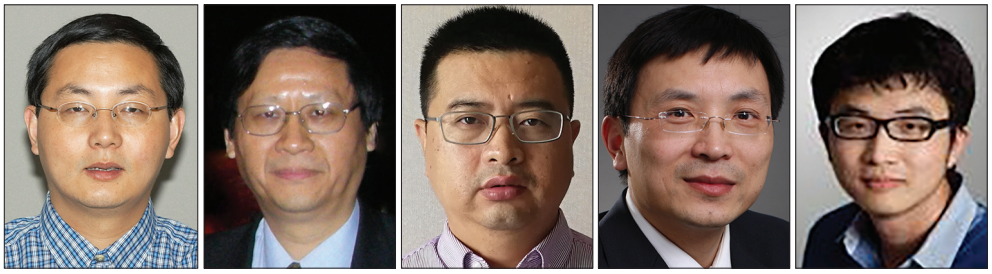
Security and Privacy in Wireless IoT



Xiaojiang Du Hsiao-Hwa Chen Liehuang Zhu Jiangli Li Zheng Chang

The articles in this Special Issue focus on security and privacy in wireless Internet of Things (IoT). IoT is a paradigm that involves networked physical objects with embedded technologies to collect, communicate, sense, and interact with the external environment through wireless or wired connections. With rapid advancements in IoT technology, the number of IoT devices is expected to surpass 50 billion by 2020, which has also drawn the attention of attackers who seek to exploit the merits of this new technology for their own benefits. There are many potential security and privacy threats to IoT, such as attacks against IoT systems and unauthorized access to private information of end users. As IoT starts to penetrate virtually all sectors of society, such as retail, transportation, healthcare, energy supply, and smart cities, security breaches may be catastrophic to the actual users and the physical world. To tackle the security challenges in the design of future wireless IoT systems, we have organized this Special Issue focusing on the security, privacy, and performance of future wireless IoT.

The response to our Call for Papers was overwhelming, with nearly 50 submissions. During the review process, each paper was assigned to and reviewed by at least three experts in the relevant areas, with a rigorous two-round review process. Thanks to the courtesy of the Editor-in-Chief, Dr. Hamid Gharavi, we were able to accept 13 excellent articles covering various aspects of security and privacy in wireless IoT. Here, we introduce them and highlight their main contributions.

In "Blockchain-Based Solutions to Security and Privacy Issues in the Internet of Things," the authors investigate several security and privacy issues in IoT and propose a framework to integrate blockchain with IoT, which can provide stronger security assurance for IoT data and various functionalities and desirable scalability including authentication, decentralized payment, and so on.

In "Active Learning for Wireless IoT Intrusion Detection," the authors present a human-in-the-loop active learning approach for wireless intrusion detection, which harnesses both the power of machine learning models and the experience of human experts to build an intrusion detection system for wireless IoT networks. Simulation studies show that the proposed approach not only can significantly decrease the labeling efforts but also allows quick update of the machine model for novel network attacks.

In "Hybrid-Augmented Device Fingerprinting for Intrusion Detection in Industrial Control System Networks," the authors propose a hybrid-augmented device fingerprinting approach by analyzing the inter-layer data response processing time and network traffic, to enhance traditional intrusion detection mechanisms in the industrial control system (ICS) network, which can effectively detect whether the ICS devices have been invaded and can fight spoofing attacks with nearly real-time performance.

In "A Castle of Glass: Leaky IoT Appliances in Modern Smart Homes," the authors analyze a set of common smart home appliances: a lightbulb, a power switch, a motion sensor, a security camera, and a home assistant — putting their security to the test to see what a home intruder could find. They discuss the security implications of these IoT devices and issues that have yet to be addressed.

In "Covert Timing Channels for IoT over Mobile Networks," the authors propose the system model of covert timing channels for IoT and investigate different kinds of construction approaches to explore the feasibility of building covert timing channels for IoT over mobile networks, which opens up several significant and refined future directions.

In "Covert Wireless Communications in IoT: Hiding Information in Interference," the authors study covert communication in noisy wireless networks, and demonstrate that introducing aggregated interference from other simultaneous transmitting nodes as noise for the adversary is actually beneficial to potential transmitters.

In "Securing Consumer IoT in Smart Home: Architecture, Challenges and Countermeasures," the authors present a novel voice liveness detection system, which leverages the wireless signals generated by IoT devices to thwart the attacks on the voice interface of smart home platforms and enhance the security of the smart home.

Privacy is an important issue for IoT devices and systems. Several articles in this Special Issue study various privacy issues in IoT systems, and they are summarized below.

In "Privacy-Preserving Authentication in Wireless IoT: Applications, Approaches, and Challenges," the authors focus on exploiting privacy-preserving authentication techniques in wireless IoT, with an emphasis on investigating the privacy-preserving authentication of wireless IoT in typical application scenarios, known as the Internet of Energy (IoE), the Internet of Vehicles (IoV), the Internet of Sensors (IoS), and machine-to-machine (M2M) communications.

In "Distributed Data Privacy Preserving in IoT Applications," the authors introduce and survey challenges from three key issues regarding aspects of data analysis, trading, and aggregation for security-critical and privacy-sensitive data, and survey-related privacy preserving techniques and approaches in the IoT.

In "Proactive Cache-Based Location Privacy Preserving for Vehicle Networks," the authors propose a strategy combining cache scheme with *K*-anonymous that can not only satisfy users' demand on obtaining required services with lowest cost, but also protect the location privacy of users.

In "KCLP: A *k*-Means Cluster-Based Location Privacy Protection Scheme in WSNs for IoT," the authors propose a *k*-means cluster routing scheme to protect location privacy, with which the source location privacy and the sink location privacy can be protected and enhanced during packet transmissions.

In "Privacy of Things: Emerging Challenges and Opportunities in Wireless Internet of Things," the authors systematically review the current major privacy issues and countermeasures with three case studies. Furthermore, some potential promising directions are provided, including personalized privacy, lightweight encryption, game theory, and AI-driven methods.

In "Privacy-Preserving Tensor Analysis and Processing Models for Wireless Internet of Things," the authors propose privacy-preserving tensor analysis and processing models for cloud/fog-enriched wireless IoT applications. The models enable users to utilize the storage and computational capabilities of clouds and fogs without disclosing users' sensitive information to the clouds or fogs.

To conclude, we would like to thank all the authors for their contributions to our community. We would also like to express our appreciation to all the reviewers for their efforts in reviewing the papers. Finally, we appreciate the advice and support of the Editor-in-Chief, Dr. Hamid Gharavi, for his help in the entire publication process.

Biographies

Xiaojiang Du [M'99, SM'09] (dxj@ieee.org) is a professor in the Department of Computer and Information Sciences at Temple University, Philadelphia, Pennsylvania. He received B.S. and M.S. degrees in electrical engineering from Tsinghua University, Beijing, China in 1996 and 1998, respectively. He received M.S. and Ph.D. degrees in electrical engineering from the University of Maryland College Park in 2002 and 2003, respectively. His research interests are security, wireless networks, and systems. He has authored over 300 journal and conference papers in these areas, as well as a book published by Springer. He has been awarded more than US$6 million in research grants from the U.S. National Science Foundation (NSF), Army Research Office, Air Force Research Lab, NASA, the State of Pennsylvania, and Amazon. He won the best paper award at IEEE GLOBECOM 2014 and the best poster runner-up award at ACM MobiHoc 2014. He serves on the Editorial Boards of three international journals. He is a Life Member of ACM.

Hsiao-Hwa Chen [S'89, M'91, SM'00, F'10] is currently a Distinguished Professor in the Department of Engineering Science, National Cheng Kung University, Taiwan. He obtained his B.Sc. and M.Sc. degrees from Zhejiang University, China, and a Ph.D. degree from the University of Oulu, Finland, in 1982, 1985, and 1991, respectively. He has authored or co-authored over 400 technical papers in major international journals and conferences, six books, and more than 10 book chapters in areas of communications. He served as the General Chair, TPC Chair, and Symposium Chair for many international conferences. He has served or is serving as an Editor or Guest Editor for numerous technical journals. He is the founding Editor-in-Chief of Wiley's *Security and Communication Networks Journal*. He was the recipient of the best paper award at IEEE WCNC 2008 and the recipient of the IEEE 2016 Jack Neubauer Memorial Award. He served as the Editor-in-Chief of *IEEE Wireless Communications* from 2012 to 2015. He was an elected Member-at-Large of IEEE ComSoc from 2015 to 2016. He is a Fellow of IET.

Liehuang Zhu (liehuangz@bit.edu.cn) is a professor at the School of Computer Science, Beijing Institute of Technology, China. He is a selected member of the Program for New Century Excellent Talents in University from the Ministry of Education, P. R. China. He is a member of the Association for Computing Machinery and China Computer Federation (CCF), Executive Director of the Cyber Security Association of China, and Executive Director of the Chinese Association for Artificial Intelligence. He served as the General Chair of the International Conference on Trustworthy Systems 2011 and 2014, and Associate Editor of the *Journal of Frontiers of Computer Science*. His research interests include cryptographic protocols and applications, cloud computing security, privacy preserving in smart grid, wireless communication security, and mobile security. He has authored over 100 journal and conference papers in these areas, as well as a book. He holds six national invention patents and received a provincial-level S&T Award.

Jiangli Li (jiangli.li@acorn-net.com) serves as the CTO of Beijing Acorn Network Technology Co., Ltd. He is also the supervisor of the Key Infrastructure Protection Technology Beijing Engineering Laboratory, the supervisor of the Zhongguancun Trusted Computing Industry Alliance Industrial Safety Committee, the deputy group leader of the Industrial Internet Industry Alliance Security Group, and a distinguished expert of the Academic Committee of Key Laboratory of Industrial Internet Security Testing and Evaluation. He has invented a number of network security related technologies and holds more than 10 patents in China. He has also published more than 30 papers in related areas.

Zheng Chang [SM'17] received a Ph.D. degree from the University of Jyvaskyla, Finland. Since August 2014, he has been working at the University of Jyvaskyla. He is an Associate Editor, on the Editorial Board, or a Guest Editor of a number of international journals. He has received Best Conference Paper awards from the IEEE Technical Committee on Green Communications and Computing (TCGCC) and *23rd Asia-Pacific Conference on Communications* in 2017. He was named an Exemplary Reviewer of *IEEE Wireless Communications Letters* in 2017. His recent research interests include IoT, cloud/edge computing, security and privacy, vehicular networks, and green communications.