapılması sonucunda

öğrencilerin bu konuda daha fazla bilinçlendiği sonucuna varılmıştır [32]. Söz konusu uygulamalar laboratuar ortamında ve gerçek sazan avlama teknikleri kullanılarak yapılmıştır.

Tüm bu çalışmalar sonucunda elde edilen bulgulara dayanılarak en üst seviye güvenliği sağlamak için üç temel savunma stratejisinden söz edilebilir[23]:

1) Kullanıcı tarafından alınabilecek önlemler:
   - Bilgisayarını koruyacak güncel ve güvenilir anti-virüs programları ve anti-spy yazılımlar kullanmak
   - İşletim sistemini güncel tutmak
   - Gelen E-postalara karşı dikkatli olmak ve başlık bilgilerini kontrol etmek
   - E-Postaların içerdiği linkleri iyi incelemek ve mümkün olduğunca bunları kullanmamak
   - Gelen e-postalarda imla ve noktalama işaretlerine dikkat etmek
   - EarthLink Toolbar[1] gibi zararlı siteleri tespit eden yazılımları kullanmak
   - Güvenilmeyen bilgisayarlardan bankacılık işlemleri yapmamak ve düzenli hesabını kontrol ederek yapılan işlemleri kontrol etmek
   - Hesap güncellemesi gerektiğine dair gelen e-postalara cevap vermemek, linki tıklamak yerine adres çubuğuna kendi yazmak
2) Sunucu taraflı alınması gereken önlemler:
   - Güvenlik açısından düzgün web uygulamaları geliştirmek
   - Kullanıcıları zor kırılır şifreler almaya zorlamak
   - Kolay hatırlanır ve kolay anlaşılır alan adı almak
3) Kurumsal düzeyde alınabilecek önlemler:
   - Otomatik yetkilendirme sağlayan e-posta sistemlerini kullanmak
   - Kendi alan adına benzer alan adlarını takip etmek
   - Ant-virüs, anti-spam gibi servisleri kullanmak
   - Kullanıcıları riskler hakkında bilgilendirmek

Sazan avlama ile mücadelede çoğu internet tarayıcısı tespit edilen zararlı siteleri engeleyici ve kullanıcıyı bu konuda uyarıcı eklentiler içerecek şekilde geliştirilmektedir. Ancak her kuruluşun veya internet tarayıcısının tespit ettiği zararlı siteleri içeren kara listeyi tutacak ve ilgili tüm kuruluşlarla paylaşacak uluslararası bir organizasyona ihtiyaç duyulmaktadır[11].

III. SONUÇ

Sazan avlama dolandırıcılığı sürekli kendini geliştiren ve çok sayıda insanı mağdur eden bir dolandırıcılık yöntemi olarak karşımıza çıkmaktadır. Saldırganların internet ortamında gerekli kaynaklara çok kolay ulaşabilmeleri bu dolandırıcılığın hızla gelişmesinin en önemli nedeni olarak karşımıza çıkmaktadır. Bu dolandırıcılık yönteminden korunmak için çeşitli çalışmalar yapılmakta olmasına rağmen çok etkili bir teknik henüz geliştirilememiştir. Bu amaçla kullanıcıların ve servis sağlayıcıların dikkat etmesi gerekenler yukarıda başlıklar halinde açıklanmaya çalışılmıştır. Bunlara ek olarak, Dünyadaki tüm sazan avlama sitelerini içeren kara listeyi tutan bir organizasyonun sorunun çözümünde büyük rol oynayacağı değerlendirilmektedir.

[1] http://www.earthlink.net/software/domore.faces?tab=toolbar

KAYNAKLAR

[1] TBB (Türkiye Bankalar Birligi), İnternet Bankacılıgı İstatistikleri, TBB-Aralık 2011, Ankara, 1-2, 2011.
[2] Anti Phishing Work Group(APWG)'s 1st Half of 2011 Phishing Activity Trends Report, http://www.antiphishing.org/reports/apwg_trends_report_h1_2011.pdf
[3] Harris B., *Yemleme*. http://tr.wikipedia.org/wiki/Yemleme. Giriş Tarihi: 12.02.2012.
[4] G. Canbek, Ş. Sağıroğlu, *Kötücül ve Casus Yazılımlar: Kapsamlı Bir Araştırma*, Gazi Üniv. Müh. Mim. Fak. Dergisi, Cilt:22, No:1,121-136,2007
[5] R. Damodaran, M. C. A. Phil, M. L. Valarmathi, *Phishing Website Detection and Optimization using Modified Bat Algorithm*, International Journal of Engineering Research and Applications, Vol. 2, Issue 1, pp. 870-876, Jan-Feb 2012.
[6] M. Jakobsson, *Modeling and Preventing Phishing Attacks*, In Financial Cryptography, 2005.
[7] A.Karakasiliotis, S.M.Furnell, M.Papadaki, Assessing end-user awareness of social engineering and phishing, Australian Information Warfare and Security Conference, 2006.
[8] Harl, *People Hacking: The Psychology of Social Engineering*, Talk at Access All Areas III Conference, http://www.genocide2600.com/~tattooman/social-engineering/aaatalk.html, 7 Mayıs 1997.
[9] N. Barrett, *Penetration Testing and Social engineering: Hacking the Weakest Link*, Information Security Technical Report, 8(4), 56-58(2003).
[10] H. Berghel, *Phishing Mongers and Posers*, Communications of the ACM, Vol. 49, No. 4, 21-25(2006).
[11] E. Kirda, C. Kruegel, *Protecting Users Against Phishing Attack with AntiPhish*", Computer Software and Applications Conference, CONPSAC 2005, 517-524(2005).
[12] Ş. Alataş, M. Atan , *Phishing: İnternet Denizinin Popüler Avlanma Yöntemi*, XII. Türkiye'de İnternet Konferansı, 226-236(2007).
[13] J. Milletary, *Technical Trends in Phishing Attacks*, US-CERT, Reading room article, http://www.us-cert.gov/reading_room/phishing_trends0511.pdf.
[14] M. Jakobsson, S. Myers, *Delayed password disclosur*, Int. J. Applied Cryptography, Vol. 1, No. 1, 47-59 (2008).
[15] G. K. Tak, N. Badge, P. Manwatkar, A. Ranganathan, S. Tapaswi, *Asynchronous Anti Phishing Image Captcha approach towards phishing*, Future Computer and Communication (ICFCC), 2nd International Conference, 694-698(2010).
[16] T. Moore, R. Clayton, *An Empirical Analysis of the Current State of Phishing Attack and Defence*, Workshop on the Economics of Information Security, 2007.
[17] S.Vijayalekshmi, S.A. Rabara, *Fending Finanicial Transaction from Phishing Attack*, Trendz in Information Sciences & Computing (TISC), 171-175(2010).
[18] J. Milletary, *Technical Trends in Phishing Attacks*, US-CERT, Reading room article, http://www.us-cert.gov/reading_room/phishing_trends0511.pdf
[19] SMiShing: *SMs phISHING*, http://en.wikipedia.org/wiki/SMiShing, Son Günselleme Tarihi: 3 Şubat 2011, Giriş Tarihi:16.02.2012.
[20] A. Castiglione, R. De Prisco, A. De Santis, *Do You Trust Your Phone*?, LNCS 5692, 50–61(2009).
[21] M. Chandrasekaran, K. Narayanan, S. Upadhyaya, *Phishing Email Detection Based on Structural Properties*, 2nd Annual Symposium on Information Assuranc, 2007.
[22] M. Jakobsson, A. Young, *Distributed Phishing Attacks*, Workshop on Resilient Financial Information Systems, Mart 2005.
[23] G. Ollman, *The Phishing Guide: Understanding & Preventing Phishing* Attacks, IBM Security Systems.
[24] Rydstedt, G., Bursztein, E. Boneh, D., Jackson, C. Busting frame busting: a study of clickjacking vulnerabilities at popular sites, IEEE Web 2.0 Security and Privacy Conference (W2SP 2010).

[25] Anti-Phishing Work Group, http://www.antiphishing.org/, Giriş Tarihi: 17.02.2012.
[26] J. Hong, *The State of Phishing Attacks*, Communıcatıons of the ACM, Vol. 55, No. 1, 74-81(2012).
[27] R. Sumathil, R.V. Prakash, *Prediction of Phishing Websites Using Optimization Techniques*, International Journal of Modern Engineering Research, Vol.2, Issue.1, 341-348(2012).
[28] A. P. E. Rossiello, E. Kirda, C. Kruegel, F. Ferrandi, *A Layout-Similarity-Based Approach for Detecting Phishing Pages*, Security and Privacy in Communications Networks and the Workshops, 454-463(2007).
[29] T. Ronda, S. Saroiu, A. Wolman, *iTrustPage: Pretty Good Phishing Protection*, Technical Report, http://research.microsoft.com/en-us/um/people/ssaroiu/publications/tr/ut/2006/ut-csrg-545.pdf, iriş Tarihi: 29.02.2012.
[30] M. Jakobsson, S. Myers, *Phishing and Countermeasures: Understanding the Increasing Problem of Electronic Identity Theft,* Waley Publishing, New York, USA,493-513(2006).
[31] A. Bergholz, G. PaaB, F.Reichartz, S. Strobel, J. Chang, *Improved Phishing Detection using Model-Based Features*, Fifth Conference on Email and Anti-Spam CEAS 2008.
[32] C.E. Frank, L.A. Werner, *Getting A Hook On Phishing*, Information Systems Education Journal, Vol 5, No 36, 2007.

Ali ŞENOL(1985) Gazi Üniversitesi Bilgisayar Mühendisliği Bölümünde yüksek lisans yapmakta ve aynı bölümde araştırma görevlisi olarak görev yapmaktadır. Bilgi Güvenliği, Zeki Sistemler ve Veri Madenciliği alanlarına ilgi duymaktadır.

Hacer KARACAN(1980) Gazi Üniversitesi Bilgisayar Mühendisliği Bölümünde öğretim üyesi olarak görev yapmaktadır. Bilgi Güvenliği, Yazılım Mühendisliği, Veri Madenciliği ve Sanal Gerçeklik alanlarında çalışmaları mevcuttur.

Server Based Encryption (SERBASEN) Protocol on Air Gap Network

Ahmet İlhan AYŞAN, Güray YILMAZ
Computer Engineering Department
Turkish Air Force Academy
{a.aysan, g.yilmaz}@hho.edu.tr
Yeşilyurt-İstanbul, Turkey

***Abstract*— In addition to the safety storage of a data, transferring information stored on the computer system in a secure manner is an important issue and a security requirement in today's information age. Transferring data as a plain text may cause security breaches for firms and companies. In order to solve these security breaches, it is essential to use encryption system for users. However, it brings an extra workload for people to apply encryption systems because entering passwords at every encrypted data transfer attempt is required. In this study we propose SERBASEN protocol which transfer file securely on air gap networks.**

***Index Terms*— encryption, public key, USB device, security.**

I. INTRODUCTION

Security in the area of information technologies became one of the most important issues after the rapid development of computer and internet techniques. Attackers have the advantage of breaking the system due to vulnerabilities of operating system, applications and network protocol. Therefore, each domain must be physically separated from Internet to prevent unauthorized access to the system. An air gap is a security measure that separates domains each other physically. This physically separation became especially from Internet. [1] Some of network air gap is:

1) Military/governmental computer networks /systems
2) Controls of nuclear power plants
3) Computers used in aviation
4) Computerized medical equipment etc.

Main problem of the air gap network is data transportation. It is hard to prevent stored information leakage because of trade-off between confidentiality and availability. Data are transferred over the USB device, CD/DVDs, floppies. Due to USB device convenience and ease of use and connectivity, it is highly preferred in data transfer. With the plug & use feature, data transferring between computers can be done easily via USB devices. Despite of convenience and easy of usage, USB devices have also some aspects that threaten the data security. It is very difficult to keep data transfer under control over the USB. In order to eliminate security weakness, many companies deny the use of USB device; however these kinds of security policies reduce the functionality of companies.

--Nevertheless the biggest problem arisen on air gap network is transferring data out of the companies' network. The encryption systems are generally used for that purpose.

--The problems that are encountered in transferring the confidential data are:

1) Storing the password: The difficulty of storing the passwords that are used in encryption systems for data transferring. User must store the password at each data transfer.
2) The security level of the air gap network: The accessibility of sender or receiver of the encrypted data, outside of the company as a plain text. User should not access confidential data as plaintext outside of the domain. Thereby, the violation of the security policy for the domain.

According to RSA Security, business-related logins need between 6 to 12 different passwords and 13 or more passwords should be remember [2]. Using so many passwords and possibility to forget these passwords are pushing the users to store the passwords as plain texts. As a result, users tend to violate the security issues because of the excess of passwords. According to Computer Emergency Response Team (CERT) passwords are related to %80 security issue [3].

This paper is organized as follows. In section II, SERBASEN protocol is proposed. SERBASEN protocol security analysis is in section III. Section IV concludes the paper.

II. PROPOSED SCHEME

In this study, a new design which aims to secure data transfer between air gap networks is elaborated. It shows on Figure 1. For data transfer both users should exchange their USB devices due to no network connection between two domains. Users that have been authenticated by the company security policies, will be authorized to transfer and receive data. There will be an Encryption Server (ES) at every domain. On each of these servers should have the other servers' public keys.

The following steps will be experienced for the data transmission:

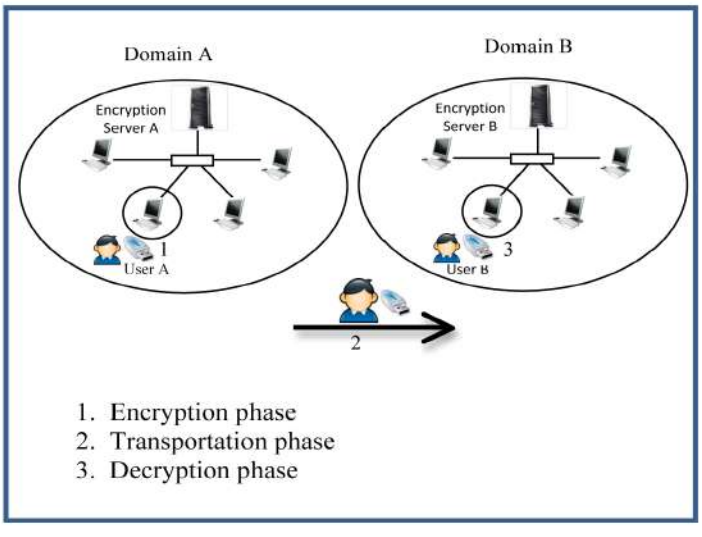


Figure1. System Design.

1) User A will plug the USB device to the computer and execute the application if only the User A has grant for data transfer.
2) User A chooses from the application that is wanted to send to the specified domain.
3) With connection between the ES A and the User A at the same domain, ES generates session key and the session key is encrypted according to the public key of the User A and ES B.
4) Data are encrypted from User A with random session key which is generated from ES A.
5) After USB device transportation, User B sends encrypted session key to ES B.
6) If User B has grant access to encrypted data, ES B decrypts encrypted session key with private key of ES B.
7) Session key is encrypted by User Bs' public key. User B decrypt session key with his private key and User B decrypts encrypted data with session key.

Before propose our scheme we describe parameters which are used in this study.

- K: Symmetric key for AES
- K(): Symmetric Function
- E(): Asymmetric Function
- D(): Asymmetric Decryption Function
- R(): Random Function
- M: plaintext messages
- C_M: Encrypted Message
- C_K: Encrypted symmetric key with server public Key
- (n,e): Public key for ES B
- (n,d): Private key for ES B
- (m,f): Public key for User A
- (m,g): Private key for User A
- (r,h): Public key for User B
- (r,i): Private key for User B

In this study we use public key and symmetric encryption systems between the domains. RSA [5] algorithms are used for the key exchange and AES [6] algorithms are used for the symmetric encryption systems. Since the public key systems are slower than symmetric encryption systems, both are used together. For efficient encryption system, asymmetric encryption use for session key exchange. Transferred data are encrypted with the AES algorithm. With the RSA algorithm; the session key of the AES algorithm is transferred securely.

Users mostly decide session key which they use on symmetric encryption. But they could use that session key to get plaintext outside of the domain. In this study, our protocol's main goal is to prevent confidential data leakage outside of the domain. Session key is generated from random function on each ES.

Our protocol has four phases for secure file transfer.

A. Authentication phase:

At this phase ES checks user whether is authenticated. ES use Lightweight Directory Access Protocol (LDAP) [7] for authentication. Each domain system administrator has authority to give permission for each user.

B. Encryption phase:

This phase has seven sub-phases. It shows on Figure 2.

1) For exchange AES key, ES A needs ES Bs' public key (n,e). We use RSA algorithm for creating public key.
2) After User A request to ES A for another domain member User B, ES A creates random symmetric session key K which it is length 256 bit. K=R().
3) At this sub-phases User A needs session key K for encrypts its own message. ES A encrypt session key K with User As' public key (m,f).

$$C_{KUA}=E(K)=K^f \bmod (m). \quad (1)$$

4) ES B needs session key K so compute the cipher K with ES Bs' public key.

$$C_{KSB}= E(K)=K^e \bmod (n). \quad (2)$$

5) After ES A encrypt session key K for User A and ES B, ES A sends value "(1) and (2)" to User A.
6) When User A gets "(1)" it decrypts its own private key to get AES session key K.

$$K=D(C_{KUA})= C_{KUA}{}^g \bmod (m). \quad (3)$$

7) User A encrypt message with using AES algorithm and use session key K. After symmetric encryption it computes

$$C_M = K(M) \quad (4)$$

User A stores (2) and (4) encrypted data to USB device. User A will transport USB device to User B. At this stage if USB device is stolen, attacker couldn't get plaintext without symmetric session key K.

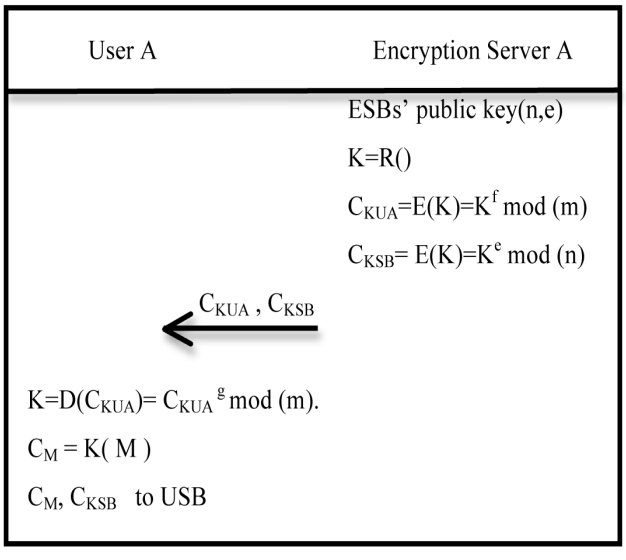


Figure2. Encryption Phase

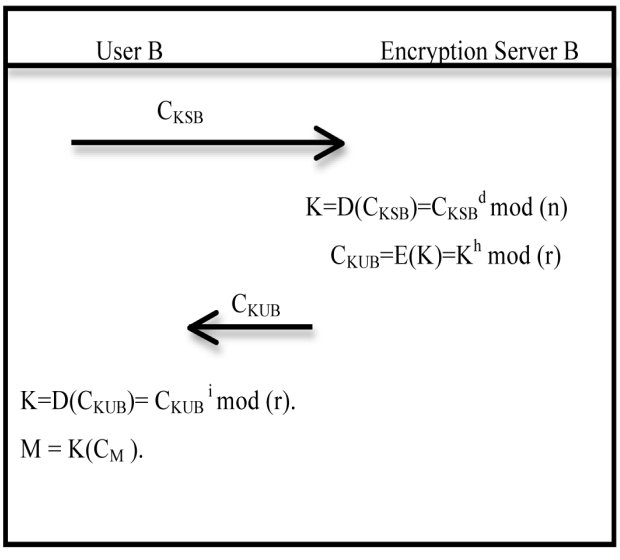


Figure3. Decryption phase.

C. Authentication phase:

At this phase ES B checks User B whether is authenticated. No authenticated user access the message. If user has not grant to access message ES B does not send session key K.

D. Decryption phase:

This phase has four sub-phases. It shows on Figure 3.

1) User B will send key value "(2)" to ES B. ES B uses its own private key to get symmetric session key K,

$$K=D(C_{KSB})=C_{KSB}{}^d \bmod (n). \quad (5)$$

2) ES B sends session key K with User Bs' public key (r,h).

$$C_{KUB}=E(K)=K^h \bmod (r). \quad (6)$$

3) When User B gets the C_{KUB} it decrypts its own private key to get AES session key K.

$$K=D(C_{KUB})= C_{KUB}{}^i \bmod (r). \quad (7)$$

4) User B decrypt data which is on USB device with session key K.

$$M = K(C_M). \quad (8)$$

The most important goal of this design is to prevent users from entering the transferred data outside of the company. Hence, the security level of domain maintenance can be obtained. When users encrypt message with AES algorithm password at encryption process they do not decide the session key K. The AES algorithm will use the session key K that are set with random function R() by the Encryption Servers. User gets "(1)" for symmetric encryption.

III. SECURITY ANALYSIS

In this chapter we analyze our system according to the general security requirements [4].

A. Confidentiality

An attackers' access attempt to plaintext should be eliminated. Our system is supported confidentiality by AES algorithm and conceals the symmetric encryption session key K by RSA. ES serves only for authenticated user therefore any malicious person who captured or steals USB device could not access to plaintext on USB device. If an attacker gets $C_{KB}= E(K)=K^e \bmod (n)$ he cannot obtain session key K from C_{KB} without private key (n,d).

B. Authentication

Only legitimate user who has access permission is supported by LDAP protocol. User grants should be set by system administrator. Each domain policy decides counts of granted user. If user has no grant to access encrypted USB device, ES does not send session key for encrypted data which are stored on USB device.

C. Impersonation attack

Illegitimate user accessing to the session key is prevented by Encryption Server. Our protocol based on LDAP to deny impersonation attack. An attacker cannot generate authenticate value without legitimate user accounts.

D. Efficiency

The system that we proposed needs computation power at data encryption phase. Symmetric encryption is utilized for data encryption. Messages are encrypted on user computers therefore ES workload is diminished. After ES generate session key with random function, ES encrypts this symmetric session key K. Therefore, it reduces encryption time.

IV. CONCLUSION

Security has become one of the most popular subjects of IT nowadays. Most enterprises put strict rules for employee to deny data leaking. We propose secure file transfer protocol on air gap network to deal with this problem. Session key distribution is major problem for secure data exchange.

SERBASEN takes session key rights from user, therefore user data leakage ability is getting low. SERBASEN protocol does not use user public key at data transmission stage in our protocol. Thus it makes it simple but efficient. Public and private keys of the users can also be used to increase the security of the system. However, in this kind of approach, since there are not any constant connections between domains, the usage of public and private keys by the users will bring out administrative difficulties. The changes in working staff will harden the usage of each individual's public keys.

REFERENCES

[1] Jack Brassil, "Physical Layer Network Isolation in Multi-tenant Clouds", 2010
[2] RSA Security, "The 2nd Annual RSA Security Password Management Survey", 2006.
[3] Kaleb Brasee and S. Kami Makki, "A Novel Distributed Authentication Framework for Single Sign-On Services", 2008.
[4] Sun-Ho Lee, "A Secure Solution for USB Flash Drives Using FAT File System Structure", 2010.
[5] R. Rivest, A. Shamir and L. Adleman, "A Method for Obtaining Digital Signatures and Public-Key Cryptosystems. Communications of the ACM", 1978.
[6] V. R. Joan Daemen, "AES Proposal: Rijndael, version2, AES submission. 1999".
[7] Xu Dawei and Hu Xiaohong, "The Design of NPKI System Based LDAP", 2011.

Encrypted Individual Multiple Choice Questions

M. K. Ulukök, Z. B. Şensoy

***Abstract*—An unusual application of cryptography on preparation of encrypted Individual Multiple Choice Questions (*IMCQ*) is investigated. The work is motivated by *ÖSYM* (National University Entrance Exam of Turkey in 2011). Individual question sheets are prepared for each student having their own answer keys. This encryption is performed using Vernam encryption method. The original exam questions are randomly ordered for each student. Thus, a separate answer key is created for each one. There is no assigned priority to any questions. In the implementation, the randomly generated one-time pads (keys) are permutations of n numbers where n is number of questions. *IMCQ* differs from usual Vernam encryption's keys with respect to true-randomness.**

***Index Terms*—Cryptography, Encryption.**

I. Introduction

SINCE the cryptology has been discovered, secure communications and data security issues of organizations and individuals have been indispensable. The encryption algorithms are used basically to encrypt a message or data. Encrypted individual multiple choice questions are an unusual application of encryption. The multiple choice exams are usually prepared with at least two different booklets. The application of Vernam method was used to prepare individual student booklets having specific order of questions for 205 students in an exam of a course called "Bilgisayar I", CME101.

II. Cryptology

Cryptography and cryptanalysis are two main fields of cryptology. Cryptography deals with the encryption of messages and data. Encryption algorithms are classified as symmetric and asymmetric encryption methods [1]. Symmetric encryption uses single key and asymmetric encryption method uses two keys, general key and special key, for encryption and decryption. Cryptanalysis is the study of decryption or analysis of encrypted message. The first crypto system was used by Julius Caesar [2]. Caesar encryption is one of the basic encryption method which based on the modular arithmetic. The process of encrypting a message in Caesar encryption can be performed by shifting the letters of an alphabet. An encryption of a letter x with key k is performed with encryption function (1) and the decryption of same letter is performed with decryption function (2).

$$E_k(x) = (x + k) \bmod 26 \quad (1).$$

$$D_k(x) = (x - k) \bmod 26 \quad (2).$$

For example, a message "CAN" is encrypted with function (1) and key k=3. The result of encryption is "FDQ" with Caesar encryption algorithm. The same key is used to decrypt the encrypted message to obtain the original one. Although Caesar algorithm is easy to use, it can be easily broken [2].

Vernam method is another symmetric encryption which also known as one-time pad encryption. One-time pad encryption firstly discovered in 1882 by Frank Miller [3]. The same method was reinvented in 1917 by Gilbert Stanford Vernam and Joseph Mauborgne without be aware of its first invention [3]. This encryption method based on a random key for each message which has the key length of original message length. One-time pad encryption is the only method which is theoretically proven as unbreakable [4]. However, this encryption method is not preferred in practice because of its implementation difficulty.

III. Literature Review

Multiple choice questions are generally generated from a list of questions. To prevent cheating, several booklets are prepared by shuffling the questions. There are some tools that generates tests from a databank of static questions [5]. This online assesment system adaptively selects question indices. Another type of automatic question generation is based on estimating students' profile. An online question generating system decides a next question to be asked depending on the student's previous answer in the area of electrical circuits analysis [6]. Both of above systems require authoring and storing huge number of questions. Uğurdağ et. al. [7] develeoped a tool that dynamically generates questions based on some parameters to have myriad number of question versions. This system also works online.

The study is generated from the national university entrance exam of Turkey in 2011 (*ÖSYM*). Same questions were used for all students' booklets having different answer keys. The examination was a written exam and it was performed in classrooms. Similarly, *IMCQ* also uses same questions and individual answer keys are generated for all booklets. Questions are stored as text of questions with corresponding correct answer and wrong answers. Neither diversification of questions nor adaptive question selection is performed in this

M. K. Ulukök is with the Computer Engineering Department, Cyprus International University, TRNC (phone: 392-671-1111; fax: 392-671-1142; e-mail: mkose@ciu.edu.tr).

Z. B. Şensoy is with the Computer Engineering Department, Cyprus International University, TRNC (e-mail: zbsensoy@ciu.edu.tr).

study.

IV. Implementation of IMCQ with Vernam Encryption

Symmetric key encryption methods encrypt and decrypt messages using the same key. Original message is called plain text and encrypted message is called as cipher text. Classical encryption and decryption of a message are shown in Fig. 1.

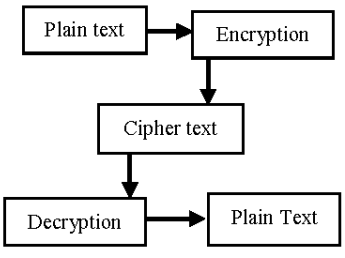


Fig. 1. Classical text encryption and decryption.

In Vernam encryption, a message m having j number of characters (m_1, m_2,..., m_j) is encrypted using function (3), and a cipher text c (c_1, c_2, ..., c_j) with key k (k_1, k_2, ..., k_j) is decrypted using function (4).

$$E(m_j, k_j) = c_j \quad (3).$$

$$D(c_j, k_j) = m_j \quad (4).$$

In this study, Vernam encryption method is used to implement IMCQ. The original exam questions are randomly ordered for each student. Thus, a separate answer key is created for each one. Each answer key is a sequence of length n. The possible number of randomly generated keys are permutations of n numbers where n is number of questions.

TABLE I
MULTIPLE CHOICE QUESTION ENCRYPTION

Student IDs	Randomly generated key for each student (k_j), $1 \le j \le N$, j is an integer	Encrypted answer keys for each student
546875	5, 9, 15, *n*, … , 20	a, c, a, b, …, d
…	…	…
153467	12, n, 3, 9, … , 17	c, b, a, b, …, a

The student numbers are assumed to be eight digit positive integer M_i (i=1,...,N, N is the number of students). Students' questions and their corresponding encrypted correct answers are summarized in Table I.

In this application, the encrypted students' answer keys are calculated by the encryption function (5).

$$E(m_j, k_j) = (m_j + k_j) \bmod 4 \quad (5).$$

In modular arithmetic operation, the second operand must be the number of choices. The result of mod operation is coded to "*a*, *b*, *c*, and *d*" respectively as correct answer choices. The encryption process produces answer keys for each student with the length of number of questions.

The number of possible keys is 1.55×10^{25} for 25 questions. Even if the same key is randomly generated for more than one student, different answer keys are created. This is because, unique student numbers are used in encryption process. If any of the students in the exam tries to decrypt the corresponding answer key, s/he needs to guess the original question index in their questions. The probability to find the possible key is 1/(25!). The student's encrypted multiple choice exam preparation process is shown in Fig. 2.

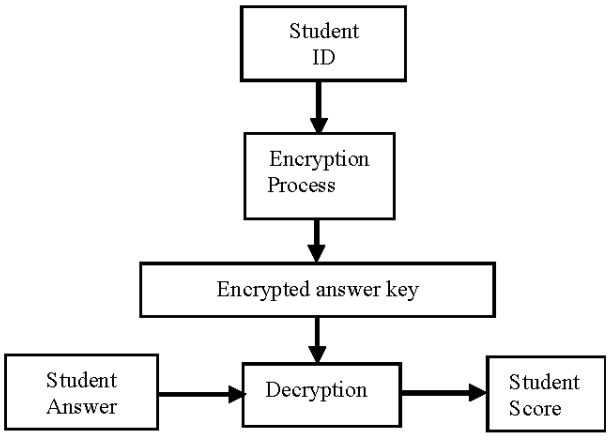


Fig. 2. Encryption and decryption processes for individual student's question booklet.

The decryption process of the implementation is performed by comparing the student answers with the corresponding answer keys. Student scores are calculated as the result of decryption.

V. Analysis of IMCQ Encryption

Vernam encryption method is applied to IMCQ exam preparation. The distribution of the original question (25 questions) with the special exam booklets for 205 students are given in Fig. 3. It is observed that there are 13 students having same question index with the original ones. The original question index remained unchanged in the question order of 12, 15, 18 and 25. This distribution of questions differs from the generation of new answer keys.

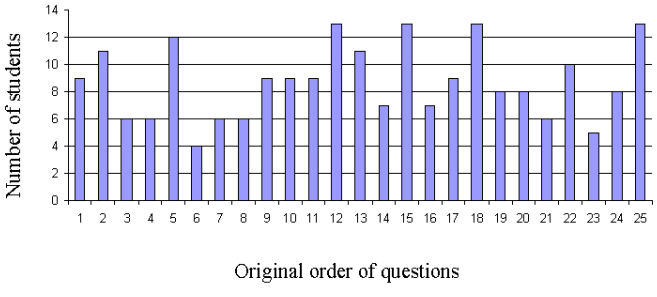


Fig. 3. Distribution of original question index to the booklets.

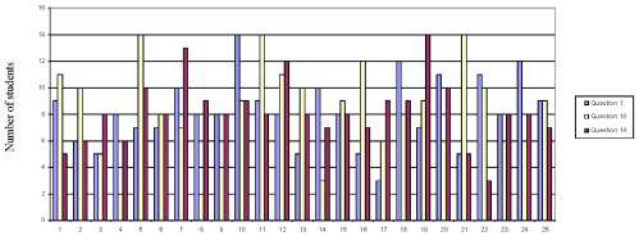
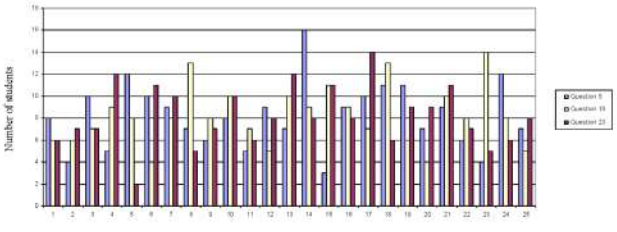


Fig. 4. (a) Distribution of questions 1, 10, 14 in booklets.



(b) Distribution of question questions 5, 18, 23 in booklets.

The randomness of selected questions (question 1, 5, 10, 14, 18, 23) is illusturated in Fig. 4 (a) and (b). These figures show that the frequency of students having same original question as appeared in same index number. For example, there are 14 booklets which have question 10 (in original index) is appeared as question 5.

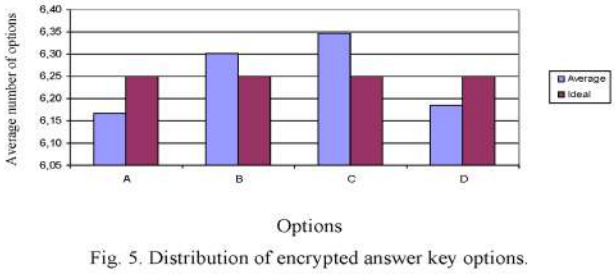


Fig. 5. Distribution of encrypted answer key options.

The average of four choices in the encrypted answer keys is found as around 6. It is observed that 53 students have maximum 8 same choices and 2 students have minimum 3 same choices. The expected number of choices in an exam having 25 questions and four choices is 6.25. The average of occurance of each choice is in Fig. 5.

VI. Conclusion

In this study, special question booklets are prepared for each student. It is found that special question booklet for each student can be easily prepared with Vernam encryption method. There is no need to have special programming software to implement such an application. The application is developed by using office programs. This method can be applied to any multiple choice test. Questions, correct answers and wrong answers must be stored in plain text format. Therefore, *IMCQ* can be easily implemented to any kind of test questions stored as text. The students' answer sheets are retrieved from an optic reader and then they scored by comparing with the corresponding encoded answer keys. The submission of special exam booklets to the students is easier than the submission of different types of booklets. Vernam encryption method is successfully implemented with *IMCQ* for a course named as Bilgisayar I where the registered number of students is 205.

References

[1] H. Kodaz and F. M. Botsalı. (2010). Simetrik ve Asimetrik Şifreleme Algoritmalarının Karşılaştırılması. Journal of Technical-Online. [Online] vol. 9(1), pp. 10-23. Available: http://alaeddin.cc.selcuk.edu.tr/~tekbil/ocaknisan2010/hkodaz/hkodaz.pdf

[2] M. Şahin, A. B. Ekin. (2011). Kriptoloji : Ankara Üniversitesi Açık Ders Materyalleri. [Online]. Available: http://acikders.ankara.edu.tr/course/view.php?id=42

[3] J. Markoff. (2011, July 25). Codebook Shows an Encription Form Dates Back to Telegraphs. The New York Times. [Online]. Available: http://www.nytimes.com/2011/07/26/science/26code.html?ref=science

[4] C. E. Shannon, "Communication Theory of Secrecy Sytems", Bell System Technical Journal, vol. 28, no. 4, pp. 656-715, 1949.

[5] A.T. Fong, H.H. Siew, P.L. Yee, L.C. Sun, "IOAS: An Intelligent Online Assessment System", Journal of WSEAS Transactions on Computers, vol. 6, vo. 3, pp. 552-559, 2007.

[6] P.D. Cristea and R. Tuduce, "Automatic Generation of Exercises for Self-Testing in Adaptive E-Learning Environments: Exercises on AC Circuits", Inter. Workshop on Authoring of Adaptive and Adaptable Educational Hypermedia (part of WBE), 2005.

[7] H. F. Ugurdag, E. Argalı, O. E. Eker, A. Basaran, S. Gören, H. Ozcan, "Smart Question (sQ): Tool for Generating Multiple-Choice Test Questions", 8th WSEAS International Conference on EDUCATION and EDUCATIONAL TECHNOLOGY, Italy, October 17-19, 2009.



Mehtap K. Ulukök- Born in Silivri in 1975. Graduated from the Department of Computer Engineering, Eastern Mediterranean University, Famagusta, T.R.N.C at 1998. Master and PhD programs were completed in the Department of Computer Engineering, Eastern Mediterranean University, in 2000 and 2009, respectively. Artificial intelligence is the main research topic.

She has several publications about metaheuristic searches, expert systems and robot control.



Zehra B. Şensoy- Born in Famagusta, 1971. Graduated from the Department of Applied Mathematics and Computer Science, Eastern Mediterranean University, Famagusta, T.R.N.C at 1993. Master and PhD programs were completed in the Department of Mathematics, Eastern Mediterranean University, in 1995 and 2006, respectively. Convex programming is the main research topic.

She has several publications about convex programming and graph theory.

Utilizing a Graphical User Interface for Image Encryption based on Chaotic Algorithm

H. Ogras, M. Turk, and T. V. Pham

Abstract— **In this study, a graphical user interface for a chaos-based image encryption scheme is proposed. The image encryption algorithm contains two major parts, namely Arnold Cat Map and Lorenz chaotic system. The Arnold Cat Map takes the concepts from linear algebra and uses them to change the positions of the pixel values of the original image and finally creates a shuffled image. Lorenz chaotic system will then take the shuffled image and change the actual grayscale values of the pixel, the result will be the final encrypted image.**

This paper also describes a software package which is designed by using Matlab's Graphical User Interface (GUI) in order to provide a tool to be used for chaos-based image encryption scheme. The basic working principle of this software package is to perform matrix calculations of source image data and chaotic key codes for both encryption and decryption process. Decryption is achieved by using the encrypted data and identical key sequences through the same algorithm technique.

Index Terms— **Chaotic cryptography, GUI, Image encryption, Lorenz system**

I. Introduction

In recent years, digital communication based on chaotic systems gains more and more concern on its research and application in the communication areas with the increasing development of nonlinear systems [1]. Chaotic signals with their inherit wideband characteristic, random-like, non-periodic and having low power spectrum density are natural candidates for the properties that coincide with requirements for signals applied in secure communication systems such as robustness in multipath environment, ease of spectrum spreading, added security etc.

Chaos is one type of complex dynamic behaviors generated by deterministic nonlinear dynamical systems and widely used in image encryption systems [2,3]. Chaotic maps are extremely sensitive to the initial conditions and its own parameters which makes them suitable for constructing encryption algorithms in secure communication. Chaotic encryption algorithm has advantages of a large space, simple implement, robustness and faster encryption over the traditional method [4]. One of the basic approaches that has been proposed to enhance the safety of chaotic communication systems is cryptosystem that simply converts the original message into apparently random non-sense message.

A chaos-based symmetric encryption, where the same secret key is needed to encrypt and decrypt the information, and stream cipher algorithm where the message is encrypted bit-by-bit with the application of a secret key is used in this paper. Decryption process will be achieved by using the same algorithm as in encryption and with the same secret key generator. The proposed encryption scheme includes Arnold Cat Map and three-dimensional Lorenz system.

The rest of this paper is organized as follows. Section II presents the proposed encryption scheme and the graphical user interface which is designed in Matlab/GUI environment. Section III describes computer-based graphical results using GUI with discussions of security analysis. Section IV introduces some security analysis of the proposed encryption method. Finally, some conclusions will be given in Section V.

II. Description of the Image Encryption Algorithm

The encryption process consists of two parts. In the first part, the algorithm takes a source image P and shuffles its pixels by using Arnold Cat Map (ACM) transformation. The second part of the algorithm changes the grayscale values of the pixels using Lorenz chaotic system.

A. Arnold Cat Map

Assume that, we have an $N \times N$ image P with the pixel coordinates, $L = \{(x, y) | x, y = 0, 1, 2, ..., N-1\}$. ACM is defined as [5]

$$\begin{bmatrix} x' \\ y' \end{bmatrix} = A \begin{bmatrix} x \\ y \end{bmatrix} = \begin{bmatrix} 1 & p \\ q & pq+1 \end{bmatrix} \begin{bmatrix} x \\ y \end{bmatrix} \bmod N$$

where p and q are positive integers and x' and y' are the coordinate values of the shuffled pixel. Notice that, $\det(A) = 1$ which makes the map area-preserving. When iterating this map for n times, we have

$$\begin{bmatrix} x' \\ y' \end{bmatrix} = A^n \begin{bmatrix} x \\ y \end{bmatrix} \bmod N = M \begin{bmatrix} x \\ y \end{bmatrix} \bmod N$$

where

$$M = \begin{bmatrix} m_{11} & m_{12} \\ m_{21} & m_{22} \end{bmatrix} = A^n \bmod N .$$

Except the two parameters of p and q, ACM also provides us with an additional key parameter which is the number of iterations n. An interesting property of the ACM is the Poincare Recurrence Theorem, which states that certain systems will return to a state very close to the initial state after a sufficiently long time. This means that after a certain number of iterations the ACM will return to its original state.

In our case, Lena image of 256×256 with a period of 192 is used in our graphical interface. Values of p=q=1 are selected for the ACM parameters that can be considered as a key for decryption process.

B. Lorenz Chaotic System

Lorenz chaotic system is a set of differential equations given as

$$\dot{x} = \sigma(y - x)$$
$$\dot{y} = rx - y - xz$$
$$\dot{z} = xy - bz$$

where σ, r and b are parameters of the system. Lorenz system [6] is chaotic when the parameters have the values of $\sigma = 10, r = 28$ and $b = 8/3$.

Lorenz chaotic system also gives us three keys, the initial values of x_0, y_0 and z_0. These are sensitive parameters due to the fact that chaotic systems exhibit a great sensitivity to its initial conditions and thus will change dramatically.

In this paper, we use Lorenz system as a chaotic key generator due to the having three-dimensions, very popular and one kind of easy chaotic system that can be modeled in computer environment.

C. The proposed Image encryption procedure

The cryptosystem in this paper is to encrypt image by shuffling pixel values and then changing the grey scale values to create a ciphered image. The pixel values are rearranged using ACM and then grey scale values ranging between 0 to 256, are changed using Lorenz chaotic system.

In this section, the algorithm of the proposed image encryption will be discussed step by step procedure as well as decryption process.

1. Take the original 256×256 image P, and apply ACM transformation to it, N times in Matlab environment. This creates a new image called shuffled image.

2. Initial values of x_0, y_0 and z_0 are randomly chosen for Lorenz system and then iterate the system to generate enough number of chaotic keys for 256×256 image.

3. After the iteration, we obtain three solutions of x, y and z from the system and then to produce chaotic keys for encryption,

$$C_x = \mathrm{mod}[(Abs(x) - Floor(Abs(x))) \times 10^{14}, 256]$$
$$C_y = \mathrm{mod}[(Abs(y) - Floor(Abs(y))) \times 10^{14}, 256]$$
$$C_z = \mathrm{mod}[(Abs(z) - Floor(Abs(z))) \times 10^{14}, 256]$$

4. Then the shuffled image from set B will be encrypted as

$$L_x = B_x \oplus C_x$$
$$L_y = B_y \oplus C_y$$
$$L_z = B_z \oplus C_z$$

The set L will be the ciphered pixel values whose gray levels have been changed; the image L will be the final encrypted image. The symbol of $\oplus$ represents bitwise "exclusive or" function.

Decryption process is achieved by using the encrypted data and identical key sequences through the same algorithm technique as shown below.

1. Lorenz chaotic system is again operated with same initial conditions to generate the identical chaotic keys.

2. After that, using the same algorithm technique, namely XOR operation provides shuffled data of the original image from the ciphered pixel values.

$$F_x = L_x \oplus C_x$$
$$F_y = L_y \oplus C_y$$
$$F_z = L_z \oplus C_z$$

3. Then reshaping the sequence F into the $N \times N$ image, obtain shuffled image of the original image.

4. It is stated that ACM is a periodic transformation, so shuffled image is needed to be iterated until we get the original image back.

D. Graphical User Interface

It is appreciated that, most of the computer simulation studies require a graphical user interface (GUI) that makes user interaction easier and more effective when compared with classical text based approaches [7].

A successful GUI not only facilitates easy and effective data preparation process but also allows post processing of the results and most importantly permits the user to see everything at once. That's why we design a GUI for the purpose of observing all results momentary in graphical manner. Flowchart of the GUI is shown in Fig. 1.

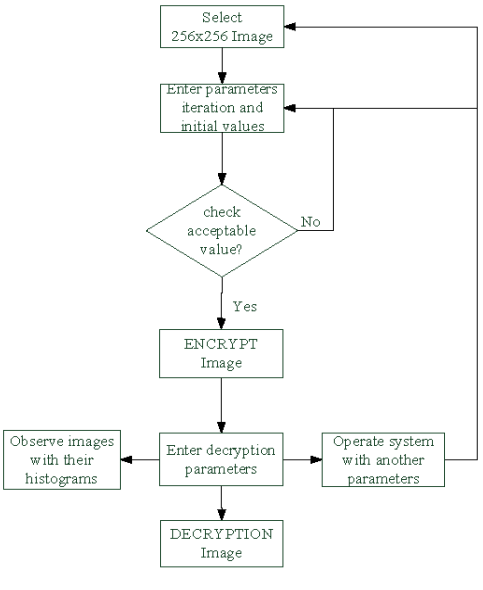


Fig. 1 Flowchart of the GUI

III. THE RESULTS AND EXPERIMENTAL ANALYSIS

As a source image, Lena image of 256×256 is used in our experimental works. Lena image is shown in Fig. 2 with its histogram.

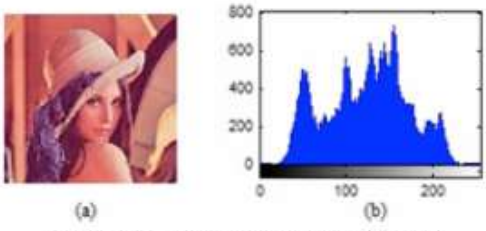


Fig. 2 Source image and its histogram

Before the encryption process, the pixel values of the source image are rearranged using ACM and shuffled image is created. The histogram of the shuffled image is the same as the histogram of the original image as seen that in Fig. 3.

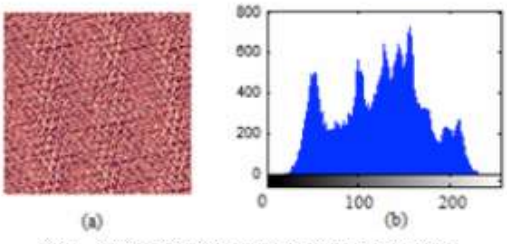


Fig. 3 Shuffled image and its histogram

The iteration number for ACM is selected as $n=7$, this value is depend on user preference in GUI. Then, the image is encrypted by using the proposed algorithm with initial values $x_0 = 2$, $y_0 = -1$ and $z_0 = 1$. The encrypted image and its histogram are shown in Fig. 4.

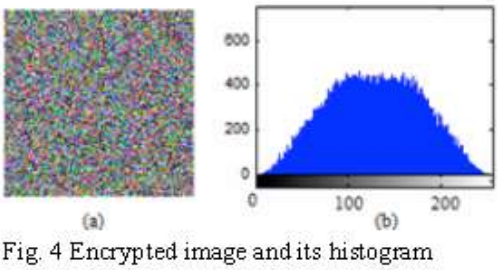


Fig. 4 Encrypted image and its histogram

The encoded message has a very good statistical characteristic, where the pixels of the digital image are changed and scrambled as shown in its histogram.



Fig. 5 Encrypted image and decrypted image

The encryption algorithm should use a map with multi-parameter with a wide range in order to enhance the security of the system for the exhaustion attack. In this situation, the initial conditions of the system and iteration number of the ACM can be considered as secret keys for the proposed encryption algorithm.

The decryption process is extremely sensitive to the initial of the system such as when $x_0 = 1.99999$ is used instead of $x_0 = 2$, then the image can not be decrypted correctly as shown in Fig. 6.

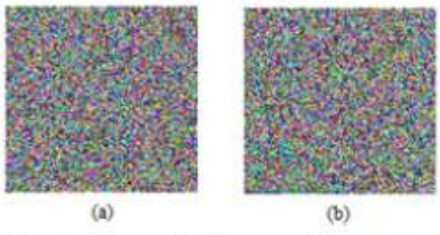


Fig. 6 a) Encrypted image with $x_0 = 2$
b) Decrypted image $x_0 = 1.99999$

When the initial values are same for both encryption and decryption, but having different iterations, the resulted image is shown in Fig. 7.

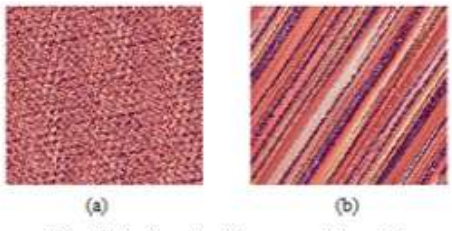


Fig. 7 a) Shuffled image with n=7
b) Recovered image with n=9

However, when the iteration number is n=199, instead of n=9, then the image can be fully recovered after the decryption process because of original image has a period of 192. This situation is shown in Fig. 8.



Fig. 8 Recovered image with n=199

IV. SECURITY ANALYSIS

A good encryption procedure should be robust against the different kinds of cryptanalytic [8] such as brute-force attacks, statistical attacks, diferential attacks, etc. In this section, the performance of the proposed encryption algorithm will be analyzed in detail.

4.1 Key Space Analysis

A good encryption scheme should be sensitive to the secret keys and the key space should be large enough to make brute-force attacks infeasible [9]. In our case, the secret key of the proposed algorithm is (x_0, y_0, z_0, p, q, n) and if the precision is 10^{-15}, then the key space size will be about 10^{90}. Apparently,

the key space is large enough to resist all kinds of brute-force attacks.

Furthermore, key sensitivity of the system has been carefully performed, as one of the key x_0 is selected with very small movement (10^{-16}), will result in an incorrect decrypted image. Therefore, it is concluded that the encryption algorithm is extremely sensitive to keys and can resist the various sensibility attacks.

4.2 Histogram Analysis

It is important to ensure that encrypted and original image do not have any statistical similarities in order to prevent leakage of information to attackers [10]. The histogram analysis clarifies how pixels in an image are distributed by showing the number of pixels at each different intensity value found in that image.

The encrypted image histogram is quite different from the source image histogram as it is shown in Fig 2 and Fig. 4.

4.3 Correlation Coefficient Analysis

It is well known that the adjacent pixels of an image have a good correlation coefficient in horizontal, vertical and diagonal directions. Hence, correlation coefficient can be used to quantify correlation property between two variables.

Correlation coefficients are calculated in Matlab environment using the following equation,

$$c = \frac{\sum_m \sum_n (A_{mn} - \bar{A}).(B_{mn} - \bar{B})}{\sqrt{(\sum_m \sum_n (A_{mn} - \bar{A})^2).(\sum_m \sum_n (B_{mn} - \bar{B})^2)}}$$

where $\bar{A}$ =mean2(A), and $\bar{B}$ =mean2(B) are source image and encrypted image respectively.

Table 1 shows the value of correlation coefficients for the source and encrypted images according to the iteration number and initial values of the system.

Table 1

Lena image	$x_0 = 1$ $y_0 = z_0 = 1$	$x_0 = 0.99999$ $y_0 = z_0 = 1$	$x_0 = 1$ $y_0 = z_0 = 1$
Corr.coefficient of source and encrypted image	0.00251	0.00649	-0.00324
	N=3	N=3	N=4

Correlation coefficients are close to zero which means that there is almost no relationship between source image and encrypted image.

4.4 Information Entropy

Information entropy is a concept from information theory that is defined to express the degree of uncertainties in the system [10].

In image processing, entropy can be used to measure the distribution of pixel values. The more even distribution of the pixel values of the image, the greater the image information entropy is.

It is known that the entropy of a message source can be calculated as

$$H(m) = \sum_{i=0}^{2N-1} p(m_i).\log_2 \frac{1}{p(m_i)}$$

where $p(m_i)$ represents the probability of symbol m_i. Suppose that, source image emits 2^8 symbols with equal probability, then the entropy is equal to 8. In fact, in practical situation, its entropy value is smaller than the ideal one. So, when the message is encrypted, its entropy should ideally be 8. The entropy values for source and encrypted image are shown in Table 2.

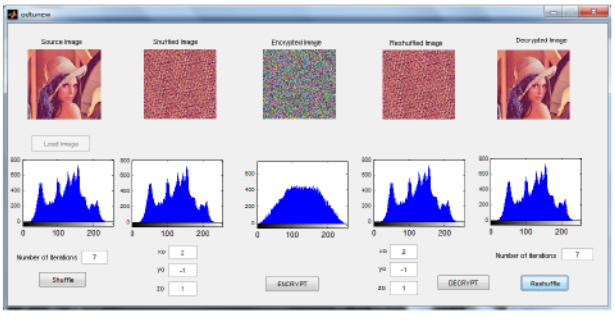
Table 2

Lena image	Source image	Encrypted image
Entropy	7.7775	7.9983

It is easily observed that the entropy value after the encryption process is 7.9983, which is so close to the theoretical maximum value which means that leakage of information is negligible.

Our designed GUI that includes the proposed encryption algorithm in its background is shown in Fig. 9. Using designed interface, any user can study and observe related graphical results of any 256×256 image under the different conditions such as initial conditions and iteration number.

Fig. 9 Designed GUI for the image encryption



V. CONCLUSION

In this paper, an image encryption algorithm based on chaotic keys is proposed for the system having ability to encrypt digital image for secure image transmission. The results of computer graphical analysis indicate that the transmitted source image can be correctly and reliably recovered using proposed scheme.

The proposed encryption scheme can be applied and improved by using other chaotic maps. It can be developed with any discrete-time chaotic map or hyper-chaos based algorithm in order to improve security of the system.

The performances of the encryption and decryption process depend on the many factors such as ACM parameters, initial conditions of Lorenz system and iteration number of the system. Then the sensitivity is compared with respect to initial values of the system in order to evaluate the system performance. It is observed that decryption algorithm is extremely sensitive to the initial conditions.

In this paper, a software package for image encryption scheme is also presented and it can be used as a visual instruction tool for proposed chaos-based image encryption technique.

As a result, this scheme can be particularly suitable for real time applications with digital hardware and attractive since it provides simple implement, fast image encryption and secure communication.

REFERENCES

[1] Xunzhang, L. Ying, L. Sun, and Z. Li, "Research on new implementation method of chaotic model based on FPGA," *ASIC 7th International conference*, pp. 241-244, Oct. 2007.

[2] P. Ying, and L. Min, H. "A color image encryption algorithm based generalized chaos synchronization for bidirectional discrete systems for audio signal communication," *International Conference on intelligent control and information processing*, pp. 443-447, August 2010.

[3] W. Wei, L. Fen-Lin, G. Xinl, and Y. Yebin, "Color image encryption algorithm based on hyper chaos," *Information management and engineering, 2010 the 2nd IEEE Int. Conference*, pp. 271-274, April 2010.

[4] Z. Yun-peng, L. Wei, C. Shui-ping, Z. Zheng-jun, N. Xuan, and D. Wei-di, "Digital image encryption algorithm based on chaos and improved DES," *Systems, Man and Cybernetics, 2009 IEEE Int. Conference*, pp. 474-479, Oct. 2009.

[5] C. Fei, W. Kwok-Wo, L. Xiaofeng, X. Tao, "Period distribution of generalized discrete Arnold Cat Map for $N = p^e$," *IEEE transactions of information theory*, Vol. 58(1), pp. 445-452, Jan. 2012.

[6] L. Xinshu, Y. Yongguang, W. Hu, "Dynamics analysis of the stochastic Lorenz system," *Chaos-Fractals Theories and Applications*, pp.32-36, Oct. 2011.

[7] C. Depcik and D. N. Assanis, "Graphical user interfaces in an engineering educational environment", *Computer Applications in Engineering Education*, 13 (2005), pp. 48-59.

[8] L. Shujun, Z. Xuan, "Cryptanalysis of a chaotic image encryption method," *Circuits and systems*, Vol. 2 (2002), pp. 708-712.

[9] M. Zeghid, M. Machhout, L. Khriji, A. Baganne, R. Tourki, "A modified AES based algorithm for image encryption," *World Academy of Science, Engineering and Technology*, Vol. 27(2007), pp. 206-211.

[10] J. Alireza, M. Abdolrasoul, "An image encryption approach using chaos and stream cipher," *Journal of theoretical and applied information technology*, Vol. 19(2), pp. 117-125, 2010.

Security Directions in Cloud Computing Environments

Zeinab Abbasi Khalifehlou, Farhad Soleimanian Gharehchopogh

Abstract—**Nowadays, cloud computing technology lead to new fundamental alteration in everyone's perception to developments models, infrastructure architectures and provided internet services. In cloud environments, computing transfers from main frame computers to client/server deployments via browsers or web services. This is new method that varies from traditional methods for increase capacity without creating new infrastructure, new software or additional equipments. This paper deals with security problems and countermeasures of them in cloud environments with introduction to cloud computing concepts. Finally, we discussed and highlighted the directions for more security in cloud computing.**

Index Terms— **Cloud Computing, Information Security, Service Providers**

I. Introduction

CLOUD computing is a new computing technology has emerged since 2006. The concept of cloud computing has been introduced during recent years with various interpretations on what is cloud computing. Generally, cloud computing is evolved technology of parallel computing, utility computing, distributed computing and grid computing technologies [1] with outcome of networks storage, load balancing among of the clouds, application and relative services. Cloud is as an internet based supercomputing paradigm. It allows customers to sharing a mass of hardware, software and data resources regarding to their actual applications and services dynamically [2].

Hence, data security is very key and effective issue in cloud environments that makes users or organizations as eager to know about security, reliability and safety measures in cloud services. Cloud services are prepared form service providers and cloud service companies. From a security view, a number of unchartered risks and challenges have been presented from this relocation to the clouds, deteriorating much of the effectiveness of traditional safekeeping mechanisms [3].

The cloud computing architecture includes cloud services, cloud storage, cloud infrastructures and cloud platform simply. Cloud security refers to management of security risks of cloud computing form the aspect of customers, service provider and government rules. In reference [2], the security risks are security risks confronted by customers, service providers and government. They depend on the customer's requirements and equipments of cloud service providers and generally above of these challenges, the quality of service has direct dependency with service providers and government rules.

In this paper, we highlighted the security issues, countermeasures of them in cloud computing services and directions for data protection in clouds. It is organized as follows: In the section 2, we discuss and review performed previous works in this domain. It has been presented the basic principles of cloud computing in section 3, and in the subsections of it, the deployment and service models of cloud computing are discussed. Section 4, is considered the security problems in the cloud environments as well as countermeasures of them which are proposed in the section 5. The conclusions of the paper are presented in the section 6, finally.

II. Literature Review

Cloud computing is as a flexible, enable and scalable model of on demand network access to a shared pool of reconfigurable computing resources [4]. In this regard, it has been performed many researches during the past years on security measures and its challenges especially. Hada et al [5] proposed a trust model for cloud architecture which applies mobile agents as security agents to reach beneficial information from the virtual machines. The used agents can move in the network dynamically and monitor virtual machine integrity and authenticity for providing secure and reliable communications.

By means of cloud computing, consumers can safe cost of software resources, hardware equipments [5]. So, it ensures trust, privacy and security of client data with effective control to client over his data using security agents. The similar researches for agent application in cloud environments are explained in [6]-[8].

In cloud architectures, attention to security issues is very significant. Subashini and kavitha [9] presented the security issues in service delivery models of the cloud computing. Also, Jamil and Zaki [10] discussed about four cloud security problems which they are XML signature element wrapping, browser security, cloud malware injection attack and flooding

Manuscript received March 11, 2012.
Zeinab Abbasi Khalifehlou is with the Department of Computer Engineering, Shabestar Branch, Islamic Azad University, Shabestar, Iran, (email: tabriz.ce@gmail.com)
Farhad Soleimanian Gharehchopogh is with the Department of Computer Engineering, Hacettepe University, Ankara, Turkey (e-mail: bonab.farhad@gmail.com).

attacks. They also proposed the possible countermeasures for these problems.

However, Okuhara et al [11] considered domestic and international trends in security requirements for cloud environments. The reviewed security architecture has been proposed e.g. access protocol, authentication and identity management and security visualization. Fujitsu provide support for drafting security policies and enabling security mechanisms as a part of consulting menu for business migrating to cloud computing [11]. This architecture allows to the cloud computing security to be evaluated independently of the service business.

Also, Zissis and Lekkas [12] are performed many studies about security issues in cloud computing and they proposed solution calls upon cryptography to ensure the authentication, integrity and confidentiality of involved communications and data transmission. Their solution presents a horizontal level of service, available to all implicated entities. They applied a security mesh with essential trust and secure which is maintained. Other researches in cloud security relevant to these are described with more details in [14]-[16]. Neisse et al [17] implemented trust in cloud infrastructure that enable periodical and necessity driven integrity measurements and remote attestations of vital parts of cloud computing infrastructures.

III. CLOUD COMPUTING

Today's cloud computing is a new processing technology which computer processing that is carried out in the internet called cloud [11]. Cloud computing technology lead to new basically alteration in everyone's perception to extend infrastructure architectures and provided internet services. It is because of no users need to know details about how processing and providing services. On the other hands, it has leveraged users from hardware equipments and decreasing overall complexity and client side requirements [12].

More precisely, cloud computing is the delivery of computing as a service rather than a product, whereby shared resources, software, and information which are provided to computers and other devices as a utility (like the electricity grid) over a network such as internet typically [18]. The principal idea of cloud computing is to create a virtualized computing resource pool by centralizing great computing resources connected with network and offers the service of infrastructures, software and platforms [2].

In cloud environments as a data centre environment, computing transfers from main frame computers to client or server deployments via browsers or web services. It allows enterprises to get their applications up and fast running with easy management and less maintenance as well as data are saved on servers at a remote locations or devices. The essential features of cloud computing are on demand self-service, broad network access, resource pooling, rapid elasticity, and measured services which are described with details in [18]. For example, Amazon.com and Google App are leading in the usage of cloud technology. This technology has many advantages such as lower hardware and software costs, availability, high performance and independence of the software, high flexibility, upgrading software quickly, sharing resources and etc. In contrast, it has several disadvantages which some of them are low speed networks (e.g. internet) relative to personal computers in the client's side, privacy, security, a permanent connection to the internet with acceptable speeds, increasing bandwidth cost, threats and sanctions that should provide solutions for them.

A. Deployment Models

The deployment models of cloud computing are composed of four fundamental parts [2], [11]. There are public cloud, private cloud, community cloud and hybrid cloud as shown in figure 1 with some of their properties.

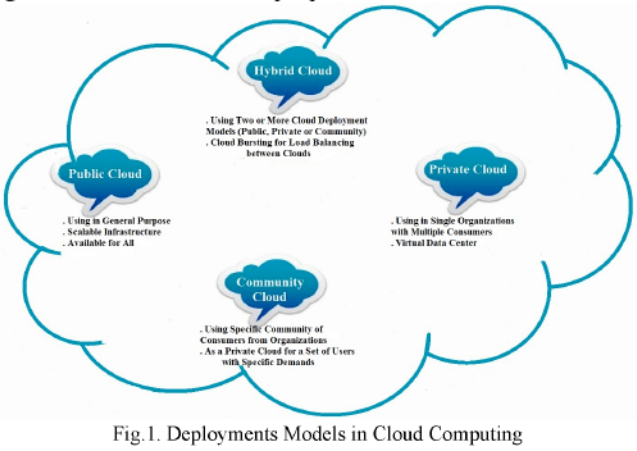


Fig.1. Deployments Models in Cloud Computing

Public cloud is used in for general purposes in organizations with scalable infrastructure and available for all with permissions from service providers. Private cloud is used in single organizations with multiple consumers e.g. in business units. Community cloud refers to a private cloud for a set of users with specific demands which it is used by specific consumers from organizations. Finally, hybrid cloud is composed of two or more clouds (public, private or community).

B. Service Models

Cloud computing providers offer their services according to three main models. They are infrastructure as a service (IaaS), platform as a service (PaaS) and software as a service (SaaS) [1], [10], [18]-[19] that are described in the figure 2. In IaaS, consumer can develop arbitrary software which includes operating systems and applications e.g. applied in Amazon.com. While in PaaS model, the consumer does not manage the cloud infrastructure that it contains servers, operating systems and other resources e.g. applied in Google App Engine, Force.com and etc. However, SaaS is achieved from several clients or a program interface without controlling or managing by consumer on cloud infrastructures. The cloud

infrastructure includes network, servers, operating systems, storages and others.

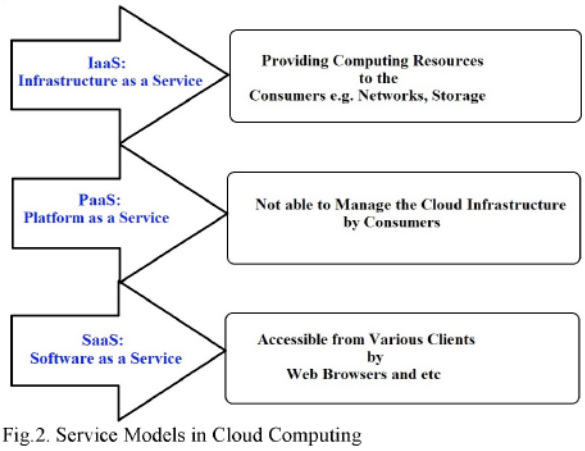


Fig.2. Service Models in Cloud Computing

IV. Security in Cloud Computing

Cloud technology is cost effective, more flexible and more scalability versus traditional deployments but has security implications. During the past years, it has been contributed some efforts to improving the security performance of cloud computing. It should be possible to detect at least the configuration of the cloud infrastructure as provided in the form of a hyper visor and administrative area software has not been changed without the customer's consent [10].

The main security risks of cloud computing in [13] consist of abuse and nefarious use of cloud, insecure interfaces, malicious insiders, shared technology issues, data loss or leakage, account or service hijacking and unknown risk profile. In organizations that use cloud computing services, all the security problems are substituted in three main groups: security problems in the home server platform that is as a cloud, security problems of workstations like clients and end points devices and finally security problems of data from end points that will be able to add the platform.

Cloud Security Alliance (CSA) [13], [18] provides valuable clues to a possible answers to achieve security demanded of cloud computing. Cloud computing infrastructures usually need customers who transfer data into the cloud to trust the providers of the cloud infrastructure [10]. In organizations which they provide cloud services, trust means that service providers behave as expected and needed exactly.

Trust in the information society refers to various different domains based on calculus and social reasons or knowledge [20]. So, no customer of cloud services is willing to grant the trust without justification [2]. Trusted Computing Group (TGA) [21] provides trust framework for enable trust in infrastructures as well as a trust basis to support server cluster provisions.

Also, service providers assure to the customers secure transmission and data security on clients as well as protecting data servers from unauthorized accesses by privacy policies and public key management. Each of the security aspects of cloud services are classified in one of the following categorizations:

1) Security problems associated with cloud services
2) Security problems associated with cloud providers
3) Organizational security problems
4) Security problems related with the users of relevant service
5) Security problems associated with national security laws
6) Security problems in information security solutions

In cloud computing, most applications are located on various other systems. Security issues presented above are limited the following security issues in cloud computing technology. These are application security, data transmission security and data storage security between the clouds provided by cloud service providers for consumers.

Application security refers to identity and access management mechanisms, public key infrastructures systems and others. Data transmission security includes security mechanisms in cloud computing which contains data transmission control. Typically, data locations are not stable or they are in multiple locations (used by cloud or hosted on cloud) leads to define the data transmission conditions [21]. Data storage security leads to using the encryption and decryption or compression mechanisms in data store processes. Regarding to achieve secure and access control to outsourced data the advanced cryptographic techniques are key policy attribute based encryption techniques, proxy re-encryption techniques and lazy re-encryption technique which are described in [22].

V. Discussion

Cloud computing means that storage devices, infrastructures and other resources from your computer will be moved a single or multiple servers on the clouds. The last security concern is the security of data transfer, effectively using coding techniques, and secure virtual private network (VPN) connections is solved.

Service providers (like Google and Microsoft) enable their services such as SaaS and PaaS [10], [18] for many users, so they able to provide the security of their services as concurrent. As this regard, they can take advantage from more effective and complex new security approaches based on new security technologies and encryption in data transmission between platforms, end points, servers and other devices.

Security of data center computing resources that are involving for service providers is simpler. It is because of the distribution future of cloud processing [19]. On the other hand, the using of cloud services among of clients and server organizations will be performed based on agreement in the contracts. All of server responsibilities have been predicted in relation to security problems and their resolutions, e.g. national security laws, confidentiality and privacy, security identification of threats, sanctions and etc.

In order to providing secure data with cloud service provider to agree that your data in a specific geographic area and maintenance process. In addition, organizations apply the

legal requirements which they can need to follow the integrity and privacy of their data. In cloud technology, may placed different data of organizations in a shared environment as cloud. Cloud service provider must ensure that the data are separated, backup data always and decreased the security risks in the shared environments.

So, the effective ways to do this consist of the encryption keys to encrypt data and access permission to the various users. In critical situations, service providers ensure that there are several sites or cloud services which have multiple copies of infrastructure, software and platform as a cloud services will be kept in data storages repeatedly.

In summary, the concerns in relation to the platform where information security to the cloud environment is related, this brings us to the conclusion that eventually all of the problems identified by users of cloud systems will be resolved successfully. Finally, there is no restriction on cloud computing. As a result, if the developers of information security tools, companies can assist in solving these problems, the environment will have a bright future cloud.

VI. Conclusion

Cloud computing share services, resources, information, application and devices based on consumer's demands. In this study, we discussed about security problems in the cloud environments and also, we considered security directions in cloud computing environments. Cloud computing provides flexible, scalable infrastructure or resources as a service over on demand internet based access. It is capable to present the trust communications, minimal management effort with service providers' interaction as well as adherence the laws governing from the government on cloud environments. With solving the security issues and providing services as high performance, the cloud environments will have a bright future cloud.

References

[1] L. M. Vaquero L.M., L. R. Merino, J. Caceres, M. Lindner, "A Break in the Clouds: Towards a Cloud Definition", ACM SIGCOMM Computer Communication, New York: ACM Press, Vol. 39, No. 1, 2009. pp. 50–55.

[2] J. Che, Y. Duan, T. Zhang, J. Fan, "Study on the Security Models and Strategies of Cloud Computing", 2011 International Conference on Power Electronics and Engineering Application, Vol. 23, pp. 586-593, 2011.

[3] P. Wilson, "Positive Perspective on Cloud Security", Information security Technical Report, Doi: 10.1016, pp. 1-5, 2011.

[4] S. Zhang, S. Zhang, X. Chen, X. Huo, "Cloud Computing Research and Development Trend", Future Networks, ICFN'10, Second International Conference, pp. 93-97, 2010.

[5] P. S. Hada, R. Singh, M. Manmohan, "Security Agents: A Mobile Agent based Trust Model for Cloud Computing", International Journal of Computer Applications (0975-8887), Vol. 36, No. 12, pp. 12-15, 2011.

[6] A. K. Srivastava, A. Goel, "Security Solution for WSN Using Mobile Agent Technology", International Journal of Research and Reviews in Wireless Sensor Networks (IJRRWSN) Vol. 1, No. 3, September 2011.

[7] R. Aversa, B. D. Martino, M. Rak, S. Venticinque," Cloud Agency: A Mobile Agent Based Cloud System", Complex, Intelligent and Software Intensive Systems (CISIS), 2010 International Conference, pp.132-137, 2010.

[8] W. J. Buchanan, M. Naylor, A.V. Scott, "Enhancing Network Management Using Mobile Agents", Engineering of Computer Based Systems, (ECBS 2000) Proceedings of Seventh IEEE International Conference and Workshop, pp. 218-226, 2000.

[9] S. Subashini, V. Kavitha, "A Survey on Security Issues in Service Delivery Models of Cloud Computing", Journal of Network and Computer Applications, Doi: 10.1016, pp.1-11, 2010.

[10] D. Jamil, H. Zaki, "Security Issues in Cloud Computing and Countermeasures", International Journal of Engineering Science and Technology, Vol. 3, No. 4, pp. 2672-2676, 2011.

[11] M. Okuhara, T. Shiozaki, T. Suzuki, "Security Architectures for Cloud Computing", Fujitsu Sci. Tech. J., Vol. 46, No. 4, pp. 397-402, 2010.

[12] D. Zissis, D. Lekkas, "Addressing Cloud Computing Security Issues", Future generation Computer Systems, Vol. 28, pp. 583-592, 2012.

[13] Cloud Security Alliance, Top threats to Cloud Computing, Availbe at: www.cloudsecurityalliance.org, Last Access: 2/29/2012.

[14] A. Sangroya, S. Kumar, J. Dhok, Vasudeva Varma, "Towards Analyzing Data Security Risks in Cloud Computing Environments". International Conference on Information Systems, Technology, and Management (ICISTM 2010).

[15] A. Bisong, S. Shawon, M. Rahman, "An Overview of the Security Concerns in Enterprise Cloud Compuitng", International Journal of Network Security & Its Applications (IJNSA), Vol.3, No.1, pp 30-45, 2011.

[16] K. Popovic, H. Zeljko, "Cloud computing security issues and challenges", MIPRO, 2010 Proceedings of the 33rd International Convention, pp. 344-349, 2010.

[17] R. Neisse, D. Holling, A. Pretschner, "Implementing Trust in Cloud Infrastructures", Cluster, Cloud and Grid Computing (CCGrid), 2011 11th IEEE/ACM International Symposium, pp.524-533, 23-26 May 2011.

[18] The NIST Definition of Cloud Computing, National Institute of Science and Technology, http://csrc.nist.gov/publications/nistpubs/800-145/SP800-145.pdf, Last Access 3/1/2012.

[19] R. Buyya, J. Broberg, A. Goscinski, "Introduction to Cloud Computing", *Cloud Computing: Principles and Paradigms*. New York, USA: Wiley Press, pp. 1-44, 2011.

[20] D. Lekkas, "Establishing and Managing Trust within the Public Key Infrastructure", Computer Communications, Vol. 26, No. 16, 2003.

[21] P. Kumar, V. K. Sehgal, D. S. Chauhan, P. K. Gupta, M. Diwakar, "Effective Ways of Secure, Private and Trusted Cloud Computing", International Journal of Computer Science Issues (1694-0814), Vol. 8, No. 2, , pp. 412-421, 2011.

[22] S. Sajithabanu, B. G. Prakash Raj, "Data Storage Security in Cloud", International Journal of Computer Science and Technology (0976-8491), Vol. 2, No. 4, pp. 436-440, 2011.

Zeinab Abbasi Khalifehlou graduated from the Department of Computer Engineering at PNU University in Iran. Since, she has been working toward the M.Sc degree in Computer Engineering at Islamic Azad University Shabestar Branch, Shabestar, Iran.

Her main research interests are Data Mining; Intelligent based Software Cost Estimation, Artificial Neural Networks, Multi Agent Systems in Health Care, Intelligent Tutoring Systems, and Bioinformatics.

Farhad Soleimanian Gharehchopogh received his B.Sc. degree in Computer Engineering from Islamic Azad University Shabestar Branch, Iran. He then received his M.Sc degree in Computer Engineering from Cukurova University, Adana, Turkey. Since, he has been working toward the Ph.D degree in Computer Engineering at Hacettepe University in Ankara, Turkey.

His research interests include Data Mining, Operating Systems, Software Cost Estimation, Artificial Neural Networks, Intelligent Tutoring Systems, and Bioinformatics.

Enhancing SIEM Correlation Rules Through Baselining

Ertuğrul Akbaş

Abstract— **In this paper, we describe research into the use of baselining for enhancing SIEM Correlation rules. Enterprise grade software has been updated with a capability that identifies anomalous events based on baselines as well as rule based correlation engine, and alerts administrators when such events are identified. To reduce the number of false positive alerts we have investigated the use of different baseline training techniques and introduce the use of 3 different training approaches for baseline detection and updating lifecycle.**

Index Terms—**Log, SIEM, Correlation, Rule Base, Baseline, Anomaly Detection, Baseline**

I. Introduction

Computer crime continues to be problematic for both public and private sectors not only in Turkey but at an international level. Over 50% of respondents to the 2006 Computer Security Institute/FBI Computer Crime and Security Survey [1] reported unauthorized use of computer systems.

The field of computer forensics has been rapidly expanding in the past twenty years in an effort to combat the continuing increase in the incidence of criminal activity involving computers. This area is normally defined by the identification, securing and analysis of evidence. Generally accepted definition of computer forensics can be made that simply attempts to detect, secure and analyze evidence from computer systems. Also some few cases will end at the court. This may be done by an organization, for instance, in response to a security incident, internal or external

The surveys show that the most common types of criminal activity are the results of virus, worm or Trojan infections. Insider abuse of Internet access, email or computer system resources, however, is the third most common type of misuse in the United States of America [1] Insider misuse can be defined as the performance of activities where computers and networks in an organization are deliberately misused by those who are authorized to use them. Some activities which can be categorized as insider misuse include: unauthorized access to information which is an abuse of privileges unauthorized use of software or applications for purposes other than carrying out one's duties theft or breach of proprietary or confidential information theft or unauthorized use of staff or customer's access credentials computer facilitated financial fraud Logging – the act of recording events occurring in a system – is a mandatory security measure in any moderately complex digital environment. Logs can be used to detect and investigate incidents after they have occurred, but also to assist in the prevention of harmful incidents, by revealing use and abuse patterns and increasing situational awareness [2]

The most efficient method for incident detection is using SIEM solution. All of the SIEM solutions are rule based systems but enhancing this rule based systems by comparing current performance to a historical metric is needed. And we need to define a methodology for updating this historical metric.

A good security tool should make comparisons with historical data, clearly presenting deviations from the norm [3]

This paper reports on work aimed at detecting anomalous events that may be indicators of misuse. First of all, we attempt to detect baselining parameters.

Then we will prose an update mechanism for selected baselines.

We suggest three possible approaches for updating the baselines. The first approach is to use a static or constant window baseline. With this approach detection of alerts is carried out on a weekly basis after the training period and the baseline remains the same for each week of testing. The drawback of this method is: decisions are always based on that initial baseline.

The second approach proposed for updating baseline is to use an extended window, where the newly added data from last baseline calculated time will be added to the baseline updating cycle. With this approach, the baseline becomes dynamic and captures changes in a baseline's behavior or in the environment. A possible problem with this approach is that the baseline may retain too much related with history.

A third approach is to use a fixed sliding time window for the baseline where the width of the time window remains fixed but data within windows always renewed. After training the baseline and making decisions based on the data from this week, the baseline is recalculated by removing the oldest week of baseline data and adding the new week of data. This approach is dynamic in nature and prune to historical data affects over baseline.

Manuscript received March 11, 2012.

Ertuğrul Akbaş is with the ANET Software Turkey (corresponding author to provide phone: 90-216-3540580; fax: 90-216-3540580; e-mail: ertugrul.akbas@ anetyazilim.com.tr).

II. RELATED WORK

Baseline detection relies on models of the intended behavior of users, applications and networks and interprets deviations from this normal' behavior [4, 5, 6, 7]. This approach is complementary with respect to misuse detection, where a number of attack descriptions (usually in the form of signatures) are matched against the stream of audited events, looking for evidence that one of the modeled attacks is occurring [8].

A basic assumption underlying anomaly detection is that attack patterns differ from normal behavior. In addition, anomaly detection assumes that this `difference' can be expressed quantitatively. Under these assumptions, many techniques have been proposed to analyze different data streams, such as data mining for network traffic [9], statistical analysis for audit records [10], and sequence analysis for operating system calls [11].

Of particular relevance to the work described here are techniques that learn the detection parameters from the analyzed data. For instance, the framework developed by Lee et al. [12] Provides guidelines to extract features that are useful for building intrusion classification models. The approach uses labeled data to derive which is the best set of features to be used in intrusion detection.

The approach described in this paper is similar to Lee's because it relies on a set of selected features.

The learning process is purely based on past data, as, for example, in [13] but we propose new learning schema.

Also we borrowed techniques from intrusion detection and anomaly detection field.

III. LOG CORRELATION

As logs are sent to the correlation engine, they are normalized into a high level event type and a more specific unique event and processed by correlation algorithms. The quality of a correlation depends on accuracy and speed. The speed depicts how many correlations can be found in a certain amount of time. The accuracy depicts how many of the identified correlations represent real existing relations between these alerts. Due to more complex attacks and large scale networks, the amount of alerts increases significantly which yields the requirement for improved quality of the correlation. The correlation accuracy depends on the used correlation algorithm.

IV. DETECTION AND LEARNING PHASE OF BASELINES

Main approach for identifying those baselines is to interview a group of experienced network administrators and ask them how they identify and tackle problems. The authors have selected different kinds of administrators ranging from small, single OS (e.g. mostly Apple or Windows) networks to large heterogeneous, multi vendor networks. Below it is summarized the original results of the survey:

1. Concentrate on core services. DNS, routing services are critical in IP networks. If core services fail then everything fail

2. Statistical analysis that deals with extracting information from data is important for baseline detection. The statistical

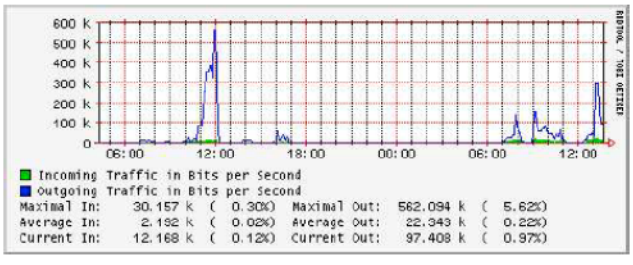


Fig. 1. DOS attack affect on network traffic.

analysis of error status over the time is another good way for detecting baselines.

3. Monitor non-unicast traffic. Non-unicast traffic that is causing high utilization of the switch. or misconfigured windows hosts that have a misspelled workgroup name create a significant amount of broadcast traffic and can be easily detected.

4. Traffic analysis is very important for baseline detection. Unwanted traffic is key concept for network monitoring. There is some heuristics [16] that have an efficient way to detect unwanted network protocols.

5. Active monitoring: Rejected connection rate can be used for TCP services. ICMP port unreachable can be used for UDP services.

6. Monitor protocol distribution.

7. Client are most vulnerable than servers. Because they are not maintained by the network administrators. Monitor clients' behavior

8. Monitor protocols that have weakness or implementation flaws like FTP, IRC and DNS.

Some other techniques are available in the literature [17,18,19]

Since baselines are mostly statistically defined elements, they need to be updated. As your SIEM usage progresses, you need to add an interim values periodically.

Although there is some previously done researches in the literature [20,21]. First of all we suggest detection methods of baselines then we list the baselines for enterprise network using case studies. As a last we suggest three possible new approaches for learning phase of the baseline detection. first approach is to use a static or constant window baseline. With this approach detection of alerts is carried out on a weekly basis after the training period and the baseline remains the same for each week of testing. The drawback of this method is: decisions are always based on that initial baseline.

The second approach proposed for updating baseline is to use an extended window, where the newly added data from last baseline calculated time will be added to the baseline updating cycle. With this approach, the baseline becomes dynamic and captures changes in a baseline's behavior or in the environment. A possible problem with this approach is that the baseline may retain too much related with history.

A third approach is to use a fixed sliding time window for the baseline where the width of the time window remains fixed but data within windows always renewed. After training the baseline and making decisions based on the data from this

week, the baseline is recalculated by removing the oldest week of baseline data and adding the new week of data. This approach is dynamic in nature and prune to historical data affects over baseline.

V. BASELINES FOR CORRELATION RULES

The concept of a baseline is not new or complex. In general, a baseline is a well-defined, well-documented reference that serves as the foundation for other activities. We will call this baseline from now on.

Understanding the network devices, applications, services etc. deployed in your network and their normal status is key to establishing a baseline.

A. Identifying Baselines

The method is marked by comparing current performance to a historical metric. Detecting baselines for correlation engine is important. One can increase the number of baselines detected as many as needed. But detecting sufficient baselines and baseline parameters will be critical in a manner of system response. For an enterprise grade SIEM solution in memory correlation is critical.

You will need to understand 'good traffic' for your network during the 'initial tuning' phase, use white lists and blacklists of signatures, and then build heuristic analysis if you want to alert on deviation from the normal. In our approach we offer methods for baseline detection in section IV. Also we analyzed some real world case studies from FAUNA installations [14]. Results of those methods are:

- Port Usage Baseline
  - oHits on port 80 over the last week
  - oCount of new ports hit on a firewall
- User Baseline
  - oSoftware Usage Baseline
  - oInternet Usage Baseline
  - oIntranet Usage Baseline
- EPS Baseline
  - oNormal Events per second (NE) :The NE metric will represent the normal number of events usage time for a device, or for your Log or Event Management scope.
  - oPeak Events per second (PE) :The PE metric will represent the peak number of events usage time for a device, or for your Log or Event Management scope. The PE represent abnormal activities on devices you create temporary peaks of EPS, for example DoS, ports scanning, mass SQL injections attempts, etc. PE metric is the more important cause it will determine your real EPS requirements.
- Traffic Baseline
  - oNumber of hosts touching each server per hour
- Network Baseline
  - oProtocols
  - oSystem Access
  - oEvent Types
- System Baseline
  - oLogin/Logout Success/Failure
  - oCPU per day
  - oMemory per day
  - oDisk availability per day
  - oUser Logins to Server X per day
  - oProcess Starts
  - oUse of "su" command per hour of day
  - oConfiguration Changes
  - oUser Rights
  - oEvent Log settings
  - oRestricted Groups
  - oSystem Services
  - oFile Permissions
  - oRegistry Permissions
- Application Baseline
  - oData Access Types
  - oUser Data Changes
  - oClient
- Database Baseline
  - oData Access Types
  - oUser Data Changes
  - oClient

As it is mentioned before that detecting baselines and baseline parameters are very critical, we did a search on use cases of an available enterprise software FAUNA [14] within real world cases then detect above baselines and baseline parameters

VI. SECURITY INCIDENT DETECTION LEVERAGING PROFILING

The challenge with correlation rules is that in a sense they are "signature based" in that you largely have to know the situation you are trying to detect. For example, "monitor my five external firewalls and tell me if you see port scans from the same public net block on more than 3 of my firewalls in the same 30 minute period."

An approach we find far more promising is Baselining. This approach will be used addition to rule based system in our case [15]. Its advantage is that it doesn't watch for anything specific, rather it attempts to identify any patterns of security events which are unusual based on previously base lined performance. Interestingly, baselining is based on the meta-data from events — not the events themselves – although the events themselves can be retrieved based on the meta data.

An example that will best illustrates the value of Anomaly Detection: A quick FTP connection attempt confirmed that FTP was indeed responding on the server and a few more minutes of sleuthing determined that a Windows reboot had restarted the FTP service a few hours prior. Within an hour a hacker had initiated a brute force admin password attack on the server. Anomaly Detection noted the unusual FTP pattern (as compared to the previous months baseline) and thwarted the security incident before any impact.

Automatically detecting anomalous behavior by looking for

unexpected statistical deviations from an ever evolving "base-line"

VII. IMPLEMENTATION DETAILS

Since FAUNA [3] has a JAVA based API for customization, we used JAVA for implementation. FAUNA has RULE based correlation engine currently with the features of:

- Support Mvel and java
- JSR94 compatible
- In-memory correlation
- Single point of correlation rules source
- Multi point of correlation rules source
- Negative condition rules
- Context based correlation
- Rule Base.
- Complex Event Processing(CEP).
  - Forward Channing.
- Backward Chaining.

With this adaptation FAUNA will have a correlation engine with the below features:

- Pre-defined pattern matching
- Statistical analysis (anomaly detection)
- Basic conditional Boolean logic statements
- Contextually relevant and/or enhanced data set with Boolean logic

Complex Event Processing, or CEP, is primarily an event processing concept that deals with the task of processing multiple events with the goal of identifying the meaningful events within the event cloud. CEP employs techniques such as detection of complex patterns of many events, event correlation and abstraction, event hierarchies, and relationships between events such as causality, membership, and timing, and event-driven processes."

The vision on FAUNA of a Behavioral Modeling Platform can only be achieved by moving away from any of the narrow modeling perspectives that see only Rules, or Processes, or Events as their main modeling concept. To effectively achieve the flexibility and power of behavioral modeling, a platform must understand all of these concepts as primary concepts and allow them to leverage on each other strengths.

FAUNA, in this scenario, is an independent module, but still completely integrated with the rest of the platform, that adds a set of features to enable it:

- understand and handle events as first class citizens of the platform
- select a set of interesting events in a cloud or stream of events
- detect the relevant relationships (patterns) among these events
- take appropriate actions based on the patterns detected

Events as first class citizens: events are a special entity that is a record of a significant change of state in the application domain. They have several unique and distinguishing characteristics, like being usually immutable, having strong temporal constraints and relationships. FAUNA understand events by what they are and allow users to model business rules, queries and processes depending on the occurrence or absence of them

Support asynchronous multi-thread streams: events may arrive at any time and from multiple sources (or streams). They can also be stored in cloud-like structures. FAUNA supports both work with streams and clouds of events. In case of streams it supports asynchronous, multi-thread feeding of events.

Support for temporal reasoning: events usually have strong temporal relationships and constraints. FAUNA adds a complete set of temporal operators to allow modeling and reasoning over temporal relationships between events.

Support events garbage collection: events grow old, quickly or slow, but they do grow old. FAUNA is able to identify the events that are no longer needed and dispose them as a way of freeing resources and scaling well on growing volumes.

Support reasoning over absence of events: the same way in that it is necessary to model rules and processes that react to the presence of events, it is necessary to model rules and processes that react to the absence of events. Example: "If the temperature goes over the threshold and no contention measure is taken within 10 seconds, then sound the alarm". FAUNA leverages on the capabilities of the Drools Expert engine, allowing it complete and flexible reasoning over the absence of events, including the transparent delaying of rules in case of events that require a waiting period before firing the absence.

Support to Sliding Windows: a especially common scenario on Event Processing applications is the requirement of doing calculations on moving windows of interest, be it temporal or length-based windows. FAUNA has complete support for Sliding Windows, providing out of the box aggregation functions as well as leveraging the pluggable function framework to allow for the use of users defined custom functions.

FAUNA correlation engine will automatically retract the event if it's not needed anymore, for example if you are calculating the average using sliding windows, as soon as the event falls out of the sliding windows and don't match any other rule it will be automatically retracted if FAUNA is operating in Stream Mode.

About persisting the internal state, we have implemented our own mechanisms storing the average and re initialize the state when it is needed

Baseline updating achieved by Rule/Model chaining. In a typical scenario, a control rule triggers a model and generates an output. This output can either be validated directly using rules or by starting other more complex inference chains.

Eventually,one or more of the inferred facts is consumed by an avaluator which in turn triggers another control rule and the processis restarted, as shown below.

```
rule " Trigger "
when
$input : Data ( <pr e c ondi t i ons> )
$model : ?Model ( . . . )
then
insert (new Re sul t ( $model . invoke ( $input ) ) ) ;
end

rule " Eval "
when
Re sul t ( value pm eval t a r g e t )
then
insert (new Data ( . . . ) ) ;
end
```

VIII. CONCLUSION

On the existing problem of the current network security event management, this paper proposed a security event correlation algorithm based on baselining and an algorithm for updating lifecycle of baselines. Additionally we listed predefined baselines and baseline parameters from real world cases.

So, when you think SIEM, don't just think "how many rules?" – think "what other methods for real-time and historical event analysis do they use?".

Sample of the rules than can be developed with the help of enhancement to rule based systems:

1. Monitor and compare with baseline "count unique port per source per hour/day"
2. Monitor and compare with baseline "protocol per hour per sensor"
3. Monitor and compare with baseline "Hits on port 80 per the week"
4. Monitor my five external firewalls and tell me if you see port scans from the same public net block on more than 3 of my firewalls in the same 30 minute period. For example, "monitor my five external firewalls and tell me if you see port scans from the same public net block on more than 3 of my firewalls in the same 30 minute period.
5. Monitor five attempts to login to a system within one minute using the same user account
6. Monitor/Associate system navigation with non-standard working hours.
7. Monitor traffic source:
    - (IF username=root AND ToD>10:00PM AND ToD<7:00AM AND Source_Country=China, THEN ALERT "Root Login During Non-Biz Hours from Foreign IP")

As a result, the developed system has features below:

- Pre-defined pattern matching
- Statistical analysis (anomaly detection)
- Basic conditional Boolean logic statements
- Contextually relevant and/or enhanced data set with Boolean logic

REFERENCES

[1] Gordon, L. A., Loeb, M. P., Lucyshyn, W. and Richardson, R. 2006 CSI/FBI computer crime and security survey: http://i.cmpnet.com/gocsi/db_area/pdfs/fbi/FBI2006.pdf. Accessed 12 Oct 2007.

[2] Stefan Axelsson, Ulf Lindqvist, Ulf Gustafson, and Erland Jonsson. An Approach to UNIX Security Logging. In Proc. 21st NIST-NCSC National Information Systems Security Conference, pages 62–75, 1998.

[3] Raffael Marty. Applied Security Visualization. Pearson Education, Inc,501 Boylston Street, Suite 900, Boston, MA, 2008.

[4] D.E. Denning. An Intrusion Detection Model. IEEE Transactions on Software Engineering, 13(2):222{232,February 1987.

[5] A.K. Ghosh, J. Wanken, and F. Charron. Detecting Anomalous and Unknown Intrusions Against Programs. In Proceedings of the Annual Computer Security Applications Conference (ACSAC'98), pages 259{267, Scottsdale, AZ, December 1998.

[6] C. Ko, M. Ruschitzka, and K. Levitt. Execution Monitoring of Security-Critical Programs in Distributed Systems: A Specification-based Approach. In Proceedings of the 1997 IEEE Symposium on Security and Privacy, pages 175{187, May 1997.

[7] T. Lane and C.E. Brodley. Temporal sequence learning and data reduction for anomaly detection. In Proceedings of the 5th ACM conference on Computer and communications security, pages 150{158. ACM Press, 1998.

[8] K. Ilgun, R.A. Kemmerer, and P.A. Porras. State Transition Analysis: A Rule-Based Intrusion Detection System. IEEE Transactions on Software Engineering, 21(3):181{199, March 1995.

[9] W. Lee, S. Stolfo, and K. Mok. Mining in a Data-Flow Environment: Experience in Network Intrusion Detection. In Proceedings of the 5th ACM SIGKDD International Conference on Knowledge Discovery & Data Mining (KDD '99), San Diego, CA, August 1999.

[10] H. S. Javitz and A. Valdes. The SRI IDES Statistical Anomaly Detector. In Proceedings of the IEEE Symposium on Security and Privacy, May 1991.

[11] S. Forrest. A Sense of Self for UNIX Processes. In Proceedings of the IEEE Symposium on Security and Privacy, pages 120{128, Oakland, CA, May 1996.

[12] W. Lee and S. Stolfo. A Framework for Constructing Features and Models for Intrusion Detection Systems. ACM Transactions on Information and System Security, 3(4), November 2000.

[13] C. Kruegel, T. Toth, and E. Kirda. Service Specific Anomaly Detection for Network Intrusion Detection. In Symposium on Applied Computing (SAC). ACM Scientific Press, March 2002.

[14] FAUNA, www.anetyazilim.com.tr

[15] FAUNA, http://www.anetyazilim.com.tr/fauna/4/286/1/1/

[16] D. Plonka, FlowScan: A Network Traffic Flow Reporting and Visualization Tool, Proc. of XIV th Lisa Conference, December 2000.

[17] Daniela Brauckhoff, Network Traffic Anomaly Detection and Evaluation , ETH ZURICH ,2010

[18] Augustin Soule, Kav´e Salamatian, and Nina Taft.Combining filtering and statistical methods for anomaly detection. In IMC'05: Proceedings of the 5th Conference on Internet Measurement 2005, Berkeley, California, USA, October 19-21, 2005,pages 331–344. USENIX Association, 2005.

[19] Animesh Patcha and Jung-Min Park. An overview of anomaly detection techniques: Existing solutions and latest technological trends. Comput. Netw., 51(12):3448–3470, 2007.

[20] Northcutt, S., Novak, J.: Network Intrusion Detection: An Analyst's Handbook. New Riders Publishing, Thousand Oaks (2002)

[21] Kruegel, C., Valuer, F., Vigna, G.: Intrusion Detection and Correlation: Challenges and Solutions. AIS, vol. 14. Springer, Heidelberg (2005)

Ertuğrul Akbaş ertugrul.akbas@anetyazilim.com.tr is currently working with ANET. He received his Ph.D. in Computer Science with a thesis on Intelligent Systems from Gebze Institute of Technology in 2005. He previously worked as research scientist TÜBİTAK-Marmara Research Center

and as project manager at National Research Institute of Electronics and Cryptology. His professional interests include network security, information security, network management and monitoring, software components and object-oriented technology.

Şifrelemenin Modellenmesi ve Modern Kriptosistemin Tasarımı

Erkan BAYAR[1] , Hakan KAPTAN[2]

[1]Marmara Üniversitesi F.B.E. Elektronik ve Haberleşme Eğitimi

[2]Marmara Üniversitesi Teknoloji Fakültesi Bilgisayar Müh.

***Abstract*— In this study, the new cryptosystem algorithm is modelled by the effect of modern cryptographic algorithms especially symmetric cryptosystem. There are two main titles in this basic model: encryption algorithm and decryption algorithm. In order to develop this new model, C# (C Sharp) programming language and .NET Framework 3.5 library are used together. Thus, any type of data stored in computers can be encrypted and decrypted by using this symmetric algorithm. The aim of this model is to increase the data security level in any computer. Also, any personal information can be protected by using this program.**

Özet— Bu çalışmada, yeni kriptosistem algoritması, modern kriptografik algoritmaların etkisiyle özellikle simetrik kriptosistemle modellenmiştir. Bu basit modelde, şifreleme algoritması ve deşifreleme algoritması olarak iki ana başlık bulunmaktadır. Bu yeni modeli geliştirmek için C# (C Sharp) programlama dili ve .NET Framework 3.5 kütüphanesi beraber kullanılmıştır. Bu simetrik algoritma modeli kullanılarak, bilgisayarlarda depolanan herhangi veri tipi şifrelenebilmekte ve deşifrelenebilmektedir. Bu modelin amacı, bilgisayarda veri güvenlik seviyesini arttırmaktır. Ayrıca, farklı kişisel bilgiler bu program kullanılarak korunabilmektedir.

***Index Terms*—Encryption, decryption, symmetric algorithm, cryptology, cryptography, cryptosystem, data security**

I. GİRİŞ

Şifreleme işlevinin güvenli bir şekilde gerçekleştirilmesi şifreleme sırasında kullanılan tüm yöntem ve bilgilerin gizliliğine dayanır. Şifreleme işlemi sırasında açık mesaj, şifre anahtarı aracılığı ile şifrelenir. Şifrelenmemiş mesaj ile şifrelenmiş mesaj arasındaki geçişler şifreleme algoritmasına ve anahtar bilgisine bağlıdır. [1]

Modern kriptosistemler, şifreleme anahtarı kullanım prensibine göre iki temel başlıkta incelenmektir:

a) Gizli Anahtarlı (Private Key) Kriptosistemler (Simetrik Şifreleme)
b) Açık Anahtarlı (Public Key) Kriptosistemler (Asimetrik Şifreleme)

Simetrik şifreleme algoritmaları, şifreleme ve deşifreleme işlemleri için sadece bir gizli anahtar kullanmaktadır ve çok hızlı çalışmaktadır. Bu algoritmalara örnekler, DES (Data Encryption Standard) ve AES (Advanced Encryption Standard) şifreleme algoritmalarıdır. [2,3,4]

Simetrik şifreleme tekniğinde anahtar dağıtım problem vardır. Bu nedenle şifreleme ve çözme işlemlerinin her birisi için ayrı ayrı anahtar kullanma prensibine dayanan şifreleme sistemleri geliştirilmiştir.

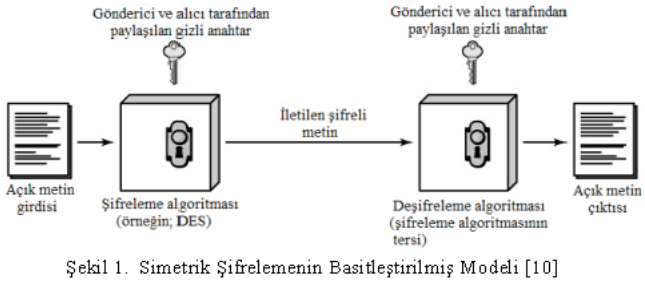
Açık anahtarlı kriptosistemde şifreleme işlemi herkes tarafından bilinen anahtarla yapılır. Şifreleme ve çözme işlemi birbirinin simetriği olmayan (yani aynısı olan) algoritmalarla gerçekleştirildiğinden dolayı asimetrik şifreleme sistemi olarak bilinmektedir. [5,6,7,8]

II. GİZLİ ANAHTARLI (SİMETRİK) KRİPTOSİSTEMLER

A. *DES (Data Encryption Standard)*

Gizli anahtarlı sistemler, gönderici ve alıcı arasında, önceden paylaşılan ve saklı tutulması gereken tek bir anahtarın şifreleme ve deşifreleme işlemlerinin her ikisinde kullanılması yönüyle gizli iletişimin sağlandığı sistemlerdir. [9]

Simetrik şifreleme sistemi, beş adet bileşenden meydana gelir. (Şekil 1.) Bu bileşenler; açık metin, şifreleme algoritması, gizli anahtar, şifreli metin ve deşifreleme algoritmasıdır.

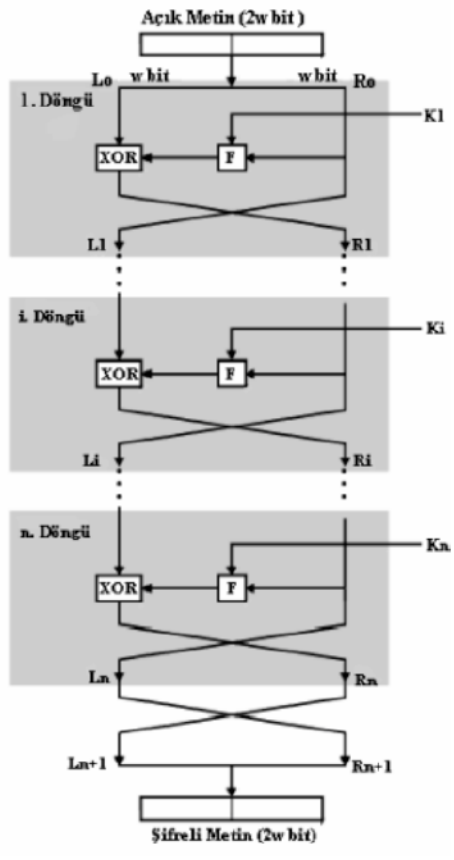


Şekil 1. Simetrik Şifrelemenin Basitleştirilmiş Modeli [10]

DES, feistel şifreleme mimarisi temel alınarak 64 bitlik veri bloklarının şifrelenmesi ve şifrelerinin çözülmesi işlemleri için geliştirilmiş bir blok şifreleme tekniğidir. 64 bitlik anahtar kullanılarak şifreleme işlemi gerçekleştirilir.

Açık metnin işlenmesi durumunda, her bir döngü sırasında yer değiştirme (substitution) adımını permütasyon (permutation-değiş tokuş) adımı takip etmektedir. Her bir döngüdeki blok 2 eşit parçaya bölünür ve parçaları L (left) ve R (right) diye gösterilmektedir. Belirtilen (L) sol taraftaki sütun için (R) ise sağ taraftaki sütun için kullanılır. Her bir döngüde, bloğun sağ tarafı (R) hiç değişmeden devam eder. Fakat sol taraf (L), yer değiştirme operasyonuna gider. L aşaması R bölmesinden gelen bölüm ile şifreleme anahtarına bağlıdır. Her bir döngünün sonunda yeniden düzenlenmiş L ve R blokları yer değiştirilmektedir. [11]

Bu adımlar aşağıdaki şekilde gösterilmiştir:



Şekil 2. Feitsel Ağın Blok Diyagramı [11]

B. *AES (Advanced Encryption Standard)*

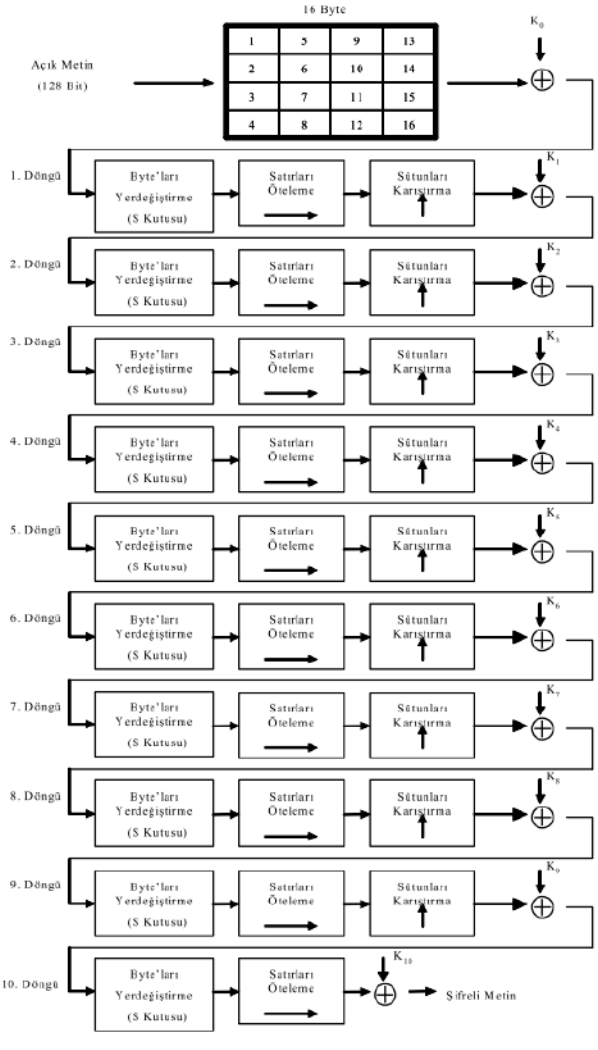
Simetrik şifreleme grubundan olan AES (Rijndael-Gelişmiş Şifreleme Standardı) algoritması, 128 bit veri bloklarını 128, 192, 256 bit anahtar seçenekleri ile şifreler. SPN (Subtitution-Permutation Network) algoritmasının geniş bir çeşidi olup döngü sayısı anahtar genişliğine göre değişkenlik göstermektedir. AES, 128 bit anahtar için 10 döngüde şifreleme yaparken 192 ve 256 bit anahtarlar için sırasıyla 12 ve 14 döngüde şifreleme işlemi yapmaktadır. Algoritmanın her döngüsü dört katmandan oluşmaktadır. [11]

AES'te ilk olarak 128 bit veri, 4×4 byte matrisine dönüştürülür. Bu işlemin ardından, her döngüde sırasıyla şu işlemler gerçekleştirilir:

a. Byte'ların yer değiştirmesi (Sub-Bytes dönüşümü)
b. Satırların ötelenmesi (Shift-Rows dönüşümü)
c. Sütunların karıştırılması (Mix-Columns dönüşümü)
d. Döngüye anahtar eklenmesi (AddRoundKey dönüşümü)

Byte'ların yer değiştirilmesinde 16 byte değerinin her biri 8 bit girişli ve 8 bit çıkışlı S kutusuna sokulur. S kutusu değerleri, Galois cisiminde ((Galois Field-GF), $GF(2^8)$), 8 bitlik polinom için ters alındıktan sonra doğrusal bir dönüşüme sokularak elde edilmiştir. Satırların ötelenmesi işleminde 4×4 byte matrisinde satırlar ötelenir ve sütunların karıştırılması işleminde herhangi bir sütun için o sütundaki değerler karıştırılır. Döngünün son katmanında ise o döngüye ait anahtar ile XOR'lama (dış veya) yapılmaktadır. [12]

Şekil 3.'de 128 bit anahtar boyutuyla çalışan AES şifreleme algoritmasının geniş bir blok şeması mevcuttur:



Şekil 3. 128 bit Anahtarlı AES Şifreleme Algoritması Blok Diyagramı. [11]

III. ŞİFRELEMENİN MODELLENMESİ VE MODERN KRİPTOSİSTEMİN TASARLANMASI

Bu çalışmada, bir simetrik şifreleme algoritması oluşturulmuş ve şifreleme-deşifreleme işlemleri bir yazılım dili yardımıyla modellenmiştir. Tasarlanan algoritmada bir şifreleme anahtarı üretilmekte ve bu anahtar şifreleme-deşifreleme işleminde kullanılmaktadır.

Bu modelleme, temel olarak iki genel başlıkta incelenmiştir. Birinci başlık şifreleme yöntemini ve adımlarını, ikinci başlık ise deşifreleme yöntemini ve adımlarını kapsamaktadır.

A. *Şifreleme Yöntemi*

Şifreleme yöntemi 6 ana başlıkta toplanmıştır. Bunlar sırasıyla, tablo oluşturma, ham veriyi paketlere ayırma, karakter değiştirme, alt anahtar oluşturma, paketleri karıştırma, ve şifreli verileri yazma işlemleridir.

Bu başlıklar aşağıdaki şekilde gösterilmektedir:



Şekil 4. Şifreleme Algoritmasının Basamakları

Şifreleme işlemine ilk olarak *tablo oluşturma işlemiyle* başlanır. Şifreleme işlemine sokulacak herhangi işlenmemiş veri çeşidi yapılan modellemeye göre *16 karakterden oluşan paketlere* (bloklara) ayrılır. 16'lık karakter paketleri, *karakter değiştirme fonksiyonuyla* işlenir. Bu adımdan sonra *alt anahtar oluşturma işleminde*, kullanıcının şifreleme esnasında girdiği 16 karakterlik anahtardan bir alt anahtar oluşturulur. Bu *alt anahtar*, bir sonraki aşamada *paketleri karıştırma işleminde* kullanılmak üzere üretilir. *Paketleri karıştırma işleminde* ise işlenmemiş her bir paket karıştırılır. Paketlerin karıştırılması aşamasından sonra paketler bir araya getirilerek *verinin şifrelenmiş hali* elde edilir.

1. Tablo Oluşturma İşlemi

Bu işlem şifreleme için bir hazırlık aşamasıdır. Bu aşamada, 65536 elemanlı (256x256 boyutunda) bir matris tablo oluşturulur. Bu tablo, ilerde karakter değiştirme işleminde kullanılacaktır. Ayrıca bu tablo, *AES'te baytları yer değiştirme (SubBytes) işleminde kullanılan S kutularına* benzetilebilir.

Tablo oluşturma işleminin adımları kısaca şunlardır:

a. İlk adımda, ham tablo (256x256) oluşturulur.
b. İkinci adımda ham tabloyla aynı boyutta boş tablo oluşturulur.
c. Ham tablo matrisinden bir karakter seçilir. Bu aşamada belirlenecek rastgele iki sayı bir indeks oluşturmak için kullanılır. Bu indeks numaraları 0 ile 255 arasında yer alır.
d. Seçilen karakterin yerine göre (köşe, kenar veya orta indeks) etrafındaki 5 veya 8 karakterden (kenar veya köşe ise 5 farklı indeks, orta ise 8 farklı indeks) rastgele 3'ü seçilir.
e. Seçilen bu üç karakterin unicode standardındaki sayısal değerleri bulunur ve sayısal değerlerinin karelerinin toplamı alınarak işlem yapılır. Seçilen üç örnek karakter sırasıyla 'a', 'b' ve 'c' ise, bu karakterlerin sayısal değerleriyle toplam değişkeni şu şekilde bulunur:

$$toplam=(97)^2+(98)^2+(99)^2=9409+9604+9801=28814 \quad (1)$$

Toplam değerinin 65536'ya göre modu alınır ve bu değer sonuç olarak adlandırılır. Böylece sonuç değeri şu şekilde bulunur:

$$sonuç = 28814 \bmod (65536) = 28814 \quad (2)$$

f. Bulunan sonuç değerine göre boş tablo için yeni indeksin satır ve sütun değerleri hesaplanmalıdır. Satır değerine L (line), sütun değerine C (column) denilir ve hesaplamalar aşağıdaki gibi yapılır:

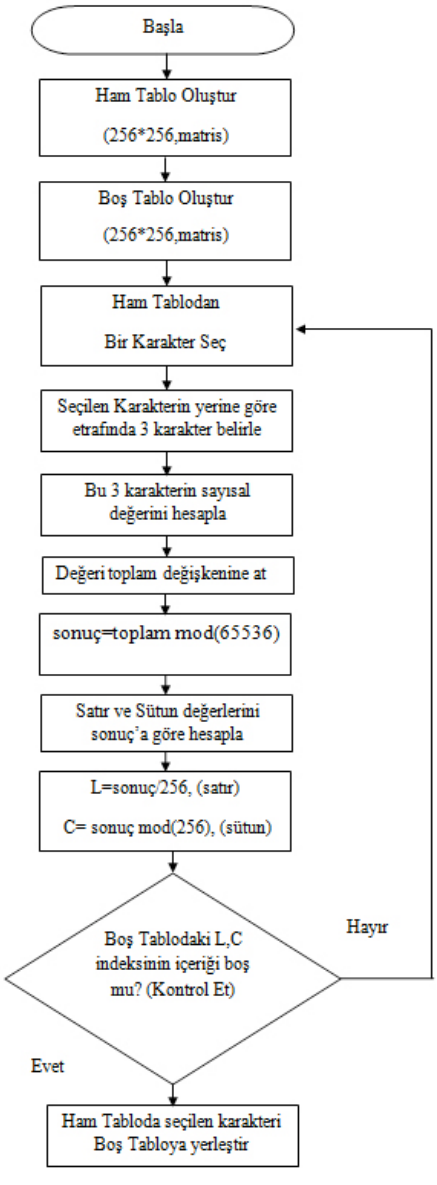
$$L = sonuç / 256,$$
$$C = sonuç \bmod (256) \quad (3)$$

Buna göre yeni hesaplanan indeks (L,C) sayı ikilisi olur.

g. Yukarıdaki işlemde sonuç değeri 28814 olarak bulunur. Bu durumda,

$$L = 28814 / 256 = 112,$$
$$C = 28814 \bmod (256) = 142, \quad (4)$$

olarak hesaplanır. Özetle yeni indeks değeri (112, 142) sayılarıdır.
h. Hesaplanan yeni indeksin (L,C) içeriği boş tablo içinde kontrol edilir. Eğer boş tabloda o indekse karşılık gelen yer boş ise ham tabloda seçilen karakter o indekse yazılır. Eğer o indekste bir karakter bulunuyorsa Şekil 5.'te gösterildiği gibi 4. adımdan itibaren tüm adımlar tekrar edilir.
i. Bu işlemler ham tablo matrisindeki tüm karakterler için yapılır.



Şekil 5. Karakter Değiştirme İşleminde Kullanılacak Tabloyu Oluşturma Süreci

2.Ham Veriyi Paketlere Ayırma İşlemi

Açık metni paketlere ayırma işlemi, veriyi 16 karaktere ayırma işlemidir. Bu işlemde, son paket 16 karakterden az ise algoritmada artık paket olarak adlandırılır. Artık paket, karakter değiştir işlemine sokulur.

3.Karakter Değiştirme İşlemi

Bu aşamada, şifrelenecek karakterin karakter karşılığı bulunarak yerine yazılması işlemi gerçekleştirilir. Her bir paket içindeki her bir karakter eşleştirildiği tabloya göre kendi indeksine karşılık gelen bir karakterle değiştirilir. Bu işlem bütün paketler için tekrarlanır. Bu işlemde kullanılan farklı iki tablo vardır. Bunlar, unicode karakter tablosu (256x256 matris) ve karakter değiştirme tablosudur ki bu *tablonun oluşumu* Şekil 5'te açıklanmıştır.

Karakter değiştirme işlemi şu şekilde yapılır:

Veri paketinden seçilen rastgele karakter 'U' olmak üzere, 'U' karakterinin unicode tablosundaki indeksi (15,21) ise, karakter değiştir tablosundaki (15,21) indeksindeki karakter ß olduğu kabul edilirse, 'U' karakterinin yerine yeni değeri 'ß' karakteri yazılır.

4. Alt Anahtar Oluşturma İşlemi

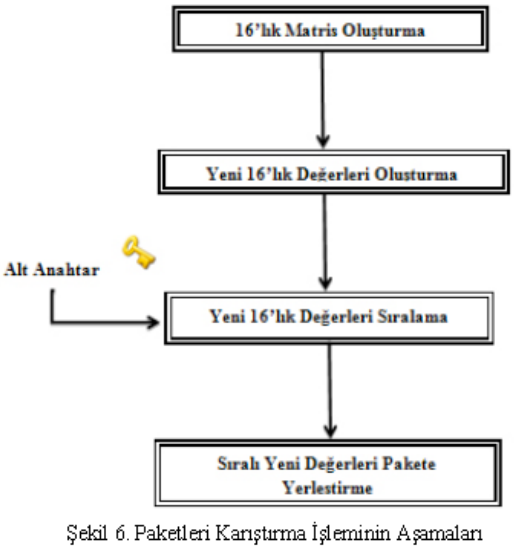
Bu aşamada, paket karıştırmada kullanılacak olan alt anahtarın oluşturma süreci gerçekleşir. Burada, kullanıcının şifreleme sırasında gireceği 16 karakterlik anahtardan, yeni bir anahtar üretme ve bu yeni anahtarın paket karıştırma işleminde kullanılması amaçlanır.

Alt anahtar 3 basamakta oluşturulur. Bunlar, karakter öteleme, karakter XOR'lama (dış veya), alt anahtarın oluşumu işlemleridir.

5.Paketleri Karıştırma İşlemi

Bu işlemde veri paketleri karıştırılır. Paketleri karıştırma işleminde artık paketler dışındaki tüm paketler karıştırılma işlemine sokulur.

Şekil 6.'daki blok şemada paketleri karıştırma işleminin 4 farklı aşaması görülmektedir:



Şekil 6. Paketleri Karıştırma İşleminin Aşamaları

a) 16'lık Matris Oluşturma

Bu adımda, her veri paketinde bulunan karakterlerin unicode tablosundaki sayısal değerleri 16'lık (hexadecimal) değerler olacak şekilde bir 16'lık matrise yerleştirilir.

b) Yeni 16'lık Değerleri Oluşturma

Bu aşamada, 16'lık matrisin bir sütununda bulunan değerlerin birbirleriyle karıştırılması sonucu yeni 16'lık değerler oluşturulur.

Bu karıştırma işlemi şu şekilde yapılmaktadır:

16'lık matrisin bir sütunundaki satır değerleri (ilk satırdan başlayarak) sırasıyla değer_1, değer_2, değer_3 ve değer_4 olarak ifade edilir. Bu değişkenler 4 elemanlı bir karakter dizisinde tutulur ve yeni değerler aşağıdaki yöntemle hesaplanır:

yenideğer_1=değer_1[0]+değer_2[3]+değer_3[0]+değer_4[3]
yenideğer_2=değer_1[1]+değer_2[2]+değer_3[1]+değer_4[2]
yenideğer_3=değer_1[2]+değer_2[1]+değer_3[2]+değer_4[1]
yenideğer_4=değer_1[3]+değer_2[0]+değer_3[3]+değer_4[0] (5)

Satır değerleri A0BF, FF4A, 4596 ve 2369 olan bir karakter dizisinden elde edilecek yeni satır değerleri aşağıdaki

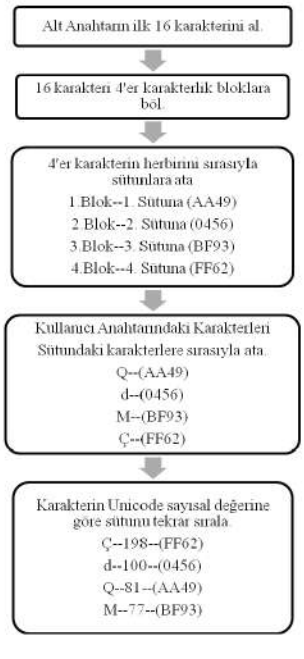
tabloda çaprazlama işlemi gösterilmek kaydıyla ifade edilmeye çalışılmıştır. Oluşan 4 farklı yeni değer satırlara yerleştirilir.

Tablo 1. Yeni 16'lık Değerler Oluşturma İşlemi

Değer_No	Ham Değerler	Çaprazlama	Yeni Satır Değerleri	Yeni Değer_No
Değer_1	A0BF	Değer_1 [0]=A Değer_2 [3]=A Değer_3 [0]=4 Değer_4 [3]=9	AA49	Yeni Değer_1
Değer_2	FF4A	Değer_1 [1]=0 Değer_2 [2]=4 Değer_3 [1]=5 Değer_4 [2]=6	0456	Yeni Değer_2
Değer_3	4596	Değer_1 [2]=B Değer_2 [1]=F Değer_3 [2]=9 Değer_4 [1]=3	BF93	Yeni Değer_3
Değer_4	2369	Değer_1 [3]=F Değer_2 [0]=F Değer_3 [3]=6 Değer_4 [0]=2	FF62	Yeni Değer_4

c) Yeni 16'lık Değerleri Sıralama İşlemi

Bu adımda, yeni 16'lık değerleri oluşturma işleminde elde edilen yeni değerler alt anahtara göre sıralanır. Bu işlemin blok diyagramı Şekil 7.'de görülmektedir:



Şekil 7. Yeni 16'lık Değerleri Sıralama Blok Diyagramı

d) Sıralı Yeni 16'lık Değerleri Paketlere Yerleştirme

Bu aşamada alt anahtara göre sıralanmış yeni 16'lık değerlerin unicode karakter tablosundaki karakter karşılıkları yeni bir pakete sırayla yazılıp verinin son işlenmiş (şifrelenmiş) hali elde edilmiş olur.

6.Verileri Yazma İşlemi

Bu basamakta, şifreleme işleminden elde edilen yeni şifrelenmiş (cipher text) veri paketleri ve deşifreleme işleminde kullanılacak olan bilgiler yazılım yardımıyla dosyaya yazılır.

B. Deşifreleme Yöntemi

Deşifreleme yöntemi ise şifreleme adımlarının tersinin sağlanması ve uygulanmasıyla şifrelenmiş veriden ham (istenen) veriyi çıkarma işlemidir.

Burada ilk olarak, şifreli veri yazılım yardımıyla elde edilmesi gerekir. İkinci olarak, şifreli veri içerisinde deşifreleme işleminde kullanılmak üzere gerekli olan bilgiler (tablo bilgisi, şifrelenmiş verinin dosya uzantısı vb…) elde edilmelidir. Üçüncü aşamada, şifrelenmiş veri paketlerini deşifrelemek için paket paket elde etme işlemi yapılır. Bir sonraki adımda, kullanıcının şifreleme işleminde girmiş olduğu anahtardan bir alt anahtar oluşturulur.

Bu adımda, her veri paketi için ters paket karıştırma ve ters karakter değiştirme işlemleri uygulanır. Artık paketler ters paket karıştırma işlemine girmezler. En son olarak deşifrelenmiş veri paketleri sırasıyla birleştirilir. Böylece deşifrelenmiş veri dosya uzantısına göre (ses, video, metin dosyası vb.) dosyaya yazılır ve kaydedilir.

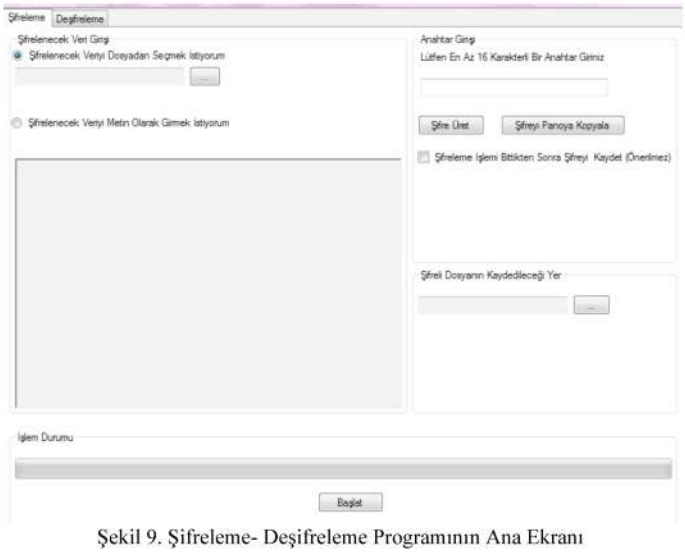
Deşifreleme işleminin basamakları aşağıdaki blok diyagramda gösterilmiştir:



Şekil 8. Deşifreleme İşleminin Basamakları

C. Şifreleme-Deşifreleme Yazılımının Modellenmesi

Bu çalışmada kullanılan şifreleme ve deşifreleme algoritmaları, C# programlama diliyle kodlanmıştır. Bu yazılım sayesinde tasarlanan modern kriptosistem modellemesi Şekil 9.'daki ana ekranda yapılmaktadır:



Şekil 9. Şifreleme- Deşifreleme Programının Ana Ekranı

IV. SONUÇ

Burada tasarlanan kriptosistem modellemesiyle kişisel bilgisayarlarda yer alan bilgiler korunabilir. Ayrıca karşılıklı haberleşmede veriler şifrelenerek iletilebilir.

Bilinen simetrik şifreleme algoritmaları (AES ve DES) temel alınarak yapılan bu yazılımın hızlı çalışması amaçlanmıştır. Windows tabanlı, 2.13GHz (Giga Hertz) işlemcili, 1GB (Giga bayt) RAM ile çalışan bilgisayarla yapılan performans testlerinde 10MB (MegaBayt) boyutundaki bir video 20 saniyede şifrelenmiştir. Bilgisayarın donanım özellikleri arttırılırsa bu sürenin düşeceği düşünülmektedir.

Bazı şifreleme programlarında, giren veri ile çıkan veri boyutu arasında farklar yer almaktadır. Burada yapılan modellemede şifrelemeye giren veri boyutu çıkan veri boyutuna eşittir.

Şifreleme anahtarındaki 1 baytlık (1 karakterlik) değişimde şifreleme işlemi sonucu elde edilen şifreli verinin farklı olduğu görülmüştür.

Bu uygulamayla yapılan şifreleme testlerinde, aynı veri metni farklı şifreleme işlemlerine girince elde edilen şifreli metinlerin farklı olduğu göze çarpar. Buna ek olarak belirli bir metin uzun bir metin içerisinde yerleştirilip şifrelendiğinde yine şifreli metnin farklı olduğu görülür.

Ayrıca, bu program sayesinde bilgisayarda yer alan her türlü veri formatı (program, video, ses, metin vb.) hiç bozulmadan şifrelenir ve deşifrelenir. Böylece kişisel verilerin güvenliği arttırılır.

V. SON DEĞERLENDİRME VE ÖNERİLER

Bu çalışmada, simetrik şifreleme modeliyle şifreleme ve deşifreleme algoritmaları tasarlanmış ve kodlanmıştır.

Günümüzde kişisel verilerin korunması için internette yer alan farklı şifreleme programları bulunmaktadır. Tasarlanan bu program sayesinde veriler şifrelenip deşifrelenebilir. Böylece internette haberleşirken bilgilerin istenmeyen kişiler tarafından elde edilmesi tehlikesi ortadan kaldırılır.

Bu çalışmadaki kodlama işlemi *objective-C*, *C++* yazılımlarıyla da gerçekleştirilebilir. Bu sayede, farklı kullanıcılar günümüzde hızla yaygınlaşan akıllı telefonlarındaki kişisel bilgilerini gizleyebilirler.

Burada ortaya konan şifreleme algoritması bilinen kriptoanaliz testlerine sokulabilir. Bu testlerin neticesinde algoritma içerisinde gerek görülen yapısal değişikliklere gidilerek daha hızlı ve daha güvenilir bir şifreleme metodu oluşturmak mümkündür.

KAYNAKLAR

[1] Yerlikaya , T.: " Yeni Şifreleme Algoritmalarının Analizi", *Doktora Tezi*, Trakya Üniversitesi Fen Bilimleri Enstitüsü, Edirne, Türkiye, (2006).

[2] Diffie W.; Hellman ,M. E.: "New Directions in Cryptography " , *IEEE Transactions on Information Theory, IT-22*, No.6, (1976) , 644-654.

[3] Tsunoo Y.; Tsujihara E.; Minematsu K.; Miyauchi H.: "Cryptanalysis of Block Ciphers Implemented on Computers with Cache", ISITA, (2002).

[4] Federal Information Processing Standards Publications.: "Data Encryption Standard" , *National Bureau of Standarts, U.S. Departman of Commerce*, FIPS PUBS 46-2, (Jan, 1977).

[5] Rivest, R..; Shamir, A.; Adleman, L.: "A Method for Obtaining Digital Signatures and Public-Key Cryptosystems,", *Communications of the ACM*, v. 21, n. 2, (Feb, 1978), pp. 120-126.

[6] Ellison C.; Schneier B.: "Ten Risks of PKI: What You're Not Being Told About Public Key Infrastructure", Computer Security Journal, vol. 16, no. 1, (2000) , pp. 1-7.

[7] Yerlikaya T.; Buluş E.; Arda D.: "Asimetrik Kripto Sistemler Ve Uygulamaları", II. Mühendislik Bilimleri Genç Araştırmacılar Kongresi-MBGAK 2005, İstanbul, Türkiye, (2005).

[8] Yılmaz, R.: " Kriptolojik Uygulamalarda Bazı İstatistik Testler ", *Yüksek Lisans Tezi*, Selçuk Üniversitesi Fen Bilimleri Enstitüsü, Konya, Türkiye, (2010).

[9] Stalling , W.: *Cryptography and Network Security : Principles and Practice* , Printice Hall, ISBN 0-13-869-017-0, New York, USA, (1998), 30-35, 110, 181-187, 259-268.

[10] Başkök, M.: " AES Şifreleme Algoritmasının Modellenmesi ", *Yüksek Lisans Tezi*, Gazi Üniversitesi Fen Bilimleri Enstitüsü, Ankara, Türkiye, (2007).

[11] Özduran, V.: " Birleşik Şifreleme ve Turbo Kodlama Sistemleri ", *Yüksek Lisans Tezi*, İstanbul Üniversitesi Fen Bilimleri Enstitüsü, İstanbul, Türkiye, (2008).

[12] Ulutürk, A.: " Gelişmiş Şifreleme Standardı", *Yüksek Lisans Tezi*, Gazi Üniversitesi Fen Bilimleri Enstitüsü,Ankara, Türkiye, (2010).

Casus Yazılımların Bilgisayar Sistemlerine Bulaşma Belirtileri ve Çözüm Önerileri

Resul DAŞ, ** Şahin KARA,M.Zekeriya GÜNDÜZ**
* Fırat Üniversitesi, Teknoloji Fakültesi, Yazılım Mühendisliği, ELAZIĞ
**Sakarya Üniversitesi, Kaynarca Seyfettin Selim Meslek Yüksek Okulu, SAKARYA
***Bingöl Üniversitesi, Teknik Bilimler Meslek Yüksek Okulu, BİNGÖL
resuldas@gmail.com sahinkara1@gmail.com zekeriyagunduz@gmail.com

Abstract – Spywares can obtain every type of record information revealing private e-mail addresses, phone numbers, personal passwords, credit card numbers and Internet surfing habits of a user. These data can be used by evil-minded people such as for profit and also for inflicting serious damage to people or institutions. In this paper, some solution offers are presented to analyze the infection indications of spyware, infecting personal and institutional computer systems, correctly and to keep these important security holes under control.

Keywords – Spyware, Protection from spyware, Information Security, Computer Security.

Özet – Casus yazılımlar kullanıcıya ait e-posta adresi, telefon numarası, kişisel şifreler, kredi kartı numaraları ve internet alışkanlıklarını ortaya çıkarabilecek her türlü kayıt bilgilerini elde edebilmektedir. Bu bilgiler kötü niyetli kişiler tarafından kâr amaçlı olarak kullanılabileceği gibi şahıslara veya kurumlara ciddi zararlar vermek için de kullanılabilir. Bu makale çalışmasında, bireysel ve kurumsal bilgisayar sistemlerine bulaşan casus yazılımların bulaşma belirtilerini doğru analiz edebilme ve bu önemli güvenlik açıklarını kontrol altına alabilmek için bazı çözüm önerileri sunulmaktadır.

Anahtar Kelimeler – Casus Yazılımlar, Casus Yazılımlardan Korunma, Bilgi Güvenliği, Bilgisayar Güvenliği.

I. GİRİŞ

Elektronik ve bilgisayar alanındaki gelişmeler, büyük bir ivme kazanarak hızlı bir şekilde gelişmekte ve insanların yaşamını kolaylaştıran çok önemli unsurlar haline gelmektedir. Günlük iş süreçlerinin elektronik ortamlara taşınması, manyetik ortamdaki bilgilerin paylaşılması, e-devlet uygulamaları gibi önem arz eden konuların yaygınlaşmaktadır. Bu sebeple, kurulan bu sitemlerin bilişim ağ güvenliğinin gerekliliği ve önemi son derece önemlidir. Bu bağlamda olası tehdit ve tehlikelerin araştırılıp, bunlara karşı gerekli önlemlerin alınması, bilgi, bilgisayar ve bilgisayar ağ güvenliğinin sağlanması açısından büyük önem kazandığı görülmektedir. Bilgisayar sistemlerinin tehdit edilmesinde karşımıza çıkan en önemli husus olarak casus yazılımlar gelmektedir [1-2].

Casus yazılımlar virüs ve solucanlardan farklı olarak, hedef sisteme bir kez bulaştıktan sonra kendi kopyasını oluşturarak yayılmaya ihtiyaç duymazlar. Casus yazılımların amacı, kullanıcıya ait e-posta adresi, telefon numarası, şifreler, kredi kartı numaraları ve internet alışkanlıklarını ortaya çıkarabilecek her türlü kayıt bilgilerini kullanıcının kendisine hissettirmeden ele geçirmektir. Elde edilen bu bilgiler kötü niyetli kişiler tarafından kâr amaçlı olarak kullanılırlar.

Casus yazılımlar genellikle başka bir program kurulurken kullanıcı onayı ile bilgisayara kurulan ve daha sonra kullanıcının internetteki gezme alışkanlıkları ile ilgili istatistiksel bilgiler, şifreler ve hesap numaraları gibi önemli bilgileri internet üzerinden kötü niyetli kişilere iletebilen yazılımlardır. Casus yazılımlar genellikle donanıma doğrudan zarar vermezler ama kişiye ait bilgileri izin almadan elde edebilirler [3]. Bazı kaynaklarda "snoopware" (burun sokan yazılım) olarak da adlandırılan casus yazılımlar, diğer kötücül yazılımlara göre özellikle İnternet kullanıcıları tarafından sistemlere farkında olmadan bulaştırılmaktadırlar [4]. Hemen hemen her yazılım, kurulumu esnasında kullanıcılara bir lisans anlaşması sunar ve kullanıcılar da genellikle bunu okumaya bile ihtiyaç duymadan onaylar. Çoğu zaman okunmayan bu lisans anlaşmalarının içeriğinde, internetten ücretsiz dağıtılan faydalı yazılımları kullanabilmek için kullanıcılar bilgisayarlarına casus yazılımların kurulmasını da kabul etmek zorunda bırakılır. "Freeware" ya da "Shareware" olarak bilinen ve genellikle web ortamından elde edilebilen bu yazılımların içerisinde gömülü olarak bulunan küçük yazılımlar kurulumla beraber kolayca bilgisayara yerleşebilirler. Kullanıcı casus yazılımların kurulumundan bile haberdar olmayabilir. Okunmadan onay verilen lisans anlaşmaları bu yükleme işlemlerini kullanıcıya hissettirmeden yasal kılar.

Casus yazılımlar bilgisayara kurulduktan sonra bilgisayarın kayıt ortamlarını taramaya başlayarak, kişiye ait özel bilgiler ararlar. Bu bilgiler genellikle çerez, kütük (log) veya standart dosyalarda tutulur. Kaydedilen bilgiler arasında internet bankacılığı işlemlerinde kullanılan, kullanıcı adı ve şifresi de bulunmaktadır. Toplanan bilgiler bir dosyada birleştirilir ve daha sonra bu dosya casus yazılımı gönderen

kötü amaçlı kişilere, genellikle truva atı tarzındaki kötücül yazılımlar aracılığıyla açık bırakılan arka kapılar kullanılarak internet üzerinden gönderilir. Çalınan bu bilgiler çoğu zaman reklam amaçlı olarak kullanılır. Kullanıcının kişisel bilgilerine sahip olan site yöneticisi, kendi ürünlerini satabilmek için izin almadan kullanıcıya ve adres defterinde bulunan kişilere e-posta gönderir. Kişinin internet alışkanlıkları öğrenildiği için bu reklamlar kişinin ilgisini çekecek hale getirilmiştir. Çalınan bilgi, eğer kredi kartı detayları veya internet bankacılığı hesap numarası ve şifresi ise bu çok daha tehlikelidir. Bilgileri çalınan kişinin banka hesapları boşaltılabilir ve kredi kartıyla internet üzerinden yapılan alışverişle limiti doldurulabilir.

Casus yazılımların bulaşma teknikleri incelendiğinde en bilindik yöntemlerin başında kullanıcı zafiyeti ve sosyal mühendislik yöntemleri gelmektedir. Bunlarla beraber özellikle download edilen crackli dediğimiz orijinal lisans numaralarına sahip programların arkasına yerleştirilen ve kullanıcının haberi bile olmadan bilgisayarlara yerleştirilen programların varlığı göze çarpmaktadır.

Literatür tarandığında casus yazılımlar konusunun ülkemiz için hızla gelişmekte olan bir konu olduğu ve bu konuda bazı tanımlamaların Türkçe'ye kazandırılmaya çalışıldığı görülmektedir. Bu çalışmalarda virüsler, solucanlar, truva atları, arka kapılar, mesaj sağanakları, kök kullanıcı takımları, telefon çeviriciler, korunmasızlık sömürücüleri, klavye dinleme sistemleri, tarayıcı soyma gibi yazılım türleri *"ana kötücül yazılım türleri"* olarak belirtilmektedir [5].

Bu makale çalışmasında, casus yazılımların çalışma yapıları ve bilgisayar sistemine bulaşma belirtileri sunulmakta ve daha sonra bulunan casus yazılımlarına karşı alınabilecek önlemlerden bahsedilmektedir. Belirtilen çözüm önerilerine göre elde edilen bulgular değerlendirilmiştir.

II. CASUS YAZILIMLARIN BULAŞMA BELİRTİLERİ

Bilgisayar sistemlerinde gerekli korunma önlemleri alınmazsa, casus yazılımlar çok kolay bir şekilde sisteme girebilir. Ancak, alınabilecek tüm önlemler yapılsa da, casus bir yazılımın bulaşması kesin engellenir şeklinde bir sonuca varmak mümkün değildir. Sisteme giren casus yazılımlar bilgisayar sisteminde amaç ve işlemlerini gizlice icra etseler de, önemli ve yaygın olarak görülen bazı belirtiler ile bilgisayar sistemine bulaştıklarını gösterebilirler. Bu belirtilerin önemli olanları, alt maddeler halinde şunlardır.

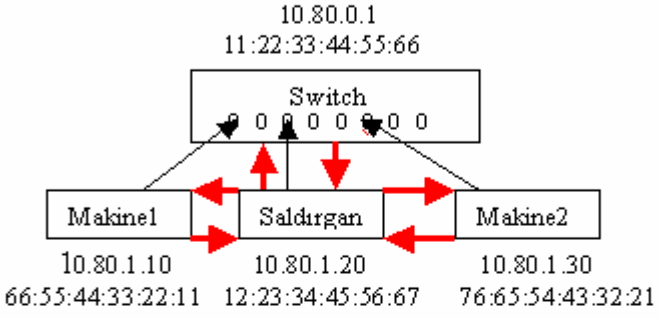
A. Açılır Reklam Pencereleri

Kullanıcı bir web sitesine girdiğinde, o site ile ilgisi olmayan açılır reklam pencereleri bombardımanına tutulabilir. Bu reklamlar genelde yetişkinler veya hoş bulunmayan başka web siteleri için olabilir. Bilgisayar açılır açılmaz veya webde gezinmezken bile görülen reklam pencereleri, bilgisayar sisteminde casus yazılımların olduğunun işaretçileri olabilir. Genellikle bu reklam pencereleri parazit yazılım şeklinde ifade edilen yazılım eklentileridir [5].

B. Web Tarayıcı Ayarlarının Değiştirilmesi

Bazı istenmeyen casus yazılımlar, web giriş sayfasını veya arama sayfasının ayarlarını değiştirebilir. Bunun anlamı, internet tarayıcısı başlatıldığında açılan ilk sayfanın veya "ara (search)" seçeneği seçildiğinde görüntülenen sayfanın tanınmayan farklı sayfalar olmasıdır. Bu değiştirilmiş ayarlar düzeltilse bile, bilgisayar yeniden açıldığında düzeltilen ayarların tekrar eski değerlerine döndüğü görülür. Bu durum, sistemde başka bir casus yazılım olabileceğinin belirtisidir.

Özellikle kullanıcıların farkına varmasının zor olduğu ARP zehirlemesi şeklinde tanımlanan durumlarda bulunmaktadır. MAC adreslerinin IP adresleri ile eşleştirildiği ARP tablolarında yapılan değişiklikler, kullanıcının farkında olmadan verilerin farklı bilgisayarlara gönderilmesine sebep olur. Şekil-1'de görüldüğü gibi saldırgan veri akışının kendi bilgisayarı üzerinden geçmesini sağlamaktadır.



Şekil-1. Ağlardaki ARP aldatmacası [6]

Bir diğer aldatmaca ise DNS ayarlarının zehirlenmesi olabilir ki kullanıcının bunun farkına varması hemen hemen mümkün değildir. DNS aldatmacasında kullanıcı bağlanmak istediği sunucudan farklı bir sunucuya yönlendirilir ve kendini aslında gerçekten bağlanmak istediği sunucuya bağlanmış zanneder. Bundan sonraki göndereceği tüm veriler korsan tarafından rahatlıkla ele geçirilmektedir. Bu tür zehirleme tarzındaki casus yazılımların tespiti zordur, ancak iyi tasarlanmış güvenlik duvarları ile engellenebilir [7].

C. Bilinmeyen İlave Bileşenler

Casus yazılımlar web tarayıcısına istenmeyen veya gerek duyulmayan pek çok araç çubuğu ekleyebilir. Bunlar kaldırılsa bile tekrar görülebilirler. Bu durum casus yazılımların işaretçileri olabilir.

D. Bilgisayar Başarımının Düşmesi

Casus yazılımların sistem üzerinde etkin olacak biçimde tasarlanmış olmaları gerekmez. Bu programlar bilgisayar sistemi üzerinde etkinlikleri izlemek ve reklam dağıtmak için kullandığı kaynaklar yüzünden bilgisayarı yavaşlatabilir. Bazen yazılımdaki hatalar bilgisayarın çökmesine neden olabilir. Bilgisayarda herhangi bir işlem yapılmadığı sırada sabit diskin çalıştığını gösteren ışık yanıyorsa bu casus yazılımlardan kaynaklanabilir. Bir programın daha çok kilitlenmeye başlaması veya bilgisayarın görevlerini her zamankinden daha yavaş yapmaya başlaması bilgisayar sisteminde casus yazılım olabileceğini gösterir [8].

E. Antivirüs ve Antispyware Yazılımlarının Çalışmaması

Casus yazılımlar, kendi varlıklarını sürdürebilmek için bu programları kapatırlar veya sistemden silerler.

F. Telefon Faturalarında Uluslararası Aramalar

Bazı şirketlere para kazandırmak amacıyla 900'lü hatları ararlar ve uluslararası hatlara aramalar gerçekleştirerek telefon faturalarının kabarmasına neden olurlar.

G. Yanlış Arama Sonuçları

Varsayılan olarak belirlenen arama motorunda yapılan aramaları kendi sitelerine yönlendirir ve beklenmedik arama sonuçlarını kullanıcının karşısına çıkarırlar.

H. Internet Hızında Yavaşlama

Sürekli bilgi toplama ve gönderme halinde olduklarından internet hızının sık sık yavaşlamasına sebep olurlar.

III. ÖRNEK CASUS YAZILIMLAR

Bilinen ve bilgisayarlara sıkça bulaşan bazı yaygın casus yazılımlar aşağıda incelenmiştir.

A. CoolWebSearch(CWS)

Adware kendi yazdığı programı satmak yerine, belirli firmalar tarafından sağlanan reklamları programın içine gömerek kullanıcıya sunan programların genel adıdır [9]. Adware (*advertising-supported software)* reklam destekli yazılım, yüklenildiği bilgisayara yüklenme işleminden sonra program kullanımdayken otomatik olarak çalışan, gösteren ve indirme yapan bir yazılım paketidir. Adware'lerin bazı tipleri spyware statüsündedir ve kişisel bilgilere gizlice ulaşılmasında kullanılırlar [3]. CoolWebSearch de adware türünde bir casus yazılımdır.

CoolWebSearch (CWS), web tarayıcı ana sayfasını, arama sayfalarını değiştirebilir, yapılan aramaları kendi arama motoruna yönlendirir ve ana sayfayı değiştirerek kendi yapımcısının ana sayfasına yönlendirir. Ayrıca, bu program tarayıcıların diğer ayarlarını da değiştirebilir. Bu adware tarayıcı ayarlarını değiştirirse, ayarlar bir daha eski haline getirilemeyebilir.

B. EliteBar

EliteBar, web tarayıcı ana sayfasını, arama sayfalarını değiştirebilir ve bilgisayarlarda çeşitli reklamlar gösterebilir. Yapılan aramaları kendi arama motoruna ve kendi web sayfasına yönlendirir.

C. PowerScan

PowerScan, dolandırıcı bir antivirüs programıdır. Yüklendiği bilgisayarda tarayıcı ana sayfasını değiştirebilir ve çeşitli reklamlar gösterebilir. Yapılan aramaları kendi arama motoruna ve kendi web sayfasına yönlendirir.

D. Look2Me

Türü adware olan Look2Me, bilgisayarda pop-up reklam gösteren bir programdır. Look2Me, bilgisayarda çeşitli rahatsız edici reklamlar gösterilmesine sebep olan karakteristiğe sahiptir.

E. PurityScan

PurityScan, bilgisayarda pop-up şeklinde çeşitli rahatsız edici reklamlar gösterilmesine sebep olan programdır.

F. Clkoptimizer

Clkoptimizer, PurityScan ile hemen hemen aynı rahatsızlık verici aktiviteleri gerçekleştiren, bilgisayarda pop-up reklam gösteren bir programdır.

G. WebSearch Toolbar

WebSearch Toolbar, web araması yapılan kelimeleri çalan bir araç çubuğu programıdır. Internet tarayıcı programına ekstra bir araç çubuğu yükleyerek, ayarları ile oynar. Ayrıca, bilgisayarda çeşitli rahatsız edici reklamlar gösterilmesine sebep olan bu program, web adreslerini izleyerek web tarayıcılarına girilen bilgileri çalar.

H. 180search Assistant/Zango

180search Assistant ve Zango, kullanıcıları sponsorlarının web sayfalarına yönlendiren adware yazılımlardır. 180search Assistant ve Zango, bazı kelimeleri tanıyarak kullanıcıları, sponsorlarının web sayfalarına yönlendirir. 180search Assistant ve Zango, çeşitli ücretsiz yazılımlar yolu ile bulaştıkları gibi internetten direkt olarak da indirilebilir ve kurulabilirler. 180search Assistant ve Zango, bilgisayarlarda sponsorların reklamı olan yeni tarayıcı pencereleri açılmasına ve sistemin yavaşlamasına neden olurlar.

I. IST Istbar

IST Istbar, internette müstehcen web sitelerini arayan bir toolbar'dır. Müstehcen içerikli pop-up pencereleri açabilir, ayrıca ana sayfanın ve arama sayfalarının üzerinde oynama yapabilir. IST Istbar, Internet Explorer'a bir toolbar yükler ve ayarlar ile oynar. Ayrıca bilgisayarda çeşitli rahatsız edici müstehcen içerikli reklamlar gösterilmesine sebep olur.

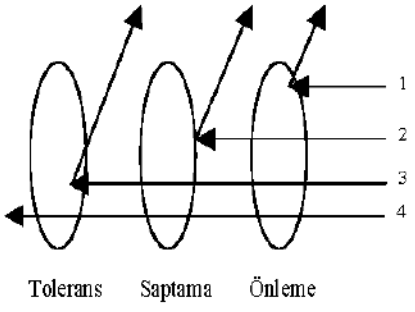
J. AbetterInternet

AbetterInternet, genellikle VX2 ya da Transponder olarak bilinen ve bilgisayarda reklam gösteren bir programdır. AbetterInternet, internet tarayıcısının ayarlarını değiştirebilen bir tarayıcı yardım nesnesi (Browser Helper Object - BHO) yazılımıdır. Bunlar tarayıcıda çalışabilen, yanlış adreslere yönlendirmeler yapabilen ve aramaların yanlış sonuçlanmasına neden olabilen programlardır. Bu programların ortak özellikleri, genellikle diyalog kutuları ve Java Script hata teknikleri ile ya da yüklenen ücretsiz ve güvensiz programlarla yayılırlar. Bilgisayarlarda rahatsız edici reklam görüntülemeye çalışırlar. Ayrıca internet tarayıcısının ve sistemin genel performansının düşmesine sebep olurlar.

IV. CASUS YAZILIMLARI ENGELLEME

Dünyada ve ülkemizde bilgi güvenliğine yönelik en büyük tehdit olan kötücül ve casus yazılımlar ile yapılan saldırılar çok yaygındır. Ancak kullanıcılar, bu tür saldırı ve tehdit oluşturduklarından çoğunlukla haberdar değillerdir [2]. "Sistem ve bilgisayarları casus yazılımlara karşı korumak %100 mümkündür" şeklinde bir kanıya varmak tam olarak mümkün olmayabilir. Ancak bir saldırının nereden ve ne şekilde yapılabileceği tahmin edilebilirse alınan önlemler de o ölçüde etkili olacaktır [10]. Sistemi korumak için alınan güvenlik önlemleri, saldırganların ya da korsanların kolay bir şekilde sisteme ulaşmasını zorlaştıracaktır. Şekil-2'de,

korunmak istenen sistemle ilgili alınabilecek önlem süreçleri temsili olarak gösterilmiştir.



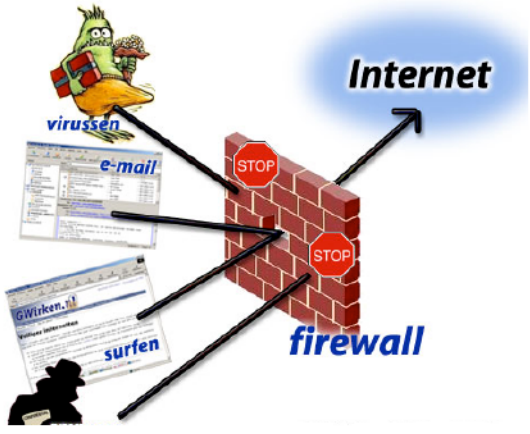
Şekil-2. Kötücül Yazılımlara Karşı Savunma Süreci [2]

Şekil 2'de belirtilen 1. türdeki kötücül ve casus yazılımlar, daha önleme aşamasında iken bertaraf edilecektir. Bu aşamada, herkesin kolayca tahmin edemeyeceği şifrelerin belirlenmesi, kişisel bilgisayarların herkesin kullanımına açılmaması, antivirüs yazılımların kullanılması gibi temel önlemlerin kullanıcı tarafından alınması yeterli olacaktır. Kurumsal yapıda oluşturulacak temel güvenlik politikaları, bu türdeki casus yazılımlardan korunmayı zaten yüksek seviyede sağlayacaktır [15].

Kötücül yazılımlara karşı 2. tür engelleme 1.türdeki engellemeye göre daha teknik korunma yolları gerektirmektedir. Güvenlik duvarları, saldırı tespit sistemleri, port tarayıcılar gibi yöntemler bu süreci güçlendirecektir [2, 12]. Şekil 2'de belirtilen 3. türdeki kötücül ve casus yazılımların bulaşmasını engellemek daha profesyonel korunma yollarını gerektirir. Bu aşamada, özellikle yapay sinir ağlarının etkin kullanımı ile casus yazılımların sınıflandırma işlemini gerçekleştirebilen saldırı tespit sistemlerinin kullanılması etkin bir güvenlik sağlayacaktır [13]. 4. tür kötücül ve casus yazılımlar için pek yapılabilecek bir şey yoktur. Artık sisteme bulaşmışlardır. Bu korunma süreçleri göz önünde bulundurularak bilgisayarların casus yazılımlara ve istenmeyen diğer yazılımlara karşı korumasına yardımcı olabilecek bazı yöntemler şunlardır.

A. Güvenlik Duvarı (Firewall)

Güvenlik duvarı, iki ağ arasındaki IP trafiğini kontrol etmek için kullanılan donanım veya yazılımlardır. Güvenlik duvarı genel olarak; çeşitli ağ saldırılarına karşı bilgisayarı korumak, ağ trafiğini ve erişim politikalarını kontrol etmek, herhangi bir şüpheli durum tespit edildiğinde uyarı göndererek durumu kullanıcıya bildirmek için kullanılır. Birçok casus yazılım ve istenmeyen yazılımlar, diğer programlarla birlikte geliyor olsalar da casus yazılımların çok az bir kısmı bilgisayarlara uzaktan bilgisayar korsanlarınca yerleştirilir. Bir güvenlik duvarının yüklenmesi ya da işletim sisteminde yerleşik bulunan güvenlik duvarının kullanılması, bu korsanlara karşı faydalı bir savunma sağlar. Güvenlik duvarının bir bilgisayarı tek başına kesinlikle koruyamayacağı unutulmamalıdır. Güvenlik duvarının en etkili şekilde çalışabilmesi, birçok parçadan oluşan bir güvenlik mimarisi içinde bulunmasına bağlıdır (Şekil-3).



Şekil-3. Güvenlik Duvarı

B. Yazılım Güncellemeleri

Yazılımlar, eksiksiz, hatasız ve tam olarak yüklendiğinde iyi bir performans sunar. Yazılımların hataları, eksiklikleri ya da güvenlik açıkları giderildikçe, o yazılımı yeniden güncellemek gerekir. Aksi halde, güvenlik açıkları bakımından ciddi riskler oluşturur. Henüz birkaç ay önce yeni bir antivirüs yazılımı yüklenmiş olsa bile, olası yeni virüs saldırılarına karşı savunmasız kalabilir. Yazılım güncellemeleri, o programa ait sorunları engelleyebilecek veya düzeltebilecek, bilgisayarın güvenliğini artırabilecek veya performansını arttırabilecek yazılım ekleridir. Pek çok yazılım üreticileri, programın yeni bir güncelleştirmesi veya sürümünü çıkardığında kullanıcıları uyarır. İşletim sisteminin güncelleştirmeleri otomatik olarak tespit edip, ek dosyaları yükleyebilmesi için ayarlanması çok önemlidir.
Bilgisayarları casus ve kötü amaçlı yazılımlardan korumak amacıyla güncel casussavar yazılımların kullanılması gerekir. Bu amaçla kullanılacak programların lisanslı olması daha faydalı olacaktır. Lisanslı yazılımlar, güvenliği göz ardı etmeyen ve korunmasızlıkların en aza indirilmesine çalışıldığı yazılımlardır. Bu tür yazılımların, kullanıcılara hizmet veren müşteri destek kanalları da bulunmaktadır [6].

C. İnternet Tarayıcısı Güvenlik Ayarları

İnternet tarayıcıları, bilgisayar korsanlarının asıl hedefidir. Kullanılan programı güvenilir hale getirmek için ilk başta genel güvenlik kuralları uygulanmalıdır. İnternet tarayıcısının güvenlik ayarları, bilgisayarın olası zararlı ve kötü amaçlı çevrimiçi içerikten korunmasına yardımcı olabilecek ayarlardır. Bu ayarlar üzerinde, "çok düşük" ile "yüksek" arasında değişen güvenlik seviye ayarları yapılabilir, değiştirilebilir. En önemli tehlikelerden korunabilmek adına, "Internet" için en az orta derece seçilmelidir. En yüksek güvenlik seviyesinde riskli hareketler engellenir veya bu tür hareketler ile ilgili karar bir diyalog kutusu ile kullanıcıya bırakılır.

D. Casus Yazılımlardan Korunma Yazılımları

Virüslere karşı antivirüs yazılımları kullanılarak önlem alınıyorsa, casus yazılımlara karşı da casussavar yazılımlar kullanılarak sistem koruma altına alınmaya çalışılır. Sistemlere kurulan bu yazılımların en güncel halleri

kullanılmalıdır. Çok sık rastlanan yanılgılardan biri de, virüs korunma programı bulunan bir bilgisayar sisteminin bütün kötücül ve casus yazılımlara karşı da korunma sağlayacağının sanılmasıdır. Virüs korunma programları elbette çok önemlidir ama sayısız kötücül ve casus yazılıma karşı ancak casus savar yazılımlar kullanılarak mücadele edilebilir [3].

E. Internet Ortamında Dikkatli Gezinti Yapma

Casus yazılımlara ve istenmeyen diğer yazılımlara karşı en iyi savunma, ilk etapta bunlara ait dosyaları bilgisayarımıza indirmemektir. İstenmeyen yazılımları, indirmeden önce koruyucu bazı önerileri maddeler halinde sıralayabiliriz.

- Programları sadece güvendiğiniz web sitelerinden indirin. İndirmeyi düşündüğünüz bir programa güvenebileceğinize emin değilseniz, programın casus yazılım içerdiğine dair herhangi bir bilgi olup olmadığını görmek için adını sık kullandığınız arama motoruna yazın.

- İndirdiğiniz her tür yazılımla ilişkili tüm güvenlik uyarılarını, lisans sözleşmelerini ve gizlilik beyanlarını üşenmeden okuyun.

- Bir pencereyi kapatmak için asla "Kabul" veya "Tamam" butonuna tıklatmayın. Bunun yerine pencerenin köşesindeki kırmızı "X" düğmesini tıklatın veya pencereyi kapatmak için klavyenizde Alt + F4 tuşlarına basın.

- Popüler olan "ücretsiz" müzik ve film dosya paylaşım programlarına dikkat edin ve bu programlarla birlikte aynı pakette yer alan yazılımların tamamını anladığınızdan emin olun.

- Yönetici hesabı yerine standart bir kullanıcı hesabı kullanın. Standart hesap, kullanıcıların bilgisayarın çalışabilmesi için gerekli olan dosyaların silinmesi gibi, bilgisayarı kullanan herkesi etkileyen değişiklikler yapmasını engelleyerek bilgisayarı korumanıza yardımcı olabilir. Her kullanıcı için standart bir hesap oluşturmanız daha güvenilir olacaktır. Windows işletim sisteminden standart hesabınızla oturum açtığınızda, yönetici hesabıyla yapabileceğiniz hemen her şeyi yapabilirsiniz, ancak yazılım yükleme veya güvenlik ayarlarını değiştirme gibi bilgisayarın diğer kullanıcılarını etkileyen şeyler yapmak istediğinizde, yönetici hesabı parolası ile işlemlerinizi yapabilirsiniz [9].

- Bir siteden kredi kartı ile işlem yaptığınızda sitenin kullandığı protokolün *http* yerine *https* olduğuna dikkat edin.

- Casus yazılımların "crackli" olarak ifade edilen kırılmış halleri ile kullanıcının haberi olmadan kurulabileceği buna karşı ise kullanılan programların lisans numaralı orijinal programlar olmasına dikkat edilmelidir.

- Sosyal paylaşım sitelerinde paylaşılan linklerin güvenilirliği konusunda şüphe duyulduğunda, hemen linki açma yoluna gidilmemelidir.

F. Güvenlik Araçlarının Kullanılması

Anlatılan tedbirler alınmış olsa bile sistemde saldırganların faydalanabileceği farklı açıklar olabilir. Şekil-2'de gösterilen tolerans basamağının casus yazılımlarca geçilmesini engellemek için sistem açıklıkları bilinmeli ve kontrol altına alınmaya çalışılmalıdır. Bu açıklıklar çeşitli güvenlik araçları kullanılarak tespit edilebilir ve gerekli önlemler alınabilir. Güvenlik araçları ayrıca sistemi izleme olanağı da sunarlar. Güvenlik araçlarının casus yazılımların tespitindeki yetenekleri tamamlayıcı bir etki oluşturmaktadır. Sistemlerimiz de kullanabileceğimiz ve genelde freeware olarak dağıtılan bazı güvenlik araçlarının isimleri şu şekildedir [11]: NMAP, NESSUS, ETHEREAL, SNORT, TCPDUMP, DSNIFF, GFI LANGUARD, ETTERCAP, JOHN THE RIPPER, TRIPWIRE. Ayrıca ücretsiz olarak dağıtılan diğer bir ağ izleme programı olarak belirtebileceğimiz Wireshark programı da bu alanda oldukça popüler kullanılan bir programdır [14].

Bu yazılımlar aracılığı ile ağdaki veri paket akışları rahatlıkla gözlemlenebilir. Böylece ağ içerisinde DoS tipindeki saldırıların olup olmadığı, portların kullanım durumları, veri akışındaki düzensizlikler, casus yazılımların sızmaya çalıştıkları açık kapılar gibi bilgiler elde edilerek sistemin çalışma yetisi belli ölçülerde kontrol altında tutulabilir.

G. Sosyal Mühendislik Zaafiyetleri

Kullanıcılar, internet veya telefon aracılığı ile özellikle yardım amaçlı bilgi aşırmaya çalışan şahıslara karşı uyanık olmak durumundadır. Özellikle sazan avlama olarak tabir edilen *phishing* ve benzeri bilindik sosyal mühendislik yöntemlerine karşı dikkatli olunmalıdır. Bir banka veya şirket, hiçbir şekilde kişisel bazı güvenlik sorularına cevap vermeden şahsı veya kişisel hesaplar ile ilgili bilgiler isteyemeyeceğini bilmelidir. Sosyal mühendislik ile ilgili casus yazılımların sistemlere bulaştırılmaması konusunda kullanıcılar temel bilgilere sahip olmalıdır.

V. SONUÇ

Bilgisayar sistemlerini ve bilgi güvenliğini tehlikeye atan tehditler gün geçtikçe artarak, çeşitlenmektedir. Son zamanlarda bilgisayar güvenliğini tehdit eden, kişisel ve kurumsal veri güvenliği için önemli bir tehlike oluşturan casus yazılımlar, oluşturdukları sorunlar ile ön plana çıkmaktadır. Bilgisayar ortamında saklanan veya bilgisayar ağ sisteminde dolaşan önemli ve kişisel bilgilerin kötü niyetli kişiler tarafından çalınmasının bir yolunun da casus yazılımlar olduğu unutulmamalıdır. Kötücül ve casus yazılımlardan korunmak için gereken önlemler alınmadığı takdirde sistemlere verebilecekleri zararlar konusunda geç kalınabilir. Hem bireysel kullanıcıların hem de kurumların casus yazılımlara karşı bilinçlenmeleri ve gereken önlemlerini almaları bu konudaki zararı en aza indirgeyecektir.

KAYNAKLAR

[1] Y.Uzunay, "Dijital Delil Araştırma Süreci", 2.Polis Bilişim Sempozyumu, Ankara, 2005.

[2] G.Canbek,Ş.Sağıroğlu, "Bilgi, Bilgi Güvenliği Ve Süreçleri Üzerine Bir İnceleme", Gazi Üniversitesi, Mühendislik Mimarlık Fakültesi, Bilgisayar Mühendisliği Bölümü, 06570 Maltepe, Ankara.
[3] *Internet:* Casus Yazılım, http://tr.wikipedia.org/wiki/Casus_yazılım(spyware) , 2011.
[4] Canbek, G., Klavye Dinleme ve Önleme Sistemleri Analiz, Tasarım ve Geliştirme, Yüksek Lisans Tezi, Gazi Üniversitesi, Fen Bilimleri Enstitüsü, Ankara, 2005.
[5] Canbek, G., Sağıroğlu, Ş., Kötücül ve CasusYazılımlar : Kapsamlı Bir Araştırma, Gazi Müh. Mim. Fak. Dergisi, Cilt 22, No: 1, Mart 2007, Ankara, Türkiye.
[6] Akgün, F., Buluş, E., Şen, Ş.,"Bilgisayar Ağları Üzerinde İletilen Verilere Zarar Vermek İçin Kullanılan Önemli Teknikler ve Korunma Yollarının İncelenmesi", Trakya Üniversitesi, Mühendislik Mimarlık Fakültesi, Bilgisayar Mühendisliği Bölümü, Edirne.
[7] Daiji, S., "Detection of Promiscuous Nodes Using ARP Packets", August 2001.
[8] Canbek, G., Sağıroğlu, Ş., Casus Yazılımlar: Bulaşma Yöntemleri ve Önlemler, Gazi Üniv. Müh. Mim. Fak. Dergisi, 2008.
[9] *Internet :* Güvenlik Duvarı, http://www.izafet.com/guvenlik-ve-guvenlik-aciklari, 2011.
[10] Güven,M.,"İnternette Güvenlik ve Hacker Cracker Meselesi", Seçkin Yayıncılık, 2007.
[11] Anuk, E., "Güvenlik Araçları", İTÜ Bilişim Enstitüsü, Bilgisayar Bilimleri, İstanbul, 2011.
[12] Canbek, G., Sağıroğlu, Ş., Bilgisayar Sistemlerine Yapılan Saldırılar ve Türleri: Bir İnceleme, Erciyes Üniversitesi, Fen Bilimleri Dergisi, Cilt : 22, Sayı : 1–2, 2007.
[13] Sazli, M., Tanrikulu, H., "Saldırı Tespit Sistemlerinde Yapay Sinir Ağlarının Kullanılması", Türkiye de internet Konferansı, Kasım 2007, Ankara.
[14] *Internet:* Wireshark, http://www.wireshark.org/, 2012.
[15] Karaarslan, E., Teke, A., Şengonca, H.," Bilgisayar Ağlarında Güvenlik Politikalarının Uygulanması", Ege Üniversitesi Uluslararası Bilgisayar Enstitüsü, Bilgisayar Mühendisliği, İzmir.

Resul DAŞ, 1975 yılında Elazığ'da doğdu. 1999 yılında Fırat Üniversitesi, Teknik Eğitim Fakültesi, Bilgisayar Öğr. bölümünü, 2002 yılında Bilgisayar Sistemleri alanında yüksek lisansını tamamladı. 2008 yılında aynı üniversitenin Elektrik-Elektronik Mühendisliği bölümünde doktora eğitimini tamamlayarak, bu alanda Doktor ünvanını aldı. 2000 – 2011 yılları arasında Fırat Üniversitesi Enformatik bölümünde öğretim elemanı olarak çalıştı. Kasım 2011 yılından beri Fırat Üniversitesi, Teknoloji Fakültesi, Yazılım Mühendisliği bölümünde öğretim üyesi olarak görev yapmaktadır. Bilgisayar Ağları, Ağ Güvenliği, Web ve Veri Madenciliği, Bilgi Keşfi, Adli Bilişim ve Güvenlik konularında çalışmalar yapmaktadır.

Şahin KARA, 1977 yılında Bitlis'te doğdu. 2002 yılında Süleyman Demirel Üniversitesi, Teknik Eğitim Fakültesi, Bilgisayar Öğretmenliği bölümünü bitirdi. Bitlis Eren üniversitesinde öğretim elemanı olarak görev yaptı. Halen Sakarya Üniversitesinde öğretim elemanı olarak görev yapmaktadır. Aynı zamanda Fırat Üniversitesi, Fen Bilimleri Enstitüsü, Elektronik ve Bilgisayar Eğitimi Anabilim dalında yüksek lisans eğitimi yapmaktadır. Adli bilişim ve güvenlik konularında araştırmalar yapmaktadır.

M. Zekeriya GÜNDÜZ, 1983 yılında Bakırköy'de doğdu. 2006 yılında Süleyman Demirel Üniversitesi, Teknik Eğitim Fakültesi, Elektronik ve Bilgisayar Sistemleri Öğretmenliği bölümünü bitirdi. 2006-2010 yılları arasında Milli Eğitim Bakanlığına bağlı Endüsri Meslek Liselerinde Bilişim Teknolojileri öğretmeni olarak görev yaptı. Halen Bingöl Teknik Bilimler Meslek Yüksek Okulu, Bilgisayar Programcılığı bölümünde öğretim görevlisi olarak çalışmaktadır. Aynı zamanda Fırat Üniversitesi, Fen Bilimleri Enstitüsü, Elektronik ve Bilgisayar Eğitimi Anabilim dalında Ağ güvenliği konusunda yüksek lisans çalışmalarına devam etmektedir.

AKILLI ŞEBEKELERDE SİBER GÜVENLİK VE MAHREMİYET

Elif Üstündağ Soykan, Seda Demirağ Ersöz

***Özet*—Akıllı şebeke teknolojisi, elektrik enerjisini verimli kullanmak ve enerji üretim, iletim ve dağıtım sistemleri arasındaki bilgi alışverişini artırmak için kullanılmaktadır. Yaygınlaşma ve standartlaşma çalışmalarının başlamasıyla, kritik altyapı niteliğindeki elektrik taşıma sistemlerinde güvenlik ve mahremiyet ilgi çeken bir konu olmuştur. Bu bildiride akıllı şebekelerde mahremiyet ve güvenlikle ilgili ele alınması gereken hususlar ve bu konularda yapılan çalışmalar anlatılacaktır.**

***Anahtar Kelimeler*—Akıllı Şebekeler, Siber Güvenlik, Mahremiyet.**

***Abstract*—Smart Grid is used to enhance the efficiency of electricity usage and the communication among power generation, transmission and distribution systems. With the start of expansion and standardization activities, security and privacy issues are getting more attention in power transportation systems which are also considered as a critical infrastructure. In this paper, the security and privacy issues in smart grid will be addressed and some studies on these issues will be discussed.**

***Keywords*—Smart Grid, Cyber Security, Privacy.**

I. GİRİŞ

ENDÜSTRİ ve bilgi teknolojilerindeki gelişmeler hızla devam ederken elektrik güç sistemleri yıllardır değişmeyen ve aynı şekilde idame ettirilen en büyük şebekeler olarak karşımıza çıkmaktadır. Güç sistemlerinde süreklilik, güvenilirlik ve sürdürülebilir enerji ihtiyaçlarının giderek artması, akıllı şebekelerin gelişmesinde en büyük etkendir. Amerika'da 14 Ağustos 2003'te meydana gelen güç kesintisi (blackout), 50 milyon kişinin enerjisiz kalmasına ve yaklaşık 6 milyar dolarlık zarara neden olmuştur [1]. Bu çöküntü çok kısa bir sürede değil birbirini takip eden olaylar sonucu oluşmuştur. Akıllı bir şebeke olmadığı için güç sistemi gerçek zamanlı kontrol edilememiş ve kısa sürede önlem alınamaması nedeniyle kesinti yayılarak ilerlemiştir. Büyük ölçekli benzer bir güç kesintisi de 2003 yılında İtalya'da gerçekleşmiş ve 56 milyon kişi bu kesintiden etkilenmiştir [2]. Bu olaylar akıllı şebekelere geçiş sürecine ivme kazandırmıştır.

Akıllı şebekelerin öne çıkmasında diğer bir etken de hava kirliliği ve iklim değişiklikleridir. Enerji üretiminin büyük bir bölümü fosil yakıtların kullanılmasıyla gerçekleşir [3]. Akıllı şebekelerin elektrik üretim/tüketimini optimize etmesi ve yenilenebilir enerji kaynaklarının entegrasyonunu kolaylaştırmasıyla fosil yakıt tüketiminin düşeceği öngörülmektedir. Amerika'daki akıllı sayaç uygulaması bunun ilk göstergesidir. General Electric'e göre Amerika'daki evlerin %10'unda akıllı sayaçların kullanılması ile 3.724.197 ton CO_2 salınımı engellenmiştir. Bu oran %50'e çıktığında 18 milyon tonun üzerinde CO_2 salınımın önüne geçileceği belirtilmektedir [4].

Diğer yandan yeni gelişmekte olan elektrikli otomobillerin (PHEV, Plug-in Hybrid Electric Vehicle), fosil yakıtlara bağımlılığı azaltmakla kalmayıp aynı zamanda akıllı şebekeye dağıtık enerji kaynağı oluşturacağı öngörülmektedir.

Şu an kullanılmakta olan güç şebekelerinin bilgi teknolojileri altyapılarıyla modernleştirilmesiyle oluşan akıllı şebekelerin ana hedefleri:

- Elektriği daha verimli taşımak ve dolayısıyla daha kaliteli güç elde etmek,
- Şebekenin siber-fiziksel saldırılar, doğal afetler ve arızalar gibi sistemi etkileyen olaylarda kendi kendini onarması,
- Dağıtık enerji kaynaklarının (rüzgar türbinleri, güneş enerjisi ve benzeri yenilenebilir enerji kaynakları) şebekeye dahil edilmesi,
- Tüketicilere alternatif tüketim politikaları ve fiyat avantajı sunabilmek

olarak özetlenebilir.

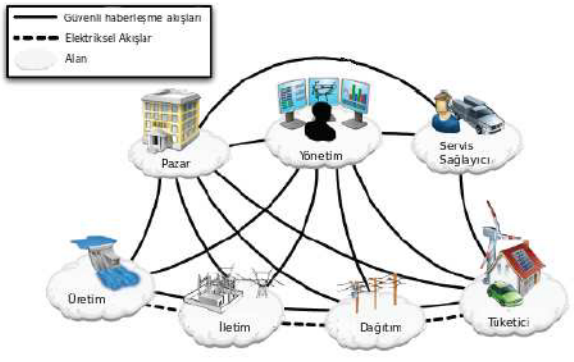
Güç sistemleri genel olarak üretim, iletim ve dağıtım sistemlerinden oluşmaktadır. Akıllı şebekeler, güç sistemlerindeki her bileşen için gerçek zamanlı çift yönlü iletişim ve bilgi akışını hedefler. Bu sebeple hem bilgi teknolojileri hem de elektrik sistem operasyon ve yönetimini gerektiren alt sistemlerin oluşturduğu karmaşık bir sistemdir. Bu kadar karmaşık ve kritik bir sistemin kuşkusuz siber güvenlik ve mahremiyet bakış açılarından incelenmesi kaçınılmaz bir gerektir.

Bildirinin devamı şu şekilde ilerleyecektir: 2. bölümde akıllı şebekelerin bileşenlerini, 3. ve 4. bölümlerde akıllı şebekelerdeki siber-fiziksel güvenlik ve mahremiyet ihtiyaçlarını inceleyeceğiz. Son olarak 5. bölümde bildiriyi sonuçlandıracağız.

II. AKILLI ŞEBEKELERE GENEL BAKIŞ

Akıllı şebekelerin mimari çerçevesi ve standartlaşma çalışmaları hala devam etmekle birlikte; NIST (National Institute of Standarts and Technology), tanımladığı referans modelde akıllı şebekeleri yedi mantıksal alana bölerek incelemektedir [5]. Bu modelde akıllı şebekeleri sistemlerin oluşturduğu bir sistem olarak tanımlamaktadır. Şekil 1'de "Customer" olarak adlandırılan tüketici alanı elektriğin son kullanıcılarını, "Markets" alanı ise elektrik pazarının işleticilerini içerir. "Service Provider" tüketicilere hizmet götüren Hizmet Sağlayıcılar, "Operations" ise yönetimden sorumlu birimleridir. "Bulk Generation, Transmission ve Distribution" güç sistemlerinin üretim (santraller vb), iletim ve dağıtım sistemleridir. Burada

E. Üstündağ Soykan, S. Demirağ Ersöz, TÜBİTAK BİLGEM UEKAE. {ustundag, seda}@uekae.tubitak.gov.tr



Şekil 1. Akıllı Şebeke İletişimlerindeki Etkileşim [5].

belirtilen her alan birbirleriyle ve kendi içlerinde iletişim halindedir. Örneğin Tüketici alanındaki sayaçlar Yönetim alanındaki dağıtım yönetim sistemiyle veri alışverişi yapmaktadır. Her alan farklı cihazlara ve uygulamalara sahip olduğu için iletişimler için önerilen yöntemler de çeşitlilik gösterebilmektedir. Cisco [6], internetteki başarısı nedeniyle buradaki iletişimler için IP protokolünün kullanılmasını önermiştir. Clark ve Pavlovski [7] kablosuz ağ teknolojilerinin kullanılmasını, mimari olarak da 3G/4G teknolojilerini örnek almayı önerirken, Gadze [8] hiyerarşik bir model ortaya koymuştur. Her ne kadar farklı öneriler bulunsa da hepsinin 4 temel problem üzerinde yoğunlaştığı görülüyor. Farklı medyalar üzerinden veri alışverişi, veriyi hızlı bir şekilde toplama ve analiz etme, fazla sayıda cihaz ve sistemi birbirine bağlama, güvenlik ve dayanıklılık.

A. Akıllı Şebeke Bileşenleri

AIM (Advanced Metering Infrastructure), kullanıcıların tüketimiyle ilgili verileri toplayan ve ileten sistemdir. Temel bileşenlerini akıllı sayaçlar, sayaç yönetim sistemi ve yönetim sistemiyle yapılan bağlantılar oluşturur. AIM, tüketicilerin kullanımlarını ve ücretlendirmeleri optimize etmeyi amaçlar. Aynı zamanda tüketim bilgilerini (örn. fazla güç çekiliyorsa vb.) sistemin sürekliliğini sağlamak için kullanır.

SCADA (Supervisory Control And Data Acquisition) sistemi şebekedeki cihazların (elektrik makinaları, kesici, ayırıcı, trafo) bir merkezden denetlenmesini, izlenmesini, işletilmesini ve saklanmasını sağlayan sistemlere verilen addır. Bu sistem sayesinde, bir tesise veya işletmeye ait tüm elemanların ve ünitelerin kontrolü ve gözetlenmesi sağlanabilir [9]. SCADA birkaç bileşenden oluşur: Uzak Uç Birimler (RTU, Remote Terminal Unit veya PLC, Programmable Logic Controllers), Saha Birimleri (Koruma röleleri vb.), İletişim Sistemi (iletişim medyası ve protokoller), Merkezi Kontrol Birimi.

Uzak terminal birimleri (RTU) bulundukları yerde ölçüm ve denetleme işlemleri yürüten birimlerdir. RTU'lar birbirlerine bağlanabilen çeşitli cihazlara kumanda edebilir, ölçülmesi gereken akım, gerilim, güç değerlerini ölçebilir. RTU'lar topladığı verileri merkeze ileterek bunların analizi sonucunda merkezden gelen komutlar doğrultusunda işlemlerini yaparlar. PLC'ler de RTU mantığıyla çalışan daha küçük birimlerdir.

Merkezi Kontrol Birimi; bilgisayarlardan, giriş-çıkış birimlerinden, insan-makina ara birimlerinden (HMI, Human-Machine Interface), RTU'larla iletişimi sağlayan birimlerinden ve veri depolama birimlerinden oluşur [9]. Temel görevi RTU, PLC ve rölelerden gelen verileri toplayarak, bu verileri depolamak, uygun yazılımlarla işlemek ve analiz etmek, analiz sonuçlarına göre alarmları operatörlere ileterek RTU'ları komuta etmektir. Bunun yanısıra dağıtım yönetim sistemi ve gerektiğinde enerji yönetim sistemleri gibi üst seviye uygulama programlarını çalıştırmak da SCADA sisteminin işlevleri arasındadır.

İletişim sistemi SCADA'nın tüm haberleşme yapısını içermektedir. Kontrol birimindeki cihazlarla, RTU'ların birbirleri arasında ve farklı kontrol birimlerinin kendi arasında haberleşebilmeleri için gerekli fiziksel medya ve iletişim protokollerini içerir. İletişim medyası olarak kiralık hatlar, fiber-obtik kablolar, uydu sistemleri ve kablosuz sistemler gibi farklı ortamlar kullanılabilmektedir [9].

İletişim protokolleri haberleşme sırasında gönderilecek mesajların yapısını belirler. Avrupa'da en geçerli ve yaygın kullanıma sahip iletişim protokolleri IEC (International Electrotechnical Commission) standart organizasyonu tarafından hazırlanan IEC 60870-5 iletişim protokolüdür. Asya ve Kuzey Amerika'da yaygın olarak kullanılan DNP3 (Distributed Network Protocol) protokolü ise IEC 60870-5 protokolünden türetilmiştir ve IEEE 1379 standartı olarak kabul görmüştür. IEC 61850 protokolünün kapsamı, IEC 60870-5 ve DNP3 protokollerinden daha geniştir ve gerçek zamanlı ve P2P (Peer-to-peer) servislerini de içerir. Bu üç protokol TCP/IP altyapısını kullanır [10].

B. SCADA Güvenliği

SCADA iletişim protokollerinin güvenlik kısıtlarını ve ihtiyaçları IEC 62351 standartında tanımlanmaktır. Standart sekiz bölümden oluşur. Üçüncü bölümde IEC 60870 ve 61850'deki TCP/IP profillerinin güvenliğini, TLS (Transport Layer Security) protokolü üzerinden ele alır ve TLS'in hangi konfigürasyonda kullanılması gerektiğini tanımlar. Gerçek zamanlı verilerin uzak uç terminallerinden SCADA'ya iletiminde kullanılan MMS (Manufacturing Message Specification) protokolünün güvenliği dördüncü bölümde incelenmektedir. Beşinci bölümde IEC 60870 ve DNP3'deki seri iletişimlerin gizlilik ve bütünlük servisleri için TLS protokolü önerilmiştir. Alternatif olarak röle gibi kısıtlı yetenekleri olan cihazlarda IPSec protokolünün de filtreleme amaçlı kullanılabileceği belirtilmektedir. Altıncı bölümde ise P2P bağlantıların güvenliği incelenmiş ve SCADA'nın haberleşme hızındaki kısıttan dolayı (mesaj iletimi 4 milisaniye ile sınırlı) genel şifreleme yöntemlerinin uygulanabilir olmadığı ve kimlik doğrulama çözümlerine gidilmesi gerektiği vurgulanmıştır. Yedinci bölüm ağ güvenliğini, sekizinci bölüm ise kontrol merkezlerindeki erişim ve yetki denetimlerini inceler.

SCADA sistemindeki her bileşenin güvenliği için kullanıcı ve cihaz doğrulama, sanal özel ağlar (VPN), IPSec protokolü, güvenlik duvarları ve sızma tespit sistemleri (IDS) gibi farklı teknolojiler kullanılmaktadır.

Bu kadar geniş ve farklı iletişim mevcutken gizlilik,

bütünlük ve erişilebilirlik için ağ güvenliğinin sağlanması kritik bir gerektir.

III. AKILLI ŞEBEKELERDE SİBER GÜVENLİK

Güvenilir bir akıllı şebeke oluşturmak için siber ve fiziksel saldırıların ortaya çıkarabileceği muhtemel etkileri ve şebekenin bu etkilere bağımlılığını iyi analiz etmek gerekmektedir. NIST, [5] akıllı şebekelerle ilişkili muhtemel riskleri aşağıdaki ana başlıklarda ifade etmektedir.

- Karmaşık bir sistem olması nedeniyle potansiyel saldırgan ve kasıtsız hatalara maruz kalma olasılığı fazladır.
- Farklı ölçeklerde ağların birbirlerine bağlanmasıyla oluşan daha büyük ağlardan oluşması nedeniyle (networks of networks) zayıflıkların ve saldırıların yayılması ve artarak genişlemesi söz konusudur.
- Fazla sayıda bağlantı olması nedeniyle, hizmet engelleme (DoS, Denial of Service), sızma, sisteme kötü niyetli kodların sokulması ya da donanımlara saldırı yapılması gibi tehditlerin oluşma olasılığı yüksektir.
- Yoğun veri toplama ve çift yönlü bilgi akışı; veri gizliliği, tüketici bilgilerinin açığa çıkması ve mahremiyetin ihlali gibi potansiyel risklerin artmasına neden olmaktadır.

Literatürde, akıllı şebekelerde siber güvenlikle ilgili şebekenin farklı alanlarına yoğunlaşılmıştır. [10]'da akıllı şebekelerde siber güvenlik; cihaz, ağ, yönetim, anomali tespiti başlıklarında incelenmiştir. Ericsson, [11] daha çok SCADA güvenliği üzerine yoğunlaşmıştır. Yan ve diğerleri, [12] güvenlik gereklerini incelemiş zorlukları ve varolan çözümleri ortaya koymuştur.

Gelenekselden akıllı şebekelere geçiş neticesinde artan iki taraflı iletişim ihtiyacı siber atakları da beraberinde getirmiştir. Güç şebekelerin güvenliğinin sağlanması beklenmedik siber olayların ve doğal afetlerin şebekenin çalışabilirliğini ve verimini etkilenmemesini sağlamayı hedeflemektedir. Akıllı şebekelerde güvenliğin sağlanmasında, şebekelerin kendine has özellikleri nedeniyle bazı zorluklarla karşılaşılmaktadır. Akıllı şebekeler yeni iletişim gereklerine (protocol, geçikme, bant genişliği vb.) sahiptirler. Eski güvenlik çözümlerini, çabuk eskime riskine karşı mümkün olduğu kadar kullanmamak gereklidir. Mevcut güç şebekelerinde yıllardır kullanımda olan birçok eski cihaz bulunmaktadır. Bu eski cihazlar sadece temel bir takım özellikler barındıran, düşük bellek alanı ve işlem kabiliyetine sahip cihazlardır. Bu nedenle modern kripto çözümlerini mevcut cihazlar üzerinde uygulayabilmek zor bir problemdir. Mevcut güç şebekelerindeki ağ yapısı bünyesinde birçok teknolojiyi ve protokolü barındırmaktadır. Ne yazık ki bunların büyük bir çoğunluğu siber güvenlikten yoksun tasarlanmışlardır. Varolan güç sistemleri genellikle kapalı ve özel sistemler kullanmakta olup, güvenlikten ziyade performans ve işlevsellik odaklı çalışmaktadır.

Akıllı şebekelerde kullanılan akıllı sayaçların topladığı veriler tüketiciden tüketiciye değişmekte ve hem tüketici hem de hizmet sağlayıcı için önem arzetmektedir. Sayaç bilgilerinin toplandığı veri tabanlarına yetkisiz erişim sonucu oluşabilecek herhangi bozulma tüketici faturalarına yansıyacaktır. Dolayısıyla veri tabanlarının erişim denetimlerinin yapılması, gizliliğinin korunması ve herhangi bir değişikliğe karşı bütünlüğünün sağlanması gerekmektedir. Bunun yanısıra akıllı sayaçlara yapılacak muhtemel fiziksel saldırıların tespit edilmesi sistemin güvenirliği açısından önemlidir. Gelecekte evlerde kullanılan cihazların AMI şebekesiyle iletişim kurabiliyor olması onları potansiyel saldırı noktaları haline getirecektir.

Akıllı şebekelerde büyük ve küçük ölçekli ağlar bulunmaktadır. Bu da farklı standartlar ve iletişim protokollerinin kullanımı anlamına gelmektedir. Ağ üzerinde bazı uygulamalar internet tabanlı gerçekleştirilebilir dolayısıyla internet ortamının maruz kaldığı tüm risklere maruz kalabilir. TCP/IP altyapısının kullanıldığı yerlerde IPSec, TLS gibi güvenlik protokollerinin benimsenmesi gerekmektedir. Kablosuz ağların tercih edildiği uygulamalarda, ikinci ve üçüncü katman güvenlik protokolleri göz ardı edilmemelidir.

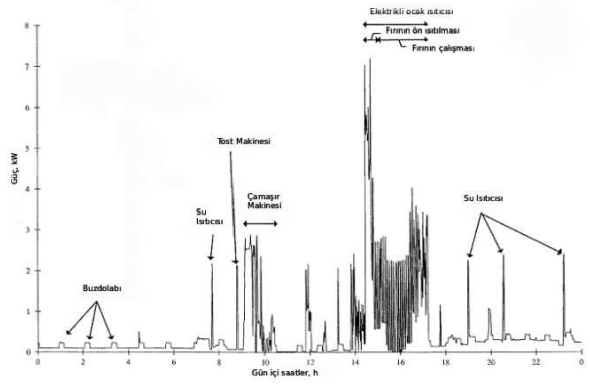
IV. AKILLI ŞEBEKELERDE MAHREMİYET

Mahremiyet kavramı insan hakları içerisinde tanımlanması en zor kavramlardan biridir. Westin'e göre [13] mahremiyet "bireylerin, grupların veya kurumların kendilerine dair bilgilerin ne zaman ve ne ölçüde diğerlerine aktarılabileceğini kendilerinin belirleyebilmesidir". Bilişim dünyasının gelişimi ile bilgilerin paylaşımı kolaylaşmıştır. Dolayısı ile mahremiyet konusu oldukça önem kazanmıştır.

Akıllı şebeke teknolojisi enerji kullanımı, sistemin yük durumu gibi bir çok verinin toplama, depolama, iletişim ve paylaşma ihtiyaçlarını beraberinde getirmektedir. Temel amaç toplanan verilerle gerçek zamanlı analizler yaparak sistemi anlamak, olaylar önlemek ve sorun çözebilmektir. Kullanıcıları ilgilendiren ve onlarla ilişkilendirilebilecek her türlü veri mahremiyet konusuna eğilmeyi gerektirmektedir.

Akıllı şebeke teknolojilerinin yürütülebilirliği için iki yönlü bir iletişim hattından bahsedebiliyor olmak gerekir. Bu iletişim hattı ile akıllı sayaçlar, sensörler, bilgisayar sistemleri ve diğer birçok cihazlardan gelen enerji tüketim verileri toplanır ve bu veriler üzerinden tüketimi optimize etmek ve daha güvenilir bir yapı oluşturmak için hareket planlaması yapılır. Bu iki yönlü iletişim hattından giden verilerin mahremiyeti üzerinde önemle durulması gereken bir husustur. Akıllı şebekelerdeki iletişim hattından tüketici ile ilgili kişisel bilgiler (örn. ad,soyad, adres vb.), aldığı servisler ile ilgili bilgiler (örn. yenilenebilir enerji kaynakları kullanımı, servis sağlayıcı bilgileri, sayaç IP adresi vb.) ve tüketim ile ilgili bilgiler (örn. tüketim analizi ile yaşam stilinin tesbiti, tercih edilen cihazların belirlenmesi vb.) elde edilebilmektedir [5].

Akıllı şebekelerde tüketim analizi sonucu (cihazların elektriksel imzası [5]) tüketimin olduğu yerin mahiyeti ile ilgili bilgi edinilebilirken (örn. hastane, ev vb.), Şekil 2'de de görüldüğü gibi [14], aynı zamanda tüketicinin yaşam tarzı, saat kaçta uyanıp kaçta uyuduğu, ne tür elektrikli cihazlar kullandığı, cihazları kullanım alışkanlığı gibi bilgiler de elde edilebilmektedir. Tüketicinin alışkanlıkları ve yaşam tarzı ile ilgili bilgiler üreticiler için çok kıymetli bir bilgi olacaktır. Zira bu bilgi ile tüketicinin alışkanlıklarına özel kampanyalar ile pazarlama yapabileceklerdir. Bunun yanında cihaz üreticileri kendi cihazlarının tüketim özelliklerini değişik kaynaklardan



Şekil 2. Evlerdeki Kişisel Tüketimlerin Analizi [14].

toplayarak daha güvenilir cihazlar üretmek ve hatta garanti pollitikalarını belirmek için kullanabilmektedirler.

Tüketim analizinden kaynaklı mahremiyet problemini çözmek amacı ile [15]'da güç karıştırma algoritması kullanılarak önceden belirlenmiş bir takım tüketim olaylarını korumayı amaçlamaktadırlar. Bu çalışmada aynı zamanda değişik güç karıştırma algoritmalarının karşılaştırmalarını da bulmak mümkündür. Mahremiyet ile ilgili yapılan bir diğer çalışma ise [16] üretim safhasında akıllı sayaçlara iki adet kimlik numarası verilmesine dayanmaktadır. Verilen kimliklerden biri sadece düşük frekanslı iletişim (örn. haftada ya da ayda bir yapılan faturalama işlemi için) için, diğeri ise daha yüksek frekanslı iletişim (örn. her dakikada bir gönderilen kullanım bilgileri) için kullanılmaktadır. Bu şekilde yüksek frekanslı iletişimler için anonimliği üçüncü şahıslarca sağlanan kimliklerin kullanımı ile tüketim bilgilerinin gerçek zamanlı izlenmesi sonucu oluşabilecek mahremiyet sorunlarının önüne geçilmesi hedeflenmektedir.

Akıllı şebekelerde tüketici mahremiyetini sağlamak amacıyla kullanılabilecek bir diğer yapı ise homomorfik şifrelemedir. Homomorfik şifreleme anlamsal olarak güvenli olan ve basit cebirsel fonksiyonların kapalı metinler üzerinde uygulanmasına olanak sağlayan bir grup şifreleme fonksiyonundan oluşmaktadır. Matematiksel olarak bir homomorfik şifreleme fonksiyonu $E()$ ile x, y şeklinde iki mesaj verildiğinde, mesajların açık halleri bilinmeden $E_k(x * y) = E_{k1}(x) * E_{k2}(y)$ eşitliği hesaplanabilmelidir. Denklemdeki $*$ toplama veya çarpma gibi cebirsel operasyonları temsil etmektedir. Homomorfik şifreleme yoğun olarak mahremiyet korumaya odaklı işlemler için (örn. e-voting) kullanılmaktadır. Homomorfik şifreleme uygulamalarından bazıları ise şöyledir: RSA, ElGamal [17], Paillier [18], Naccache-Stern [19], Boneh-Goh-Nissim [20]. Akıllı sayaçlardan tüketicinin kullanımına yönelik bilgilerin toplanması hususunda homomorfik şifreleme kullanılabilir çözümlerden biri olarak görülmektedir. Zira [21]'de homomorfik şifrelemenin toplama özelliği kullanılarak akıllı sayaçlardan veri toplama işlemi yapılması hedeflenmektedir. Bu makalenin çözüm sunduğu ağ yapısında akıllı sayaçlar bir hiyerarşik ağaç yapısına oturtulmuştur. Ağaç yapısında kök verilerin toplandığı merkezi temsil eder. Her akıllı sayaç doğrudan veri toplama merkezi ile konuşmak yerine ağaç yapısında durduğu yere göre alt düğümlerinden verileri toplayıp bir üst düğümüne iletmektedir. Toplama işleminde Paillier homomorfik şifreleme algoritmasının modifiye edilmiş hali kullanılmaktadır. Bu şekilde tüketici mahremiyeti sağlanmış olmaktadır.

V. SONUÇLAR

Bu çalışmada, son zamanlarda elektrik güç sistemleri için önem arzeden akıllı şebekelerde siber güvenlik ve mahremiyet unsurları incelenmiştir. Akıllı şebekelerin temel bileşenleri arasındaki iletişimlere ve ilgili standartlara değinilmiştir. Literatürden verilen örnekler ile akıllı şebekelerde siber güvenlik ve mahremiyet kavramının hem ekonomik hem de bireysel yönlerinin olduğu görülmektedir. Yeni şekillenen bu teknoloji içerisinde siber güvenlik ve mahremiyet konularının hassasiyet ile incelenmesi büyük önem taşımaktadır.

KAYNAKLAR

[1] B. Parks, "Transforming the grid to revolutionize electric power in North America," in *Edison Electric Institute's Fall 2003 Transmission, Distribution and Metering Conference*, Oct. 2003.
[2] S. Corsi and C. Sabelli, "General blackout in italy sunday september 28, 2003, h. 03:28:00," in *IEEE Power Engineering Society General Meeting*, vol. 2, 2004, pp. 1691-1702.
[3] Y. Ateş, M. Uzunoğlu, and R. Yumurtacı "Dağıtık Üretim tesislerinin şebekeye entegrasyonunda akıllı şebekelerin rolü ve gelecek öngörüleri," in *4. Enerji Verimliliği ve Kalitesi Sempozyumu*, May 2011.
[4] General Electric, "Plug into the Smart Grid, Smart Meters," available at http://ge.ecomagination.com/smartgrid/#/smart_meters.
[5] NIST-IR-7628, "Guidelines for smart grid cyber security," National Institute of Standards and Technology, Tech. Rep., Aug. 2010.
[6] Cisco Systems, Inc., "Internet protocol architecture for the smart grid," White paper, Jul. 2009, available at http://www.cisco.com/web/strategy/doc/energy/ CISCO_IP_INTEROP_-STDS_PPR_TO_-NIST_WP.pdf.
[7] A. Clark and C. J. Pavlovski, "Wireless networks for the smart energy grid: Application aware networks," in *Proc. of the International MultiConference of Engineers and Computer Scientists 2010IMECS2010*, vol. II, Hong Kong, Mar. 2010.
[8] J. Gadze, "Control-aware wireless sensor network platform for the smart electric grid," *International Journal of Computer Science and Network Security*, vol. 9, no. 1, pp. 16-26, 2009.
[9] N. O. Çalışkan, "Elektrik dağıtım sisteminin bilgisayarla programlanması ve otomasyon," Master's thesis, Gazi Üniversitesi, Ankara, 2007.
[10] J. Liu, Y. Xiao, S. Li, W. Liang, and C. L. P. Chen, "Cyber security and privacy issues in smart grids," *IEEE Communication Surveys & Tutorials*, accepted for publication.
[11] G. Ericsson, "Cyber security and power system communication - essential parts of a smart grid infrastructure," *IEEE Transactions on Power Delivery*, vol. 25, no. 3, pp. 1501–1507, July 2010.
[12] Y. Yan, Y. Qian, H. Sharif, and D. Tiiper, "A survey on smart grid communication infrastructures: Motivations, requirements and challenges," *IEEE Communication Surveys & Tutorials*, accepted for publication.
[13] A.F. Westin, "Privacy and Freedom", *Atheneum publishers*, 1967.
[14] M. Newborough and P. Augood, "Demand-side Management Opportunities for the UK Domestic Sector", *IEE Proceedings of Generation Transmission and Distribution*, vol. 146 no. 3 pp. 283-293, 1999.
[15] R. Kalogridis and R. Cepeda, *ElecPrivacy: Evaluating the Privacy Protection of Electricity Management Algorithms. IEEE Transactions on Smart Grid*, 2011.
[16] C. Efthymiou and G. Kalogridis "Smart grid privacy via anonymization of smart metering data," *Smart grid communications (Smartgridcomm) conference*, 2010.
[17] T. E. Gamal, "A public key cryptosystem and signature scheme based on discrete logarithms" in *proceedings of CRYPTO 84 on Advances in cryptology*, Springer-Verlag New York, Inc. 1985, pp.10-18.
[18] P Paillier, "Public-key cryptosystem based on composite degree residuosity classes" in *proceeding to Eurocrypt '99*,'1999.

[19] D. Naccache and J. Stern, "A new public key cryptosystem based on higher residues" in *CCS '98: proceeding s of the 5th ACM conference on Computer and communications security*,1998, pp. 59-66.
[20] D. Boneh, E. Goh and K. Nissim, "Evaluating 2-dnf formulas on ciphertexts" in *Proceedings of Theory of Cryptography (TCC)*,2005, pp. 325-341.
[21] F. Li, B. Luo and P. Liu, "Secure information aggregation for smart grids using homomorphic encryption" in *Proc. 1st IEEE SmartGrid-Comm 2010, Gaithersburg, MD*,Oct. 2010, pp. 327-332.
[22] Y. Yan, Y. Qian, H. Sharif, and D. Tipper, "A survey on cyber security for smart grid communications," *IEEE Communication Surveys & Tutorials*, accepted for publication.
[23] T. Flick and J. Morehouse, *Securing the Smart Grid Next Generation Power Grid Security*. Elsevier Inc., 2011.
[24] NERC, "Reliability assessment 1991–2000," North American Reliability Council, Princeton, New Jersey, Tech. Rep., Sept. 1991.

Elif Üstündağ Soykan 2002 yılında İstanbul Üniversitesi Bilgisayar Mühendisliği Bölümü'nden Lisans derecesini, 2005 yılında İstanbul Teknik Üniversitesi Hesaplamalı Bilim ve Mühendislik Bölümü'nden Yüksek Lisans derecesini almıştır. 2005 yılından bu yana TÜBİTAK BİLGEM UEKAE Kriptoloji Bölümü'nde uzman araştırmacı olarak çalışmaktadır.

Seda Demirağ Ersöz 2005 yılında İstanbul Bilgi Üniversitesi Bilgisayar Bilimleri Bölümü'nden Lisans derecesini, 2010 yılında Boğaziçi Üniversitesi Bilgisayar Mühendisliği'nden Yüksek Lisans derecesini almıştır. 2005 yılından bu yana TÜBİTAK BİLGEM UEKAE Kriptoloji Bölümü'nde uzman araştırmacı olarak çalışmaktadır.

Siber Güvenlik ve Savunma
Cyber Security and Defence

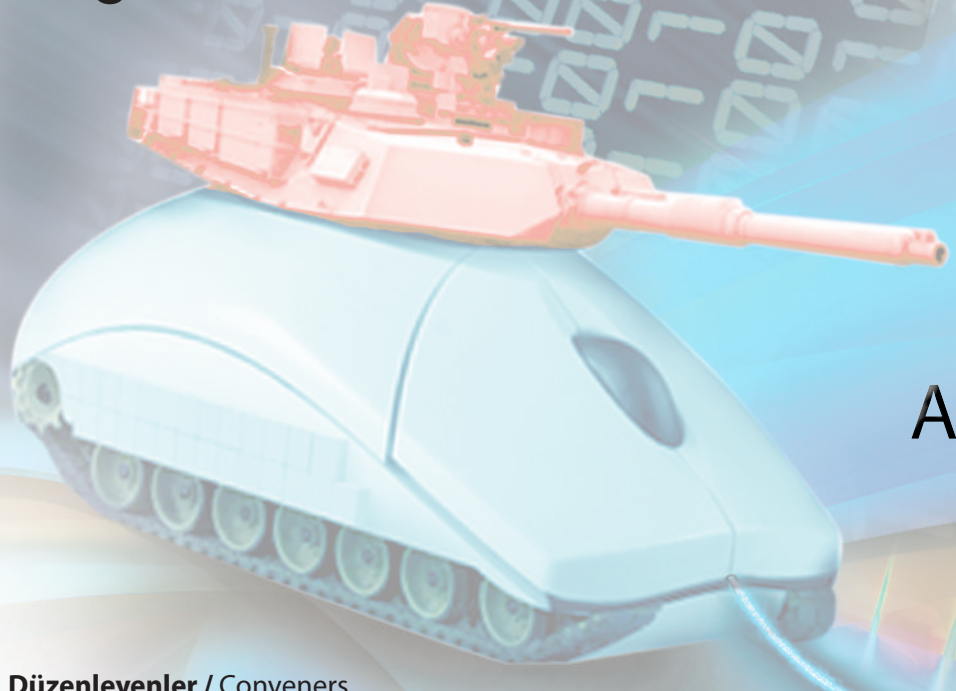
BİLGİ GÜVENLİĞİ VE KRİPTOLOJİ KONFERANSI
ISC Turkey

5. Uluslararası Bilgi Güvenliği ve Kriptoloji Konferansı

5th International Conference on Information Security & Cryptology

17-18 Mayıs May 2012

ODTÜ Kültür ve Kongre Merkezi
METU Culture and Congress Center
Ankara-TURKEY



Author Index

Düzenleyenler / Conveners

T.C. ULAŞTIRMA DENİZCİLİK VE HABERLEŞME BAKANLIĞI

BİLGİ GÜVENLİĞİ DERNEĞİ

Destekleyenler / In Collaboration with

BTK BİLGİ TEKNOLOJİLERİ VE İLETİŞİM KURUMU

YAZAR DİZİN / AUTHOR INDEX

Atilla ÖZGÜR	11
Arzu KAKIŞIM	28
Ahmet EJDER	50
Amir Jalaly BIDGOLY	81
Ahmad Baraani DASTJERDI	81
Alper BİLGE	93
Alhusain M. TAHER	298
Ali ŞENOL	302
Ahmet İlhan AYŞAN	308
Amadou Moctar KANE	141
Ali D. SEZER	138
Adnan BAYSAL	187
Ahmet Bedri ÖZER	224
Atilla HASEKİOĞLU	256-268
Alper ÖZBİLEN	55
Boshra PİSHGOO	23-316
Behrouz Tork LADANI	81-112
Barış B. KIRLAR	132-160
Begüm MUTLU	235
Burcu A. KORKMAZ	256
Celal Z. ÇİL	38
Cihan KALELİ	93
Canan ÖZEL	155
Cüneyt F. BAZLAMAÇCI	262
Çağlar ÜLKÜDERNER	34
Çetin ÜRTİŞ	175
Devrim SERAL	218
Ertuğrul AKBAŞ	325
Erkan BAYAR	331
Elif Üstündağ SOYKAN	343
Esra ŞAHİN	235
Ebubekir KAYA	206
Evrim FURUNCU	285
Feyza YILDIRIM OKAY	100
Fatih BİRİNCİ	106-118
Farhad Soleimanian GHAREHCHOPOGH	321
Ferruh ÖZBUDAK	138-155
Fevzi ÜNLÜ	61-69
Fatih ÖZKAYNAK	224
Ferhat KARAKOÇ	230
Fikret HACIZADE	268
Ghazaleh JAVADZADEH	17

Güray YILMAZ 308
Güzin ULUTAŞ 211
Gulshan KUMAR 291

Hamit ERDEM 11
Hakan ŞENTÜRK 38
Harith A. DAWOOD 294
Hacer KARACAN 302
Hüseyin POLAT 93
Hidayet OGRAS 316
Hakan KAPTAN 331
Hasan ERDOĞAN 195
Hakan TEKEDERE 251

Ibrahim YAKUT 93
İbrahim SOĞUKPINAR 28-285
İsmail KOYUNCU 279
İhsan PEHLİVAN 279
İlhami ÇOLAK 55

Kerim GÖZTEPE 50
Kamil OTAL 175
Kemal BIÇAKCI 75

M. K. ULUKÖK 313
Mustafa B. ABUGHARSA 298
Mohamed A. SULLABİ 298
Murat AKPULAT 75
Mehmet TEKEREK 87
Mehmet Sabır KİRAZ 106-118
Muhammed Ali BİNGOL 19
Mustafa TURK 316
M.Zekeriya GÜNDÜZ 337
Mustafa ULUTAŞ 211
Muhammad ASHRAF 132-160
Mustafa Hakan SOLMAZ 195
Mary AGOYİ 218
Mustafa ALKAN 251
Mustafa ÜNVER 251
Murat KOYUNCU 245
Mustafa TOYRAN
Muhammet Ali CAN 256-268
Mustafa TOYRAN 256-268
Murat AK 273
Mritunjay Kumar RAİ 291

Neda Afzali SERESHT 23-316
Najmeh S. MIRAMIRKHANI 148
Neşe ÖZTOP 179
Nursel AKÇAM 245

Orhun KARA 183-187-230
Onur Koçak 179
Onur Kurt 179
Orkun DİLLİ 245

Pars MUTAF 256
Resul DAŞ 337
Rasool JALILI 148
Reza AZMİ 17-23-316
Rıza AYKAÇ 195
Rahul SAHA 291

Seda Demirağ ERSÖZ 343
Sedat AKLEYLEK 155
Seda KAHRAMAN 169
Süleyman KARDAŞ 106
Somayeh NAGHSHBANDI 112
Dr. Sattar B. SADKHAN 201
Sırma YAVUZ 224
Salih YILDIRIM 262
Suat ÖZDEMİR 3-100

Şeref SAĞIROĞLU 3-38-55
Şahin KARA 337

T. V. PHAM 316
Thomas B. PEDERSEN 256-268
Turgut HANOYMAK 273

Uğur Kaşif BOYACI 118
Uraz YAVANOĞLU 3-235
Uğur ÇİL 75

Üstün YILDIRIM 138

Veysel ASLANTAŞ 206
Vasif V. NABİYEV 211

Yılmaz UYAROĞLU 279

Zülfükar SAYGI 169-175-179
Zeinab Abbasi KHALIFEHLOU 321
Z. B. ŞENSOY 313