## **GUEST EDITORIAL**

# TRUST, SECURITY AND PRIVACY OF 6G













Zheng Yan

Laurence T. Yang

Tieyan Li

Yoan Miche

Shui Yu

Stephen S. Yau

### **BACKGROUND AND MOTIVATION**

With 5G adoption for commercial use, researchers and practitioners have engaged into exploring 6G telecommunication technologies. In early 2020, they specified 6G basic concepts, perspectives, proposals and suggestions in a number of white papers, including the one about 6G trust, security and privacy (TSP) [1]. 6G is expected to offer the 6th sense. It follows the footsteps of 5G and pursues the integration of communications and sensing. Through sensing the physical world and human-beings, 6G should be capable of programming to offer automation systems that span a rich variety of devices, several types of network and communication technologies and humans. Thus theoretically, 6G should timely offer user expected and satisfied networking services for social communications, health, logistic, entertainment, business, and so on. It will embrace emerging technologies, such as quantum communication, molecular communication, real-time intelligent edge, Internet of everything, etc. As a consequence, personal and national safety will highly depend on network and information security. Anticipating future development, ITU-T specifies that Trustworthy Networking should be provided [2]. 6G TSP white paper [1] also indicates that trust should be embedded into networking. On the other hand, security is always a mandatory requirement, which is one of key performance indicators of trust. But sensing human-beings and physical world brings serious concern on privacy preservation, which however, conflicts with trust. All above drives us to pursue a trust management solution for trustworthy networking in 6G, which should ensure security and overcome privacy leakage in an integrated way.

Another view of 6G is it is a large-scale heterogeneous network (LS-HetNet) by integrating terrestrial networks, space satellite networks, marine networks [2]. Such an integrated network can seamlessly support anywhere and anytime networking. But we hope high quality-of-trust offered by LS-HetNet to meet mobile user expectations and be robust against various failures and malicious attacks. By integrating with cloud computing, edge computing, network resources can be economically arranged with high flexibility across multiple domains according to user demands. But this requests virtual collaboration among multiple network operators in a trustworthy way with privacy preservation at both operator level and user level. In summary, 6G is expected to hold such attractive features as trustworthy and autonomous networking based on effective sensing of the

This work was supported in part by the National Natural Science Foundation of China under Grant 62072351; in part by the Open Project of Zhejiang Lab under Grant 2021PD0AB01 and in part by the 111 Project under Grant B16037. Shui Yu's work is partially supported by Australia ARC DP200101374.

physical world to automatically satisfy user demands through integration of heterogeneous communication and networking technologies. The promising features of 6G introduce new challenges that motivate our efforts and practice.

Obviously, we are facing many new open issues to offer trust, security and privacy in 6G due to its design goals and specific features. New research issues with regard to security, privacy, and trust request deep insight investigation. For example, how to unify anonymous identity authentication, provide efficient network access and handover, offer personalized routing, conduct verifiable accounting, and realize operator-exclusive end-toend security? Apart from the above, 6G raises special concern on privacy in terms of both users and network operators since collaboration among network domains either vertically or horizontally become essential in 6G. For all aforementioned problems, a core challenge could be how to provide a general and universal solution that can integrate security and privacy through trust management across multiple trust-centric network domains to realize end-to-end trust. In this process, user identity, information and related data should be well controlled with authorized access, without depending on any parties that may not be fully trusted. In addition, intelligence offered in each step of the above process should be verified or ensured as trustworthy with explanation. Especially important, an incentive mechanism is expected to motivate all stakeholders to behave as expected for automatically managing the trust of future networks.

Facing such a lot of open issues, it becomes significant to edit a Special Issue (SI) to discuss 6G trust, security and privacy in order to collect current opinions on future networks for the purpose of directing next-step research and practice. We received a total of 51 submissions and finally selected 11 articles for publication through rigorous reviews. In what follows, we introduce each accepted article by classifying them into three categories: 6G trust, 6G security and 6G privacy. Note that if all aspects of trust, security and privacy are concerned in an article, we put it into the category of 6G trust. If both security and privacy are considered in an article, we put it into the category of 6G security.

## ACCEPTED PAPER INTRODUCTION

#### **6G TRUST**

To enhance the trust of the triangle of telecommunications formed by clients, service providers (SPs), and manufacturers and ensure the trustworthiness of manufacturers, Ling et al. attempted to develop a blockchain-based framework to rebuild and maintain the trust triangle in the article "Blockchain-Based Network Hawkeye Function: Building the Trust Triangle in 6G." Facing potential threats and vulnerabilities, the authors first design a blockchain-based network hawkeye function (NHEF)

100 IEEE Network • July/August 2022

# **GUEST EDITORIAL**

to allow clients to watch SPs, SPs to monitor manufacturers, and manufacturers to prove their trustworthiness in an open and privacy-preserving way. Then, they offered a practical NHEF solution compatible with 5G and envisioned its potential for the beyond 6G networking. Furthermore, two NHEF-aided mechanisms were proposed from the interests of clients in order to construct a complete trust triangle. Experimental testing results illustrate the effectiveness of the proposed framework.

In order to guarantee the reliability and trustworthiness of post-authorized network nodes, trust and reputation management (TRM) becomes essential to continuously evaluate the trustworthiness of each participant by collecting and processing trust-related data. In the article "Toward Blockchain-Based Trust and Reputation Management for Trustworthy 6G Networks," the authors showed the effectiveness of using blockchain to construct such a TRM system for 6G networks. Concretely, blockchain can be utilized to build up a decentralized platform for collecting and processing trust evidence in order to quantify trust. A case study about resource management in 6G networks was performed to show that the blockchain-based TRM can digitally evaluate reputation scores based on fulfillment of resource owner's obligations and consumer feedback. In addition, inherent challenges and future directions regarding blockchain-based TRM for 6G are also discussed.

To deploy effective trust management-based intrusion detection solutions in the era of 6G, the article "BCTrustFrame: Enhancing Trust Management via Blockchain and IPFS in 6G Era" identifies key challenges and discusses two major ways of trust management design: information-based and consultation-based. It proposes BCTrustFrame, a blockchain-based trust management framework, which can build a trust map among a plenty of 6G devices with blockchain and InterPlanetary File System (IPFS). By applying the IPFS technology, both the size of shared data and trust management latency can be reduced. Experimental results demonstrate that the proposed framework can enhance the robustness of trust management when traffic is overloaded, as compared with traditional schemes.

Autonomous network is an indispensable component of 6G. It lets artificial intelligence (AI) models make decisions autonomously to operate the network and meet service requirements. Ethical issues and trustworthiness of the AI models have to be well addressed before autonomous networks can be introduced into production networks. The article entitled "Ethically-Responsible and Trustworthy Autonomous Systems for 6G" by Wu presents a framework for ethics-responsible and trustworthy autonomous systems for 6G by embedding an ethical platform for the responsible delivery of an AI project into system design. A case study on edge offloading was provided to show practicality of the proposed framework.

Al is also treated important for 6G trust management. In the article "Generative Adversarial Learning for Intelligent Trust Management in 6G Wireless Networks," Yang et al. proposed a generative adversarial learning-enabled trust management method for 6G. This method aims to secure clustering and achieve reliable and real-time communications, which enhances intelligent trust management with robustness.

#### **6G SECURITY**

Confronting the weakness of centralized identity management for cross-domain interoperability, decentralized identity management shows great advance for future multi-stakeholder 6G networks without relying on centralized identity providers or certification authorities. In the article "Decentralized Identifiers and Self-Sovereign Identity in 6G," Garzon et al. brought decentralized identifiers together with self-sovereign identity into cross-domain and privacy-preserving identity and key management in 6G networks and discuss their application opportunities and potential benefits.

In the context of 5G and its beyond including 6G, network intrusion detection is always an important measure to confront network security risk. Facing the large amount and complexity of rules for intrusion detection, the article "A Fuzzing-Based Method for Testing Rules in Intrusion Detection System in 6G Networks" proposes a fuzzing framework to test detection rules for evaluating their soundness. Particularly, a tunable respondor is applied to generate context-specific responses to construct network states. Fuzzing strategies are further designed to test as more as possible rules. A number of security threats are discovered by this work, such as conflicted rules, performance degradation and intrusion detection bypassing.

Facing such security attacks as man-in-the-middle hijacking and bypass listening, information hiding has become a new way of security countermeasure. In the article entitled "Large-Capacity Local Multi-Dimensional Information Hiding Method for 6G Networks," Li et al. proposed a local multi-dimensional information hiding method with large capacity. It hides multi-layer information in the multi-dimensional space of digital signals by using orthogonal space and spread transform. Interestingly, this method can hide information in multi-layers at the same location while allowing independent information extraction from multiple layers.

The amount of data is increasing dramatically in 6G era, and as a result, the demand for privacy protection is becoming prominent. The article "Toward Data Security in 6G Networks: A Public-Key Searchable Encryption Approach" by Shi et al. analyzes some typical security and privacy problems in 6G based applications, discusses the solutions to these problems, and presents a framework of 6G based smart cities with searchable encryption, which guarantees the privacy and availability, including ciphertext search and access control, of smart city data.

#### **6G PRIVACY**

Channel State Information (CSI) could be widely applied in 6G to support new applications and personalized networking services. However, CSI analysis poses threats to people's privacy and security. In the article "Integrating CSI Sensing in Wireless Networks: Challenges to Privacy and Countermeasures," Cigno et al. discussed the current state-of-arts of CSI-based sensing and present some important technologies to protect privacy and allow legitimate use of CSI for offering good services.

For securing federated learning for 6G empowered Internet of Medical Things (IoMT), the article "SMPC-Based Federated Learning for 6G Enabled Internet of Medical Things" proposes a convolutional neural network (CNN) based federated learning framework that combines secure multi-party computation (SMPC) based aggregation and encrypted inference methods for generating an encrypted global model, which is returned to edge servers for localized training and further improving model accuracy with data and model privacy preservation.

#### CONCLUSION

Based on the above SI article review, we observe that current research on 6G trust, security and privacy pays much attention to applying emerging technologies such as blockchain and machine learning to facilitate 6G development in order to achieve decentralized trust management and high intelligence. Meanwhile, security and privacy are also enhanced in order to ensure 6G robustness and satisfy user privacy requirements.

Editing this SI is a fruitful experience. We would like to thank all authors and reviewers for their tremendous contributions to this SI. We appreciate the kind support from Dr. Chonggang Wang, the Editor-in-Chief of IEEE Network Magazine, for steering our editing work and ensuring the quality of this SI. 6G trust, security and privacy is emerging as a hot topic in both industry and academia. We believe there are many attractive and significant research issues worth our exploration, which may not be covered herein. We hope this SI can stimulate future deep research and investigation in this field.

IEEE Network - July/August 2022

# **GUEST EDITORIAL**

#### REFERENCES

- [1] M. Ylianttila et al., "6G White Paper: Research Challenges for Trust, Security and Privacy," arXiv preprint arXiv:2004.11665, 2020.
- [2] ITU-T Y.3053, "Framework of Trustworthy Networking with Trust Centric Network Domains," 2018.
- [3] J. Wang et al., "A Survey on Trust Models in Heterogeneous Networks," IEEE Commun. Surveys and Tutorials, 2021, DOI: 10.1109/COMST.2022.3192978.

#### **BIOGRAPHIES**

ZHENG YAN [SM] (zyan@xidian.edu.cn) is currently a full professor at the Xidian University, China. Her research interests are in trust, security, privacy, and data analytics. She authored over 330 peer-reviewed publications and solely authored two books. She is the inventor of 41 patents and 50 PCT patent applications, all of which have been adopted by industry. She was invited to delivery about 30 keynotes and talks in international conferences. She served or is serving as an area/associate editor for over 20 journals, including Information Fusion, IEEE Internet of Things Journal, Information Sciences, IEEE Network Magazine, IEEE Consumer Electronics Magazine, etc. She served as a general or program chair for over 30 international conferences. She initiated IEEE international conference on Blockchain as a steering committee co-chair. Recently, she achieved the Distinguished Inventor Award of Nokia, ELEC Impact Award, the IEEE ComSoc TCBD best journal paper award (2017), the best paper award of SpaCCS2019, and the best associate editor of IEEE Access (2017, 2018). She is a Fellow of IET.

LAURENCE T. YANG (Ityang@gmail.com) got his BE in Computer Science and Technology and BSc in Applied Physics both from Tsinghua University, China and Ph.D in Computer Science from University of Victoria, Canada. He is a professor in Hainan University, China as well as a professor at St. Francis Xavier University, Canada. His research includes Cyber-Physical-Social System Design and Data Analytics. He has published 250+ papers in the above areas on top IEEE/ACM Transactions with total citations of 30907 and H-index of 89 including 8 and 40 papers as top 0.1% and top 1% highly-cited ESI papers, respectively. He has been involved actively act as a steering chair for 10+ IEEE international conferences. He is the chair of IEEE CS Technical Committee of Scalable Computing (2008-2011, 2018-2021), the co-chair of IEEE SMC Technical Committee on Cybermatics (2016-), the co-chair of IEEE SC Hype-Intelligence Technical Committee (2021-), and the chair IEEE CIS Cyber-Physical-Social Systems Task Force (2019–) and the vice-chair of IEEE CIS Technical Committee on Smart World (2016-2019). In addition, he is serving as an editor for many international journals and is an author/co-author or an editor/co-editor of more than 25 books from well-known publishers, invited to give around 50 keynote talks at various international conferences and symposia.

TIEYAN LI (Li.Tieyan@huawei.com) is an expert on security and applied cryptography, and a technology generalist on applications, systems and networks. He is currently leading Digital Trust research, on building the trust infrastructure for future digital world, and previously on mobile security, loT security, and AI security at Shield Lab., Singapore Research Center, Huawei Technologies. He is also the director of Trustworthy AI C-TMG and the vice-chairman of ETSI ISG SAI. He received his Ph.D. Degree in Computer Science from National University of Singapore. He has more than 20 years experiences and is proficient in security design, architect, innovation and practical development. He was also active in academic security fields with tens of publications and patents. He has served as the PC members for many security conferences, and is an influential speaker in industrial security forums. His current research topics include: Trustworthy AI, Trustworthy Computing, Trustworthy Identity and Future Network Infrastructure.

YOAN MICHE (yoan.miche@nokia-bell-labs.com) is currently the head of the cybersecurity research team in Nokia Bell Labs, Finland. He received a double M.Sc. degree in Telecoms and Signal/Image processing from the ENSIMAG and Gipsa Lab, France. He received a double degree Ph.D. in Applied Machine Learning (to watermarking and steganography) from both Aalto University, Finland (then Helsinki University of Technology) and the INP Grenoble, France. He was a postdoctoral researcher on industry collaboration projects during 4 years at Aalto University, mainly focusing on applications of machine learning to (cyber) security problems. He joined Nokia Research (now Bell Labs) Finland in 2014 as a cybersecurity researcher and took the lead of the cybersecurity research team in 2018. His topics of predilection include neural networks, anomaly detection, data mining, network security, and he is still fascinated by watermarking and steganography technologies. He was Associate Editor for Elsevier's Neurocomputing from 2012 to 2021, and now serves as a member of the Advisory Board for the journal. He is also on the editorial board (and one of the co-founders) of the Machine Learning and Knowledge Extraction (MAKE) journal. He has been on the Advisory and Stakeholder Boards of several EU projects, recently including the SHERPA project (on the Ethics of AI/ML) and the SAPPAN project (on the sharing and automation of security knowledge).

SHUI YU (Shui.Yu@uts.edu.au) is a Professor of School of Computer Science, University of Technology Sydney, Australia. His research interest includes Big Data, Security and Privacy, Networking, and Mathematical Modelling. He has published three monographs and edited two books, more than 350 technical papers, including top journals and top conferences, such as IEEE TPDS, TC, TIFS, TMC, TKDE, TETC, TON, and INFOCOM. His h-index is 52. Dr Yu initiated the research field of networking for big data in 2013, and his research outputs have been adopted by industrial systems. He is currently serving a number of prestigious editorial boards, including IEEE Communications Surveys and Tutorials (Area Editor), IEEE Communications Magazine, and IEEE Internet of Things Journal. He is a Senior Member of IEEE, a member of AAAS and ACM, and a Distinguished Lecturer of IEEE Communications Society.

STEPHEN S. YAU (yau@asu.edu) is currently a Professor of Computer Science and Engineering at Arizona State University. He was professor and chair of the Computer Science and Engineering Department at Arizona State University in 1994– 2001, and the Computer and Information Sciences Department at the University of Florida, Gainesville in 1988-1994. From 1988-1992, he was also the director of the Software Engineering Research Center at the University of Florida. In 1961, he joined Northwestern University, Evanston, Illinois as an Assistant Professor of Electrical Engineering in 1961 and later became Walter P. Murphy Chair Professor and the chair of the Electrical Engineering and Computer Science Department at Northwestern University until 1988. He is a Fellow of the Institute of Electrical and Electronics Engineers (IEEE) and a Fellow of the American Association for the Advancement of Science. He received numerous awards, including the Louis E. Levy Medal of the Franklin Institute, the Golden Plate Award of the American Academy of Achievement, the Richard E. Merwin Award of the IEEE Computer Society, the IEEE Centennial Medal, the IEEE Third Millennium Medal, the International Federation for Information Processing (IFIP) Silver Core Award, the American Federation of Information-Processing Societies (AFIPS) Special Award, and various special awards of the IEEE and its Computer Society. He was the President of the IEEE Computer Society in 1974-1975 and the American Federation of Information Processing Societies in 1985-1986. He served as a member of the IEEE Board of Directors in 1976–1977 and the Board of Directors of the Computing Research Association in 1996-2000.

102 IEEE Network - July/August 2022