Challenges and Novel Solutions for 5G Network Security, Privacy, and Trust


Wojciech Mazurczyk


Pascal Bisson


Roger Piqueras Jover


Koji Nakao


Krzysztof Cabaj

In this *IEEE Wireless Communications* Special Issue (SI), the Guest Editors invited researchers from academia, industry, and government to discuss challenging ideas, novel research contributions, demonstration results, and standardization efforts on 5G network security, privacy and trust. After a rigorous review process, five papers were accepted.

Currently it is expected that the generation (5G) wireless systems will soon provide rich ubiquitous communication infrastructure with wide a range of high-quality services. It is foreseen that 5G communications will offer significantly greater data bandwidth and much improved capability for networking, resulting in unfaltering user experiences for services such as: massive content streaming, telepresence, virtual/augmented reality, crowded area communications, user-centric computing, smart personal networks, Internet of Things (IoT), smart buildings, smart cities, etc.

5G systems are currently at the center of attention of academia, industry, and governments worldwide as they drive many new requirements for different network capabilities. As 5G aims at utilizing many promising network technologies, such as Software Defined Networking (SDN), Network Functions Virtualization (NFV), Information Centric Network (ICN), Network Slicing, Cloud Computing, MEC, etc., supporting a huge number of connected devices integrating the above mentioned advanced technologies and innovating new techniques will surely bring tremendous challenges for security, privacy and trust. Therefore, secure network architectures, mechanisms, and protocols are required as the basis for 5G to address this problem and follow security-by-design but also security by operations rules. Finally, as in 5G networks even more user data and network traffic will be transferred, the big data security solutions assisted by AI techniques should be sought in order to address the magnitude of the data volume and to ensure security concerns at stake (e.g. data security, privacy, etc.).

Considering the above, this Special Issue aimed at collecting the most relevant ongoing research efforts in the 5G network security field. It covered topics which are important for 5G networks in order to release their full potential. The second aim was to bring together the research accomplishments provided by researchers in academia and industry. For this Special Issue we received many submissions; however, in the end after a rigorous review process only five papers were accepted.

In the first article, "NOMA Assisted Secure Short-Packet Communications in IoT," Xiang *et al*. analyze the secure short-packet communications in IoT by utilizing the inherent characteristics of nonorthogonal multiple access (NOMA) without introducing extra security mechanisms. The authors design both downlink and uplink NOMA schemes for secure transmission. Obtained simulations results prove that although secrecy performance is deteriorated in short-packet communications, the performance gains of NOMA over traditional orthogonal multiple access are significant. Finally, the authors outline the challenges and future trends in this emerging research area.

In the next article, "Security Risk Assessment for 5G Networks: National Perspective," Batalla *et al*. propose a methodical approach to developing 5G security regulations based on an analysis of different risk scenarios and the EN-ISO/IEC 27005 standard. The risk assessment was performed with special attention to trust models between users and network operators and between network operators and service providers. The authors also introduce the applicable government-level mitigation measures that are designed to counteract any 5G security threats. When implemented efficiently, they ensure that the new networks will be designed properly.

In the third article, "A Secure Federated Learning Framework for 5G Networks," Liu *et al*. address the data privacy leakage issues related to ensuring secure federated learning in 5G networks. To achieve this goal, the authors propose a blockchain-based framework to defend against poisoning attacks. In this approach, a market is created to trade model updates based on smart contracts in blockchain to validate the model updates against poisoning attacks automatically. Moreover, it utilizes local differential privacy techniques to prevent membership inference attacks to smart contracts. Performed experimental evaluation on two datasets proves that the introduced solution is able to effectively counter poisoning and membership inference attacks.

In the article "A Physical Layer Security Framework for Cognitive Cyber Physical Systems," Topal *et al*. provide an adaptive security framework for a Cognitive Cyber Physical System (CCPS) which takes into account QoS, cost dimensions and security. The authors analyze in detail the security attacks to CPS and review frequently used PLS policies. Then they suggest to use utility as a metric for comparing various PLS policies, and the PLS framework selects the appropriate transmission policy by maximizing the associated utility while taking user requirements into account. The real-time applicability of the proposed framework is evaluated using a software defined radio-based measurement campaign.

Finally, in the last article, "UAV-Assisted Attack Prevention, Detection, and Recovery of 5G Networks," Abdalla *et al*. sug-

gest to utilize unmanned aerial vehicles (UAVs) in order to help in prevention, detection, and recovery against attacks directed toward 5G networks. The authors focus especially on jamming, spoofing, eavesdropping threats and the corresponding countermeasures that are enriched by the versatility of UAVs. The simulation results in the article prove the benefits of the introduced approach using low-altitude aerial points of transmission.

We hope that *IEEE Wireless Communications* readers will find these articles interesting and informative. We would like to thank the authors who submitted their articles, and our committed reviewers for their timely reviews. They have made great efforts to provide useful feedback to the authors, as well as to help us select the best manuscripts for this Special Issue. We are also grateful to the Editor-in-Chief and the Communications Society publications staff for their help and support.

Acknowledgment

The authors gratefully acknowledge the financial support of the EU Horizon 2020 program toward the Internet of Radio-Light project no. H2020-ICT 761992.

Biographies

Wojciech Mazurczyk received his M.Sc., Ph.D., and D.Sc. degrees in telecommunications from the Warsaw University of Technology (WUT), Poland, in 2004, 2009, and 2014, respectively. He is currently a university professor with the Institute of Computer Science at WUT and a researcher at the Faculty of Mathematics and Computer Science, FernUniversitaet, Germany. Since 2016, he has been the Editor-in-Chief of the *Journal of Cyber Security and Mobility* and since 2018 an Asociate Editor *IEEE Transactions on Information Forensics and Security*.

Pascal Bisson is advance studies program manager at There-SIS Laboratory of Thales SIX GTS France. He received an engineering degree from Superior School of Computer Science, Electronics and Automatism, and has a background in AI and security applied to intelligent systems. He is deeply involved in 5G-PPP as the Co-Chair of the 5G Security WG and a member of 5G TB as Technical Manager of 5GDrones and INSPIRE-5Gplus projects. He also fosters liaison with Cybersecurity PPP (ECSO).

Roger Piqueras Jover received a Dipl.Ing. from the Polytechnic University of Catalunya, Spain, and an M.Sc. in electrical and computer engineering from the University of California at Irvine. He spent five years at the AT&T Security Research Center. He is currently a senior security architect with the CTO Security Architecture Team at Bloomberg, where he is a technical leader in mobile security architecture and strategy, corporate network security architecture, wireless security analysis and design, and data science applied to network anomaly detection.

Koji Nakao received his B.E. degree in mathematics from Waseda University, Japan, in 1979. Since then, he has been engaged in research on information security technology for telecommunications including IoT security and 5G security. His present positions are distinguished researcher in NICT and guest professor at Yokohama National University on IoT security research. He has also been an advisor on cybersecurity for the Cabinet Secretariat in the Japanese government since April 2017.

Krzysztof Cabaj holds M.Sc (2004), Ph.D. (2009), and D.Sc. (habilitation) (2019) degrees in computer science from WUT. He is an assistant professor at WUT. His research interests include network security, honeypots, dynamic malware analysis, data mining techniques, IoT, and industrial control systems security. He is the author or co-author of over 60 publications. He has taken part in over a dozen research projects. He is the co-leader of the Computer Systems Security Group at the Institute of Computer Science.