ADVANCES IN INTELLIGENT SYSTEMS AND COMPUTING 176

Natarajan Meghanathan
Dhinaharan Nagamalai
Nabendu Chaki (Eds.)

Advances in Computing and Information Technology

Springer

Advances in Intelligent Systems and Computing 176

Editor-in-Chief

Prof. Janusz Kacprzyk
Systems Research Institute
Polish Academy of Sciences
ul. Newelska 6
01-447 Warsaw
Poland
E-mail: kacprzyk@ibspan.waw.pl

For further volumes:
http://www.springer.com/series/11156

Natarajan Meghanathan, Dhinaharan Nagamalai,
and Nabendu Chaki (Eds.)

Advances in Computing and Information Technology

Proceedings of the Second International Conference on Advances in Computing and Information Technology (ACITY) July 13–15, 2012, Chennai, India – Volume 1

Springer

Editors
Dr. Natarajan Meghanathan
Department of Computer Science
Jackson State University
Jackson
USA

Dr. Dhinaharan Nagamalai
Wireilla Net Solutions PTY Ltd
Melbourne
VIC
Australia

Dr. Nabendu Chaki
Department of Computer Science &
Engineering
University of Calcutta
Calcutta
India

ISSN 2194-5357
ISBN 978-3-642-31512-1
DOI 10.1007/978-3-642-31513-8
Springer Heidelberg New York Dordrecht London

e-ISSN 2194-5365
e-ISBN 978-3-642-31513-8

Library of Congress Control Number: 2012940793

Preface

The Second International Conference on Advances in Computing and Information Technology (ACITY-2012) was held in Chennai, India, during July 13–15, 2012. ACITY attracted many local and international delegates, presenting a balanced mixture of intellect from the East and from the West. The goal of this conference series is to bring together researchers and practitioners from academia and industry and share cutting-edge development in the field. The conference will provide an excellent international forum for sharing knowledge and results in theory, methodology and applications of Computer Science and Information Technology. Authors are invited to contribute to the conference by submitting articles that illustrate research results, projects, survey work and industrial experiences describing significant advances in all areas of Computer Science and Information Technology.

The ACITY-2012 Committees rigorously invited submissions for many months from researchers, scientists, engineers, students and practitioners related to the relevant themes and tracks of the conference. This effort guaranteed submissions from an unparalleled number of internationally recognized top-level researchers. All the submissions underwent a strenuous peer-review process which comprised expert reviewers. These reviewers were selected from a talented pool of Technical Committee members and external reviewers on the basis of their expertise. The papers were then reviewed based on their contributions, technical content, originality and clarity. The entire process, which includes the submission, review and acceptance processes, was done electronically. The overall acceptance rate of ACITY-2012 is less than 20%. Extended versions of selected papers from the conference will be invited for publication in several international journals. All these efforts undertaken by the Organizing and Technical Committees led to an exciting, rich and a high quality technical conference program, which featured high-impact presentations for all attendees to enjoy, appreciate and expand their expertise in the latest developments in various research areas of Computer Science and Information Technology. In closing, ACITY-2012 brought together researchers, scientists, engineers, students and practitioners to exchange and share their experiences, new ideas and research results in all aspects of the main workshop themes and tracks, and to discuss the practical challenges encountered and the solutions adopted. We would like to thank the General and Program Chairs, organization staff, the members of the Technical

Program Committees and external reviewers for their excellent and tireless work. We sincerely wish that all attendees benefited scientifically from the conference and wish them every success in their research.

It is the humble wish of the conference organizers that the professional dialogue among the researchers, scientists, engineers, students and educators continues beyond the event and that the friendships and collaborations forged will linger and prosper for many years to come.

Natarajan Meghanathan
Dhinaharan Nagamalai
Nabendu Chaki

Organization

General Chairs

David C. Wyld	Southeastern Louisiana University, USA
E.V. Krishnamurthy	Australian National University, Australia
Jae Kwang Lee	Hannam University, South Korea
Jan Zizka	SoNet/DI, FBE, Mendel University in Brno, Czech Republic
V.L. Narasimhan	Pentagram R&D Intl. Inc., New Bern, USA
Michal Wozniak	Wroclaw University of Technology, Poland

Steering Committee

Abdul Kadhir Ozcan	Karatay University, Turkey
Brajesh Kumar Kaushik	Indian Institute of Technology-Roorkee, India
Dhinaharan Nagamalai	Wireilla Net Solutions PTY LTD, Australia
Eric Renault	Institut Telecom - Telecom SudParis, Evry, France
Jacques Demerjian	Communication & Systems, France
James Henrydoss	AT&T and University of Colorado, USA
Krzysztof Walkowiak	Wroclaw University of Technology,Poland
Murugan D.	Manonmaniam Sundaranar University, India
Nabendu Chaki	University of Calcutta, India
Natarajan Meghanathan	Jackson State University, USA
Raja Kumar M.	Taylor's University, Malaysia
Salah Al-Majeed	University of Essex, UK
Selma Boumerdassi	Conservatoire National des Arts Et Metiers (CNAM), France
Sundarapandian Vaidyanathan	VelTech Dr. RR & Dr. SR Technical University, India

Program Committee Members

A.H.T. Mohammad	University of Bradford, UK
A.P. Sathish Kumar	PSG Institute of Advanced Studies, India
AAA. Atayero	Covenant University, Nigeria
Abdul Aziz	University of Central Punjab, Pakistan
Abdul Kadhir Ozcan	Karatay University, Turkey
Abdul Kadir Ozcan	The American University, Cyprus
Abdulbaset Mohammad	University of Bradford, United Kingdom
Ahmad Saad Al-Mogren	King Saud University, Saudi Arabia
Ahmed M. Khedr	Sharjah University, Sharjah, UAE
Ahmed Nada	Al-Quds University, Palestinian
Ajay K. Sharma	Dr. B R Ambedkar National Institute of Technology, India
Alaa Ismail Elnashar	Taif University, KSA
Alejandro Garces	Jaume I University, Spain
Alejandro Regalado Mendez	Universidad del Mar - México, USA
Alfio Lombardo	University of Catania, Italy
Ali El-Rashedy	University of Bridgeport, CT, USA
Ali M.	University of Bradford, United Kingdom
Ali Maqousi	Petra University, Jordan
Alireza Mahini	Islamic Azad University-Gorgan, Iran
Alvin Lim	Auburn University, USA
Amandeep Singh Thethi	Guru Nanak Dev University Amritsar, India
Amit Choudhary	Maharaja Surajmal Institute,India
Anand Sharma	MITS-Rajasthan, India
Anjan K.	RVCE-Bangalore, India
Ankit Thakkar	Nirma University, India
Ankit	BITS, PILANI India
Anthony Atayero	Covenant University, Nigeria
Aravind P.A.	Amrita School of Engineering India
Arun Pujari	Sambalpur University, India
Arunita Jaekel	University of Windsor, Canada
Ashok Kumar Das	IIT Hyderabad, India
Ashok kumar Sharma	YMCA Institute of Engineering, India
Ashutosh Dubey	NRI Institute of Science & Technology, Bhopal
Ashutosh Gupta	MJP Rohilkhand University, Bareilly
Athanasios Vasilakos	University of Western Macedonia, Greece
Azween Bin Abdullah	Universiti Teknologi Petronas, Malaysia
B. Srinivasan	Monash University, Australia
Babak Khosravifar	Concordia University, Canada
Balakannan S.P.	Chonbuk Nat. Univ., Jeonju
Balasubramanian K.	Lefke European University, Cyprus
Balasubramanian Karuppiah	Dr. MGR University, India
Bari A.	University of Western Ontario, Canada

Beatrice Cynthia Dhinakaran	TCIS, South Korea
Bela Genge	European Commission Joint Research Centre, Belgium
Bharat Bhushan Agarwal	I.F.T.M University, India
Bhupendra Suman	IIT Roorkee , India
Biju Pattnaik	University of Technology, India
Bikash singh	Islamic University-Kushtia, Bangladesh
Binod Kumar Pattanayak	Siksha O Anusandhan University, India
Bobby Barua	Ahsanullah University of Science and Technology, Bangladesh
Bong-Han	Kim, Chongju University, South Korea
Boo-Hyung Lee	KongJu National University, South Korea
Brajesh Kumar Kaushik	Indian Institute of Technology, India
Buket Barkana	University of Bridgeport, USA
Carlos E. Otero	University of South Florida Polytechnic, USA
Charalampos Z. Patrikakis	National Technical University of Athens, Greece
Chin-Chih Chang	Chung Hua University ,Taiwan
Cho Han Jin	Far East University, South Korea
Choudhari	Bhagwati Chaturvedi College of Engineering, India
Christos Politis	Kingston University, UK
Cristina Ribeiro	University of Waterloo, Canada
Cristina Serban	Ovidius University of Constantza, Romania
Danda B. Rawat	Old Dominion University, USA
David C. Wyld	Southeastern Louisiana University, USA
Debasis Giri	Haldia Institute of Technology, India
Debdatta Kandar	Sikkim Manipal University, India
Dhinaharan Nagamalai	Wirella Net Solutions PTY Ltd, Australia
Diego Reforgiato	University of Catania, Italy
Dimitris Kotzinos	Technical Educational Institution of Serres, Greece
Doreswamyh hosahalli	Mangalore University, India
Durga Toshniwal	Indian Institute of Technology, India
E. Martin	University of California, Berkeley, USA
E.V. Krishnamurthy	ANU College of Engg & Computer Science, Austraila
Emmanuel Bouix	iKlax Media, France
Eric Renault	Institut Telecom - Telecom SudParis, Evry, France
Ermatita Zuhairi	Sriwijaya University, Indonesia
Farag M. Sallabi	United Arab Emirates University, UAE
Farshad Safaei	Shahid Beheshti University, Iran
Ford Lumban Gaol	University of Indonesia
Genge Bela	Joint Research Centre, European Commission, Italy
Ghalem Belalem	University of Oran, Algeria
Giovanni Cordeiro Barroso	Universidade Federal do Ceara, Brasil
Giovanni Schembra	University of Catania, Italy
Girija Chetty	University of Canberra, Australia

Gomathi Kandasamy	Avinashilingam Deemed University for Women, India
Gopalakrishnan Kaliaperumal	Anna University, Chennai
Govardhan A.	JNTUH College of Engineering, India
Guo Bin	Institute TELECOM SudParis, France
H.V. Ramakrishnan	Dr. MGR University, India
Haider M. Alsabbagh	Basra University, Iraq
Haller Piroska	Petru Maior University-Tirgu Mures, Romania
Hao Shi	Victoria University, Australia
Hao-En Chueh	yuanpei University, Taiwan
Hari Chavan	National Institute of Technology, Jamshedpur, India
Henrique J.A. Holanda	UERN - Universidade do Estado do Rio Grande do Norte, Brasil
Henrique Joao Lopes Domingos	University of Lisbon, Portugal
Hiroyuki Hisamatsu	Osaka Electro-Communication University, Japan
Ho Dac Tu	Waseda University, Japan
Homam Reda El-Taj	Universiti Sains Malaysia, Malaysia
Hong yu	Capitol College, USA
Huosheng Hu	University of Essex, UK
Hussein Al-Bahadili	Petra University, Jordan
Hussein Ismail Khalaf Al-Bahadili	Petra University, Jordan
Hwangjun Song	Pohang University of Science and Technology,South Korea
Ignacio Gonzalez Alonso	University of Oviedo, Europe
Indrajit Bhattacharya	Kalyani Govt. Engg. College, India
Intisar Al-Mejibli	University of Essex, UK
Ioannis Karamitsos	Itokk Communications, Canada
J.K. Mandal	University of Kalyani, India
Jacques Demerjian	Communications & Systems, France
Jae Kwang Lee	Hannam University, South Korea
Jalel Akaichi	University of Tunis, Tunisia
Jan Zizka	SoNet/DI, FBE, Mendel University in Brno, Czech Republic
Jeong-Hyun Park	Electronics Telecommunication Research Institute, South Korea
Jeyanthy N.	VIT University, India
Jifeng Wang	University of Illinois at Urbana Champaign, USA
Johann Groschdl	University of Bristol, UK
Jose Enrique Armendariz-Inigo	Universidad Publica de Navarra, Spain
Juan Li	North Dakota State University, USA
Jyoti Singhai	Electronics and Communication Deptt-MANIT, India
Jyotirmay Gadewadikar	Alcorn State University, USA
Kai Xu	University of Bradford, United Kingdom
Kamalrulnizam Abu Bakar	Universiti Teknologi Malaysia, Malaysia

Karim Konate	University Cheikh Anta DIOP, Dakar
Kaushik Chakraborty	Jadavpur University, India
Kayhan Erciyes	Izmir University, Turkey
Khaled Shuaib	United Arab Emirates University, UAE
Khamish Malhotra	University of Glamorgan, UK
Khoa N. Le	University of Western Sydney, Australia
Krishnamurthy E.V.	ANU College of Engg & Computer Science, Austraila
Krzysztof Walkowiak	Wroclaw University of Technology, Poland
Kuribayashi	Seikei University, Japan
L. Nirmala Devi	Osmania University - Hyderabad, India
Laiali Almazaydeh	University of Bridgeport, USA
Lu Yan	University of Hertfordshire, UK
Lus Veiga	Technical University of Lisbon, Portugal
Lylia Abrouk	University of Burgundy, France
M. Aqeel Iqbal	FUIEMS, Pakistan
M. Rajarajan	City University, UK
M. Ali	University of Bradford, UK
Maode Ma	Nanyang Technological University, Singapore
Marco Folli	University of Pavia, Italy
Marco Roccetti	Universty of Bologna, Italy
Massimo Esposito	ICAR-CNR, Italy
Md. Sipon Miah	Islamic University-Kushtia, Bangladesh
Michal Wozniak	Wroclaw University of Technology, Poland
Michel Owayjan	American University of Science & Technology, Lebanon
Miguel A. Wister	Juarez Autonomous University of Tabasco, Mexico
Mohamed Hassan	American University of Sharjah, UAE
Mohammad Ali Jabreil Jamali	Islamic Azad University, Iran
Mohammad Hadi Zahedi	Ferdowsi University of Mashhad, Iran
Mohammad Hajjar	Lebanese University, Lebanon
Mohammad Kaghazgaran	Islamic Azad University, Iran
Mohammad Mehdi Farhangia	Universiti Teknologi Malaysia, Malaysian
Mohammad Momani	University of technology Sydney, Australia
Mohammad Talib	University of Botswana, Botswana
Mohammad Zaidul Karim	Daffodil International University, Bangladesh
Mohammed Feham	University of Tlemcen, Algeria
Mohammed M. Alkhawlani	University of Science and Technology, Yemen
Mohsen Sharifi	Iran University of Science and Technology, Iran
Muhammad Sajjadur Rahim	University of Rajshahi, Bangladesh
Murty	Ch A S, JNTU, Hyderabad
Murugan D.	Manonmaniam Sundaranar University, India
Mydhili Nair	M S Ramaiah Institute of Technology, India
N. Krishnan	Manonmaniam Sundaranar University, India
Nabendu Chaki	University of Calcutta, India

Nadine Akkari	King abdulaziz University, Saudi Arabia
Naohiro Ishii	Aichi Institute of Technology, Japan
Nasrollah M. Charkari	Tarbiat Modares University, Iran
Natarajan Meghanathan	Jackson State University, USA
Nicolas Sklavos	Technological Educational Institute of Patras, Greece
Nidaa Abdual Muhsin Abbas	University of Babylon, Iraq
Nour Eldin Elmadany	Arab Acadmy for Science and Technology, Egypt
Ognjen Kuljaca	Alcorn State University, USA
Olakanmi Oladayo	University of Ibadan, Nigeria
Omar Almomani	Universiti Utara Malaysia, Malaysia
Orhan Dagdeviren	Izmir University, Turkey
Osman B. Ghazali	Universiti Utara Malaysia, Malaysia
Othon Marcelo Nunes Batista	Universidade Salvador, Brazil
Padmalochan Bera	Indian Institute of Technology, Kharagpur, India
Partha Pratim Bhattacharya	Mody Institute of Technology & Science, India
Patricia Marcu	Leibniz Supercomputing Centre, Germany
Patrick Seeling	University of Wisconsin - Stevens Point, USA
R. Thandeeswaran	VIT University, India
Phan Cong Vinh	London South Bank University, UK
Pinaki Sarkar	Jadavpur University, India
Polgar Zsolt Alfred	Technical University of Cluj Napoca, Romania
Ponpit Wongthongtham	Curtin University of Technology, Australia
Quan (Alex) Yuan	University of Wisconsin-Stevens Point, USA
Rafael Timoteo	University of Brasilia - UnB, Brazil
Raied Salman	Virginia Commonwealth University, USA
Rajendra Akerkar	Technomathematics Research Foundation, India
Rajeswari Balasubramaniam	Dr. MGR University, India
Rajkumar Kannan	Bishop Heber College, India
Rakhesh Singh Kshetrimayum	Indian Institute of Technology, Guwahati, India
Raman Maini	Punjabi University, India
Ramayah Thurasamy	Universiti Sains Malaysia, Malaysia
Ramayah	Universiti Sains Malaysia, Malaysia
Ramin karimi	University Technology Malaysia
Razvan Deaconescu	University Politehnica of Bucharest, Romania
Reena Dadhich	Govt. Engineering College Ajmer
Reshmi Maulik	University of Calcutta, India
Reza Ebrahimi Atani	University of Guilan, Iran
Rituparna Chaki	West Bengal University of Technology, India
Robert C. Hsu	Chung Hua University, Taiwan
Roberts Masillamani	Hindustan University, India
Rohitha Goonatilake	Texas A&M International University, USA
Rushed Kanawati	LIPN - Universite Paris 13, France
S. Geetha	Anna University - Tiruchirappalli, India
S. Hariharan	B.S. Abdur Rahman University, India

S. Venkatesan	University of Texas at Dallas - Richardson, USA
S.A.V. Satyamurty	Indira Gandhi Centre for Atomic Research, India
S. Arivazhagan	Mepco Schlenk Engineering College, India
S. Li	Swansea University, UK
S. Senthil Kumar	Universiti Sains Malaysia, Malaysia
Sajid Hussain	Acadia University, Canada
Salah M. Saleh Al-Majeed	University of Essex, United Kingdom
Saleena Ameen	B.S.Abdur Rahman University, India
Salem Nasri	ENIM, Monastir University, Tunisia
Salim Lahmiri	University of Qubec at Montreal, Canada
Salini P.	Pondichery Engineering College, India
Salman Abdul Moiz	Centre for Development of Advanced Computing, India
Samarendra Nath Sur	Sikkim Manipal University, India
Sami Ouali	ENSI, Compus of Manouba, Manouba, Tunisia
Samiran Chattopadhyay	Jadavpur University, India
Samodar reddy	India school of mines , India
Samuel Falaki	Federal University of Technology-Akure, Nigeria
Sanjay Singh	Manipal Institute of Technology, India
Sara Najafzadeh	University Technology Malaysia
Sarada Prasad Dakua	IIT-Bombay, India
Sarmistha Neogy	Jadavpur University, India
Satish Mittal	Punjabi University, India
S.C. SHARMA	IIT - Roorkee, India
Seetha Maddala	CBIT, Hyderabad
Selma Boumerdassi	Cnam/Cedric, France
Sergio Ilarri	University of Zaragoza, Spain
Serguei A. Mokhov	Concordia University, Canada
Shaoen Wu	The University of Southern Mississippi, USA
Sharvani G.S.	RV College of Engineering, Inida
Sherif S. Rashad	Morehead State University, USA
Shin-ichi Kuribayashi	Seikei University, Japan
Shivan Haran	Arizona state University, USA
Shobha Shankar	Vidya vardhaka College of Engineering, India
Shrikant K. Bodhe	Bosh Technologies, India
Shriram Vasudevan	VIT University, India
Shrirang Ambaji Kulkarni	National Institute of Engineering, India
Shubhamoy Dey	Indian Institute of Management Indore, India
Solange Rito Lima	University of Minho, Portugal
Souad Zid	National Engineering School of Tunis, Tunisia
Soumyabrata Saha	Guru Tegh Bahadur Institute of Technology, India
Sridharan	CEG Campus - Anna University, India
Sriman Narayana Iyengar	VIT University, India
Srinivasulu Pamidi	V R Siddhartha Engineering College Vijayawada, India

Sriram Maturi	Osmania University, India
Subhabrata Mukherjee	Jadavpur University, India
Subir Sarkar	Jadavpur University, India
Sundarapandian Vaidyanathan	VelTech Dr. RR & Dr. SR Technical University, India
Sunil Singh	Bharati vidyapeeth's College of Engineering, India
Sunilkumar S. Manvi	REVA Institute of Technology and Management Kattigenhalli, India
SunYoung Han	Konkuk University, South Korea
Susana Sargento	University of Aveiro, Portugal
Swarup Mitra	Jadavpur University, Kolkata, India
T. Ambaji Venkat Narayana Rao	Hyderabad Institution of Technology and Management , India
T.G. Basavaraju	National Institute of Technology Karnataka (NITK), India
Thomas Yang	Embry Riddle Aeronautical University, USA
Tri Kurniawan Wijaya	Technische Universitat Dresden, Germany
Tsung Teng Chen	National Taipei Univ., Taiwan
Utpal Biswas	University of Kalyani, India
V.M. Pandharipande	Dr. Babasaheb Ambedkar Marathwada University, India
Valli Kumari Vatsavayi	AU College of Engineering, India
Vijayalakshmi S.	VIT University, India
Virgil Dobrota	Technical University of Cluj-Napoca, Romania
Vishal Sharma	Metanoia Inc., USA
Wei Jie	University of Manchester, UK
Wichian Sittiprapaporn	Mahasarakham University, Thailand
Wided Oueslati	l'institut Superieur de Gestion de Tunis, Tunisia
William R. Simpson	Institute for Defense Analyses, USA
Wojciech Mazurczyk	Warsaw University of Technology, Poland
Xiaohong Yuan	North Carolina A & T State University, USA
Xin Bai	The City University of New York, USA
Yahya Slimani	Faculty of Sciences of Tunis, Tunisia
Yannick Le Moullec	Aalborg University, Denmark
Yaser M. Khamayseh	Jordan University of Science and Technology, Jordan
Yedehalli Kumara Swamy	Dayanand Sagar College of Engineering, India
Yeong Deok Kim	Woosong University, South Korea
Yogeshwar Kosta	Marwadi Education Foundations Group of Institutions, India
Yuh-Shyan Chen	National Taipei University, Taiwan
Yung-Fa Huang	Chaoyang University of Technology, Taiwan
Zaier Aida	National Engeneering School of GABES, Tunisia
Zakaria Moudam	Université sidi mohammed ben Abdellah, Morocco
Zuqing Zhu	Cisco Systems, USA

External Reviewers

A. Kannan	K.L.N. College of Engineering, India
Martin	Sri Manakula Vinayagar Engineering College, India
Abhishek Samanta	Jadavpur University, Kolkata, India
Ayman Khalil	Institute of Electronics and Telecommunications of Rennes, France
Cauvery Giri	RVCE, India
Ch. V. Rama Rao	Gudlavalleru Engineering College, India
Chandra Mohan	Bapatla Engineering College, India
E.P. Ephzibah	VIT University-Vellore, India
Hameem Shanavas	Vivekananda Institute of Technolgy, India
Kota Sunitha	G. Narayanamma Institute of Technology and Science, Hyderabad
Kunjal B. Mankad	ISTAR, Gujarat, India
Lakshmi Rajamani	Osmania University, India
Lavanya	Blekinge Institute of Technology, Sweden
M.P. Singh	National Institute of Technology, Patna
M. Tariq Banday	University of Kashmir, India
M.M.A. Hashem	Khulna University of Engineering and Technology, Bangladesh
Mahalinga V. Mandi	Dr. Ambedkar Institute of Technology, Bangalore, Karnataka, India
Mahesh Goyani	G H Patel College of Engineering and Technology, India
Maragathavalli P.	Pondicherry Engineering College, India
M.P. Singh	National Institute of Technology, Patna
M. Tariq Banday	University of Kashmir, India
M.M.A. Hashem	Khulna University of Engineering and Technology, Bangladesh
Mahalinga V. Mandi	Dr. Ambedkar Institute of Technology, India
Monika Verma	Punjab Technical University, India
Moses Ekpenyong	University of Uyo, Nigeria
Mini Patel	Malwa Institute of Technology, India
N. Kaliammal	NPR College of Engg &Tech, India
N. Adhikari	Biju Pattnaik University of Technology, India
N.K. Choudhari	Bhagwati Chaturvedi College of Engineering, India
Naga Prasad Bandaru	PVP Siddartha Institute of Technology, India
Nagamanjula Prasad	Padmasri Institute of Technology, India
Nagaraj Aitha	I.T, Kamala Institute of Tech & Science, India
Nana Patil	NIT Surat, Gujrat
Nitiket N. Mhala	B.D. College of Engineering - Sewagram, India
P. Ashok Babu	Narsimhareddy Engineering College, India
P. Sheik Abdul Khader	B.S. Abdur Rahman University, India

Pesn Krishna Prasad	Aditya Engineering College, India
Partha Pratim Bhattacharya	Mody Institute of Technology & Science, India
Pappa Rajan	Anna University, India
Pooja Jain	JUIT Waknaghat, India
Prabu Dorairaj	NetApp Inc, India
Pradeepini Gera	Jawaharlal Nehru Technological University, India
Pravin P. Karde	HVPM's College of Engineering & Technology - Amravati, India
Premanand K. Kadbe	Vidya Pratishthan's College of Engineering, India
Priti Sajja	Sardar Patel University, India
R. Baskaran	Anna University - Chennai, India
R. Murali	Dr. Ambedkar Institute of Technology, Bangalore
R.M. Suresh	Mysore University
Rabindranath Bera	Sikkim Manipal Inst. of Technol., India
Rajashree Biradar	Ballari Institute of Technology and Management, India
Rajesh Kumar Krishnan	Bannari Amman Inst. of Technol., India
Rajesh Kumar P.	The Best International, Australia
Rajeshwari Hegde	BMS College of Engineering, India
Rajagopal Palsonkennedy	Dr. MGR University, India
Selvakumar Ramachandran	Blekinge Institute of Technology, Sweden

Contents

Network Security and Applications

Networks and Communications

Wireless and Mobile Networks

Peer-to-Peer Networks and Trust Management

Intelligent Network-Based Intrusion Detection System (iNIDS)

P.R. Mahalingam

Department of Computer Science
Rajagiri School of Engineering & Technology, Rajagiri valley, Cochin, India
prmahalingam@gmail.com

Abstract. Networks are regarded as one of the biggest advancements in the field of computer science. But they enable outsiders to "intrude" into our information. Intrusions can be in the form of simple eavesdropping, or gaining access to the host itself. Here, intruders are identified using two main methods – signature analysis and anomaly analysis. The proposed method is such that the signature analysis is strengthened by anomaly analysis, which in turn uses some level of intelligence based on the traffic parameters, obtained and processed using neural networks. The initial intelligence is obtained using the KDDCUP99 dataset, which trains a neural network. The neural network will take care of further detections, and it strengthens itself during the run itself. The result obtained suggests that even with minimal initial intelligence, iNIDS can reach accuracy levels of over 70%, and by increasing the initial set a little more, it reaches accuracy levels exceeding 80%.

Keywords: Intrusion detection, neural networks, intelligence, anomaly analysis, signature analysis, KDDCUP99, JpCap.

1 Introduction

Advancements and increased usage of computer networks paved way for increase in variety and complexity of security threats. The scenario is getting worse in the sense even single firewall strategies are insufficient to counter security threats[1]. Nowadays people are aware of the risks involved in securing a computer network. So a system which is capable of detecting network security threats is developed [2]. Here, an Network based Intrusion Detection System (NIDS) is proposed that uses real time internet traffic for analysis. Also, the system uses Artificial Intelligence for improving the performance and speed of detection.

Real time packets in the network are captured online i.e. from the internet as and when they reach the interface of the network, using suitable Java[3]-based packages. iNIDS is designed to provide the basic detection techniques so as to secure the systems inside a computer network that are directly or indirectly connected to the Internet.

Network intrusion[4] can be defined as any deliberate attempt to enter or gain unauthorized access to a network and thereby break the security of the network and thus gaining access to confidential information present in the computers inside the

N. Meghanathan et al. (Eds.): Advances in Computing & Inform. Technology, AISC 176, pp. 1–9.
springerlink.com

network. An IDS[4] captures and inspects all traffic, regardless of whether it's permitted or not. Based on the contents of the packet, their flow, length etc, at either the IP or application level, an alert is generated.

An *intrusion signature*[4] can be defined as a special TCP state set such as [SYN|RST] in one packet, special bytes in the IP header, or a special byte stream in the payload of a packet that will provide a pattern which can be used for packet analysis for identifying threats.

The primary goals of the whole proposal can be summarized to the following.

1) Detect Network intrusions[8][9]
2) Use of Artificial Intelligence to improve detection[5][6]
3) Use Network traffic for analysis and detection[5][7].

2 NIDS and ANN

Dr. Dorothy E Denning proposed an Intrusion detection system in 1987 which became a benchmark in the research in this area[2]. Many researches have been conducted based on this paper and currently researchers are more interested in developing intrusion detection systems based on Artificial Neural Networks. Artificial Neural Networks possess features like generalization, flexibility etc. Wang Zhenqi and Wang Xinyu proposed a Netflow[1] based intrusion detection system, which can resist network attacks and intrusions. It was found to be cost effective and does not affect the performance of backbone network.[1][13]

Usually, sampled data from Kddcup99 dataset[14], an attack or intrusion database is the standard for evaluating the security detection mechanisms. This dataset is used for signature analysis, for training neural network for anomaly analysis and for testing the IDS itself. The advantage of using Backpropagation algorithm is that it can train (learn) data at a faster rate and it provides efficient generalization and flexibility when compared to other existing Neural Network technologies[13]. But, the performance of a Neural Network depends mainly on the amount of training data given[15][16][17].

The strategy[18] dictates that NIDS uses a hybrid detection engine i.e. a combination of Signature detection and Anomaly detection capabilities. "Rule –based" detection technique is used for signature analysis and "Pattern matching" is used for anomaly analysis.

3 Signature Analysis and Anomaly Analysis

Firewalls cannot or do not analyze packets once they are inside the network and it only analyze them while it enters the network.[19] So, if some anomalies or activities happen from inside the network, then firewalls won't respond to those activities. But, NIDS analyze network packets internally as well as while it enters or leaves the network. With the explosive growth of networking and data sharing, NIDS have become the most popular form of Intrusion Detection[19]. A NIDS is capable of detecting network security threats. Many different NIDSs have been developed and each of them has its own advantages and disadvantages.

Signature Analysis: An NIDS use signature based detection, based on known traffic data to analyze network traffic. This type of detection is very fast, and easy to configure[20]. However, an attacker can slightly modify an attack to render it undetectable by a signature based IDS. Still, signature-based detection, although limited in its detection capability, can be very accurate. A common strategy for IDS in detecting intrusions is to memorize signatures of known attacks. These signatures are written based on data collected from known and previous attacks, and this unfortunately ensures that these signatures "will always be a step behind the latest underground exploits" [20][21].

Anomaly Analysis: Anomaly analysis[17][21] is an efficient way to detect intrusions and thus forms a vital part of the next generation Intrusion Detection Systems. The most efficient Anomaly analysis technique is the pattern based anomaly detection. In pattern based anomaly analysis, the Intrusion Detection System is given a pre-defined set of intrusion patterns. Network packets are collected for a specified period of time or till a specified number of packets. These packets are considered as a block for analysis. The predefined patterns are then matched with this packet block and if any patterns match, an alert is given. During anomaly analysis, a normal behavior model is used as the base for analyzing incoming traffic and any deviation or variation from the normal behavior model is considered as an intrusion or threat[22]. But this can produce a rather high degree of false alarms.

The following attacks are stressed upon in iNIDS.

- Denial of Service[23] - UDP Flooding[24], TCP SYN Attack[26], Smurf attacks[28]
- User to Root (U2R)[29] - Type signatures
- Remote to Local (R2L)[8]
- Probing Attack[30] - Portsweep, Satan, Nmap, etc.

Each possesses its own signature, and attack characteristics, which make it easier to detect and handle. They can sometimes be identified directly from the signature, or by using the anomaly detection methods.

4 KDDCUP99 Dataset

The "KDD CUP'99" dataset [14], which derived from the DARPA dataset, was used for the KDD (Knowledge Discovery and Data Mining Tools Conference) Cup 99 Competition. The complete dataset has around 5 million input patterns and each record represents a TCP/IP connection that is composed of 41 features. The dataset used in this study is a smaller subset (10% of the original training set), it has 494 021 instances (patterns) and it was employed as the training set in the original competition. Each record of the KDD Cup 99 dataset captures various features of the connections, as for example, the source and destination bytes of a TCP connection, the number of failed login attempts or the duration of a connection. Complex relationships exist between the features, which are difficult for human experts to discover.

An NIDS must therefore reduce the amount of data to be processed so as to maintain an accurate and real-time detection. Some input data may not be useful to the Network based IDS and thus can be eliminated before processing. In complex classification systems, the features may contain false correlations, which block the process of detecting intrusions/attacks. Furthermore, some features may be redundant since the information they add is contained in other features.[14][31]

KDD Cup 99 dataset feature selection[32] consists of detecting the relevant features and discarding the irrelevant features. Relevant features are features that can be used for analysis with ease and that can deliver relevant information as well as can work without any performance degradation.

KDDCUP99 attributes[33] can be categorized into four. They are: *Intrinsic Attributes*, *Content Attributes*, *Traffic Attributes*, and *Class Attributes*.

5 JPCAP

Jpcap(Java Packet Capturer)[34] is a Java library for sniffing, capturing and sending network packets, from an available network interface. It also facilitates visualization, creation and analysis of network packets by appropriate coding in Java. The Java language gives it the capability to work in multiple platforms (Operating systems). Jpcap has been tested on Microsoft Windows (98/2000/XP/Vista), Linux (Fedora, Mandriva, Ubuntu), Mac OS X (Darwin), FreeBSD, and Solaris and was found to be working successfully. Jpcap can capture Ethernet, IPv4, IPv6, ARP/RARP, TCP, UDP, and ICMPv4 packets[34]. It is open source, and is licensed under GNU LGPL.

6 Artificial Neural Networks

Artificial Neural Networks, also known as “Artificial Neural Nets”, “neural nets”, or ANN for short, is a computational tool modeled based on the interconnection of the biological neurons in the nervous systems of the human body. ANN can be trained / taught to solve certain type of problems using a training method and data to train. [35] By following this method, Artificial Neural Networks made can be used to perform different tasks depending on the amount training given. A properly trained ANN is capable of generalization, the ability to recognize similarities among many different number and type of input patterns, especially patterns that have been corrupted by noise which has a wide variety of applications.

Artificial Neural Networks have a number of features and characteristics that make them an attractive alternative to traditional problem-solving techniques. We can design a complex network of neurons using multiple layers[35][36], the first of which was called the *Multi-layered Perceptron*. There are a variety of thresholds[37] available for ANN, an example of which is the *sigmoid*.

No matter what organization is used, the ANN has to be trained (or it learns)[38]. It can be *supervised* or *unsupervised*. Here, Backpropagation is preferred due to its speed, which is essential in networked environments. It works on a supervised training model. So, the initial training data, extracted fron KDDCUP99 dataset is important.

7 Implementation

During development, an existing packet capture program based of JpCap was used. The anomaly analysis module was added on top of that by analyzing the parameters of the packets on the fly, and reporting any threats before the attacker has a chance to enter.

The overall system looks like below.

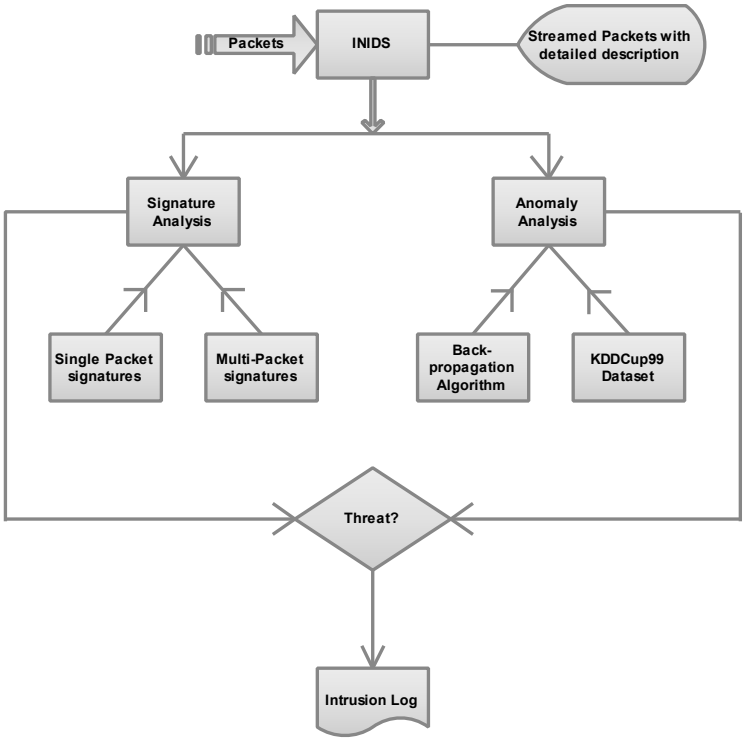


Fig. 1. Implementation

When newer threats are identified by the neural network, it implicitly trains itself to identify that pattern, and it is in turn added to the library. So, further analysis will check for this pattern also. Also, since we use neural networks, it doesn't need an exact match. Any similar pattern of that genre can be caught. So, iNIDS improves on the go, by learning newer ways in which attackers can threaten the integrity and security of the data.

8 Results

The performance was as expected during the design phase. The initial training data was taken such that there was only one sample for each type of intrusion expected.

So, the initial performance was very bad, at about 10%. But eventually, it improved by adding more patterns to the arsenal, and finally, it was able to reach accuracy of more than 70%, in just 21 runs.

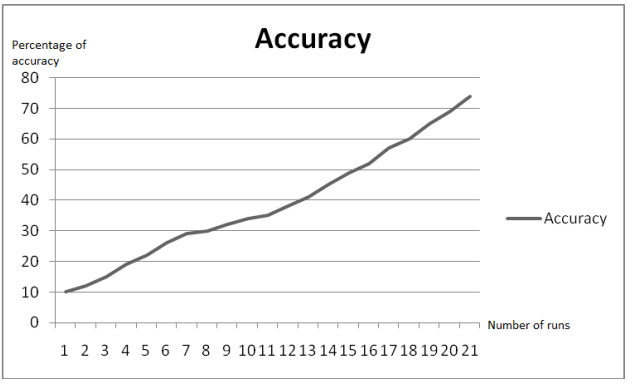


Fig. 2. Accuracy plot with smaller training data, over 21 runs

On a later run, the initial training data itself was improved, with multiple patterns per type of attack. In this case, the initial performance itself went up to 40%, and later, it improved to more than 85% in the same number of runs.

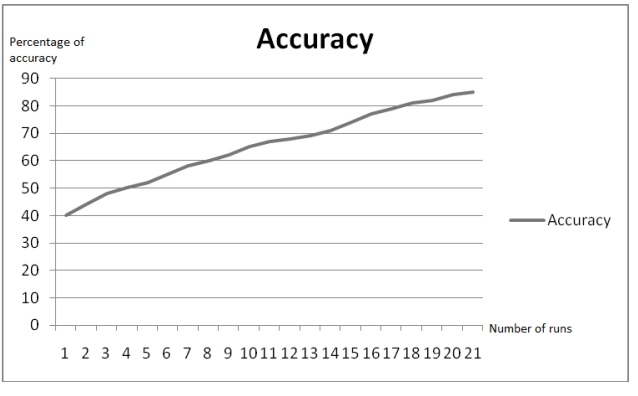


Fig. 3. Accuracy plot with more comprehensive training data, over 21 runs

9 Conclusion

iNIDS initially kicked off as an abstract deign that can improve the current packet capture and analysis routines in intrusion detection, by adding a level of knowledge and intelligence to the analysis. In this case, the threat detection is reinforced by past knowledge of similar attacks, and we are able to achieve levels of accuracy much higher than conventional systems that use the same level of knowledge.

10 Future Work

Even though the research proposes a new technique, it can't be claimed as the best possible technique. The field of network security is subject to continuous research in search for new and better techniques that can ensure better security capabilities. Applying Artificial Intelligence to an NIDS gives it the capability to detect unknown threats which is an important characteristic.

The intelligence thus given to the NIDS can be improved by the use of a better Neural Network architecture as well as a much better training algorithm than Backpropagation which is used in this implementation. A better Neural Network architecture will give better input processing capabilities such as improved speed, pattern matching etc. This will thus enable the ANN to detect patterns much more efficiently with very little data. Better training algorithms can provide reduced training time thereby allowing more training data to be used in very limited time. This will thus improve the training speed and also the training data thereby resulting in an improved performance. So a thorough research is recommended in the field of NIDSs based on Artificial Intelligence.

References

[1] Wang, Z., Wang, X.: NetFlow Based Intrusion Detection System. In: International Conference on MultiMedia and Information Technology, MMIT 2008, December 30-31, pp. 825–828 (2008)

[2] Denning, D.E.: An Intrusion-Detection Model. IEEE Transactions on Software Engineering SE-13(2), 222–232 (1987)

[3] The JavaTM Tutorials, `http://download.oracle.com/javase/tutorial/` (accessed August 20, 2011)

[4] Garuba, M., Liu, C., Fraites, D.: Intrusion Techniques: Comparative Study of Network Intrusion Detection Systems. In: Fifth International Conference on Information Technology: New Generations, ITNG 2008, April 7-9, pp. 592–598 (2008)

[5] Shun, J., Malki, H.A.: Network Intrusion Detection System Using Neural Networks. In: Fourth International Conference on Natural Computation, ICNC 2008, October 18-20, vol. 5, pp. 242–246 (2008)

[6] Wang, Y., Huang, G.X., Peng, D.G.: Model of Network Intrusion Detection System based on BP Algorithm. In: 2006 1st IEEE Conference on Industrial Electronics and Applications, May 24-26, pp. 1–4 (2006)

[7] Liu, B., Lin, C., Ruan, D., Peng, X.: Netfiow Based Flow Analysis and Monitor. In: International Conference on Communication Technology, ICCT 2006, November 27-30, pp. 1–4 (2006)

[8] Ahmad, I., Abdullah, A.B., Alghamdi, A.S.: Remote to Local attack detection using supervised neural network. In: 2010 International Conference for Internet Technology and Secured Transactions (ICITST), November 8-11, pp. 1–6 (2010)

[9] Stolfo, S.J., Fan, W., Lee, W., Prodromidis, A., Chan, P.K.: Cost-based modeling for fraud and intrusion detection: results from the JAM project. In: Proceedings of DARPA Information Survivability Conference and Exposition, DISCEX 2000, vol. 2, pp. 130–144 (2000)

[10] Zihao, S., Hui, W.: Network Data Packet Capture and Protocol Analysis on Jpcap-Based. In: 2009 International Conference on Information Management, Innovation Management and Industrial Engineering, December 26-27, vol. 3, pp. 329–332 (2009)
[11] Al-Shaer, E.: Managing firewall and network-edge security policies. In: IEEE/IFIP Network Operations and Management Symposium, NOMS 2004, April 23-23, vol. 1, p. 926 (2004)
[12] Yang, Y., Mi, J.: Design and implementation of distributed intrusion detection system based on honeypot. In: 2010 2nd International Conference on Computer Engineering and Technology (ICCET), April 16-18, vol. 6, pp. V6-260–V6-263 (2010)
[13] Ahmad, I., Ansari, M.A., Mohsin, S.: Performance Comparison between Backpropagation Algorithms Applied to Intrusion Detection in Computer Network Systems. In: 9th WSEAS International Conference on Neural Networks, May 2-4, pp. 47–52 (2008)
[14] KDD Cup 1999 Data (1999), http://kdd.ics.uci.edu/databases/kddcup99/kddcup99.html (accessed August 13, 2011)
[15] Lee, S.M., Kim, D.S., Park, J.S.: A Hybrid Approach for Real-Time Network Intrusion Detection Systems. In: 2007 International Conference on Computational Intelligence and Security, December 15-19, pp. 712–715 (2007)
[16] Abdel-Azim, M., Abdel-Fatah, A.I., Awad, M.: Performance analysis of artificial neural network intrusion detection systems. In: International Conference on Electrical and Electronics Engineering, ELECO 2009, November 5-8, pp. II-385–II-389 (2009)
[17] Yu, X.: A new model of intelligent hybrid network intrusion detection system. In: 2010 International Conference on Bioinformatics and Biomedical Technology (ICBBT), April 16-18, pp. 386–389 (2010)
[18] Successful software development - Google Books, http://books.google.co.uk/books?id=lrix5MNRiu4C&pg=PA184&dq=software+development+life+cycle+preliminary+design+detailed+design&hl=en&ei=0h1SToP2GdKwhAf9rNHaBg&sa=X&oi=book_result&ct=result&resnum=1&ved=0CDAQ6AEwAA#v=onepage&q=software%20development%20life%20cycle%20preliminary%20design%20detailed%20design&f=false (accessed August 22, 2011)
[19] Network-Based IDS (NIDS) overview | IDStutorial, http://idstutorial.com/network-based-ids.php (accessed August 13, 2011)
[20] Wu, T.M.: Intrusion Detection Systems, September 25 (2009), http://iac.dtic.mil/iatac/download/intrusion_detection.pdf (accessed August 12, 2011)
[21] SANS institute, Host- vs. Network-Based Intrusion Detection Systems (2005), http://www.giac.org, http://www.giac.org/paper/gsec/1377/host-vs-network-based-intrusion-detection-systems/102574 (accessed August 12, 2011)
[22] Zhang, W., Yang, Q., Geng, Y.: A Survey of Anomaly Detection Methods in Networks. In: International Symposium on Computer Network and Multimedia Technology, CNMT 2009, January 18-20, pp. 1–3 (2009)
[23] Gill, K., Yang, S.-H.: A scheme for preventing denial of service attacks on wireless sensor networks. In: 35th Annual Conference of IEEE Industrial Electronics, IECON 2009, November 3-5, pp. 2603–2609 (2009)

[24] Chang, R.K.C.: Defending against flooding-based distributed denialof-service attacks: a tutorial. IEEE Communications Magazine 40(10), 42–51 (2002)
[25] IntelliGuard I.T. - Eliminate DDoS and Flash crowd problems, http://www.intelliguardit.net/library_attackscenarios.html (accessed August 19, 2011)
[26] Wang, H., Zhang, D., Shin, K.G.: Detecting SYN flooding attacks. In: Proceedings of the Twenty-First Annual Joint Conference of the IEEE Computer and Communications Societies, p.1530 (June 2002)
[27] ASA/PIX 7.x and Later: Mitigating the Network Attacks - Cisco Systems, http://www.cisco.com/en/US/products/ps6120/products_tech_note09186a00809763ea.shtml (accessed August 19, 2011)
[28] Mirkovic, J., Reiher, P.: A taxonomy of DDoS attack and DDoS defense mechanisms. ACM SIGCOMM Computer Communication Review, 39–53 (2004)
[29] Ahmad, I., Abdullah, A.B., Alghamdi, A.S.: Applying neural network to U2R attacks. In: 2010 IEEE Symposium on Industrial Electronics & Applications (ISIEA), October 3-5, pp. 295–299 (2010)
[30] Ahmad, I., Abdullah, A.B., Alghamdi, A.S.: Application of artificial neural network in detection of probing attacks. In: IEEE Symposium on Industrial Electronics & Applications, ISIEA 2009, October 4-6, vol. 2, pp. 557–562 (2009)
[31] MIT Lincoln Laboratory: Communication Systems and Cyber Security: Cyber Systems and Technology: DARPA Intrusion Detection Evaluation, http://www.ll.mit.edu/mission/communications/ist/corpora/ideval/data/index.html (accessed August 14, 2011)
[32] Bolon-Canedo, V., Sanchez-Maroo, N., Alonso-Betanzos, A.: A combination of discretization and filter methods for improving classification performance in KDD Cup 99 dataset. In: International Joint Conference on Neural Networks, IJCNN 2009, June 14-19, pp. 359–366 (2009)
[33] Index of /acwaldap/gureKddcup, http://www.sc.ehu.es/acwaldap/gureKddcup/README.pdf (accessed August 14, 2011)
[34] Jpcap - a Java library for capturing and sending network packets, http://netresearch.ics.uci.edu/kfujii/Jpcap/doc/index.html (accessed August 14, 2011)
[35] Artificial Neural Networks/Neural Network Basics - Wikibooks, open books for an open world, http://en.wikibooks.org/wiki/Artificial_Neural_Networks/Neural_Network_Basics (accessed August 14, 2011)
[36] Advances in Data Analytical Techniques, http://www.iasri.res.in/ebook/EBADAT/5-Modeling%20and%20Forecasting%20Techniques%20in%20Agriculture/5-ANN_GKJHA_2007.pdf (accessed August 14, 2011)
[37] Neural Networks: Tutorials: Paras Chopra, http://paraschopra.com/tutorials/nn/index.php (accessed August 14, 2011)
[38] Basic Concepts for Neural Networks, http://www.cheshireeng.com/Neuralyst/nnbg.html (accessed August 14, 2011)

Mutual Authentication for Wireless Communication Using Elliptic Curve Digital Signature Based on Pre-known Password

Tumpa Roy[1], Poonam Sisodia[1], Divye Upadhyay[1], and Kamlesh Dutta[2]

[1] GLNA Institute of Technology, Mathure- 281406
tumpa.nit@gmail.com,
poonamsisodi22@gmail.com,
divs08divyaa@gmail.com
[2] National Institute Of Technology Hamirpur
Hamirpur, Himachal Pradesh-177005
India
kdnith@gmail.com

Abstract. The appearance of public access wireless networks enables ever-present Internet services, whereas it inducing more challenges of security due to open air mediums. As one of the most widely used security mechanisms, authentication is provide for secure communications by preventing unauthorized usage and negotiating credentials for verification. In the intervening time, it generates heavy overhead and delay to communications, further deteriorating overall system performance. First, a system model based on challenge/response authentication mechanism by using the elliptic curve cryptographic digital signature is introduced, which is wide applied in wireless environment to reduce the computational cost, communication bandwidth and the server overload . Then, the concept of security levels is proposed to describe the protection of communications with regard to the nature of security.

Keywords: Elliptic curve cryptography (ECC), security, wireless communication, Public key cryptography (PKC), Authentication, verification.

1 Introduction

You Wireless communications is advancing rapidly in recent years. After 2G (e.g. GSM) widely deployed in the world, 3G mobile communication systems are spreading step by step in many areas. At present, some countries have already launched investigations beyond 3G (B3G) and 4G. Along with the wireless communications' rapid development, the secure access authentication of the users within wireless networks is becoming very critical, and so, more and more attention is focused on it. As the wireless industry explodes, it faces a growing need for security. Applications in sectors of the economy such as healthcare, financial services, and government depend on the underlying security already available in the wired computing environment. Both for secure (authenticated, private) Web transactions and for secure (signed, encrypted) messaging, a full and efficient public key

N. Meghanathan et al. (Eds.): Advances in Computing & Inform. Technology, AISC 176, pp. 11–22.
springerlink.com

infrastructure is needed. Three basic choices for public key systems are available for these applications:

- RSA
- Diffie-Hellman (DH) or Digital Signature Algorithm (DSA) modulo a prime p
- Elliptic Curve Diffie-Hellman (ECDH) or Elliptic Curve Digital Signature Algorithm (ECDSA).

RSA is a system that was published in 1978 by Rivest, Shamir, and Adleman, based on the difficulty of factoring large integers. Whitfield Diffie and Martin Hellman proposed the public key system now called Diffie-Hellman Key Exchange in 1976. DH is key agreement and DSA is signature, and they are not directly interchangeable, although they can be combined to do authenticate key agreement. Both the key exchange and digital signature algorithm are based on the difficulty of solving the discrete logarithm problem [15] in the multiplicative group of integers modulo a prime p. Elliptic curve groups were proposed in 1985 as a substitute for the multiplicative groups modulo p in either the DH or DSA protocols. For the same level of security per best currently known attacks, elliptic curve based systems [7,10] can be implemented with much smaller parameters, leading to significant performance advantages. Such performance improvements are particularly important in the wireless arena where computing power, memory, and battery life of devices are more constrained. In this article we will highlight the performance advantages of elliptic curve systems [8] by comparing their performance with RSA in the context of protocols from different standards.

Authentication is the act of establishing or confirming something as authentic, that is, that claims made by or about the subject are true. There are several methods concerning strong authentication. The main difference consists whether secret-key or public-key cryptography is used. In secret-key cryptography the signer and the verifier must share a secret where the problem of the key exchange must be solved. The main difference consists whether secret-key or public-key cryptography is used. In secret-key cryptography the signer and the verifier must share a secret where a public key is distributed for signature verification. The method using public-key cryptography is known as a digital signature. The protocols used for authentication consists of zero-knowledge protocols and challenge-response protocols. The Diffie-Hellman protocol [9] is used in wireless communication.

Deffie-hellman algorithm has five parts:

1. Global Public Elements
2. User A Key Generation
3. User B Key Generation
4. Generation of Secret Key by User A
5. Generation of Secret Key by User B

Global Public Elements:

q is a Prime number
$\alpha, \alpha < q$ and α is a primitive root of q

The global public elements are also sometimes called the domain parameters.

User A Key Generation:

Select private X_A, where $X_A < q$
Calculate public Y_A ,where $Y_A = \alpha .X_A \bmod q$

User B Key Generation:

Select private X_B, where $X_B < q$
Calculate public Y_B, where $Y_B = \alpha. X_B \bmod q$

Generation of Secret Key by User A:

$K = (Y_B).X_A \bmod q$

Generation of Secret Key by User B:

$K = (Y_A).X_B \bmod q$

If user A and user B are genuine then they can communicate to each other. The ECC version of algorithm is used in wireless communication for authentication proof.

2 Preliminaries

2.1 Elliptic Curve Cryptography

Elliptic curves [11] take the general form of the equation:

$$Y_2 + axy + by = x_3 + cx_2 + dx + e$$

where a, b, c, d and e are real numbers satisfy some conditions which depends on the field it belongs to, such as real number or finite field. Finite field may be F(p) or $F(2^m)$

The F(p) Field:

The elements of Fp [13] should be represented by the set of integers: {0, 1,. . . p − 1} With addition and multiplication defined as follows:

Addition: If a, b ∈ F(p), then a + b = r where r is the remainder of the division of a + b by p and 0< r < p-1. This operation is called addition modulo p.

Multiplication: if a, b ∈ F(p), then a . b = s where s is the remainder of the division of a . b by p and 0< s < p-1. This operation is called multiplication modulo p.

The $F(2^m)$ Field:

The elements of $F(2^m)$ should be represented by the set of binary polynomials of degree m – 1 or less: $a = \alpha_{m-1}x^{m-1} + \ldots + \alpha_1 x + \alpha_0$ with addition and multiplication defined as follows:

Addition: $a + b = c = \{_{cm-1},..c_1,c_0\}$ where $c_i = (a_i + b_i) \bmod 2$. $c \in F(2^m)$.

Multiplication: a . b = c = $\{c_{m-1},..c_1,c_0\}$ where c is the remainder of the division of the polynomial a(x) . b(x) by an irreducible polynomial of degree m. $c \in F(2^m)$.

There is a point 0 called the point at infinity or the zero point [12]. The basic operation of elliptic curve is addition. The addition of two distinct points on elliptic curve can be illustrated by the following figure [3] (figure 1):

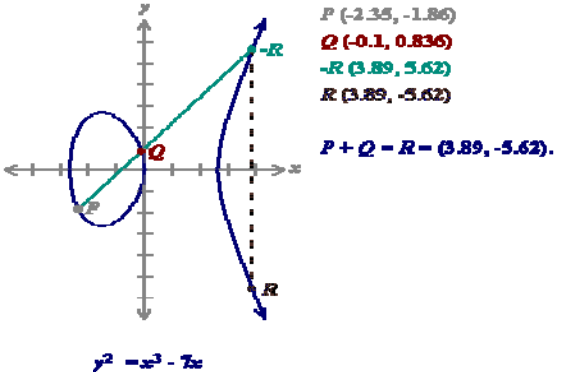


Fig. 1.

Elliptic Curve over F(p):
Let F(p) be a finite field, p > 3, and let a, b ∈ F(p) are constant such that

$$4a^3 + 27b_2 \equiv 0 \pmod{p}.$$

An elliptic curve, E(a,b)(F(p)), is defined as the set of points (x,y) ∈ F(p) * F(p) which satisfy the equation

$$y^2 \equiv x^3 + ax + b \pmod{p}$$

together with a special point, O, called the point at infinity.

Elliptic Curve over F(2m) for some m ≥ 1. :
Elliptic curve E(a,b)(F(2m)) [14] is defined to be the set of points (x,y) ∈ F(2m) * F(2m) which satisfy the equation

$$y^2 + xy = x^3 + ax^2 + b;$$

where a, b ∈ $F(2^m)$ and b≠0, together with the point on the curve at infinity, O.The points on an elliptic curve form an abelian group under a well defined group operation. The identity of the group operation is the point O.

P and Q be two points on E(a,b)(F(p)) or F(2m) and O is the point at infinity.

P+O = O+P = P
If $P = (x_1,y_1)$ then $-P = (x_1, -y_1)$ and P + (-P) = O.
If $P = (x_1,y_1)$ and $Q = (x_2,y_2)$, and P and Q are not O.
Then $P + Q = (x_3, y_3)$ where
$x_3 = \lambda_2 - x_1 - x_2$,
$y_3 = \lambda(x_1 - x_3) - y_1$ and
$\lambda = (y_2-y_1)/(x_2-x_1)$ if $P \neq Q$; $\lambda = (3x_1^2+a)/ 2y_1$ if P = Q

2.2 Elliptic Curve Digital Signature Algorithm

The private key in DSA is a number X. It is known only to the signer. The public key in DSA consists of four numbers:

P = a prime number, between 512 and 1024 bits long
Q = a 160-bit prime factor of P-1.
G = h(P - 1)/Q, where H< P -1 and G mod Q> 1.
Y = G X mod P, which is a 160-bit number.

A signature on a document's hash value H consists of two numbers R and S:

R = (G K mod P) mod Q, where K is a randomly-chosen number <Q.
S = (K -1 (H + XR)) mod Q

To verify the signature, a recipient must compute a value V from the known information:

W = S -1 mod Q
U1 = HW mod Q
U2 = RW mod Q
V = ((G U1 Y U2) mod P) mod Q

If V = R, then document was signed by the person with the public key (P, Q, G, Y). The security of DSA is based on the computational infeasibility of finding a solution for the equation S = (K -1 (H + XR)) mod Q, when X is not known.

3 Proposed Protocol

Choosing a finite field Fq. An elliptic curve E defined over Fq with large group order and a point P of large order n is selected and made public, where n is a prime number. Zn is a class of modulo n, where n is the order of p over E(Fq). Given r,t $\in$ Zn , where r+t = o mod n, r is called the additive inverse of t and denoted as r =-t mod n. the server and client share a secret password S and a secret key K. the server and client individually compute two integers t and r. t is derived from Sand (n-1) in any predetermined way and it yields a unique value. The whole protocol divided into two phases:

Key establishment phase,
Verification phase.

3.1 Key Establishment Phase

The steps of the key establishment phase are explain bellow:

e.1 the client choose a random integer r_c which is belongs in between 1 to n-1 ie. $r_c \in (1, n-1)$. And compute $Q_c =(r_c+t)P$. the client send Q_c to the server.

e.2 The server then select a random integer r_s which is belongs in between 1 to n-1 ie. $r_s \in (1, n-1)$. And compute $Q_s =(r_c+t)P$. the server send Q_s to the client.

e.3 client compute $X=Q_s+rP$

$=(r_s+t)P+rP$
$= r_sP+tP+(-t)P$
$=r_sP$

And compute the session key $K_c=r_cX=r_cr_sP$

e.4. Server compute $Y=Q_c+rP$
$=(r_c+t)P+rP$
$= r_cP+tP+(-t)P$
$=r_cP$

And compute the session key $K_s=r_sY=r_cr_sP$

The session key computed by the server and client individually are same ie. Kc=Ks.

The figure 2 show the key establishment procedure between the client and server.

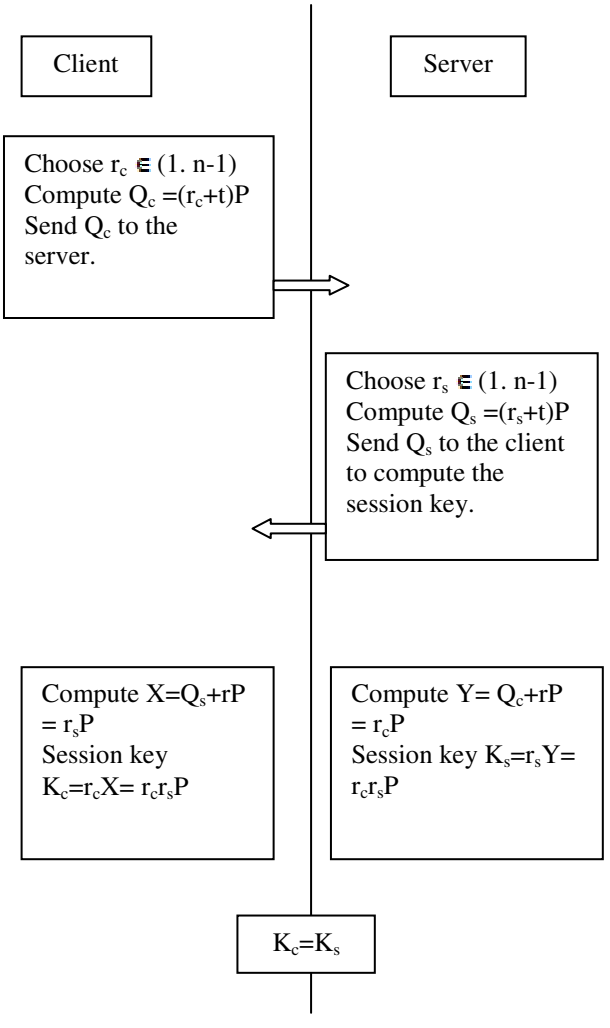


Fig. 2. Key Establishment Phase

3.2 Verification Phase

v.1 The client compute $K*K_c=K*r_c*r_s*P$ where K is the secret key which is known by the server and client. Client send the $K*K_c$ to the server to proof its validation.

v.2 server checks whether $K*K_c=K*K_s$ hold or not. if it dose server believes that it and the client have obtain the same session key i.e $K_c=K_s$ and the client is not duplicate because it knows the secret key which is only known by the server and the clinent. Since the server knows r_s , it believes it has obtain the accurate Q_C. Since client knows r_c , server believes client obtain the correct Q_c ie server condensed that the K_s is valid and the server compute $K*Q_c$ and send it to the client.

v.3 client checks $K*Q_c$. If $K*Q_c$ is correct, client believes that B has obtain the correct Q_c . since only server knows the the secret key K which is shared between the server and client and t is known by the server. So the server is not duplicate. The server knows the t beside client. Client believes that it has obtain the correct Qs and they have obtain the same session key $K_c=K_s$. Client convinced that the K_c is valid.

After the verification procedure has been completed by both sides, the client and the server are now ready to use the session key.

The figure 2 show the Verification procedure between the client and server.

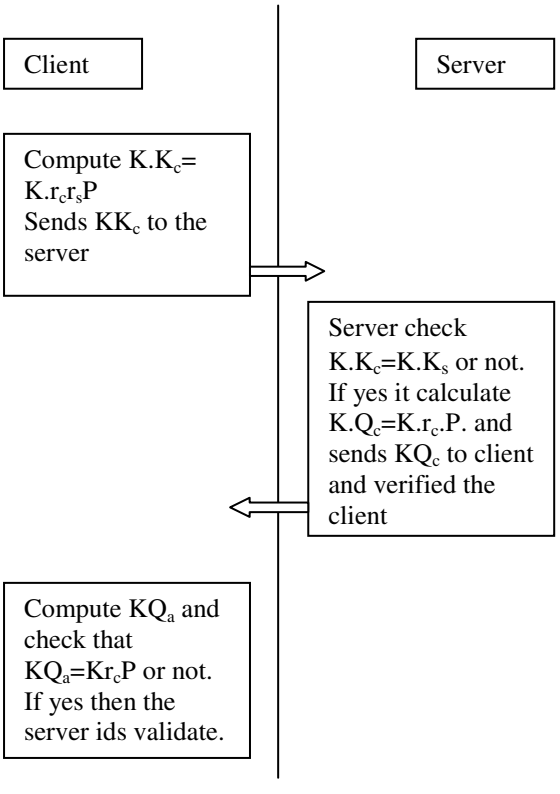


Fig. 3. Validation Phase

4 Analysis of the Proposed Protocol

4.1 Security Analysis

In this section, we scrutinize our proposed key agreement protocol in detail so as to ensure that our protocol is able to achieve the desired security attributes of a key agreement protocol and also able to resist against the known cryptographic attacks.

Known session key security (KSK-S). As shown in our protocol description, the session key is derived from the ephemeral keys (r_c, r_s) of the specific session and the long term keys (S,K) of the protocol entities. This would result in distinct independent session key in each protocol execution. On top of that, a one-way collision-resistant cryptographic function is used to derive the session key. Thus, obtaining any other session keys would not benefit the adversary in mounting a successful attack against a protocol run without the information set (r_c ,r_s),(t,r) which is required in the computation of the shared secret K. Therefore, we claim that the knowledge of some previous session keys would not allow the adversary to gain any advantage in deriving any future and other previous session keys.

Weak Perfect Forward secrecy (wPFS). Suppose that both client and server's long term secret key and password S and K have been exposed. However, the adversary, with the eavesdropped information of any particular session, would not be able to recover the respective established session key since the adversary does not know the involved ephemeral private key r_c or r_s which are needed in the computation of the shared secret K_c and K_s . And also, the intractability of ECCDHP has significantly thwarted the adversary's attempt in computing K_c and K_s by using S and K . Hence, we claim that our enhanced protocol enjoys weak perfect forward secrecy.

Key-Compromise Impersonation Resilience (KCI-R). Suppose that client's and server's long term private key S, K has been compromised and instead of directly impersonating client, the adversary now wishes to impersonate server in order to establish a session with client. However, the adversary is unable to compute the shared secret K_c with the available information (S, r_s, K) since the required information set is (r_c,S, K). Hence, the adversary is significantly prevented from launching a successful KCI attack against our protocol. Generally, the same situation will result when the long term key S is compromised (the adversary would impersonate client in this case and her effort will be foiled in computing K_c as our key agreement protocol is symmetric. As a result, we claim that this protocol is able to withstand the KCI attack under all circumstances.

Key Replicating Resilience (KR-R). The key replicating attack was first introduced by Krawczyk [1] where the illustration of it involves oracle queries described in Bellare and Rogaway's random oracle model [2,3]. This attack, if successfully carried out by the adversary, would force the establishment of a session, K (other than the Test session or its matching session) to agree on a same session key as the Test session, by means of intercepting and altering the message from both communicating parties during transmission. Since the Test session and K are non-matching, the adversary may issue a Reveal query to the oracle associated with K and she can then distinguish whether the Test session key is real or random. Notice that the message

integrity of Qc and Qs has been guaranteed by having each party to calculate K_c and K_s which will be bound to X and Y respectively. Since the adversary has no idea in forging X or Y along with Q_c or Q_b she would not be able to force the establishment of non matching sessions to possess a common session key. As a result, if the adversary reveals client's session key, she would not be able to guess server's session key correctly with non-negligible probability and vice versa. Therefore, we claim that our protocol is secure against the key replicating attack.

Replay Resilience (R-R). In any protocol run, an adversary may attempt to deceive a legitimate participant through retransmitting the eavesdropped information of the impersonated entity from a previous protocol execution. Although the adversary might be unable to compute the session key at the end of the protocol run, her attack is still considered successful if she manage to trick the protocol entity to complete a session with her, believing that the adversary is indeed the impersonated party. In this replay analysis, we reasonably assume that the prime order n of point P is arbitrarily large such that the probability of a protocol entity selecting the same ephemeral key (r_c , r_s ∈ [1, n − 1]) in two different sessions is negligible. Consider a situation where the adversary (masquerading as A) replays A's first message from a previous protocol run between client and server. After server has sent her a fresh (Q_s, Y) in the second message flow, the adversary would abort since she could not produce (by means of forging or replaying) X corresponding to Q_s . Notice that the same replay prevention works in the reverse situation where server's message is replayed. The adversary would fail eventually in generating Y corresponding to the fresh Q_c. Hence, we claim that message replay in our protocol execution can always be detected by both client and server.

Identity authentication. On the one hand, assuming Eve can impersonate B. When Eve receives Q_c, E →A: Q_e= (r_e + t)P. But Eve does not know t and re, and she cannot make the validation message KrcrsP, thus the key validation fails. On the other hand, with (v.2) and (v.3), A and B believe that only knowing t can generate the valid validation messages.

Man-in-the-middle attacks. In the original Diffie-Hellman protocol, Eve can alter the public values such as g_a mod n or g_b mod n with her own values. Thus Eve can share session keys with client or server. In our protocol, when Eve receives Qc= (r_c+ t)P, she cannot guess rc and t. If she still tries to eavesdrop, she mus t generate $r_eP = (r^{c'} + t)P$ and send it to server; server will obtain a wrong value rc'rsP, which is impossible for Eve to know. Thus Eve cannot share a session key with server or client. Based on ECDH algorithm [4], our protocol with pre-shared password is proposed. It makes use of the difficulty of computing discrete logarithms over elliptic curves. It provides identity authentication, key validation and perfect forward secrecy, and it can foil man-in-the-middle attacks.

4.2 Performance Analysis

Efficiency Analysis

Atay et. al. have conducted detailed studies on Computational Cost Analysis of Elliptic Curve Arithmetic [5]. They have reported the point addition arithmetic is applied on two and three dimensional coordinate systems. The computational cost of

each arithmetic operation should be taken into consideration in order to compare the efficiency of algorithms in different coordinate systems. The efficiency is measured as the computational cost, which is in terms of elapsed time. The measured units in Fig. 4 [10] are as follows:

1. Inversion (I) is the multiplicative inverse in modular arithmetic. It has the highest computational cost and one inversion is approximately equals nineteen times of the cost of multiplication cost and denoted as 1I =19M .
2. Multiplication (M) has a lower cost than inversion; therefore all inversions should be converted either to multiplication or to addition.
3. Addition (A) and subtraction (S) have the lowest cost, therefore omitted.

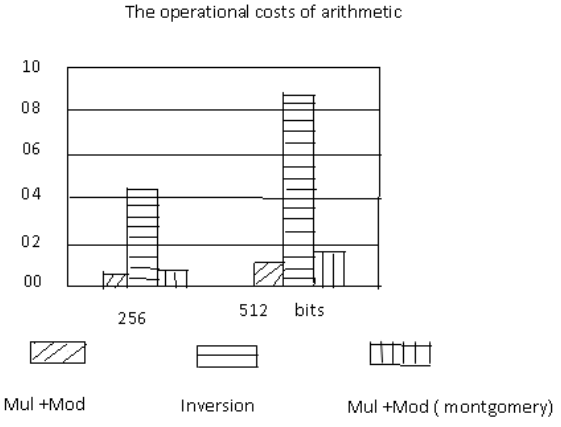


Fig. 4. The operational cost of Arithmetic operation

Computational Cost Analysis
The major advantage of ECC over RSA is ECC needs less computation than RSA but still can achieve the same or even higher level of security. Table 1[6] gives cost-equivalent key sizes. It gives the size, in bits, for equivalent keys. The time to break is computed assuming a machine can break a 56-bit DES key in 100 seconds, and then scaling accordingly.

Table 1.

ECC key	RAS key	Time to break	Machines	Memory
112	430	<5 minutes	105	`Trivial
106	760	600 months	4300	4Gb
192	1020	3 million years	114	170 Gb
256	1620	10^16 years	16	120Gb

5 Conclusion

Attack that monitor side-channel information, Key Replicating Resilience (KR-R).the key replicating attack was first introduced by Krawczyk have recently been receiving much attention in wireless communication. The result presented in this paper conform that the key replacing attack quite powerful and need to be addressed. Any addition to memory or processing capacity increases the cost of each card. ECC needs less computation power, thus it is more suitable than RSA. We have described an authentication and key agreement protocol for wireless communication based on elliptic curve cryptographic techniques. The proposed protocol is a public key type with the feature of signature generation procedure. The new protocols are based on previous classic authentication protocols, including the protection of integrity and session key exchange. This can be used to provide the integrity of the data being transferred during the authentication process in order to prevent from active attacks. The smaller key sizes result in smaller system parameters, smaller public key signatures, bandwidth savings, faster implementations, and smaller hardware processors.

References

1. Krawczyk, H.: HMQV: A High-Performance Secure Diffie-Hellman Protocol. In: Shoup, V. (ed.) CRYPTO 2005. LNCS, vol. 3621, pp. 546–566. Springer, Heidelberg (2005)
2. Bellare, M., Rogaway, P.: Provably Secure Session Key Distribution: The Three Party Case. In: 27th ACM Symposium on the Theory of Computing - ACM STOC, pp. 57–66 (1995)
3. Blake-Wilson, S., Johnson, D., Menezes, A.: Key Agreement Protocols and their Security Analysis. In: Darnell, M.J. (ed.) Cryptography and Coding 1997. LNCS, vol. 1355, pp. 30–45. Springer, Heidelberg (1997)
4. Miller, V.S.: Use of Elliptic Curves in Cryptography. In: Williams, H.C. (ed.) CRYPTO 1985. LNCS, vol. 218, pp. 417–426. Springer, Heidelberg (1986)
5. Atay, S., Koltuksuz, A., Hışıl, H., Eren, S.: Computational Cost Analysis of Elliptic Curve Aurithmetic. In: International Conference on Brid Information Technology, ICHIT 2006, vol. 1, pp. 578–582 (2006)
6. Chatterjee, K., Gupta, D.: Secure access of smart cards using Elliptic curves Cryptography. In: 5th International Conferences on Wireless Communications, Networking and Mobile Computing, WiCom 2009, pp. 1–4 (2004)
7. Blake, I.F., Seroussi, G., Smart, N.P.: Elliptic Curves in Cryptography. London Math. Soc. Lecture Note Series, vol. 265. Cambridge Univ. Press (2000)
8. Aydos, M., Sunar, B., Koç, Ç.K.: An Elliptic Curve Cryptography Based Authentication and Key Agreement Protocol for Wireless Communication. In: 2nd Int. Workshop Discrete Algorithms and Methods for Mobility, DIALM 1998, Dallas, TX (1998)
9. Diffie, W., Hellman, M.: New Directions in Cryptography. IEEE Transactions on Information Theory 22(6), 644–654 (1976)
10. Strangio, M.A.: Efficient Diffie-Hellmann Two-Party Key Agreement Protocols based on Elliptic Curves. In: Proceedings of the 2005 ACM Symposium on Applied Computing, pp. 324–331 (2005)

11. Miller, V.S.: Use of Elliptic Curves in Cryptography. In: Williams, H.C. (ed.) CRYPTO 1985. LNCS, vol. 218, pp. 417–426. Springer, Heidelberg (1986)
12. Blake, I.F., Seroussi, G., Smart, N.P.: Elliptic curves in cryptography. Cambridge University Press, New York (1999)
13. Chen, L., Yanpu, C., Zhengzhong, B.: An implementation of fast algorithm for Elliptic Curve Cryptosystem over GF(p). Journal of Electronics 21(4), 346–352 (2004)
14. Morales-Sandoval, M., Feregrino-Uribe, C., Cumplido, R., Algredo-Badillo, I.: An area/performance trade-off analysis of a GF(2m) multiplier architecture for Elliptic Curve Cryptography. Computers and Engineering 35, 54–58 (2009)
15. Smart, N.P.: The discrete logarithm problem on elliptic curves of trace one. Journal of Cryptology 12(3), 193–196 (1999)
16. Lin, X., Wong, J.W., Kou, W.: Performance analysis of secure web server based on SSL, pp. 249–261. Springer, Heidelberg (2000)

Securing Multi-agent Systems: A Survey

S.V. Nagaraj

Dept. of Computer Science
RMK Engineering College
RSM Nagar, Kavaraipettai 601206, India
http://www.rmkec.ac.in

Abstract. We look at various security aspects of multi-agent systems that are often overlooked by developers designing such systems. We look at some of the key security challenges in multi-agent systems. We focus on techniques that help to ensure that security of multi-agent systems is not compromised.

Keywords: Security, Multi-agent systems, Design, Implementation, Applications.

1 Introduction

A multi-agent system is a system made up of multiple interacting agents that are intelligent (see [33], [69]). Agent technologies have rapidly moved from the research laboratory to industrial application over the last few years [62]. Mobile agents are agents with the ability to migrate from one host to another where they can resume their execution. Security issues pertaining to mobile agents have been studied in [9], [21], [25], [32], [36], [37], [41], [45], [46], [64], [71]. Many of these issues also apply to multi-agents systems. The development of secure protocols for mobile agent computation against static, semi-honest or malicious adversaries without relying on any third party or trusting any specific participant in the system is quite challenging. There are few results in this direction [71]. Security issues related to the protection of host resources as well as the agents themselves form a major obstacle in the application of the agent paradigm [36]. It is important to protect servers from malicious agents and likewise agent data from tampering by malicious servers. Multi-agent systems are quite different from systems that make use of stand alone agents. There seems to be a lack of trust in multi-agent systems that are being developed or that have been already deployed mainly due to the security issues involving them not being addressed properly. Hence, it becomes necessary to establish the confidence of users in multi-agent systems. We look at those aspects pertaining to the security of multi-agent systems that are often overlooked by developers of such systems.

N. Meghanathan et al. (Eds.): Advances in Computing & Inform. Technology, AISC 176, pp. 23–30.
springerlink.com

2 Security Aspects often Overlooked When Designing Multi-agent Systems

Numerous multi-agent based systems are being developed with practical applications such as the multi-agent based marketplace [34]. However, in such systems often the developers tend to overlook important security features. This only leads to loss of confidence in such systems. Standard mechanisms for specifying security in multi-agent systems must be developed [52]. It is often said that agent-oriented software engineering methodologies have not integrated security concerns throughout their development phase (see [48]).

The integration of security concerns during the whole range of the development stages will be beneficial for the development of more secure multi-agent systems [49]. However, such an integration is no easy task (see [48]). Methodologies such as secure Tropos have been proposed for this integration to take place (see [48]). Here too modeling can play a vital role. It is often stated that security requirements of any system (and multi-agent systems in particular) must also be addressed in the early stages of system development. They must also be addressed throughout the development of the system [35]. Analysis of the security requirements of multi-agent systems is often neglected (see [10], [11]). The usual approach towards the inclusion of security within a system is to identify security requirements after the definition of the system. This has aggravated the growth of computer systems impaired with security vulnerabilities. An analysis of the security requirements helps in identifying security bottlenecks.

In many real-life applications such as a multi-agent based e-learning environment [68] and health-care applications such as the one discussed in [4] security is paramount. Agents themselves need to be protected from each other as well from the systems in which they will be deployed. Agents must be protected from the vulnerabilities of the systems in which they will be deployed. It is important to secure agents and systems from malicious agents. Sandboxing is a technique often used in providing a secure execution environment for agents. However, sandboxing has certain limitations too. Often, encryption is not employed for securing agent communication. Models for secure communication between agents have been studied in [15], [50]. Such models can provide guarantees for code, data and execution integrity, data privacy and prevention from malicious routing. Models for agent coordination, authentication and authorization have been studied by [13]. Privacy and integrity of information is not often provided when it is needed.

It is very important to protect agents from the misbehavior of other agents. Such unacceptable behaviors may include denial-of-service by malicious agents as well as spying by such agents. Many systems that are otherwise good do not have the provision for strong authentication and authorization mechanisms [66]. This greatly affects their usability. Very often in multi-agent systems simple access control models are employed. Such models may be unsatisfactory.

The issue of trust amongst agents is often not clearly established in many multi-agent systems (see [53]). It is necessary to establish clearly which agents can be trusted and which agents cannot be trusted. Very often in multi-agent systems there is a strong reliance on the security mechanisms of the underlying operating system. Often multi-agent systems seem to rely heavily on the security policies of the underlying operating system: for example, for file access control. If the security provided by the underlying operating system is weak then the multi-agent system also provides weak security.

In some situations, the confidentiality of communication between agents may need to be ensured by employing encryption. However, this is often not done. Some multi-agent systems may require non-repudiation to be in built. However, the designers may not be offering non-repudiation. Digital signatures need to be employed in e-commerce multi-agent system applications. Secure transport should be ensured by using appropriate protocols. X.509 certificates need to be used for security purposes. A secure execution environment for agents needs to be established. Fault tolerance mechanisms should be included in safety-critical applications. In some applications, there may be a need for public key infrastructures. This is especially true in case of e-commerce applications. Role-based access control mechanisms can be set up so that access is controlled to the extent it is required. Privilege management is an often overlooked aspect in many software applications and this also applies to those involving multi-agent systems. The principle of least privilege is often not used by developers in order to ensure better security. Protocols that are often employed to provide security include IPSec, SSL, and TLS.

It is expected that unauthorized access to information must be prevented. Unauthorized alteration of data should also be prevented. In some multi-agent based systems, man-in-the-middle attacks should be overcome. The use of cryptography should be considered in multi-agent systems when confidentially becomes critical. Some multi-agent systems may require single sign-on since users may not prefer to login too many times. Single sign-on in case of Web services based applications is not easy to achieve in terms of implementation as there are many complexities involved. Traditionally, security is provided by making use of firewalls, proxies, intrusion detection systems, and intrusion prevention systems. In e-health applications such as those discussed in [4] and [70], the confidentiality of health records must be maintained.

In many applications it is necessary to maintain the confidentiality of agent interactions [6]. Delegation is frequently not done in a proper fashion. Insecure delegation leads to security breaches. Accountability should be ensured within multi-agent systems. Modal logic has been employed in [40] for characterizing the relationship among trust, information acquisition and trust in multi-agent systems. Public key infrastructure (PKI) may be used as in [31] for access control and delegation purposes. Identity certificates may be used as explained in [31] for authentication of agents whereas authorization certificates may be used for authorization of agents. PKI may also be useful for authentication purposes (see [23]).

Table 1. Security aspects often overlooked when designing multi-agent systems

No.	Aspect
1	Authentication
2	Authorization
3	Confidentiality
4	Non-repudiation
5	Agent Integrity
6	Message Integrity
7	Host Integrity
8	Message Privacy
9	Trust
10	Availability
11	Delegation
12	Integration of security concerns during the development phase
13	Analysis of security requirements
14	Protection from the vulnerabilities of the underlying system
15	Secure execution environment for agents
16	Spying by malicious agents
17	Fault tolerance
18	Least privilege
19	Reliance on the security mechanisms of the underlying operating system

3 Challenges in Multi-agent Systems

Malicious hosts pose a major problem for agents (refer [8], [28], [29], [45]). Many experts believe that this problem has no easy solution. A malicious host can observe code, data, and control flow. Malicious hosts may also manipulate code, data and control flow. They may also alter the routes of agents. Malicious hosts can cause incorrect execution of code and sometimes re-execution of code. Such hosts may also deny execution by agents. This may be in entirety or perhaps partially. Malicious hosts may also pretend as if they are some other hosts. Communication between agents may also be observed by malicious hosts. Communication between agents is also vulnerable to manipulation by malicious hosts.

There are many threats in multi-agent systems. Some of the common threats include: man-in-the-middle attacks, modification of data, replay attacks, breaking crypto-systems by deriving private key data from public key data, and denial of service attacks. So it becomes important to develop countermeasures to deal with such threats (refer [14], [16]). Attack trees may be used for identifying possible attacks. Ensuring privacy in multi-agent applications handling sensitive personal data is a key challenge [22].

4 Conclusion

We have seen various security aspects of multi-agent systems that are often overlooked by developers. It is important to ensure the security of multi-agent

systems. Often the success or failure of multi-agent systems depends on the robustness of the security provided by them.

Acknowledgment. The author is thankful to his institution for encouragement.

References

1. Special issue on multi-agent and distributed information security. IET Information Security 4(4), 185–421 (December 2010) ISSN 1751-8709
2. Beautement, P., Allsopp, D.N., Greaves, M., Goldsmith, S., Spires, S.V., Thompson, S.G., Janicke, H.: Autonomous Agents and Multi –agent Systems (AAMAS) for the Military - Issues and Challenges. In: Thompson, S.G., Ghanea-Hercock, R. (eds.) DAMAS 2005. LNCS (LNAI), vol. 3890, pp. 1–13. Springer, Heidelberg (2006)
3. Becerra, G.: A security pattern for multi-agent systems. In: Proc. of ATS 2003, pp. 142–153 (2003)
4. Bergenti, F., Poggi, A.: Multi-agent systems for e-health: recent projects and initiatives. In: 10th Int. Workshop on Objects and Agents (2009)
5. Bibu, G.D.: Security in the context of multi-agent systems (Extended Abstract). In: Yolum, Tumer, Stone, Sonenberg (eds.) Proc. of 10th Int. Conf. on Autonomous Agents and Multiagent Systems, AAMAS 2011, Taipei, Taiwan, May 26, pp. 1339–1340 (2011)
6. Biskup, J., Kern-Isberner, G., Thimm, M.: Towards Enforcement of Confidentiality in Agent Interactions. In: Proceedings of the Twelfth International Workshop on Non-Monotonic Reasoning (2008)
7. Boella, G., van der Torre, L.W.N.: Permission and Authorization in Policies for Virtual Communities of Agents. In: Moro, G., Bergamaschi, S., Aberer, K. (eds.) AP2PC 2004. LNCS (LNAI), vol. 3601, pp. 86–97. Springer, Heidelberg (2005)
8. Borelius, N.: Multi-agent system security for mobile communication, PhD Thesis, Royal Holloway, University of London (2003)
9. Borelius, N.: Mobile agent security. IET Electronics and Communication Engineering Journal 14(5), 211–218 (2002)
10. Bresciani, P., Giorgini, P., Mouratidis, H.: On security requirements analysis for multi-agent systems. In: Second Int. Workshop on Software Engineering for Large-Scale Multi-Agent Systems, SELMAS, Portland, Oregon (2003)
11. Bresciani, P., Giorgini, P., Mouratidis, H., Manson, G.: Multi-agent Systems and Security Requirements Analysis. In: Lucena, C., Garcia, A., Romanovsky, A., Castro, J., Alencar, P.S.C. (eds.) SELMAS 2003. LNCS, vol. 2940, pp. 35–48. Springer, Heidelberg (2004)
12. Chi Wong, H., Sycara, K.: Adding security and trust to multi-agent systems. Applied Artificial Intelligence 14(9), 927–941 (2000)
13. Cremonini, M., Omicini, A., Zambonelli, F.: Multi-Agent Systems on the Internet: Extending the Scope of Coordination towards Security and Topology. In: Garijo, F.J., Boman, M. (eds.) MAAMAW 1999. LNCS, vol. 1647, pp. 77–88. Springer, Heidelberg (1999)
14. Endusuleit, R., Calmet, J.: A security analysis on JADE(-S) V. 3.2. In: Proceedings of NORDSEC, pp. 20–28 (2005)
15. Endusuleit, R., Mie, T.: Secure multi-agent computations. In: Proc. of Int. Conf. on Security and Management, vol. 1, pp. 149–155 (2003)

16. Endusuleit, R., Wagner, A.: Possible Attacks on and Countermeasures for Secure Multi-Agent Computation. In: Proceedings of the International Conference on Security and Management, SAM 2004, pp. 221–227, Las Vegas, Nevada, USA. CSREA Press (2004) ISBN 1-932415-37-8
17. Fasli, M.: On agent technology for e-commerce: trust, security, and legal issues. Knowl. Eng. Rev. 22, 3–35 (2007)
18. Fatih, T.: Developing a security mechanism for software agents, M.Sc Thesis, Izmir Institute of Technology (2006)
19. Ferber, J., Gutknecht, O.: A meta-model for the analysis and design of organizations in multi-agent systems. In: Proc. International Conference on Multi Agent Systems, pp. 128–135 (1998)
20. Ferber, J., Gutknecht, O., Michel, F.: From Agents to Organizations: An Organizational View of Multi-agent Systems. In: Giorgini, P., Müller, J.P., Odell, J.J. (eds.) AOSE 2003. LNCS, vol. 2935, pp. 214–230. Springer, Heidelberg (2004)
21. Fernandes, D.L., Saboia, V.F.S., De Castro, M.F., De Souza, J.N.: A secure mobile agents platform based on a peer-to-peer infrastructure. In: Int. Conf. on Networking, Systems and Mobile Communications and Learning Technologies, pp. 186–189 (2006)
22. Foner, L.N.: A security architecture for multi-agent matchmaking. In: Proc. of Second International Conference on Multi-Agent System, Mario Tokoro (1996)
23. Fugkeaw, S., Manpanpanich, P., Juntapremjitt, S.: Multiapplication authentication based on multi-agent system. IAENG Int. J. Comput. Sci. 33(2), 37–42 (2007)
24. Fugkeaw, S., Manpanpanich, P., Juntapremjitt, S.: Achieving DRBAC Authorization in Multi-trust Domains with MAS Architecture and PMI. In: Ghose, A., Governatori, G., Sadananda, R. (eds.) PRIMA 2007. LNCS, vol. 5044, pp. 339–348. Springer, Heidelberg (2009)
25. Garrigues, C., Robles, S., Borrell, J., Navarro-Arribas, G.: Promoting the development of secure mobile agent applications. J. Syst. Softw. 83(6), 959–971 (2010)
26. Gerhard, W. (ed.): Multiagent Systems, A Modern Approach to Distributed Artificial Intelligence. MIT Press (1999) ISBN 0-262-23203-0
27. Gokce, B., Laleci, D.A., Olduz, M., Tasyurt, I., Yuksel, M., Okcan, A.: SAPHIRE: a multi-agent system for remote healthcare monitoring through computerized clini- cal guidelines. In: Series, W. (ed.) Agent Technology and e-Health 2008. Agent Technology and e-Health Whilestan Series in Software Agent Technologies. Springer and Autonomic Computing, pp. 25–44 (2008)
28. Gray, R.S.: Agent Tcl: A flexible and secure mobile-agent system. PhD Thesis, Dartmouth College (June 1997)
29. Gray, R.S., Kotz, D., Cybenko, G., Rus, D.: D'Agents: Security in a Multiple-Language, Mobile-Agent System. In: Vigna, G. (ed.) Mobile Agents and Security. LNCS, vol. 1419, pp. 154–187. Springer, Heidelberg (1998)
30. Gunupudi, V., Tate, S.R.: SAgent: a security framework for JADE. In: Proc. Fifth Int. Joint Conf. on Autonomous Agents and Multiagent Systems, pp. 1116–1118 (2006)
31. Hu, Y.-J., Tang, C.-W.: Agent Oriented Public Key Infrastructure for Multi-Agent E-service. In: Palade, V., Howlett, R.J., Jain, L. (eds.) KES 2003. LNCS, vol. 2773, pp. 1215–1221. Springer, Heidelberg (2003)
32. Ismail, L.: A secure mobile agents platform. J. Commun. 3(2), 12 (2008)
33. Jacques, F.: Multi-Agent Systems: An Introduction to Artificial Intelligence. Addison-Wesley (1999) ISBN 0-201-36048-9
34. Jaiswal, A., Kim, Y., Gini, M.: Design and Implementation of a Secure Multi-Agent Marketplace. Electronic Commerce Research and Applications 3(4), 355–368 (2004)
35. Janicke, H.T.: The development of secure multi-agent systems. PhD Thesis. De Montfort University (2007)

36. Karnick, N.M., Tripathi, A.R.: Security in the Ajanta Mobile Agent System. Software Practice and Experience 31(4), 301–329 (2001)
37. Karygiannis, T., Jansen, W.: Mobile agent security. Technical Report NIST SP 800-19, National Institute of Standards and Technology (1999)
38. Karygiannis, A., Antonakakis, E.: Security and Privacy Issues in Agent-Based Location-Aware Mobile Commerce. In: Barley, M., Mouratidis, H., Unruh, A., Spears, D., Scerri, P., Massacci, F. (eds.) SASEMAS 2004-2006. LNCS, vol. 4324, pp. 308–329. Springer, Heidelberg (2009)
39. Laleci, G.B., Dogac, A., Olduz, M., Tasyurt, I., Yusel, M., Okcan, A.: SAPHIRE: A Multi-Agent System for Remote Healthcare Monitoring through Computerized Clinical Guidelines, Project Deliverable. METU, Turkey
40. Liau, C.-J.: Belief, information acquisition and trust in multi-agent systems - A model logic formulation. Artificial Intelligence, 31–60 (2003)
41. Malik, N.S., Kupzog, F., Sonntag, M.: An Approach to Secure Mobile Agents in Automatic Meter Reading. In: Proc. of International Conference on Cyberworlds, pp. 187–193 (2010)
42. Mamadou, T.K., Shimazu, A., Nakajima, T.: The State of the Art in Agent Communication Languages (ACL). Knowledge and Information Systems Journal (KAIS) 2(2), 1–26 (2000)
43. Maña, A., Muñoz, A., Serrano, D.: Towards Secure Agent Computing for Ubiquitous Computing and Ambient Intelligence. In: Indulska, J., Ma, J., Yang, L.T., Ungerer, T., Cao, J. (eds.) UIC 2007. LNCS, vol. 4611, pp. 1201–1212. Springer, Heidelberg (2007)
44. Martínez-García, C., Navarro-Arribas, G., Borrell, J., Martín-Campillo, A.: An Access Control Scheme for Multi-agent Systems over Multi-Domain Environments. In: Demazeau, Y., Pavón, J., Corchado, J.M., Bajo, J. (eds.) PAAMS 2009. AISC, vol. 55, pp. 401–410. Springer, Heidelberg (2009)
45. Marques, P., Silva, L., Silva, J.: Security mechanisms for using mobile agents in electronic commerce. In: 18th IEEE Symp. on Reliable Distributed Systems, Lausanne, Switzerland (1999)
46. McDonald, J.T., Yasinsac, A.: Trust in Mobile Agent Systems, Florida State University. Tech. Rep. (2005)
47. Moradian, E., Håkansson, A.: Approach to Solving Security Problems Using Meta-Agents in Multi Agent System. In: Nguyen, N.T., Jo, G.-S., Howlett, R.J., Jain, L.C. (eds.) KES-AMSTA 2008. LNCS (LNAI), vol. 4953, pp. 122–131. Springer, Heidelberg (2008)
48. Mouratidis, H., Giorgini, P.: Enhancing Secure Tropos to Effectively Deal with Security Requirements in the Development of Multiagent Systems. In: Barley, M., Mouratidis, H., Unruh, A., Spears, D., Scerri, P., Massacci, F. (eds.) SASEMAS 2004-2006. LNCS, vol. 4324, pp. 8–26. Springer, Heidelberg (2009)
49. Mouratidis, H., Giorgini, P., Mason, G.: Modelling secure multiagent systems. In: Proceedings of the Second International Joint Conference on Autonomous Agents and Multiagent Systems, pp. 859–866 (2003)
50. Novák, P., Rollo, M., Hodík, J., Vlcek, T.: Communication Security in Multi-agent Systems. In: Mařík, V., Müller, J.P., Pěchouček, M. (eds.) CEEMAS 2003. LNCS (LNAI), vol. 2691, pp. 454–463. Springer, Heidelberg (2003)
51. Pechoucek, M., Marik, V.: Industrial deployment of multi-agent technologies: review and selected case studies. Auton. Agent Multi-Agent Syst. 17, 397–431 (2008)
52. Poslad, S., Charlton, P., Calisti, M.: Specifying Standard Security Mechanisms in Multi-agent Systems. In: Falcone, R., Barber, S.K., Korba, L., Singh, M.P. (eds.) AAMAS 2002. LNCS (LNAI), vol. 2631, pp. 163–176. Springer, Heidelberg (2003)

53. Ramchurn, S.D., Dong, H., Jennings, N.R.: Trust in multiagent systems. The Knowledge Engineering Review 19(01), 1–25 (2004)
54. Ramchurn, S.D., Jennings, N.R.: Trust in agent-based software. Cyber Trust and Crime Prevention Project, Review
55. Ramchurn, S.D.: Multi-agent negotiation using trust and persuasion. PhD Thesis, University of Southampton (2004)
56. Rashvand, H.F., Salah, K., Calero, J.M.A., Harn, L.: Distributed security for multi-agent systems - review and applications. IET Inf. Secur. 4(4), 188–201 (2010)
57. Rindebck, C.: Designing and maintaining trustworthy online services. Blekinge Institute of Technology Licentiate Dissertation Series No 2007:08, Sweden (2007) ISSN 1650-2140, ISBN 978-91-7295-120-4
58. Shoham, Y., Leyton-Brown, K.: Multiagent Systems: Algorithmic, Game-Theoretic and Logical Foundations. Cambridge University Press (2008) ISBN 9780521899437
59. Sulaiman, R., Sharma, D., Ma, W., Tran, D.: A Multi-agent Security Framework for e-Health Services. In: Apolloni, B., Howlett, R.J., Jain, L. (eds.) KES 2007, Part II. LNCS (LNAI), vol. 4693, pp. 547–554. Springer, Heidelberg (2007)
60. Takahashi, K., Mitsuyuki, Y., Mine, T., Sakurai, K., Amamiya, M.: Design and Implementation of Security Mechanisms for a Hierarchical Community-Based Multi-Agent System. In: Ghose, A., Governatori, G., Sadananda, R. (eds.) PRIMA 2007. LNCS, vol. 5044, pp. 134–145. Springer, Heidelberg (2009)
61. Tweedalea, J., Ichalkaranjeb, N., Sioutisb, C., Jarvisb, B., Consolib, A., Phillips-Wrenc, G.: Innovations in multi-agent systems. Comput. Appl. 30, 1089–1115 (2007)
62. Van Dyke Parunak, H.: Agents in Overalls: Experiences and Issues in the Development and Deployment of Industrial Agent-Based Systems. Expanded version of invited talk at PAAM (1999)
63. Van Dyke Parunak, H.: A Practitioners' Review of Industrial Agent Applications. Autonomous Agents and Multi-agent Systems 3(4), 389–407 (2000)
64. van 't Noordende, G.J., Brazier, F.M.T., Tanenbaum, A.S., Security in a Mobile Agent System. In: IEEE First Symposium on Multi-Agent Security and Survivability, pp. 35–45 (2004)
65. Vigna, G. (ed.): Mobile Agents and Security. LNCS, vol. 1419, pp. 3–540. Springer, Heidelberg (1998)
66. Vila, X., Schuster, A., Riera, A.: Security for a multi-agent system based on JADE. Comput. Sec. 26, 391–400 (2007)
67. Vitabile, S., Conti, V., Militello, C., Sorbello, F.: An extended JADE-S based framework for developing secure multiagent systems. Comput. Stand. Interfaces 31, 913–930 (2009)
68. Webber, C.G., De Fatima, M., Lima, W.P., Casa, M.E., Ribiero, A.M.: Towards securing e-learning applications: A multiagent platform. Journal of Software 2(1), 60–69 (2007)
69. Woolridge, M.: An Introduction to Multi-agent Systems. John Wiley and Sons (2002) ISBN 0-471-49691-X
70. Xiao, L., Peet, A., Lewis, P., et al.: An adaptive security model for multi-agent systems and application to a clinical trials environment. In: 31st IEEE Annual Int. Computer Software and Applications Conf., COMPSAC 2007 (2007)
71. Xu, K.: Mobile agent security through multi-agent cryptographic protocols. PhD Thesis, University of North Texas (2004)
72. Zhao, S., Liu, H., Sun, Z.: Scalable trust in multi-agent e-commerce system. In: Int. Symp. on Electronic Commerce and Security, pp. 990–993 (2008)

Personal Secret Information Based Authentication towards Preventing Phishing Attacks

Gaurav Varshney, Ramesh Chandra Joshi, and Anjali Sardana

Electronics and Computer Engineering Department, Indian Institute of Technology, Roorkee, India
{gauravdtsi,rcjosfec,dr.anjalisardana}@gmail.com

Abstract. Phishing is a well-known technique used by internet fraudsters for acquiring sensitive and personal information from users by impersonating a real identity. A Phishing attack involves various deceptions & advanced cybercrime techniques, some of them includes email spoofing, exploiting browser side vulnerabilities, fraudulent emails and Phished websites creation techniques using scripting languages and technologies. Phishing causes identity, goodwill and money loss to companies and individuals. One of the major problems we identified is the reduced usage and reliability on the email Infrastructure as a communication medium between customers and companies. Previous schemes for phishing prevention such as those which use browser extension, Quick Response code, Extended Authentication server & device and smart card based techniques are complex and difficult to make use in real world scenario. We present an architecture that can be used by companies for preventing phishing attacks by sharing a piece of secret information with every customer and using it as an authentication mechanism to prove their originality when a customer login to their websites using links provided in their emails. The unavailability of secret information which is securely shared between customer and the company will prevent a phisher in creating deception and hence will prevent phishing attacks which occur due to malicious links in phished emails. This will increase the reliability of email service as an authentic communication medium. The efficacy of this technique does not rely on results of any spam or phishing prevention scheme provided at email service provider side.

Keywords: Phishing, phisher, authentication.

1 Introduction

Phishing was known to people in the year 1996. It can be defined as an art of deceiving people on the internet, so as to steal the personal information secret to them such as user names, passwords, bank account numbers, credit card details etc. The concept was termed as phishing as the fraudsters are using emails as a medium to "Phish" user information such as usernames and passwords in the sea of internet users. The name resembles the word fishing; 'ph' is used instead of 'f' for two reasons:

N. Meghanathan et al. (Eds.): Advances in Computing & Inform. Technology, AISC 176, pp. 31–42.
springerlink.com

1. To make it a different word
2. The letter 'ph' is derived from the word "phreaking" which is known to be the earliest form of hacking of telephone lines.

Phishing come first time into the knowledge of people as a severe attack in 1996 when cyber criminals stole American Online Passwords by deceiving the AOL users through phishing [11].

Phishing is a deception technique used by attackers (Commonly known as Phishers) for gaining personal information from end users, with the help of fraudulent and spoofed emails, Phished Websites and various deception techniques. The aim of the phisher lies in obtaining personal information or credentials from an end user such as bank account numbers their passwords, credit card details etc. They use this information in doing mischievous and fraudulent activities such as accessing important information and secrets, withdrawing money of an individual on web.

Phishing starts when an attacker uses a mass-mailer for sending fraudulent and spoofed emails by impersonating themselves as an authenticated bank, financial or social institution to a large population of end users. Phishing generally starts with a mass mailing activity to increase the population of end users that will eventually fall for Phishing. Phishers also use a phished website that looks exactly same as that of the original one he is targeting to phish, except for the domain name and the DNS entry it will use. The attack scenario starts when the attacker sends a phished email using spoofing and advanced email creation techniques such as those used in email newsletters, with other fraudulent techniques to fulfill their specific needs. The end user or the victim opens the email and because of deception techniques used inside it, trusts on the originality of its contents and its sender and clicks on the URL specified in it. The URL looks normal but it will take to a phished Web site.

The phished website is created in a way to look like an original highly trusted site that a phisher is targeting. As an example a phishing website can be of a highly trusted bank having the same text the same logo and animations as it is on the original bank website. When a user reaches a phished website which he can't identify as phished one, he enters information asked by the website such as user id's password, credit card numbers etc. which eventually get stored in the servers of the phisher.

Phishing is termed as a deception technique as it creates an illusion to the receiver of an email that, it is from an entity on which user's trust, but behind the scenes it is not as expected. Email phishing is carried out with the help of many other tricky techniques which are used for internet fraud in today's internet world, one of which is Email spoofing. Email spoofing technique allow an attacker to send email using other's identity which causes a severe problem, because now he can send anything such as wrong information, malicious codes etc. and held others responsible for his wrongdoings. Spoofing creates two problems: one is of creating wrong trust in the mind of end user, hence gaining confidence, so that he will do what is required and second is of wrong backtracking because an innocent user or group will be held responsible for the problems created. Email spoofing plays an important role in carrying out email phishing as it makes the user to believe on the illusion of reality, created by a Phisher.

The statistics as obtained from Avira shown in Table 1. are of February 2011 which shows that phishing attacks are more Top level domain and business centric. The most phishing attacks are on the .com top level domain and the companies which gets most affected are those which involve some kind of electronic money transfers

and social networking. Hence Phishing is from one of the most important threats in the internet world that is to be taken care of. The damages that it causes include loss of money, information and good will.

Table 1. Statistics of Phishing Attacks

#	Top Level Domain	%	#	Brand Name	%
1	.com	51.56	1	PayPal	53.59
2	Others	15.82	2	Others	20.03
3	.org	6.20	3	HSBC Bank	5.07
4	.net	5.94	4	Chase Bank	4.43
5	.uk	3.69	5	Facebook	4.09
6	IP address	3.22	6	EBay	3.48
7	.br	2.44	7	Bank Of America	3.16
8	.tk	2.18	8	Visa	2.19
9	.ru	2.01	9	Lloyds	2.07
10	.tl	1.23	10	Banco Satander	1.88

In this paper we propose an architecture that will solve the problem of phishing that is launched through Phished website links in emails. The problem created by this attack is of bad trust in email service as an authentic communication medium and loss of credentials of users.

The next section will describe the previous schemes for phishing prevention. Section 3 will describe our proposed scheme with section 4 giving the description of overall benefits. Section 5 ends the discussion with conclusions and future work.

2 Previous Work

A detailed description of previous schemes proposed for preventing phishing attacks with their assumptions, advantages and disadvantages are in a Table shown on the next page. From the study of previous techniques we concluded that there are some common shortcomings in them which are as follows:

1. Various Schemes based on Secret Images shared between website and user and which are revealed during pre-logging when the user enters the secret key are annoying and vulnerable. As they ask users to enter a new watermark image and its position each time a user logs out, also a Phisher can obtain the secret key from the user by creating fake login pages and can obtain the Watermark image and its location from the original web page by using the secret key obtained from the user.
2. Use of Advanced Technologies such as Radio frequency Identification Technology (RFID) for authentication requires that a user must carry the RFID reader and Tokens for Login.

3. External authenticating device usage in prevention of phishing attacks add on to the cost and complexity. Complexity is increased because the user interaction will be secure but complex as now it requires external device communicating with the browser which will then eventually contact to the target server. Also it will always require an external device for secure access.
4. Those solutions that require client server support require changes in the underlying frameworks and architectures also their maintenance and proper synchronization is a requirement. Also real time implementation, deployment and performance are of great concern.
5. Email Authentication and verification schemes require key management activities which will increase an extra burden on the system as now system has to take care of keys for each and every user.
6. Techniques implemented for avoiding key logging and improving password schemes are complex with respect to a normal user as he certainly doesn't want to annoy on every time he logs on to the website by entering keys through keypads and hence require initial user training.
7. Those schemes that implement security of user passwords at client's side with browser extensions are difficult to implement.
8. Client server interaction for authentication during every secure transaction increases the communication and computation cost at both client and server side.
9. Schemes based on short time passwords and certificates require special systems such as offline card readers (FINREAD reader) and Smart cards for their generation which add up extra cost and complexity to the underlying system.

Abbreviation	Proposed Scheme	Paper name	Assumptions	Advantages	Disadvantages
Watermarking Based [1]	Author proposed an anti-phishing approach based on Dynamic watermarking technique. According to this approach user will be asked for some additional information like watermark image, its fixing position and secret key at the time of user's registration and these credentials of particular user will be changed at per login. During each login phase a user will verify the authentic watermark with its position and decide the authenticity of website.	**Detection and Prevention of Phishing Attack Using Dynamic Watermarking** A.P. Singh et.al **2011**	User will select a watermark image and its position at website while logging out. User Account database that will store secret key & Watermark Image with regular credentials.	Doesn't require any external mobile device. Feasible to implement with minimal changes.	During every logout user is asked for reentering new watermark image and its position which is annoying. A phisher can obtain the initial secret key through phishing and can obtain the watermark position and its location.
RFID Based [2]	Authors proposed a RFID (Radio Frequency Identification Technology) Factor Authentication Application (RFAA) techniques; an enhanced technique from SofToken scheme that acts as a technique for two-factor authentication.	**A Sophisticated RFID Application on Multi-Factor Authentication** J.C. Liou et.al 2011	RFID tags and RFID reader and changed Login Infrastructure.	RFAA is a two factor authentication scheme for more secure identification. RFAA can be used for both online transactions and computer system access as opposed to the SofToken application that primary addresses to online transaction security	RFID reader and Tokens will be required each time user login.

External Authentication Device based [3]	Author proposed techniques based on external authenticator. They proposed that user's must be authenticated by an external authenticator that they cannot reveal to malicious parties. Scheme uses additional authenticator on a trusted device, which can be a cell phone or a PDA, such that the attacker will have to compromise the device to obtain user password and to obtain user account.	**Phool-proof Phishing Prevention** B. Parno et.al 2005	User can establish a secure connection between their cellphone and their browser and the cellphone itself has not been compromised.	Prevent active man in middle attacks. Use of cellphones allows us to minimize the effect of hijacked browser windows and facilitates user convenience since it can be used at multiple machines.	Requires the usage of external authenticating device to solve the purpose which will add complexity in the way a user account will be accessed.
Post Phishing Rescue based [4]	Authors proposed post Phishing Rescue technique. Here client identifies whether user have entered valid credentials on a faked website and Server capture this information from various clients. if there is some phishing going on server transfer the information to target domain for immediate attention.	**Password Rescue: A New Approach to Phishing Prevention** D. Flor˜encio and C. Herley 2006	Assuming that a white list and a black list are maintained and updated regularly and a notion of trusted client and server ends who will cooperate.	The scheme doesn't protect the user from information leakage but rather try to detect and then rescue the user from bad trust decisions.	Complex and require client and server deployment and synchronization. Also require to maintain white list and blacklist of sites. Real time implementation considerations
Email spoofing detection based [5]	Authors proposed a novel key distribution architecture and identity based digital signature for making email trustworthy and hence detecting & mitigating spam mails by detecting email spoofing	**Fighting phishing attacks lightweight trust architecture for detecting phished mails.** B. Adida et.al 2005	Upgraded email client and at least one key server.	The scheme is lightweight neither pre-established public key infrastructure nor cooperation between email domains is required. all legitimate uses of email remain fully functional after the changes required by the scheme	Real time implementation considerations. Requires noticeable changes in the email service provider's side
Picture passwords Based [6]	Author has shown the usability of Picture passwords and shown how picture keypads can be used for entering credentials instead of typing through keyboard. A number of features of keypad are personalized to the user such as background color border design of keypad which differ from other users, and selected from the user's stored account record by means of the user's username. This provides protection against phishing, by alerting the user when any changes to their familiar keypad 'look-and-feel' occur, which is unknown to the phisher.	**The usability of picture passwords** N. Fraser	Set of pictures from which a subset of pictures will be issued as password to a particular user	Avoid logging by key loggers, also it is impossible for a user to disclose their password on a randomly generated phisher keypad as it is hard for a phisher to randomly generate a keypad that contains all picture necessary for entering the password by a user.	It will be complex from user's perspective to enter the password each time during login by picture keypad and will require user training.
Dynamic security skin based [7]	Authors proposed two interaction techniques to prevent spoofing. 1. Browser extension provides a trusted Window in the browser for username and password entry. A photographic image for creating a trusted path between the user and the window so as to prevent spoofing of the Window and text entry fields. 2. The scheme allows the remote server to generate a Unique abstract image for individual user for each transaction. The image will create a "skin" that will automatically customize the Window or the user interface elements in the content of a remote web page. The extension will allow the browser to inde-	**The Battle Against Phishing: Dynamic Security Skins** R. Dhamija, J.D. Tygar 2005	Configured remote server and browser extension.	To authenticate, the user has to recognize only one image and remember one low entropy password, no matter how many Servers he wishes to interact with. To authenticate content from an authenticated server, the user only needs to perform one visual matching operation to compare two images.	Increases the complexity of user interface, require initial user training requires client server interaction each time a transaction is performed. Extended browser window, increases the complexity of user interaction.

	pendently compute the image it expects to receive from the remote server. To authenticate content from the server, the user can visually verify that the images match.				
Browser Extension Based [8]	Authors described a browser extension, PwdHash that transparently produces a different password for each site, which improves web password security and defends against phishing and other attacks. Browser extension apply a cryptographic hash function to a combination of the plaintext password entered by the user, data associated with the web site, and (optionally) a private salt which is stored on the client machine.	**Stronger Password Authentication Using Browser Extensions** B. Ross et.al 2005	Browser Extension, a good cryptographic hash function.	The scheme requires no changes on the server side. Theft of password received at one of the website will not reveal the password that will be used at another website.	Implementing this password method securely and transparently in a web browser extension turns out to be quite difficult
Smart card based [9]	Authors proposed two solutions: 1. Short-time password solution. This authentication scheme uses an offline card reader and a smart card to produce short-lived passwords on demand. 2. Certificate-based solution. This authentication scheme uses a secure online card reader, the FINREAD card reader, and a smart card to sign SSL/TLS challenges on demand	**Secure Internet Banking Authentication,** A. Hiltgen, et.al 2006	Java Applet Websites that can detect FINREAD card reader, Card Readers.	The user's credentials are stored on the smart card and can only be accessed via an offline smartcard reader, so malicious software can't get the user's symmetric cryptographic key or related functionality. Scheme effectively thwarts both offline credential-stealing attacks as well as online channel-breaking attacks.	Necessity of mobile equipment's. Require major changes in underlying system. Complex.
QR Code based [10]	Author proposed an anti-phishing single sign-on (SSO) authentication model using QR code. This scheme is secure against phishing attack and even on the distrusted computer environment. Scheme consists of three phases: login request phase, QR code generation phase, and verification phase.	**A mobile based anti-phishing authentication scheme using QR code**, K. Choi et.al 2011	QR (Quick Response) Code reader, extended authentication server, External Mobile device.	User can access the web sites in online Environment of distrust local computer and web server using mobile device. Even if the user's sensitive information is exposed, attacker cannot obtain the mobile information because user data is encrypted by the mobile device. Users can check the web server whether this server is the phishing server through the extended authentication server	Complex Scheme for deployment Requires an extended authentication server, whose reliability is a concern. Requires a secure external mobile device. Feasible, efficient and transparent deployment in real world is a question.

10. Extended authentication schemes for prevention of Phishing requires configuration, management and security consideration for extended authentication servers which are used to authenticate the web-servers a user is communicating with. Also it increases the communication time and cost for each user login.

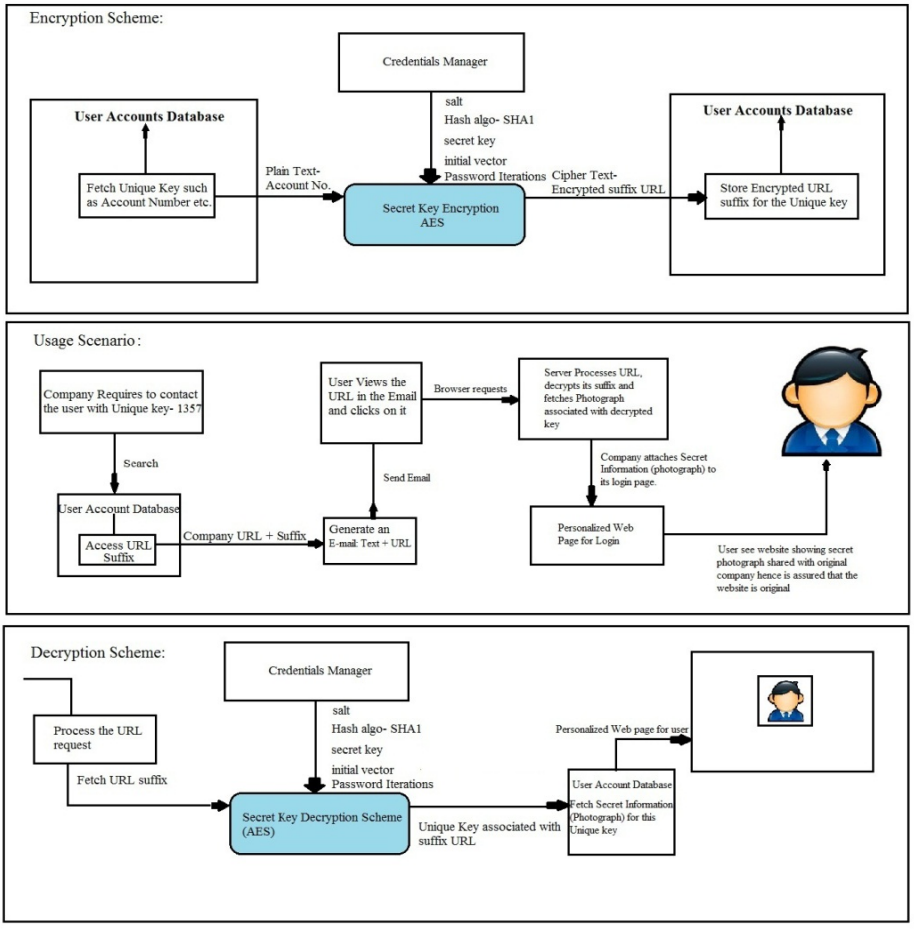
3 Personal Secret Information Based Authentication towards Preventing Phishing Attacks

Our proposed sheme is for prevention of phishing attacks by providing users a way to verify the originality of the website they are logging with while they click on a link in the e-mail that comes to their E-mailbox. This is achieved by using a piece of secret information that can be a photograph or a key which is shared between the user and the website and is provided by the user at the time of online account creation. In our implementation we will use a photograph as a piece of secret information. The overall architecture proposed is shown in fig1.

The architecture proposed require minimal changes to the underlying database that is used by websites for storing user credentials. Generally websites of online banking, social networking and others store userid and passwords as secret credential for a unique user and the verification includes checking these credentials when a user login with them. Our proposed scheme requires that websites should include some more user secret information to prevent phishing and use them in a way that will help the user to discriminate between original and phished websites. By secret information we mean userid, password as usual with the additional use of a user's photograph or a secret phrase.

The overall scenario and the underlying scheme we propose is based on the assumption that if a user can see the login pages of their websites personlaized then there will be low chances that they will fall for phishing as a phisher cannot provide such a personalization on a phished website as he is unaware of the secret information shared between user and the original company website and which is being used as a way to provide personalized experience to each unique user.

The personalization for each user while they click on the links sent to them through email from original companies is achieved by storing URL suffix for each user which is encrypted userid and will be used with the compaanies URL whenever company wants any communication. This will result in URL suffixes for each individual user which are stored with the user credentials in the database. these will be then sent to the user whenever company wants to contact the specific customer. when the user click on such a link the url suffix will be retrieved and processed to get the user id associated from where he can extract the secretv information shared with the website and display them at appropriate places during login to provide user a kind of personlization. The Encryption scheme for converting unique user information such as user id's to URL suffixes with the decryption scheme showing the server side processing of URL to obtain the userid for providing user personlization is shown in Fig.1 also explains the usage scenario in which the scheme will be deployed and used.



Username	Password
10535010	bbc
10535019	rma
10535018	vin

Fig. 1. Proposed Architecture

3.1 Encryption Scheme

When a user supplies the user credentials in the form of userid, password and secret information(photograph) the information will be stored as usual in the companies database. From there the userid (unique key) is extracted and is encrypted by a symmetric encryption scheme (AES) to develop a URL suffix that will be stored in

the user database with that user id and is then sent as URL suffix with the companies URL link that company will sent to the user for logging in emails.

3.2 Decryption Scheme

Whenever a user will click on the link in the mail from the original companies website the link is processed at the server side. The processing includes fetching the URL suffix associated with the URL and then decrypting it with the symmetric decryption scheme(AES) to obatin the userid which was encrypted. the user id is then used to extract the secret information which is photograph associated with the user and then eventually displaying it on the login window. This will make sure the user that the page with which is he logging with is original as phisher has no knowledge of the secret photograph he shared with the company during account creation.

Both Encryption and decryption schemes require the usage of a trusted component at the server side that will store the secrets for encryption and decryption scheme. we call it in our scheme as Credentials manager. for encryption and decryption we have proposed Advanced Encryption standard (AES). The initial study shows that AES is a good symmetric enryption scheme as the only way of breaking it is through brute force attacks and those kind of attacks on hug key sizes as provided by AES are proven to be difficult and is also used in [10]. The credential manager will store the information for the AES encryption scheme and are as follows:

1. Salt which act as second secret password
2. Hash Algorithm can be SHA-1 or MD-5.
3. Secret key used for encryption and decryption
4. Initial vector which is an collection of 16 ASCII characters
5. Password iteration that defines the no of times the algorithm is run on the plain text.

The screenshots of our prototype implementation are shown below:

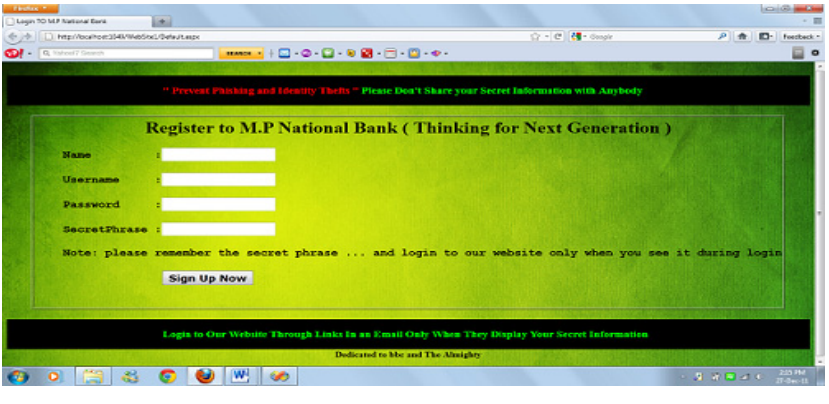


Fig. 2. Sign up page of a website as per proposed scheme

Fig. 3. Login page

Fig. 4. Comapny Generating URL for user aheadpec

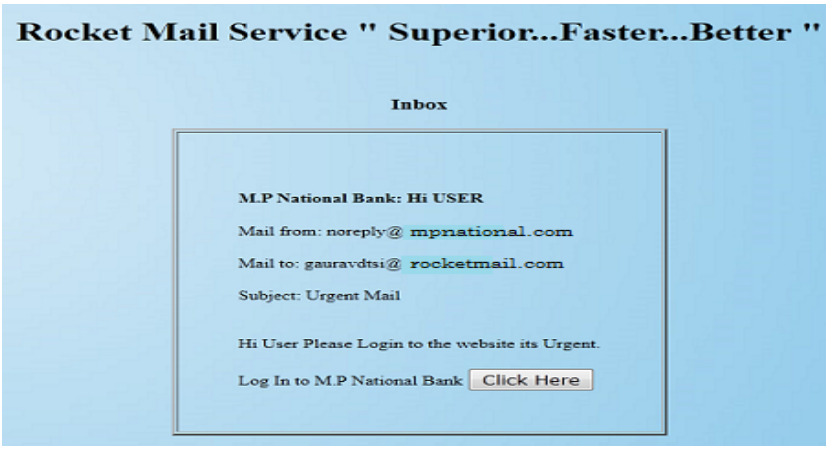


Fig. 5. Mail Sent from company to user aheadpec

Fig. 6. Login page showing secret phrase aheadpec shared with website during sign up

4 Advantages of Proposed Scheme

The advantages of our scheme wll provide compared to other techniques are as follows:

1. Our Proposed scheme does not require any kind of support from spam and phished mail filters provided by email service providers and also don't rely on their accuracy in detecting phished email.
2. This scheme can be implemented in real time by companies with minimal changes to their server side processing.
3. Key management is not a task as no sharing of key is done anywhere in the scheme. However the credentials managers have to be designed in a way so that the credentials can be protected from attackers reach. Also credentials manager can refresh the scheme by changing the values of the credentials stored after a certain period of time.
4. The scheme can rely on a single unique key used for encryption and decryption of all user ids. But generally credentials manager can implement numerous other schemes in which he can allot certain group of user id's a different set of credentials for encryption and decryption and the other group a different one that will eventually increase the security.
5. Our scheme require no changes in the browser or the at the client machine.
6. There is no requirement for any external authenticating device.
7. It requires no user training and is not annoying compared to other techniques. Also user doesn't have to remember the position, color, shape and sizes of any browser window or watermark Image.
8. Our Scheme doesn't require any special external card readers or tokens as used in some techniques for phishing preventions and hence our solution doesn't add cost and complexity to the underlying system.
9. There is no requirement for extended authentication server which cuts off extra server maintenance and configuration with reduced time per login.

5 Conclusion and Future Work

We have proposed a novel scheme based on personal secret information for authentication towards preventing Phishing attacks which are launched through Phished website links in emails. The Scheme is easy to deploy in real world scenario with minimal changes and better efficiency. A working prototype of the proposed scheme is developed and its accessment on various measures such as communication cost, time and efficiency is under study.

In future we will try to apply this technique in a way to prevent Web Phishing which occurs when a user reaches a Phished website through typing mistakes on browsers etc. and not from links in Phished emails.

References

1. Singh., A.P., et al.: Detection and Prevention of Phishing Attack Using Dynamic Watermarking. Information Technology and Mobile Communication Communications in Computer and Information Science, Part 1 147, 132–137 (2011), doi:10.1007/978-3-642-20573-6_212011
2. Liou, J., et al.: A Sophisticated RFID Application on Multi-Factor Authentication. In: 2011 Eighth International Conference Information Technology: New Generations (ITNG), Las Vegas, pp. 180–185 (2011), doi:10.1109/ITNG.2011.38
3. Parno, B., Kuo, C., Perrig, A.: Phoolproof Phishing Prevention. In: Di Crescenzo, G., Rubin, A. (eds.) FC 2006. LNCS, vol. 4107, pp. 1–19. Springer, Heidelberg (2006)
4. Florencio, D., Herley, C.: Password Rescue: A New Approach to Phishing Prevention. In: Proceedings of the 1st USENIX Workshop on Hot Topics in Security, HOTSEC (2006)
5. Adida., B., et al.: Fighting Phishing Attacks: A Lightweight Trust Architecture for Detecting Spoofed Emails. In: DIMACS Workshop on Theft in E-Commerce (2005)
6. Fraser, N.: The usability of picture password (unpublished)
7. Dhamija, R., Tygar, J.D.: The Battle Against Phishing: Dynamic Security Skins. In: Proceedings of the 2005 symposium on Usable privacy and security, SOUPS (2005)
8. Ross, B., et al.: Stronger Password Authentication Using Browser Extensions. In: Security 2005 Technical Program (2005)
9. Hiltgen, A., et al.: Secure Internet banking authentication. IEEE Security & Privacy 4(2), 21–29 (2006), doi:10.1109/MSP.2006.50
10. Kyeongwon, C., et al.: A mobile based anti-phishing authentication scheme using QR code. In: 2011 International Conference on Mobile IT Convergence (ICMIC), September 26-28, pp. 109–113 (2011)
11. APWG.: Origins of the Word "Phishing", `http://www.antiphishing.org/word_phish.html`

Key Distribution Schemes in Wireless Sensor Networks: Novel Classification and Analysis

Premraj Mahajan and Anjali Sardana

Electronics and Computer Science Department,
IIT Roorkee, India
{prem228434,dr.anjalisardana}@gmail.com

Abstract. Security is one of the important and challenging aspects in wireless sensor network owing to their wireless nature combined with limited memory, energy, and computation. We can classify security issue of the wireless sensor network into five broad categories as cryptography techniques, key management, routing protocols, intrusion detection and data aggregation. Since the key management forms an underlying factor for efficient routing protocol and cryptography in wireless sensor network, we focus on key management issue. This paper outlines the constraints, security requirements and attacks, which are related to the key management and routing. Further novel classification of key distribution schemes have been proposed. The proposed novel classification and comparison distinctly brings to the fore gaps in the existing solutions of research which can be put to use by researchers in the area to identify current challenges for designing efficient key distribution scheme. The paper concludes with possible future research directions on key distribution in WSNs.

Keywords: Key distribution schemes, Security, Sensor network.

1 Introduction

Wireless Sensor Network contains hundreds or thousands of sensor nodes and these sensor nodes have the ability to communicate either amongst each other or directly to an external base station (BS). Figure 1 shows a schematic diagram of sensor node components. Basically, sensor node comprises of sensing, processing, transmission, mobilizer, position finding system, and power units. The same figure shows the communication architecture of a wireless sensor network (WSN) [1, 2].

These types of the sensor nodes are deployed into the field for the purpose of sensing some specific information. But these sensor nodes are resource constraints. Sensor nodes have limitations like computational power, storage, battery etc. So possibility of the attacks like hello flood on sensor node is more. Hence it is important to utilize available resources effectively with fulfilling the basic requirements like encryption, authentication etc. These (encryption, authentication) services are based on operations which involves the different [3]keys like encryption-decryption keys, cluster key, key which is used in hash function etc. So energy efficient key distribution in sensor nodes plays vital role in security of WSNs Section 2 of this paper presents constraints of the wireless sensor network along with security requirements. Section 3

N. Meghanathan et al. (Eds.): Advances in Computing & Inform. Technology, AISC 176, pp. 43–53.
springerlink.com

presents attacks related to the key management and routing. In section 4, a novel classification of the key management schemes is presented. Section 5 discusses about conclusions and future work to be done.

2 Constraints in Wireless Sensor Network

Sensor nodes have limited processing power, storage capacity and transmission range because of the energy and the physical size.

Energy: Energy in sensor network is conserved for many purposes like sensing, ADC, computation, communication. So for long lasting working of the sensor, all these operations should be performed efficiently.

Computation: Embedded processors in sensor nodes are not so powerful that they can perform the complex cryptographic functions. Typically 8bit, 4-12 MHz[4].

Memory: Memory includes flash memory and RAM. Flash memory is used for storing downloaded application code and RAM is used for sensed data, intermediate computation. In SmartDust project, tiny OS code space is 3500bytes, and only 4500bytes [4] are there for the security application.

Transmission range: Again range is also dependent on the energy limitation. It also depends on the environment factors like whether and terrain.

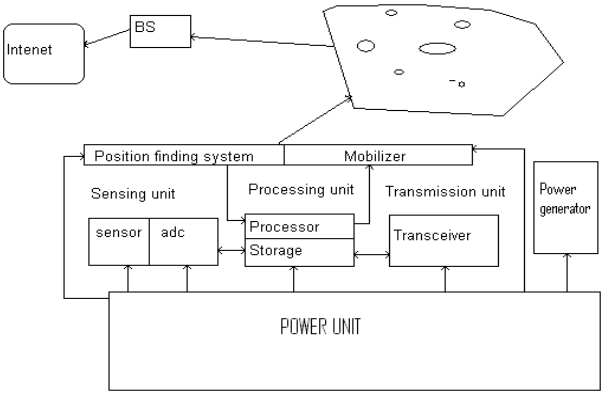


Fig. 1. The component of sensor network [3]

Security requirement: To protect the information and resource from attacks, security services are provided in WSNs. These security requirements include:

- **Authentication:** It ensures that communicating nodes are genuine and no any malicious node can inject or spoof the message.
- **Availability:** It ensures that message is made available to the destination node even in presence of the intermediate node capture or Denial-of-service attack.

- **Authorization:** It ensures that only authorized nodes can be involved in providing information to network services.
- **Confidentiality:** It ensures that the given information cannot be understood by the attacker or any unauthorized person.
- **Integrity:** It ensures that information cannot be altered by any intermediate malicious node.

3 Attacks Related to Key Management and Routing

Wireless Sensor Network is vulnerable to various types of attacks. In following section the attacks which are related to key management and routing are considered.

Spoofing, altering and replaying attack: In presence of the spoof and replay attack, the network traffic can be extensively corrupted. Continuous alteration in the message transmits the incorrect message and source node has to retransmit the packets. It reduces the battery life in large extend due to power exhaustion. In replay attack, malicious node may capture the any of the network message and replay that message, and hence damaging the network performance.[4, 5]

Selective forwarding attack: Normally sensor nodes are multi-hop systems and the assumption in such network is that intermediate nodes faithfully forward the received message. In this type of attack the malicious node may refuse or simply drop some part of message [4-6]. Such type of attack is most effective when attacker is explicitly included on the path of data flow.

Sybil attack: The Sybil attack is a case in which malicious node shows multiple identities. Malicious node behaves as it is a large number of the nodes for example impersonating other node or simply claiming false identities. In worst case, an attacker may generate an arbitrary number of additional node identities, using single device [4, 7].

Sinkhole attack: The attacker tries to pass nearly all the traffic from a particular area through a particular/malicious node. An attacker makes a compromised node look more attractive to the surrounding nodes by forging routing information and ultimately surrounding nodes will choose next node to route the information through the compromised node giving access to all data. Many attacks can be initiated [4, 5] through the sinkhole attack ex. Wormhole, selective forwarding or eavesdropping.

Wormhole attack: A wormhole is low-latency link between two portions of the network over which attacker replays the network messages [5, 8]. An attacker receives the packets at one portion of network and tunnels them to another portion, and then replays them into the network. These tunneled packets arrive sooner than the other packets transmitted over normal multi-hope route because these tunneled distances are longer than the normal wireless transmission range of a single hop. The wormhole attack is possible even if the attacker has not compromised any hosts and even if all communication provides authenticity and confidentiality.

Hello flood attack: Many of protocol use HELLO packets for getting the list of the neighboring nodes and assume that replied nodes are within their transmission range and are therefore neighbors. But an attacker may use high-powered transmitter to

track maximum areas[5] so that, other nodes will believe that they are neighbor. If the attacker falsely broadcast a superior route to the base station then all nodes will pass the information through those attacking nodes even that node is out of range.

Acknowledgement spoofing attack: Acknowledgements are sometimes required in the sensor networks. An attacker node can spoof acknowledgements. Goal of the spoofing the acknowledgement is that attacker can convince[5] the sender node by giving false information like a weak link as strong or dead node as alive.

Tampering attack: Tampering is a physical layer attack. Given physical access to node, attacker can extract sensitive information such as cryptographic keys and some other data on a node [9] and may create false identity.

Table 1. Different types of attacks and their defense mechanism along with related issue

TYPES OF ATTACK	DEFENSE MECHANISM	ISSUE
Tampering	a. Tamper-proofing b. Hiding	High cost
Spoofed, Altered, or Replayed Routing Information	a. MAC b. Monitoring c. Lightweight Authentication d. SPINS protocol	Computation power Computation power
Selective Forwarding	a. Multi path routing b. Probing	Computation power
Sinkhole	a. Authentication b. Geographical routing c. Redundancy d. Monitoring	Computation power, key distribution Energy consumption
Sybil	a. Use of symmetric keys b. Probing	Computation power, key distribution Energy Consuming
Wormhole	a. Authentication b. Time synchronization c. Packet leashing by geographical and temporal information	Computation power, key distribution Infeasible
Hello flood Attack	a. Authentication b. Verify the bidirectional link	Computation power, key distribution
Ack. Spoofing	a. Authentication	Computation power, key distribution
Node replication attack	a. Localized voting system b. Key renewing	Replication attacks

4 Key Distribution Schemes

In wireless sensor network, to provide the basic security requirement like encryption, decryption, authentication etc. we have to perform some operations involving the different types of keys. With considering the constraints of the sensor node, we have to distribute these keys to all the sensor nodes. This key distribution operation must be energy efficient so as to increase the life-time of sensor node. An open research problem is how to set-up secrete keys among the communicating nodes. There are different schemes are proposed for key distribution among the sensor nodes. These schemes are categorized with the following properties [3, 10, 11]:

- **Pre-distribution/Post-distribution:** In pre-distribution schemes the keys are stored into nodes before deployment into the field and in post-distribution schemes the keys are distributed after the deployment into the field with the help of trusted server or self-enforcing property.
- **Homogeneous/Heterogeneous:** In homogeneous sensor network, all the nodes are identical and having the same computational power, storage capacity and energy level whereas in case of the heterogeneous sensor network, small number of sensor nodes are more powerful in terms of the energy, storage and computational power than other large number of the sensor nodes.
- **With deployment knowledge/without deployment knowledge:** Sensor network which knows that where and how the sensor nodes are deployed into the network that comes under deployment knowledge category. And other sensor networks, which don't have information about the deployment knowledge, that comes under without deployment knowledge category.

Different types of key distribution schemes are classified as shown in the figure 2:

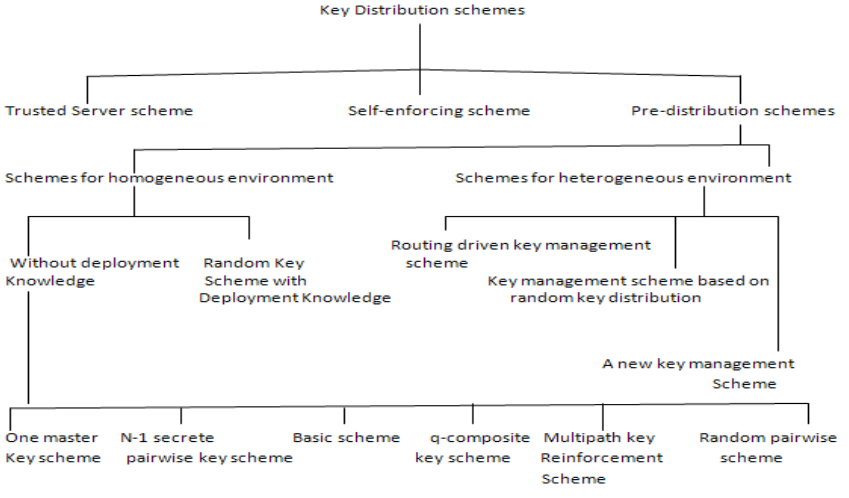


Fig. 2. Classification of key distribution schemes

4.1 Trusted Server Scheme

Trusted server scheme depends on the trusted server for key agreement between two different nodes, e.g. Kerberos. Such a third party key distribution requires infrastructure which is impractical [11, 12]for sensor network.

4.2 Self-enforcing Scheme

Self-enforcing scheme depends on asymmetric cryptography. it is very good solution for key management and distribution in WSN but sensor nodes have lot of limitations

like memory and processing power. Limited computation and energy resources of the sensor nodes often make it undesirable to use public key algorithms, such as Diffie-Hellman key agreement or RSA. Several works shows[13] that lightweight versions of the public key algorithms can be utilized in the sensor networks.

4.3 Pre-distribution Schemes

In pre-distribution schemes the keys are stored into nodes before deployment into the field. These can be further divided into schemes for homogeneous and heterogeneous environment.

4.3.1 Schemes for Homogeneous Network

In homogeneous sensor network, all the nodes are identical and having the same computational power, storage capacity and energy level.

4.3.1.1 Without Deployment Knowledge. In these schemes, deployment knowledge is not considered.

4.3.1.1.1 One Master Secrete Key Scheme [11]: In one master secrete key scheme, each node carry one master key, pre-distributed before deployment. This master key is used to achieve the key agreement and obtain a new pair wise key. Because of one master key, this scheme doesn't exhibit desirable network resilience. If any node is compromised then the entire sensor network will be compromised. In this scheme giving the temper proofing mechanism, will increase the cost as well as energy consumption of each node.

4.3.1.1.2 N-1 Secrete Pair-Wise Key[11]: In N-1 secrete pair-wise key scheme, if there are N nodes then each node should have to carry n-1 secrete pair-wise keys. Each of which is known to this sensor and one of the other to n-1 sensor node. Resilience is perfect as compared to other scheme because if any of the nodes is compromised then that node does not affect the security of communications of other nodes. But this system has main two drawbacks. It is not practical because of extremely limited amount of memory. As the network grows (N), memory required for storing keys also increases. Second one is, adding new node to pre-existing network is complex because the existing nodes do not have the keys of the new sensor node.

4.3.1.1.3 Basic Scheme [14]: It consists of three phases. Key pre-distribution, shared key discovery and path key establishment. First phase store small number of the keys into nodes key ring, taken from generated pool of keys to ensure that two node share at least one key with a chosen probability. Second phase establishes the secure link between two nodes only when they carry secrete key common. Third phase assigns the path-key to selected pairs of sensor nodes in wireless communication range that do not share a key but are connected by two or more two or more links at the end of the shared key discovery phase.

4.3.1.1.4 q–composite Key Scheme [10]: In previous scheme, we require common single key from key rings of two communicating nodes in order to secure link in the key–setup phase. In q –composite key scheme, q>1 common keys are needed. In this

way it increases the resilience of the network against node capture. This scheme uses Merkle puzzle in key set-up phase. After key set-up and discovery a new communication link key is generated as: $K = \text{hash}(K_1||K_2||\ldots||K_q)$ and hashed in canonical order. This scheme has no resistance against node replication since node degree is not constrained and there is no limit on the number of times each key can be used.

4.3.1.1.5 Multipath Key Reinforcement [10]: This method conjunction with basic scheme strengthens the security of an established link key by establishing the link through multiple paths and improves the resilience against node capture. Key set-up is as per basic scheme. Then each link is secured using a single key from key pool. This single key may be the part of any other node and if that node is captured then the link may not be secured further. So to address this problem, multipath reinforcement scheme update the communication key to a random value after key set-up through multiple paths between the nodes. The more the path we can find between the nodes, the more security multipath key reinforcement provides for the link between any two nodes. A link is considered completely compromised if all its reinforcement paths are also compromised.

4.3.1.1.6 Random Pairwise Key scheme [10]: In initialization phase, a node can only store random set of np pairwise keys where n is total nodes can be used in sensor network and p is probability. Total n node unique identifiers are generated. Size of network may be less than n and other unused identifiers are used for future network expansion that means provides some range of scalability. In post-deployment key set-up phase, each node first broadcasts its node ID to its immediate neighbors. Scheme provides node-to-node authentication by using identifiers. Provides distributed node revocation with adding some overhead in key storage and provides perfect resilience against node capture as it does not reveals any information about links.

4.3.1.2 With Deployment Knowledge. In pre-distribution schemes the keys are stored into nodes before deployment into the field

4.3.1.2.1 ABAB Scheme [15]: This scheme uses approximate deployment prior knowledge to improve the performance of a random key pre-distribution scheme. Motivation of this scheme is to design simple, flexible key distribution scheme[14] that are easily applicable, extensible and sufficiently secure. This scheme uses two large key pools for overall network with some common keys in common. This scheme is totally based on “the basic scheme”.

4.3.1.2.2 ABCD Scheme [15]: ABAB scheme is easily applicable in sensor network but it has a resilience problem since same keys are used in different zones several times. ABCD scheme is more complex than ABAB but it is more efficient and resilient scheme as it uses 2r keys pools, where r is the number of rows of deployment. Direct key and path key establishment is as per the basic scheme.

4.3.2 Schemes for Heterogeneous Network

In homogeneous scheme, it is assumed that all sensor nodes are of same power and same capacity. But the works have suggested [16]that connectivity, lifetime, reliability and resilience can be improved substantially if few nodes are given greater power and transmission capacity.

Some Common Assumptions of heterogeneous sensor network environment are:

- There are two types of sensor nodes H (powerful and provided with temper-resistance) and L (ordinary).
- Each L nodes and H nodes have unique node ID.
- Routing in Heterogeneous sensor network consists of two phases:
  1. Intra cluster routing (each L sensor sends data to its cluster Head)
  2. Inter cluster routing (Each cluster head sends may aggregate data from multiple

L-sensors and then sends compressed data to sink via the H-sensor backbone.

Following are some heterogeneous key distribution schemes in heterogeneous wireless sensor network:

4.3.2.1 Routing Driven Key Management Scheme [17]: This scheme is referred as ECC based key management scheme. This scheme requires only small number of ECC computations in each L-sensor as compared to ECC public key cryptography. Server generates pair of ECC public and private keys, one pair for each L-sensor and H-sensor. Each H-sensor are pre-loaded with public keys of all the L-sensors, association between each L-sensor and its private key, and a special key K_h, which is used by a symmetric cryptography algorithm for verifying newly deployed sensors and for secure communications. Each L-sensor is pre-loaded with private key and public keys of H-sensors. In this scheme it is assumed that each L-sensor can determine its location. L-sensor sends key request message to H-sensor, which include its location and its ID via shortest distance path. After receiving the request message, H-sensor uses MST or SPT algorithm to determine the tree structure in the cluster. Then H-sensor generates shared keys for each L-sensor and its c-neighbors, Then H-sensor unicasts the message to respective L-sensor node with their private key. After receiving the message L-sensor decrypt the message and communicate securely with their neighbors. The scheme utilizes the fact that a sensor node communicates with a small portion of neighbors only and thus greatly reduces the communication and computation overheads of key set-up as compared to homogeneous schemes. It Stores small number of keys into the L-sensor.

4.3.2.2 Key Management Scheme Based on Random Key Distribution [3]: This scheme pre-load only one secrete key of key pool into L-sensor generate new key by applying one way function on key and its ID. H-sensors are pre-loaded with all keys of key pool along with a special master key for inter cluster communication. With Hello message L-sensor and H-sensor find their neighbors and then L-sensor sends the list of its neighbor to the H-sensor. After that H-sensor generates the data encryption key and integrity check key and forwards the MAC check along with nonce. After receiving the nonce L-sensor calculates the data encryption key and integrity check key. After setting the keys, Ha generates the shared pair-wise keys between a node and its neighbors. This scheme significantly reduces the storage requirement as compared to random key pre-distribution schemes.

4.3.2.3 A New Key Management Scheme [18]: During cluster formation this scheme scheme obtains the distance between the cluster head and other sensor nodes. This

scheme uses the concepts of level, as each level has separate seed used for deriving the new keys that are only used in that level and neighboring level. The key pool consists of base key and derived keys. Derived key are hash of base keys with different seeds. In pre-distribution phase, scheme stores only base key and not derived key. It stores randomly k keys into each sensor and c base keys into each H-sensor where c>>k. Pair-wise key between sensor and base station is stored in L-sensor and will be used for authentication purpose. Each CH sends location to base station by GPS and obtains the maximum distance a point can have in his cluster. In this scheme, the number of base keys has effect on connectivity between nodes and number of seeds has effect on resiliency against node capture.

Table 2. Comparison of key distribution schemes

Scheme	Pre-distribution	Deployment knowledge	Hetero-geneity	Features	Drawback
Trusted serevr [11]	No	No	No	1.Good Resilience to attack 2.Low memory required.	1.Require third party 2.Trust issue
Self enforcing [13]	No	No	No	1.Easy node addition. 2.Good Resilience to attack. 3.Most secure	1.High computational power 2.Large memory
One master key [11]	Yes	No	No	1.Easy node addition 2.Low Memory required	1.Bad Resilience to attack
N-1 pair-wise secrete key [11]	Yes	No	No	1.Better Resiliecne to attack	1. Node addition Difficult 2.Large memory required
Basic scheme [14]	Yes	No	No	1.Good Resilience to attack. 2.Easy Node addition.. 3.Simple method	1.Large Memory required
q-composite scheme [10]	Yes	No	No	1.More resilience to attack 2.Support Large network	1.Large memory required
Miltipath Key reinforcement [10]	Yes	No	No	1. Strongly secure links 2.Good resilience agianst node capture.	1.Add overhead key estabilishment traffic. 3.Large Memory required.
Random pair-wise scheme [10]	Yes	No	No	1.Provides node-to-node authentication. 2.Good resilince aginst node attack.	1.Large Memory required. 2.Scalable to some extend.
ABAB [15]	Yes	Yes	No	1.Very simple and flexible. 2.Less secure 3.Very much scalable.	1.Required prior deployment knowledge 2.Large Memory required
ABCD [15]	Yes	Yes	No	1.More secure than ABAB. 2.Highly scalable. 3.Requires less communicational cost.	1.Complicated than ABAB. 2.Required Prior deployment knowledge.
Routing driven [17]	Yes	No	Yes	1.Highly secure and scalable 2.Low memory storage.	1.Sensor node has to send its location through GPS.
Key mgnt. scheme based on random key distribution [3]	Yes	No	Yes	1.Better resillience to attack. 2.Low memory required. 3.Low computational cost. 4.Addition of node is easy.	1.Scalable to some extend. 2.H sensor exhuastion may occur with large network
A new key management scheme [18]	Yes	No	Yes	1.Reduces tradeoff between resilience and connectivity. 2.Require low memory.	1.Sensor node has to send its location through GPS.

Table 2 gives the comparison of the different key distribution schemes.

In homogeneous wireless sensor environment all sensor nodes have to store the large number of keys which may lead poor resilience to node capture attack. In heterogeneous wireless sensor environment the given schemes [3, 17, and 18] uses the

GPS unit to communicate to location to the cluster head. This adds additional overhead to the network. So such a hybrid key distribution scheme must be proposed which can be used for long lifespan and scalable network without additional overhead of GPS unit.

5 Conclusions

In wireless sensor network, encryption and authentication services are based on the operations involving keys. So energy efficient key distribution is an important issue. In this article we present a comprehensive survey of key distribution schemes in wireless sensor network. They have common objective of trying to distribute the keys to all sensor node with efficient use of the memory, computation power with consideration of the security aspect.

Overall, key distribution techniques can be classified on network structure as homogeneity, pre-distribution of keys and deployment knowledge basis.

Finally, we have given the comparison of all the key distribution schemes. Although, many of the techniques look promising, there are still many challenges that need to be solved in future key distribution scheme in wireless sensor network like large scalability and lifespan of the wireless sensor network.

References

1. Yong, W., et al.: A survey of security issues in wireless sensor networks. IEEE Communications Surveys & Tutorials 8, 2–23 (2006)
2. Al-Karaki, J.N., Kamal, A.E.: Routing techniques in wireless sensor networks: a survey. IEEE Wireless Communications 11, 6–28 (2004)
3. Kausar, F., et al.: Key Management and Secure Routing in Heterogeneous Sensor Networks. In: IEEE International Conference on Wireless and Mobile Computing, Networking and Communications, WIMOB 2008, pp. 549–554 (2008)
4. Habib, A.: Sensor network security issues at network layer. In: 2nd International Conference on Advances in Space Technologies, ICAST 2008, pp. 58–63 (2008)
5. Karlof, C., Wagner, D.: Secure routing in wireless sensor networks: attacks and countermeasures. In: Proceedings of the First IEEE, International Workshop on Sensor Network Protocols and Applications, pp. 113–127 (2003)
6. Huijuan, D., et al.: Selective forwarding attack detection using watermark in WSNs. In: ISECS International Colloquium on Computing, Communication, Control, and Management, CCCM 2009, pp. 109–113 (2009)
7. Newsome, J., et al.: The Sybil attack in sensor networks: analysis & defenses. In: Third International Symposium on Information Processing in Sensor Networks, IPSN 2004, pp. 259–268 (2004)
8. Hu, Y.C., et al.: Packet leashes: a defense against wormhole attacks in wireless networks. In: Twenty-Second Annual Joint Conference of the IEEE Computer and Communications, INFOCOM 2003, vol. 3, pp. 1976–1986. IEEE Societies (2003)
9. Kaiping, X., et al.: Security improvement on an efficient key distribution mechanism for large-scale Wireless Sensor Network. In: 2nd International Conference on Anti-Counterfeiting, Security and Identification, ASID 2008, pp. 140–143 (2008)

10. Haowen, C., et al.: Random key predistribution schemes for sensor networks. In: Proceedings of 2003 Symposium on Security and Privacy, pp. 197–213 (2003)
11. Wenliang, D., et al.: A key management scheme for wireless sensor networks using deployment knowledge. In: Twenty-Third Annual Joint Conference of the IEEE Computer and Communications Societies, INFOCOM 2004, 597 p. (2004)
12. Ibriq, J., Mahgoub, I.: A Hierarchical Key Establishment Scheme forWireless Sensor Networks. In: 21st International Conference on Advanced Information Networking and Applications, AINA 2007, pp. 210–219 (2007)
13. Pathan, A.S.K., Choong Seon, H.: Feasibility of PKC in resource-constrained wireless sensor networks. In: 11th International Conference on Computer and Information Technology, ICCIT 2008, pp. 13–20 (2008)
14. Eschenauer, L., Gligor, V.D.: A key-management scheme for distributed sensor network. In: 9th ACM Conference on Computer and Communications Security, Washington DC, pp. 41–47 (2002)
15. Tasci, S.E., et al.: Simple and Flexible Random Key Predistribution Schemes for Wireless Sensor Networks Using Deployment Knowledge. In: International Conference on Information Security and Assurance, ISA 2008, pp. 488–494 (2008)
16. Lu, K., et al.: A framework for distributed key management schemes in heterogeneous wireless sensor networks. In: 25th IEEE International Performance, Computing, and Communications Conference, IPCCC 2006, p. 7, 520 (2006)
17. Xiaojiang, D., et al.: A Routing-Driven Key Management Scheme for Heterogeneous Sensor Networks. In: IEEE International Conference on Communications, ICC 2007, pp. 3407–3412 (2007)
18. Banihashemian, S., Bafghi, A.G.: A new key management scheme in heterogeneous wireless sensor networks. In: 2010 The 12th International Conference on Advanced Communication Technology (ICACT), pp. 141–146 (2010)

An Integrated Intrusion Detection System for Credit Card Fraud Detection

M. Sasirekha, I. Sumaiya Thaseen, and J. Saira Banu

VIT University, Vellore -632014, TamilNadu, India

Abstract. Computer security is one of the key areas where lot of research is being done. Many intrusion detection techniques are proposed to ensure the network security, protect network resources and network infrastructures. Intrusion detection systems (IDS) attempt to detect attacks by gathering network data and analyze the information from various areas to identify the possible intrusions. This paper proposes an IDS combining three approaches such as anomaly, misuse and decision making model to produce better detection accuracy and a decreased false positive rate. The integrated IDS can be built to detect the attacks in credit card system using Hidden Markov approach in the anomaly detection module. The credit card holder's behaviours are taken as attributes and the anomalous transactions are found by the spending profile of the user. The transactions that are considered to be anomalous or abnormal are then sent to the misuse detection system. Here, the transactions are compared with predefined attack types and then sent to the decision making model to classify it as known/unknown type of attack. Finally, the decision-making module is used to integrate the detected results and report the types of attacks in credit card system. As abnormal transactions are analyzed carefully in each of the module, the fraud rate is reduced and system is immune to attacks.

Keywords: Intrusion detection, Anomaly detection, Misuse detection, Hidden Markov Model.

1 Introduction

The amount of online shopping is increasing day by day and millions of people are using the online services to fulfil their needs. As a result a large number of credit card transactions are being carried out in the net. These credit card transactions are vulnerable to malicious intruders attempting to negotiate on the integrity, confidentiality or any resource availability. The spending pattern of the card holder has to be analysed to determine if any inconsistency occurs in comparison with the usual pattern. Hence an Intrusion Detection System (IDS) is proposed to detect the attackers by analyzing the spending profile of the customer along with the type of purchase. Many fraud detection systems have been proposed using data mining and neural network approaches but an IDS combining such as anomaly detection, misuse detection and decision making model has not been developed for a credit card fraud system. As the system is of

N. Meghanathan et al. (Eds.): Advances in Computing & Inform. Technology, AISC 176, pp. 55–60.
springerlink.com

hybrid nature, it attempts to increase the detection attack rate and also reduce the number of false positives which is of major concern in any IDS.

The rest of the paper is organized as follows. In section 2 we summarize the relevant work on intrusion and fraud detection systems. Section 3 discusses the detailed description of the proposed system. The experimental results and snapshots of anomaly detection module are discussed in section 4 and 5. Section 6 concludes the paper.

2 Related Work

Many anomaly IDS have been proposed in the literature. We briefly discuss some of the proposed solutions. Ghosh and Reilly [10] proposed a neural network for credit card fraud detection. Stolfo et al. [11] [12] developed a credit card fraud detection system (FDS) using meta learning techniques to study models of fraudulent credit card transactions. Performance metrics like True Positive—False Positive (TP-FP) spread and accuracy have been defined by them. The BOAT adaptive method was proposed by sherly et al [15]. Each individual transaction amount depends on the purchase of the corresponding type of item. Standard performance metrics, True Positive (TP) and False Positive (FP) are used to characterize the effectiveness of the system. Then the fraudulent transactions are identified. The difficulty with most of the above specified approaches is that they need labelled data for both real as well as fraudulent transactions to train the classifiers. In contrast, we present a Hidden Markov Model (HMM)-based credit card FDS, which does not need fraud signatures and yet it is able to identify frauds by considering the spending habit of the credit card holder.

Ourston et al. [13] have proposed the application of HMM in identifying multistage network attacks. Hoang et al. [14] present a innovative method to analyze series of system calls for anomaly detection using HMM. Another major advantage of the HMM-based approach is a severe decrease in the number of False Positives (FPs)—transactions detected as malicious by a FDS although they are actually genuine. Hence with the tremendous increase in attacks, there is a need to design an Intrusion Detection System that secures the credit card sector.

3 Proposed System

The proposed system uses the Hidden Markov Model to identify fraudulent transactions in the anomaly detection module. HMM is advantageous over other statistical approaches because it effectively reduces the false positive rate which is an important metric to measure the performance of Intrusion Detection System. The fraudulent transactions identified in the anomaly detection module are sent to Misuse detection module to identify the type of fraud. The role of anomaly module is to identify the fraud and the role of misuse module is to classify the fraud. Then the results are sent to decision making model.

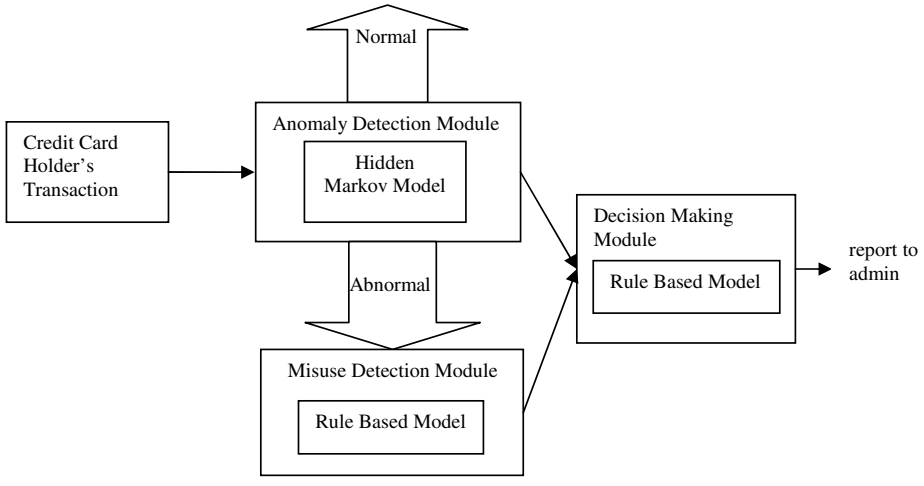


Fig. 1. Proposed Architecture of Integrated IDS

3.1 Anomaly Detection Module

The HMM model is mainly used to identify the false positive attacks. The false positive attack is the number of normal transactions that are identified as anomalous. The types of purchase are the hidden states. The new transaction is classified as anomalous or normal transaction based on the transaction history. Using the HMM [2], the user is grouped based on his spending profile. The false positive rate is the number of normal transactions identified as anomalous. The False Positive Rate (FPR) is identified using the following formula,

FPR=(Number of anomalous transactions/Number of normal transactions)* 100%

3.2 Misuse Detection Module

Misuse detection is an effective approach to handle attacks that are known by the system. When the particular type of attack is identified, the result is sent to Decision Making Module. The attacks are Cross-site, SQL, Path Traversal, etc can be identified using this module.

3.3 Decision Making Module

The decision making module provides the result as attack if both anomaly and misuse detection module identifies it as an attack. The Rule-based method is used for Decision making module. The rules are

- If anomaly detection model detects a fraud and misuse detection model does not detect the same fraud, then the detected fraud is not a fraud and it is an erroneous classification.
- If anomaly detection model detects a fraud and misuse detection model does detects the same fraud, then the detected fraud is a fraud and the fraud mode is classified.

- If anomaly detection model detects a fraud and misuse detection model finds it to be an unknown fraud, then the detected fraud is a new fraud.

4 Experimental Results

Initially the users are grouped based on his spending habit. The low range is between 0 and 5000, medium between 5000 and 12500 and high above 12500. The observation symbol for low cluster is denoted by 'l' and medium by 'm' and high by 'h'. The sequence length of 5-10 is used to identify the fraudulent transaction. The fraudulent transaction identification is as follows.

Low=(0-5000), Medium=(5000-12500), High=(above 12500).

The results below specify how fraudulent transactions are identified in each spending profile cluster. Calculations have been shown only for high spending profile. Low and medium profile can be calculated in the similar manner.

High Spender Profile(HS)

α_i: Transaction Sequence={15000,18000,6000,200,25000}. The state sequence is $\{s_3,s_1,s_2,s_3,s_1\}$and the observation sequence is {h,h,m,l,h}.

Table 1. Probability of observation sequence based on past history in high spending profile

	1	2	
α_1	1/3	0	1/6
α_2	0.16666666	0	0
α_3	0	0.1666667	0
α_4	0	0	0.08333333

5 Screen Shots

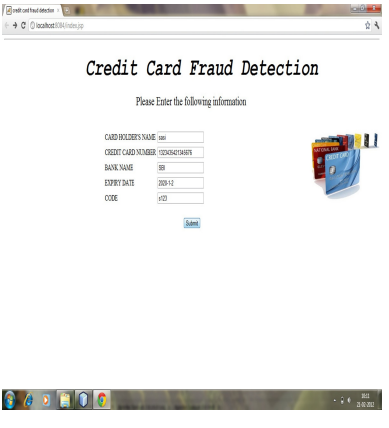


Fig. 2. User Login

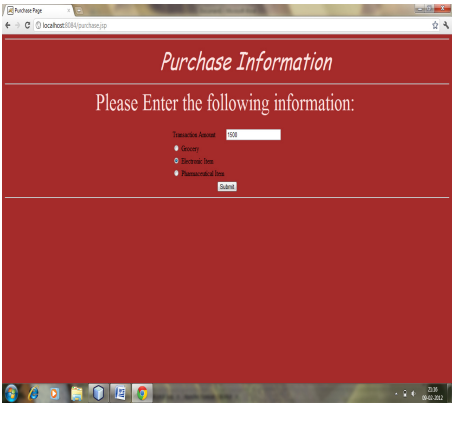


Fig. 3. User's Purchase

Fig. 4. Estimating alpha2 using forward backward algorithm

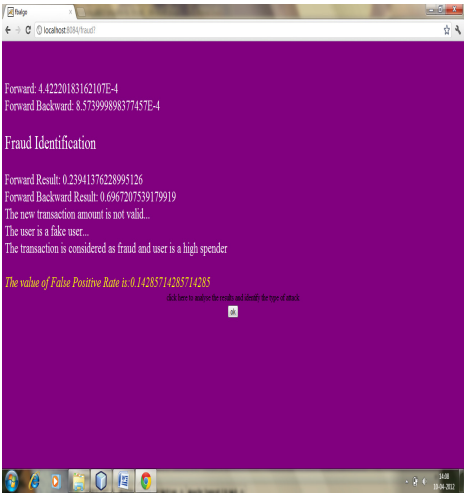


Fig. 5. Fraud Identification

6 Conclusion

This paper proposes an integrated intrusion detection system for credit card fraud detection by combining three approaches anomaly, misuse and decision making models. Anomaly detection module is implemented using Hidden Markov approach classifies the credit card transaction as normal or abnormal based on the threshold of the spending profile of the credit card user. Comparative studies reveal that the HMM technique results in higher accuracy over a wide variation in the input data and the proposed system can be scalable for handling large transaction data. The false positive rate (FPR) is calculated. Second, the Misuse detection module screens the abnormal transactions for type detection. The main aim of the attacker is to steal the details of the authorised user by using XSS and SQL Injection attack. Finally the results of the two detection modules are integrated by the decision making module to determine the fraud, type of fraud and return the same to the administrator for necessary action. The experimental results discussed are of anomaly detection module. Our future work will integrate the results of the anomaly module with the misuse module to produce effective detection accuracy.

References

1. Wang, S.-S., Yan, K.-Q., Wang, S.-C., Liu, C.-W.: An Integrated Intrusion Detection System for Cluster-based Wireless Sensor Networks (2011), doi:10.1016/j.eswa.2011.05.076
2. Srivastava, A., Kundu, A., Sural, S., Majumdar, A.K.: Credit Card Fraud Detection Using Hidden Markov Model. IEEE Transactions on Dependable and Secure Computing 5(1) (January-March 2008), doi:10.1109/TDSC.2007.70228