REN Kui, WANG Zhibo

# Editorial: Special Topic on Wireless Communication and Its Security: Challenges and Solutions

## Guest Editors >>>

**REN Kui** is a professor and the Dean of School of Cyber Science and Technology at Zhejiang University (ZJU), China, where he also directs the Institute of Cyber Science and Technology. Before that, he was SUNY Empire Innovation Professor at State University of New York at Buffalo, USA. He received his PhD degree in electrical and computer engineering from Worcester Polytechnic Institute, USA. Prof. REN's current research interests include data security, IoT security, AI security, and privacy. He received many recognitions including Guohua Distinguished Scholar Award of ZJU, IEEE CISTC Technical Recognition Award, SUNY Chancellor's Research Excellence Award, Sigma Xi Research Excellence Award, NSF CAREER Award, etc. Prof. REN has published papers extensively in peer-reviewed journals and conferences and received the Test-of-Time Paper Award from IEEE INFOCOM and many Best Paper Awards, including ACM MobiSys, IEEE ICDCS, IEEE ICNP, IEEE Globecom, ACM/IEEE IWQoS, etc. His h-index is 87, with a total citation exceeding 41 000 according to Google Scholar. Prof. REN is a Fellow of ACM and IEEE. He is a frequent reviewer for funding agencies internationally and serves on the editorial boards of many IEEE and ACM journals. Among others, he currently serves as Chair of SIGSAC of ACM China Council, a member of ACM ASIACCS steering committee, and a member of S&T Committee of Ministry of Education of China.

**WANG Zhibo** is a professor of the School of Cyber Science and Technology at Zhejiang University, China. He received his BE degree in automation from Zhejiang University in 2007, and his PhD degree from the Department of Electrical Engineering and Computer Science from University of Tennessee, Knoxville, USA in 2014. His research interests include Internet of Things, AI security, edge intelligence and security. He has published more than 100 papers in top-tier journals and conferences, such as *ToN*, *JSAC*, *CCS*, Mobicom, S&P, INFOCOM, ICCV and CVPR. He serves as an editor of *IEEE Transactions on Cloud Computing*, and the TPC member of many flagship conferences including INFOCOM, WWW, ICDCS, AAAI, KDD and IWQoS. He is the recipient of the National Science Foundation for Excellent Young Scholars, the best student paper award of FUSION 2019, and the outstanding paper award of IEEE HPCC 2019. He is a senior member of IEEE and CCF and a member of ACM.

Recent years have witnessed the phenomenal growth of wireless technologies and applications on a massively large scale since the fifth generation (5G) wireless technologies were proposed as a key propellent to meet the increasing demands of future networks. Going further, the sixth generation (6G) wireless technologies have already been under preparation. However, wireless communication technologies are faced with new opportunities as well as challenges.

On the one hand, emerging technologies provide fundamental issues including higher system capacity, higher data rate, lower latency, higher security, and improved quality of service (QoS), which enables the application of wireless communication technologies in the Internet of Things (IoT) scenarios such as industry, automobile, drone, port, and subway. On the other hand, these new technologies will also introduce new vulnerabilities, which lead to new threats to the security of wireless communication systems. Concerns about security have triggered research in this domain to build up a highly effective safeguard.

The goal of this special issue is to stimulate discussions around open problems of security issues in wireless communication. Focusing on wireless communication and its security, this special issue receives both theoretical and application-based contributions which demonstrate both the challenges and solutions with the rapid development of wireless technologies and applications.

The call-for-papers of this special issue have brought excellent submissions in both quality and quantity. After two-round reviews, five excellent papers have been selected for publica-

DOI:10.12142/ZTECOM.202204001
Citation: K. Ren and Z. B. Wang, "Editorial: wireless communication and its security: challenges and solutions," *ZTE Communications*, vol. 20, no. 4, pp. 1–2, Dec. 2022. doi: 10.12142/ZTECOM.202204001.

tion in this special issue which is organized as follows. We assembled five papers with a balanced selection between theoretical research and practical engineering: three of them carry out comprehensive surveys and the other two propose novel mechanisms. The topics addressed in this special issue cover a broad range, including security in edge blockchains, data collection with local differential privacy (LDP) for mobile devices, security technologies in 6G, federated learning (FL) for secure 6G, and physical layer security for mmWave communication. The detailed information is as follows.

The first paper titled "Security in Edge Blockchains: Attacks and Countermeasures" is the first survey that discusses the attacks and countermeasures of edge blockchains. In this paper, the authors summarize the three-layer architecture of edge blockchains (i. e. blockchain management, blockchain consensus, and blockchain lightweight client) and point out the inherent vulnerabilities of edge blockchains. On this basis, they also summarize the security issues caused by the deployment of vulnerable edge blockchain devices and networks. To be specific, seven specific attacks on edge blockchain components and the corresponding countermeasures are concretely demonstrated in detail. At last, the authors discuss the future directions for researchers to design and implement secure edge blockchains.

Titled "Utility-Improved Key-Value Data Collection with Local Differential Privacy for Mobile Devices", the second paper proposes a utility-improved data collection framework with LDP to deal with key-value data generated by mobile devices. This paper focuses on the problem of limited utility caused by excessive privacy protections and achieves personalized privacy protection by dividing the key-value data into sensitive and non-sensitive parts. The authors validate the mechanism based on two real datasets and prove in experiments that the proposed mechanism can provide better utility and simultaneously protect privacy.

The third paper titled "Key Intrinsic Security Technologies in 6G Networks" provides a general overview of 6G intrinsic security in the industry. In this paper, the authors not only review key security technologies in 5G and security technology enhancement in 5G-Advanced evolution but also analyze the vision and requirements of 6G intrinsic security. Although the technical systems and standards of 6G intrinsic security have not yet reached a unified understanding in the industry, this paper still pays close attention to the disruptive impact that intrinsic 6G security may bring and preliminarily focuses on the key technologies of 6G intrinsic security, including the massive equipment connection security technology, physical layer security technology, and blockchain technology.

Aiming to solve the problem that limited energy restricts the popularization of UAV-enabled FL applications, the fourth paper titled "Air-Ground Integrated Low-energy Federated Learning for Secure 6G Communications" proposes an air-ground integrated low-energy federated learning framework. In this paper, the authors optimize the deployment of unmanned aerial vehicles (UAVs) with a deep Q-network approach to minimize the overall energy consumption of the application communication. This paper shows in the experiment that the proposed method can reduce energy consumption while maintaining the quality of the FL model.

The fifth paper titled "Physical Layer Security for MmWave Communications: Challenges and Solutions" presents a comprehensive overview of physical layer security (PLS) issues in mmWave Communication. In this paper, the theoretical foundation of PLS and the most typical PLS techniques are briefly introduced together with the typical PLS performance metrics secrecy rate, and outrage probability. Several schemes based on these techniques are discussed in detail to compare their advantages and constraints in the mmWave environment and to point out the future direction for researchers.

As demonstrated above, we have briefly introduced the main content of this special issue and given a general overview of the five papers collected in the issue. We would like to express our sincere gratitude to all the authors for their valuable contributions. In the meanwhile, we also want to show our appreciation to all the reviewers for their timely and insightful comments on the submissions. This special issue would not be possible without their help and collaboration. We hope that this special issue can serve as an informative and significant collection to lay a solid foundation for future research works about wireless communication and its security.