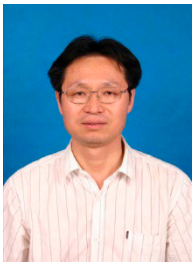
SECURITY ISSUES IN EMERGING EDGE COMPUTING


Fuhong Lin


Lei Yang


Xianwei Zhou

Edge computing is an emerging technology for revolutionarily tackling the network bottlenecks of cloud-device ecosystems. There are about 20 billion edge devices connected to the Internet, with 507.9 ZB data generated, which has reached the limits of central clouds and network bandwidth. It is vitally important for distributed and decentralized edge devices to perform necessary computations on-device rather than outsourcing it to the cloud. However, the openness, heterogeneity and limited computing and storage resources of edge devices have greatly increased the difficulty of security protection in edge computing.This SI targets to address challenges related to developing architectures, algorithms, and techniques to guarantee the security of edge computing. This Special Collection aims to address all these topics and invite contributions from worldwide leading researchers. These works have investigated a wide spread of topics with respect to security issues in emerging edge computing, which are summarized as follows in details.

The first article "An Overview of Privacy Preserving Schemes for Industrial Internet of Things," mainly reviewed privacy issues in a cloud-or an edge-based industrial IoT system. First, the paper investigated the current research status of privacy protection in IoT from different types of privacy analysis, and review privacy solutions when applying software defined network and blockchain under the above two systems. Second, they analyzed the computational complexity and privacy protection performance of these solutions. Finally, they discuss open issues to facilitate further studies.

The Second article "Online Optimization of Physical-Layer Secure Computation Offloading in Dynamic Environments," proposed an online approach to jointly optimize local processing, transmit power and task offloading decisions. The proposed approach can guarantee the secure offloading and asymptotically minimize the time-average energy consumption of devices while maintaining the stability of the ergodic secrecy queues and task queues. By exploiting the Lyapunov optimization, the local processing, transmit power and task offloading variables can be decoupled between time slots, and the subproblems on local processing and computation offloading can be solved separately. Simulation results show that this method has better performance.

The third article "Mobility-Aware Partial Computation Offloading in Vehicular Networks: A Deep Reinforcement Learning Based Scheme" mainly investigated the application of partial computing offloading in-vehicle networks. Aim at shortening the application execution delay,the authors extend the optimization problem from the single-vehicle computing offloading scenario to the multi-vehicle computing offloading by taking multiple constraints into account. To get the solution of the optimized problem， the authors proposed an algorithm basedon deepreinforcement learning. Simulation results show proposed algorithm achieves superior performance mechanisms in deducing application execution delay.

The fourth article "When Edge Computing Meets IoT Systems: Analysis of Case Studies," mainly analyzed some types of architectures relevant for various edge computing problems. Focusing on aim of edge computing, leading features of edge systems and analysis of some edge systems applications. Finally, this article has discussed advantages and possible future developments of edge computingto facilitate further studies.

The fifth article "Secrecy Capacity Maximization for a UAV-Assisted MEC System" proposed an optimized iterative algorithm to realize maximum secure capaci-

ty of the MEC system for the security of UAV-assisted MEC system and assurance secure transmission, which enabling to solve secure transmission problems of two-staged offloading model of UAV-assisted MEC system. The maximum security capacity of the system is gained through joint optimization of UAV positions, transmitted power of UAV, task offloading ratio and allocation of offloading users with considerations to the limited time and energy of UAV. Simulation results demonstrate that the proposed iterative algorithm can improve secure capacity of the system.

The last article "Deeply Understanding Graph-Based Sybil Detection Techniques via Empirical Analysis on Graph Processing," analyzed graph-based Sybil defenses in edge computing and evaluated the sensitivity of Sybil detection methods. In this article, the authors proved that applying graph processing methods to transform the original social graph does affect the performance of graph-based Sybil detections. In seed selection aspect, the seed degree bias has a bigger impact than distributing seeds corresponding to the community structure. Finally, adding the nodes label information to the social graph can effectively improve the robustness of Sybil detections to different attack scenarios and the label noise.

Finally, we would like to thank all the authors who contribute to this feature topic. We also appreciate the great efforts of the reviewers, and the guidance from the Editor-in-Chief, managing editors and staff members.

Biographies

Fuhong Lin, received his M.S. degree and Ph.D. degree from Beijing Jiaotong University, Beijing, P. R. China, in 2006 and 2010, respectively, both in Electronics Engineering. Now he is a professor in department of Computer and Communication Engineering, University of Science and Technology Beijing, P. R. China. His research interests include Edge/Fog Computing, Network Security, and AI. He won "Provincial and Ministry Science and Technology Progress Award 2" in 2017 and 2019. His two papers won "Top 100 most Cited Chinese Papers Published in International Journals" in 2015 and 2016. He served as co-chair of the first and third IET International Conference on Cyberspace Technology, and general chair of the second IET International Conference on Cyberspace Technology. He was the leading editor of the Special issue "Recent Advances in Cloud-Aware Mobile Fog Computing" for Wireless Communications and Mobile Computing. Currently, he also serves as a reviewer more than 10 international journals including IEEE Transactions on Industrial Informatics, IEEE Access, Information Sciences, IEEE Internet of Things Journal, The Computer Journal and China Communications. He received the track Best Paper Award from IEEE/ACM ICCAD 2017.

Lei Yang, received the B.S. and M.S. degrees in electrical engineering from Southeast University, Nanjing, China, in 2005 and 2008, respectively, and the Ph.D. degree from the School of Electrical Computer and Energy Engineering, Arizona State University, Tempe, AZ, USA, in 2012. He was a Postdoctoral Scholar with Princeton University, Princeton, NJ, USA, and an Assistant Research Professor with the School of Electrical Computer and Energy Engineering, Arizona State University. He is currently an Assistant Professor with the Department of Computer Science and Engineering, University of Nevada, Reno, NV, USA. His research interests include big data analytics, AI/ML for cyber-physical systems (smart grids and smart cities), edge computing and its applications in IoT and 5G, data privacy and security in crowdsensing, mobile social networks, and wireless communication networks. He was a recipient of the Best Paper Award Runner-up at the IEEE INFOCOM 2014.

Xianwei Zhou, received his B.S. degree in Department of Mathematics from Southwest Normal University in 1986 and M.S. degree from Zhengzhou University in 1992. In 1999, he obtained Ph.D. degree in Department of Transportation Engineering from Southwest Jiaotong University, China. He was engaged in postdoctor study at Beijing Jiaotong University from 1999 to 2000. Now, he is a professor in Department of Communication Engineering, School of Computer and Communication Engineering, University of Science and Technology Beijing. His research interests include the security of communication networks, edge computing and AI.