Recent Advances in Security and Privacy for Future Intelligent Networks




Xiaojiang Du Meng Shen Zheng Chang Zhao Cao

The articles in this Special Issue focus on recent advances in security and privacy for future intelligent networks. Recent booming advancements in networking techniques have led to an evolution toward future intelligent networks (FINs). This trend takes place under a circumstance in which a great number of devices are connected for specific purposes by a variety of novel techniques. In FINs, we envision the benefits of integrating intelligence into networks. Contemporarily, these emerging techniques are still at the exploration stage, leaving many privacy and security challenges unaddressed. Existing researchers have already uncovered a great amount of attacks and threats. The situation will be more complicated when incorporating artificial intelligence (AI) techniques into networking, as AI techniques are facing unknown or new types of privacy and security threats. To tackle the security challenges in the design of FINs, we organize this Special Issue focusing on the security and privacy of future FINs.

The response to our Call for Papers was overwhelming, with 47 submissions. During the review process, each paper was reviewed by at least three experts in the relevant areas, with a rigorous two-round review process. Thanks to the support of the Editor-in-Chief, Prof. Mohsen Guizani, we were able to accept 12 excellent articles covering various aspects of security and privacy in FINs. Here, we introduce them and highlight their main contributions.

In "Achieving a Covert Channel over Open Blockchain Network," the authors propose a practical data secret transmission mechanism in existing blockchain systems. Through the use of kleptography algorithms, the transmission channel is highly concealed, and it can resist network eavesdroppers and even internal malicious users.

In "Data Security and Privacy Challenges of Computing Offloading in FINs," the authors discuss the design issues for data security and privacy in FINs. In particular, they present the unique data security and privacy design challenges caused by the computation offloading, and highlight the reasons why the data protection techniques in the current Internet of Things, cloud computing, and edge/fog computing cannot be directly applied.

In "A Security-Enhanced Certificateless Aggregate Signature Authentication Protocol for InVANETs" the authors propose a security enhanced certificateless aggregate signature authentication (SE-CLASA) protocol for InVANETs. A novel factor-contained aggregation mechanism is introduced to resist the so-called information injection attack.

In "Toward Blockchain-Powered Trusted Collaborative Services for Edge-Centric Networks," the authors focus on a blockchain-powered framework that delivers trusted collaborative edge computing (CEC) services in edge-centric networks, in which both decentralized accountability and automatic incentives are used for attracting more distributed edge nodes as detectors to participate in trustworthy verifications for CEC results.

In "Security and Privacy Challenges in 5G-Enabled Vehicular Networks," the authors focus on exploiting new security and privacy challenges brought by a variety of emerging applications in 5G-enabled vehicular networks. As a case study, they investigate the security and privacy issues of a 5G-enabled autonomous platoon, and propose several candidate solutions.

In "Blockchain-Based Privacy-Aware Content Caching in Cognitive Internet of Vehicles," the authors focus on privacy-aware content caching utilizing blockchain in cognitive Internet of Vehicles. To preserve the privacy of users' content requirements, they obtain content from RSUs or surrounding vehicles without submitting requests. The cognitive engine can improve cache hit rate, and blockchain technology can develop a trusted content communication environment.

In "Location Privacy Challenges in Mobile Edge Computing: Classification and Exploration," the authors provide an LBS Classification Principle, which relies on three aspects: location access pattern, identity dependence, and required data type. They show how to classify the existing LPPMs according to their fundamentals.

In "Waving Gesture Analysis for User Authentication in the Mobile Environment," the authors propose a behavior-based authentication system that utilizes the hand waving gesture to identify users. The proposed approach consists of data acquisition, data preprocessing, feature extraction, and authentication modules.

In "Toward Secure Storage in Cloud-Based eHealth Systems: A Blockchain-Assisted Approach," the authors provide a comprehensive picture of designing a secure and efficient EHR protection mechanism for cloud-based eHealth systems and a blockchain-based secure eHealth framework to protect outsourced EHRs from leakage and modification.

In "Mobility Enabled Security for Optimizing IoT-Based Intelligent Applications," the authors propose an efficient resource allocation model for IoT-based systems by adopting the security, energy drain, and cost factors. A mobility management enabled security algorithm by incorporating security with mobility is considered and validated.

In "Fog Intelligence for Network Anomaly Detection," the authors present fog intelligence, a distributed machine learning architecture for network anomaly detection. The proposed architecture is scalable, privacy-preserving, and well suited for intelligent service quality management for 5G networks.

In "BlockSDN: Blockchain as a Service for Software Defined Networking in Smart City Applications" the authors focus on securing the SDN-enabled network architecture toward reliable data forwarding in smart cities, with an emphasis on investigating the permissioned blockchain model-based service framework.

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, Prof. Mohsen Guizani, for his help in the entire process.

Biographies

Xiaojiang Du [M'99, SM'09, F'20] (dxj@ieee.org) is a tenured professor in the Department of Computer and Information Sciences at Temple University, Philadelphia, Pennsylvania. He received his B.S. and M.S. degrees in electrical engineering from Tsinghua University, Beijing, China, in 1996 and 1998, respectively. He received his 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 wireless communications, wireless networks, security, and systems. He has authored over 400 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), U.S. Army Research Office, U.S. Air Force, 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.

Meng Shen [M'14] (shenmeng@bit.edu.cn) is an associate professor at the Beijing Institute of Technology. He received his B.S. degree from Shandong University, Jinan, China in 2009, and his Ph.D. degree from Tsinghua University in 2014, both in computer science. His research interests include data security and privacy protection, blockchain applications, and encrypted traffic analysis. He has authored more than 60 journal and conference papers in these areas. He received the Best Paper Runner-Up Award at IEEE IPCCC 2014.

Zheng Chang [SM'17] (zheng.chang@jyu.fi) is an assistant professor at the University of Jyväskylä, Finland. He received a Ph.D. degree from the University of Jyväskylä in 2013. He was a visiting researcher at Tsinghua University in 2013, and at the University of Houston in 2015. He has received awards from the Ulla Tuominen Foundation, the Nokia Foundation, and the Riitta and Jorma J. Takanen Foundation for research excellence. He has published more than 60 papers in peer reviewed conference proceedings (e.g. IEEE GLOBECOM, ICC, PIMRC, VTC, INFOCOM, WCNC), journals (e.g., *IEEE JSAC*, *TWC*, *TVT*, *TCOM*, *IEEE Network*, *WCM*, *CL*) and books. He has served as a Technical Program Committee (TPC) member for IEEE flagship conferences, such as ICC, INFOCOM, WCNC, GLOBECOM, VTC, PIMRC, and ISCC. He is also an Eeditor of *Springer Wireless Networks*, *IEEE MMTC Communications Frontier*, and *IEEE Access*, and has been a Guest Editor for the *IEEE Internet of Things Journal*, *Wireless Communications*, *Moble Computing*, and *IEEE Communications Magazine*.

Zhao Cao (caozhao1@huawei.com) is a technical expert and architect of blockchain at Huawei where he leads the blockchain team and released the Huawei Blockchain Service. Before joining Huawei, he was an associate professor at the Beijing Institute of Technology, and a research staff member and senior researcher at IBM Research and HP Labs. He received his Ph.D. and B.E. degrees in computer science from the Beijing Institute of Technology in 2010 and 2004, respectively. He was a visiting student supervised by Prof. Yanlei Diao at the University of Massachusetts, Amherst from September 2008 to March 2010. His research interests include distributed systems, blockchain, data management, big data, stream data processing, and more. He was a PC member of VLDB 2017, ICDE 2017/2018, and ICDCS 2016. He is a Standing Committee member of the CCF Blockchain Technical Committee and a member of the CCF Database Technical Committee.