2014 IEEE Conference on Communications and Network Security

(CNS 2014)

San Francisco, California, USA
29-31 October 2014

IEEE Catalog Number: CFP14CNM-POD
ISBN: 978-1-4799-5891-7

Workshop on Cognitive Radio and Electromagnetic Spectrum Security (CRESS 14): 2014 IEEE Conference on Communications and Network Security (CNS): Workshop on Cognitive Radio and Electromagnetic Spectrum Security (CRESS'14) - Program

Welcome Address / Workshop Co-Chairs' Introduction

Session I

Session II

Keynote Presentation

Session III

Session IV

M2MSec'14: Workshop on Security and Privacy in Machine-to-Machine Communications (M2MSec'14) - Program

Welcome and committee

Opening Remarks

Keynote

Securing the Internet of Things

Abstract: The Internet of Things already surrounds us and is making our lives better in both small and large ways. Toll tags, smart thermostats, and automated industrial monitoring and control systems are just the beginnings of an Internet of Things world. These are the early touch, easily quantified benefits applications. However, the future of the Internet of Things goes beyond these simple applications to a world of truly pervasive computers and smart things that provide us a sixth sense of our world (both nearby and around the globe) and, ultimately, shape the way we think and interact with both physical and virtual objects. As a result of the potential impacts that the Internet of Things will have on how we live our lives, it has become a critical interdisciplinary research field among communications, silicon design, AIDC, data science and systems engineering communities to name just a few. Despite its common popular name, the Internet of Things is defined differently among researchers and developers from different fields. These inconsistencies, or different views of the Internet of Things, lead to a number of technical benefits; however, their integration and deployment will introduce new threats to the security and privacy of users. In this talk, the topic of the Internet of Things will be explained in a new bottom-up manner with some of the main challenging issues including networking, data management and analysis, and security and privacy of smart thing users will be described. Security and privacy are the ultimate gate keepers to the utopian world envisioned with the large scale adoption and use of smart things. As such, the integration of appropriate security mechanisms into the next generation of Internet of Things enabled objects will determine whether smart things are adopted in the near future or their use is left to a distant future.

Networking Break

Session 1 (Secure Smart Environments)

Securing Smart Home: Technologies, Security Challenges, and Security Requirements
Changmin Lee (George Washington University, USA)
pp. 67-72

Integration and Evaluation of Intrusion Detection for CoAP in Smart City Applications
Jana Krimmling (IHP, Germany); Steffen Peter (University of California, Irvine, USA)
pp. 73-78

An Experimental Study of Security and Privacy Risks with Emerging Household Appliances
Sukhvir Notra and Muhammad Siddiqi (University of New South Wales (UNSW), Australia); Hassan Habibi Gharakheili and Vijay Sivaraman (University of New South Wales, Australia); Roksana Boreli (National ICT Australia & University of NSW, Australia)
pp. 79-84

Lunch Break

Panel

Machine-to-Machine (M2M) Security and Privacy: Challenges and Opportunities

List of Panel Members: Geoff Brown (Machine-To-Machine Intelligence (M2Mi) Corporation) Qi Chai (Google) David Kravitz (IBM) Vijay Sivaraman (University of New South Wales)

Networking Break

Session 2 (Secure Data Communications)

Practical and Secure Machine-to-Machine Data Collection Protocol in Smart Grid
Suleyman Uludag (The University of Michigan - Flint, USA); King-Shan Lui (The University of Hong Kong, Hong Kong); Wenyu Ren and Klara Nahrstedt (University of Illinois at Urbana-Champaign, USA)
pp. 85-90

Identity-Based Protocol Design Patterns for Machine-to-Machine Secure Channels
Francisco Corella and Karen Lewison (Pomcor, USA)
pp. 91-96

Concluding Remarks

Wokshop on Physical layer Methods for Wireless Security (PhySec 14): 2014 IEEE Conference on Communications and Network Security (CNS): Wokshop on Physical-layer Methods for Wireless Security (PhySec'14) - Program

Opening Remark

Keynote 1

PMWS1

RF-Fingerprint Based Authentication: Exponents and Achievable Rates
Onur Gungor and Can Emre Koksal (The Ohio State University, USA)
pp. 97-102

The Security of Link Signature: A View from Channel Models
Xiaofan He (North Carolina State University, USA); Huaiyu Dai (NC State University, USA); Yufan Huang (North Carolina State University, USA); Dong Wang (Southeast University, P.R. China); Wenbo Shen and Peng Ning (North Carolina State University, USA)
pp. 103-108

On Secure Communication over Multiple Access Wiretap Channels under Channel Uncertainty
Rafael F. Schaefer and H. Vincent Poor (Princeton University, USA)
pp. 109-114

Parity Modifications and Stopping Sets in High-Rate Codes for Physical-Layer Security
Willie K Harrison and Parker Boyce (University of Colorado Colorado Springs, USA)
pp. 115-120

On the Fading Gaussian Wiretap Channel with Statistical Channel State Information at Transmitter
Pin-Hsun Lin and Eduard Jorswieck (TU Dresden, Germany)
pp. 121-126

Uniform Distributed Source Coding for the Multiple Access Wiretap Channel
Remi A Chou (Georgia Institute of Technology, USA); Matthieu Bloch (Georgia Institute of Technology & Georgia Tech Lorraine, France)
pp. 127-132

Keynote 2

PMWS2

MCR Decoding: A MIMO Approach for Defending Against Wireless Jamming Attacks
Wenbo Shen, Peng Ning and Xiaofan He (North Carolina State University, USA); Huaiyu Dai (NC State University, USA); Yao Liu (University of South Florida, USA)
pp. 133-138

Relay-based Secret Key Generation in LTE-A
Kan Chen and Bala Natarajan (Kansas State University, USA); Steve Shattil (De part ment 13, LLC, USA)
pp. 139-144

Signal Alignment for Secure Underwater Coordinated Multipoint Transmissions
Chaofeng Wang, Zhaohui Wang and Saeid Nooshabadi (Michigan Technological University, USA)
pp. 145-150

Portability of an RF Fingerprint of a Wireless Transmitter
Saeed Ur Rehman (Unitec Institute of Technology, New Zealand)

pp. 151-156

Concluding Remarks

Program

K.1: Opening Session and Keynote 1

Security and Privacy of Information Sources: Information Theoretic Insights

Abstract:

The ubiquity of technologies such as wireless communications and on-line data repositories has created new challenges in information security and privacy. Information theory provides fundamental limits that can guide the development of methods for addressing these challenges. This talk will review two areas to which these ideas have been applied: wireless physical layer security, which examines the ability of the radio channel to provide secrecy in data transmission; and utility-privacy tradeoffs of data sources, which quantify the safety of confidential information contained in such sources while still providing a measurable benefit to legitimate information consumers. Some recent results and applications will also be discussed.

BIO:

H. Vincent Poor is the Michael Henry Strater University Professor at Princeton University, where he is also the dean of the School of Engineering and Applied Science. His research interests are in wireless communications and related fields such as social networks and smart grid. An IEEE Fellow, Dr. Poor is a member of the National Academy of Engineering and the National Academy of Sciences, and a foreign member of the Royal Society. He received the ComSoc's Marconi and Armstrong Awards in 2007 and 2009, respectively. Recent recognition of his work includes the 2014 URSI Booker Gold Medal, and honorary doctorates from several universities.

A.1: Internet Security I

The Drunk Motorcyclist Protocol for Anonymous Communication
Adam Young (Cryptovirology Labs, USA); Moti Yung (CertCo Inc, USA)
pp. 157-165

Modelling IP darkspace traffic by means of clustering techniques
Felix Iglesias (Technical University of Vienna, Austria); Tanja Zseby (Vienna University of Technology, Austria)
pp. 166-174

Location Verification on the Internet: Towards Enforcing Location-aware Access Policies Over Internet Clients
AbdelRahman Abdou, Ashraf Matrawy and Paul C. van Oorschot (Carleton University, Canada)
pp. 175-183

Analyzing the Dangers Posed by Chrome Extensions
Lujo Bauer (Carnegie Mellon University, USA); Shaoying Cai (Singapore Management University, Singapore); Limin Jia (CMU, USA); Tim Passaro and Yuan Tian (Carnegie Mellon University, USA)
pp. 184-192

Detecting Smart, Self-Propagating Internet Worms
Jun Li (University of Oregon, USA); Shad Stafford (Palo Alto Software, USA)
pp. 193-201

B.1: Wireless Security I

Location Spoofing Attack and Its Countermeasures in Database-Driven Cognitive Radio Network
Kexiong (Curtis) Zeng (Virginia Tech, USA); Sreeraksha Kondaji Ramesh (Virginia Polytechnic Institute and State University, USA); Yaling Yang (Virginia Tech, USA)
pp. 202-210

Accurate Rogue Access Point Localization Leveraging Fine-grained Channel Information
Xiuyuan Zheng, Chen Wang and Yingying Chen (Stevens Institute of Technology, USA); Jie Yang (Florida State University, USA)
pp. 211-219

Self-Healing Wireless Networks under Insider Jamming Attacks
Longquan Li (Penn State University, USA); Sencun Zhu (The Pennsylvania State University, USA); Don Torrieri (US Army Research Laboratory, USA); Sushil Jajodia (George Mason University, USA)

pp. 220-228

NRE: Suppress Selective Forwarding Attacks in Wireless Sensor Networks
Biru Cui and Shanchieh Jay Yang (Rochester Institute of Technology, USA)
pp. 229-237

CETAD: Detecting Evil Twin Access Point Attacks in Wireless Hotspots
Hossen Mustafa and Wenyuan Xu (University of South Carolina, USA)
pp. 238-246

P.1: Panel I: "Networks Security: The Triumph and Tribulation"

Moderator: Mukesh Singhal, University of California-Merced, USA

Panelist:

Wenjing Lou, Virginia Tech, USA Sushil Jajodia, George Mason University, USA Neeraj Suri, Technical University of Darmstadt, Germany Aziz Mohaisen, VeriSign, USA

Abstract:

Computer networks are integral part of any computer system and as a result of technological advancements over the last two decades, computer networks of today have highly complex architectures,consisting of highly diverse set of components: Nodes comprise of diverse computing devices, sensors, smart phones, mobile units embedded on a vehicle, UAVs, ammunition, or soldiers; networks are networks of fixed wired networks, cellular networks, and wireless ad hoc networks; and communication links can be copper, optical, radio or satellite links. These can be highly dynamic 3-D networks and span ground, air, and under-water. Securing such networks against cyber attacks is a major challenge because these networks have a large attack surface and operate in large, highly dynamic environments with severe constraints on the computational devices, battery power, limited and noisy wireless bandwidth, and unpredictable node mobility.

Challenges in securing today's complex computer networks include adversary and attack modeling, risk analysis, risk management, attack detection, attack prevention, damage analysis and recovery from attacks, development of protocols and cryptographic methods to deal with security threats and formal methods to prove the security of a network. To comprehensively and effectively address these challenges, we have assembled a panel of excellent researchers with complementary expertise to effectively cover all important aspects of securing computer networks of today and tomorrow.

A.2: Intrusion Detection

Towards Effective Feature Selection in Machine Learning-Based Botnet Detection Approaches
Elaheh Biglar Beigi Samani, Hossein Hadian Jazi, Natalia Stakhanova and Ali A. Ghorbani (University of New Brunswick, Canada)
pp. 247-255

Security Configuration Analytics Using Video Games
Mohammed Noraden Alsaleh (UNC Charlotte, USA); Ehab Al-Shaer (University of North Carolina Charlotte, USA)
pp. 256-264

An Evasion and Counter-Evasion Study in Malicious Websites Detection
Li Xu, Zhenxin Zhan, Shouhuai Xu and Keying Ye (University of Texas at San Antonio, USA)
pp. 265-273

Exploiting Altruism in Social Networks for Friend-to-Friend Malware Detection
Matthew Probst (VMWare, USA); Jun Cheol Park (Adobe, USA); Sneha Kumar Kasera (University of Utah, USA)
pp. 274-282

Chatter: Exploring Classification of Malware based on the Order of Events
Aziz Mohaisen and Andrew G. West (Verisign Labs, USA); Allison Mankin (U.S. National Science Foundation, USA); Omar Alrawi (Qatar Foundation, USA)
pp. 283-291

B.2: Security and Privacy in Emerging Networks

Two-tier Data-Driven Intrusion Detection for Automatic Generation Control in Smart Grid
Muhammad Qasim Ali (University of North Carolina Charlotte, USA); Reza Yousefian (UNC Charlotte, USA); Ehab Al-Shaer (University of North Carolina Charlotte, USA); Sukumar Kamalasadan (University of North Carolina at Charlotte, USA); Quanyan Zhu (New York University, USA)
pp. 292-300

Sensory Channel Threats to Cyber Physical Systems: A Wake-up Call
A. Selcuk Uluagac (Florida International University & Electrical and Computer Engineering, USA); Venkatachalam Subramanian and Raheem Beyah (Georgia Institute of Technology, USA)
pp. 301-309

iKUP Keeps Users' Privacy in the Smart Grid
Fábio Borges (Technische Universität Darmstadt - Telecooperation Lab & CASED - Center for Advanced Security Research Darmstadt, Germany); Leonardo A. Martucci (Karlstad University, Sweden)
pp. 310-318

Secret Message Sharing Using Online Social Media
Jianxia Ning (University of California, Riverside, USA); Indrajeet Singh and Harsha V. Madhyastha (UC Riverside, USA); Srikanth V. Krishnamurthy (University of California, Riverside, USA); Guohong Cao (The Pennsylvania State University, USA); Prasant Mohapatra (University of California, Davis, USA)
pp. 319-327

VirtualFriendship: Hiding interactions on Online Social Networks
Filipe Beato (KU Leuven, Belgium); Mauro Conti (University of Padua, Italy); Bart Preneel (KU Leuven, Belgium); Dario Vettore (University of Padua, Belgium)
pp. 328-336

K.2: Keynote 2

Introducing the Samsung KNOX

Abstract:

The industry has been looking for a trustworthy mobile platform as smart phones and tablets are increasingly a part of people's daily life. I was fortunate to join the Samsung KNOX team and lead the R&D engineers to build the Samsung KNOX platform for mobile devices. As one of the most trusted mobile platforms today, Samsung KNOX has won a number of recognitions for its security features, such as US DoD STIG, Common Criteria MDFPP certification, and UK Government CESG EUD Guidance. In this talk, we will present some key KNOX features, including SE Android, application container, data-at-rest protection, and TIMA features such as trusted boot, remote attestation, key store, Client Certificate Manager (CCM), and real-time kernel protection.

BIO:

Dr. Peng Ning is Vice President, Enterprise Security at Samsung Research America, leading the Samsung KNOX R&D team in Santa Clara, CA, and acting as the Chief Security Architect for Samsung KNOX. His team has successfully developed and/or commercialized multiple mobile security features for Android, including TrustZone-based Integrity Measurement Architecture (TIMA), which offers real-time kernel protection, trusted boot, remote attestation, TrustZone-based key store and client certificate management, as well as smart card support, SE for Android, application container, VPN framework, and universal MDM support, all available through Samsung KNOX. More information on Samsung KNOX can be found at http://www.samsungknox.com.

Peng is currently on leave from North Carolina State University, where he is Professor in the Department of Computer Science in College of Engineering. He joined NC State University in August 2001 after he graduated from George Mason University with a PhD degree in Information Technology. Peng Ning received a BS degree in Information Science and an ME degree in Communication and Electronic System in 1994 and 1997, respectively, both from University of Science and Technology of China. Peng is a recipient of NSF CAREER award. His research has been supported by the National Science Foundation (NSF), the Army Research Office (ARO), the Advanced Research and Development Activity (ARDA), IBM Open Collaboration Research (OCR) program, SRI International, and the NCSU/Duke Center for Advanced Computing and Communication (CACC). He was elected the Secretary/Treasurer of the ACM Special Interest Group on Security, Auditing and Control (SIGSAC) in 2009. He served/or is serving on the editorial boards of IEEE Transactions on Dependable and Secure Computing, ACM Transactions on Sensor Networks, Journal of Computer Security, Ad-Hoc Networks, Ad-Hoc & Sensor Networks: an International Journal, International Journal of Security and Networks, and IET Proceedings Information Security. Peng Ning served as the Program Chairs or Co-Chairs of NDSS'13, ESORICS'09, ACM SASN'05 and ICICS'06, the General Chair of ACM CCS'07 and CCS'08, and Program Vice Chair for ICDCS'09 & '10--Security and Privacy Track. He was a Steering Committee member of ACM CCS and a founding Steering Committee member of ACM WiSec. He has served on the organizing committees or program committees for over fifty technical conferences or workshops related to computer and network security. Peng Ning is a senior member of the ACM, the ACM SIGSAC, and a member of the IEEE and the IEEE Computer Society.

A.3: Security and Privacy in Cloud Computing

A Tale of Two Clouds: Computing on Data Encrypted under Multiple Keys
Boyang Wang and Ming Li (Utah State University, USA); Sherman S. M. Chow (Chinese University of Hong Kong, Hong Kong); Hui LI (Xidian University, P.R. China)
pp. 337-345

Towards Verifiable File Search on the Cloud
Fei Chen (Shenzhen University & The Chinese University of Hong Kong, P.R. China); Tao Xiang (Chongqing University, P.R. China); Xinwen Fu (University of Massachusetts Lowell, USA); Wei Yu (Towson University, USA)
pp. 346-354

Enabling Trusted Data-Intensive Execution in Cloud Computing
Ning Zhang (Virginia Tech & Raytheon Company, USA); Wenjing Lou (Virginia Tech, USA); Xuxian Jiang (NC State, USA); Thomas Hou (Virginia Tech, USA)
pp. 355-363

Integrity for Distributed Queries
Sabrina DeCapitanidiVimercati (Universita` di Milano, Italy); Sara Foresti (Università degli Studi di Milano, Italy); Sushil Jajodia (George Mason University, USA); Giovanni Livraga (Università degli Studi di Milano, Italy); Stefano Paraboschi (University of Bergamo, Italy); Pierangela Samarati (Universita' degli Studi di Milano, Italy)
pp. 364-372

Lightweight (k,n)-File Sharing Scheme for Distributed Storages with Diverse Communication Capacities
Young-Hoon Park (Seoul National University & Brain Korea 21, Korea); Eun-Dong Lee (Seoul National University, Korea); Seung-Woo Seo (Seoul National University, Korea, Korea)
pp. 373-381

B.3: Internet Security II

An Optimistic Certified E-mail Protocol for the Current Internet E-mail Architecture
Gerard Draper Gil (University of the Balearic Islands, Spain); Pep-Lluis Ferrer (Universitat de les Illes Balears, Spain); Maria Francisca Hinarejos (University of the Balearic Islands, Spain); Arne Tauber (Graz University of Technology, Austria)
pp. 382-390

Attribute-based Access Control for ICN Naming Scheme
Bing Li, Ashwin Prabhu Verleker, Dijiang Huang and Zhijie Wang (Arizona State University, USA); Yan Zhu (University of Science & Technology Beijing, P.R. China)
pp. 391-399

Mitigating Eclipse Attacks in Peer-to-Peer Networks
Daniel Germanus (Technical University of Darmstadt, Germany); Stefanie Roos and Thorsten Strufe (TU Dresden, Germany); Neeraj Suri (Technische Universitaet Darmstadt, Germany)
pp. 400-408

Reroute on Loop in Anonymous Peer-to-Peer Content Sharing Networks
Guanyu Tian and Zhenhai Duan (Florida State University, USA); Todd Baumeister (University of Hawaii at Manoa, USA); Yingfei Dong (University of Hawaii, USA)
pp. 409-417

Identifying Global Hot Items in Distributed Dynamic Data Streams
Wenji Chen and Yong Guan (Iowa State University, USA)
pp. 418-426

P.2: Panel II: "Wireless Security: Securing the Lower and Higher Layers"

Moderator: Wenyuan Xu, University of South Carolina, USA

Panelist:

David Wagner, University of California at Berkeley, USA Yingying Chen, Stevens Institute of Technology, USA Walid Saad, Virginia Tech, USA Jesse Walker, Intel, USA

Abstract:

Gone are the days of secure routing protocols and such, instead there has been a shift towards researching wireless security at the higher and lower layers. This is particularly evident given the significant amount of research being done in smartphone security and privacy, as well as the vast amount of research being initiated in the area of "physical layer security." This panel will examine this observation and touch upon diverse topics such as mobile OS security, usable security, location security and privacy, etc. In the process of the discussion, the panel intends to address the high-level question "Where has the middle of the stack gone in wireless security research?".

A.4: Wireless Security II

LAPWiN: Location-Aided Probing for Protecting User Privacy in Wi-Fi Networks
Yu Seung Kim, Yuan Tian, Le T Nguyen and Patrick Tague (Carnegie Mellon University, USA)
pp. 427-435

TouchIn: Sightless Two-factor Authentication on Multi-touch Mobile Devices
Jingchao Sun (Arizona State University, USA); Rui Zhang (University of Hawaii, USA); Jinxue Zhang and Yanchao Zhang (Arizona State University, USA)
pp. 436-444

MagPairing: Exploiting Magnetometers for Pairing Smartphones in Close Proximity
Rong Jin (University of Michigan - Dearborn, USA); Liu Shi (University of Michigan-Dearborn, USA); Kai Zeng (George Mason University, USA); Amit Pande (University of California Davis, CA, USA); Prasant Mohapatra (University of California, Davis, USA)
pp. 445-453

Uncooperative Localization Improves Attack Performance in Underwater Acoustic Networks
Xiaoyan Lu (University of Conneticut, USA); Michael Zuba, Jun-Hong Cui and Zhijie Shi (University of Connecticut, USA)
pp. 454-462

B.4: Information Theoretical Security

Multi-trapdoor Hash Functions and their Applications in Network Security
Santosh Chandrasekhar (University of California, Merced, USA); Mukesh Singhal (University of California at Merced, USA)
pp. 463-471

Manipulating the Attacker's View of a System's Attack Surface
Massimiliano Albanese (George Mason University, USA); Ermanno Battista (University of Naples Federico II, Italy); Sushil Jajodia (George Mason University, USA); Valentina Casola (Università di Napoli "Federico II", Italy)
pp. 472-480

A Tunable Proof of Ownership Scheme for Deduplication Using Bloom Filters
Jorge Blasco and Agustin Orfila (Universidad Carlos III de Madrid, Spain); Roberto Di Pietro (Bell Labs, France); Alessandro Sorniotti (IBM Research, Switzerland)
pp. 481-489

IEEE CNS 2014 - Poster Session: IEEE CNS 2014 Poster Session - Program

Poster: Poster Session

Application-Layer DDoS in Dynamic Web-Domains: Building Defenses against Next-Generation Attack Behavior
Natalija Vlajic and Dusan Stevanovic (York University, Canada)
pp. 490-491

P2P Networks Monitoring Based On the Social Network Analysis and the Topological Potential
Yixin Jiang (University of Waterloo, Canada); Hong Wen (UESTC, P.R. China); Bin Wu (Tianjin University, P.R. China)
pp. 492-493

Physical Layer Assist Mutual Authentication Scheme for Smart Meter System
Yixin Jiang (University of Waterloo, Canada); Hong Wen (UESTC, P.R. China); Bin Wu (Tianjin University, P.R. China)
pp. 494-495

Radio Frequency Fingerprinting and its Challenges
Saeed Ur Rehman (Unitec Institute of Technology, New Zealand)
pp. 496-497

DroidGraph: Discovering Android Malware by Analyzing Semantic Behavior
Jonghoon Kwon, Jihwan Jeong, Jehyun Lee and Heejo Lee (Korea University, Korea)
pp. 498-499

A MIMO Cross-layer Precoding Security Communication System
Tang Jie (UESTC in China, P.R. China); Huan-huan Song and Fei Pan (University of Electronic Science and Technology of China, P.R. China); Hong Wen (UESTC, P.R. China); Bin Wu (Tianjin University, P.R. China); Yixin Jiang (University of Waterloo, Canada); Xiaobin Guo (EPRI, China Southern Power Grid Co. Ltd., P.R. China)
pp. 500-501

Blind Detection Approach for LDPC, Convolutional, and Turbo Codes in Non-noisy Environment
Ahmed Refaey (University of Western Ontario, Canada); Raheleh Niati (Mircom Technologies Ltd., Canada); Xianbin Wang (The University of Western Ontario, Canada); Jean-Yves Chouinard (Laval University, Canada)
pp. 502-503

A Multi-factor Re-authentication Framework with User Privacy
A. Selcuk Uluagac (Florida International University & Electrical and Computer Engineering, USA); Wenyi Liu (Georgia Tech, USA); Raheem Beyah (Georgia Institute of Technology, USA)
pp. 504-505

Guidelines for Vehicle Cyber Risks
Hirofumi Onishi (Alpine Electronics Research of America, USA)
pp. 506-507

Introducing Asymmetric DC-Nets
Fábio Borges (Technische Universität Darmstadt - Telecooperation Lab & CASED - Center for Advanced Security Research Darmstadt, Germany); Johannes Buchmann (Technische Universität Darmstadt, Germany); Max Muehlhaeuser (Technical University Darmstadt, Germany)
pp. 508-509

Ubiquitous support of multi path probing: Preventing man in the middle attacks on Internet communication
Johannes Braun (Technische Universität Darmstadt, Germany)
pp. 510-511

Towards Time-varying Classification Based on Traffic Pattern
Yiyang Shao (Tsinghua University, P.R. China); Luoshi Zhang and Xiaoxian Chen (Harbin University of Science and Technology, P.R. China); Yibo Xue (Tsinghua university, P.R. China)
pp. 512-513

Physical Integrity Check in Wireless Relay Networks
Sang Wu Kim (Iowa State University, USA)