Digital Object Identifier 10.1109/OJVT.2023.3288457

Guest Editorial
Special Section on Recent Advances in Security and Privacy for 6G Networks

The emergence of new disruptive technologies is paving the way towards shaping the upcoming sixth generation (6G) of wireless networks, which are envisioned to enable a large number of innovative applications over a ubiquitous, secure, unified, self-sustainable, and fully intelligent platform. These technologies include but are not limited to, virtual/augmented/mixed reality services, haptics, flying vehicles, brain-machine interface, and telepresence, to name a few. The successful operation of their associated functionalities is subject to meeting stringent network requirements, such as extremely high data rates, ultra-low latency, low complexity, uniquely small-sized designs, and high energy and spectral efficiencies. Therefore, the evolution of 6G networks will be accompanied by diverse novel technological trends, including artificial intelligence, data mining, cloud and edge computing, wireless mobile caching, network slicing, network function virtualization, as well as centralized and decentralized deep learning. While 6G wireless paradigms are envisaged to support the realization of self sustaining, self optimized networks with personalized user experience, privacy and security remain a predominant concern due to the centralized and decentralized data exchange, storage, and process, needed for the successful operation of 6G networks.

Accordingly, particular attention should be devoted to developing and integrating effective trust, security, and privacy mechanisms into the 6G architecture. It should be highlighted that, although there are a considerable number of highly efficient security and privacy schemes, their applicability to 6G networks is still debatable. This calls for a compelling need to revisit conventional security and privacy approaches and to design advanced energy-efficient, lightweight, reliable, and low-cost security solutions, that perfectly fit in the context of 6G wireless communication systems.

The goal of this special section was to promote research in the development of efficient and novel security and privacy designs and enabling techniques by bringing together leading researchers from both industry and academia to present their creative views on the current trends and publish their innovative approaches for addressing various fundamental and practical challenges related to security and privacy in future. At the end of the review process, 10 articles have been accepted for publication in this special section. To help the reader identify the research works that are most interesting for them, the articles are categorized into four areas: (i) Secure Massive MIMO Systems; (ii) Physical Layer Security in Non-Terrestrial Networks; (iii) Novel Machine Learning-Based Security Approaches; and (iv) Security and Privacy for Smart Cities. The contributions made by each of the articles are summarized next. We hope that this special section will serve as a useful reference for researchers, scientists, engineers, and academics in the field of security and privacy for 6G networks.

I. SECURE MASSIVE MIMO SYSTEMS

In [A1], Roth et al. designed a novel physical layer authentication scheme, that jointly incorporate the channel and process system parameters for enhanced security level. The developed framework is based on Kalman filter and follows the threshold-based principle. In particular, the Kalman filter is utilized to estimate the system and channel states, which are then leveraged as inputs to a hypothesis test for node authentication. The authors further optimized the threshold value in the hypothesis testing procedure for guaranteed security. The robustness of the authentication scheme is corroborated in several scenarios, including, a small number of antennas, massive single-input multiple-output (SIMO), and massive SIMO with channel hardening.

An efficient secure offloading mechanism was proposed by Yilmaz et al. in [A2]. In specific, they developed a cooperative mobile edge computing (MEC) scheme, which incorporates massive MIMO and non-orthogonal multiple access (NOMA) for improved communication between cell-edge users and MEC servers. The framework takes into consideration the limited computing capabilities, power budget, and security constraints at cell-edge and cell-center users, and aims to minimize the overall delay over the downlink and uplink communications.

II. PHYSICAL LAYER SECURITY IN NON-TERRESTRIAL NETWORKS

Abdrabou et al. in [A3] developed a physical layer authentication scheme for low earth orbit (LEO) satellites, through leveraging Doppler frequency shift (DS) and received power (RP) for hypothesis testing. The hypothesis testing is performed through threshold-based approach, as well as machine learning (ML) algorithms, e.g., one-class classification support vector machine. The algorithm was trained using real satellite data of legitimate nodes. The authors showed the effective impact of DS in improving the authentication rate in small elevation angles, while it was demonstrated that for large elevation angles, the RP has more effect on the authentication performance.

The performance study conducted by Erdogan et al. in [A4] aimed at quantifying the secrecy performance of different eavesdropping scenarios in an optical high altitude platform station (HAPS) setup. The authors studied the secrecy outage probability (SOP), probability of positive secrecy (PPSC), average secrecy capacity (ASC), and secrecy throughput (ST). Through the developed mathematical framework in [A4], the authors drawn useful conclusions on the design aspects to be taken into consideration in optical HAPS systems, e.g., eavesdropper's SNR, the scattered information level, zenith angle, and distance, for improved physical layer security.

III. NOVEL MACHINE LEARNING-BASED SECURITY APPROACHES

In [A5], Al-Jarrah et al. developed a new ML-based intrusion detection system (IDS) for detecting novel cyber-attacks in intra-vehicle networks, specifically in controller area networks (CANs) of modern vehicles. The proposed IDS framework implements the Recurrence Plot (RP) to generate high-level representations of CAN messages incorporating both the content transported by a message and its relative context. The captured complex relationships and temporal dependencies among the messages are fed into a bespoke Neural Network, designed and trained to detect novel intrusions.

The efforts of Uysal et al. [A6] were devoted to providing a comprehensive review of the theoretical and experimental data-driven malware detection literature in the large-scale data-intensive field. The contribution of the article is two fold: (i) discussing new concepts in multi-domain to multi-target continuous learning and the challenges associated with unseen/unknown data, imbalanced data, and data scarcity; (ii) shedding light on the novel concept of explainability via visualization with a multi-labeling approach which allows identifying malware by their recipes while improving the interpretability of its decision process.

The study by Shi et al. [A7] proposed a reinforcement learning (RL)-based network slicing to maximize the total reward of accepted user requests in next generation (NextG) radio access networks (RAN). By exploiting adversarial ML, the authors introduced a novel over-the-air attack to manipulate the RL algorithm and disrupt NextG network slicing. The adversary reduces the RL algorithm's reward by observing the spectrum and building its own RL-based surrogate model to selectively jam the available resource blocks (RBs) so that the RL algorithm for the network slicing receives an incorrect reward (feedback), thereby leading to a significant performance loss of resource allocation for NextG RAN slicing. The authors designed novel defense schemes by considering various characteristics of the RL algorithms and showed the effectiveness of the designed attack and defense schemes using different benchmarks.

In the article [A8], Duong et al. presented a comprehensive overview of the state-of-the-art in quantum computing (QM). They identified several quantum-inspired ML applications for 6G networks and discussed their underlying potentials and challenges in terms of resource allocation and network security, considering their enabling technologies. This article highlighted some dominating research issues and offered future research directions for quantum-inspired ML in 6G networks. The presented study provided insights into QC with ML and offered substantial guidelines for the quantum developers and researchers of the next generation of quantum computers and how they transform the quantum ML algorithms into practical applications.

IV. SECURITY AND PRIVACY FOR SMART CITIES

The survey presented by Aldahmani et al. [A9] focused on the cyber-security of embedded IoTs in Smart Homes and highlighted relevant challenges, requirements, countermeasures, and trends. After overviewing IoT's design, objects, and standards for smart homes, the authors provided an in-depth discussion on state-of-the-art privacy and security approaches for smart homes. In addition, the article detailed the major smart home components that must be safeguarded and addressed the tiered IoTs framework and associated security concerns by introducing a taxonomy related to vulnerabilities, threats, and attacks on IoT devices in this domain. Moreover, the authors highlighted several recommended and countermeasures security solutions that can be used to keep IoT devices, networks, and applications cyber-safe and protect them against cyberattacks.

In [A10], Gheisari et al. developed a novel privacy-preserving mechanism for Internet-of-Things (IoTs) devices within a smart city environment. Considering the deployment of software-defined networking (SDN) in IoT devices, the authors proposed a dynamic differential privacy scheme, which frequently selects either the Laplace distribution or the exponential distribution to protect the sensitive data produced by IoT devices. The selected privacy-preserving method of each IoT device changes every minute, ensuring sensitive data disclosure is prevented. The study demonstrated that, compared to the traditional static privacy-preserving methods, the proposed dynamic scheme is more effective in preserving network privacy and bringing flexibility to network management.

ACKNOWLEDGMENT

The Guest Editors would like to express their gratitude to all the authors for their outstanding contributions to this special section, and all the anonymous reviewers for their efforts and valuable comments, which helped to improve the quality of the articles. The Guest Editors also would like to extend their gratitude to the Editor-in-Chief, Sun Sumei, for her diligence and support throughout the entire process of this special section.

LINA MOHJAZI, *Guest Editor*
James Watt School of Engineering,
University of Glasgow
G12 8QQ, Glasgow, U.K.
l.mohjazi@ieee.org

LINA BARIAH, *Guest Editor*
Technology Innovation Institute
Abu Dhabi, 9639, UAE
lina.bariah@ieee.org

SAMI MUHAIDAT, *Guest Editor*
KU Center for Cyber-Physical Systems,
Department of Electrical and Computer Engineering
Khalifa University
Abu Dhabi, 127788, UAE

Department of Systems and Computer Engineering
Carleton University
Ottawa, ON K1S 5B6, Canada
muhaidat@ieee.org

XIANFU LEI, *Guest Editor*
Provincial Key Lab of Information Coding and Transmission
Southwest Jiaotong University
Chengdu, 610031, China
xflei@swjtu.edu.cn

ABDALLAH SHAMI, *Guest Editor*
Department of Electrical and Computer Engineering
Western University
London, ON, N6A 3K7, Canada
abdallah.shami@uwo.ca

IV. APPENDIX
RELATED ARTICLES

[A1] S. Roth, A. Sezgin, R. Bessel, and H. V. Poor, "Approximative threshold optimization from single antenna to massive SIMO authentication," *IEEE Open J. Veh. Technol.*, vol. 4, pp. 193–207, 2023, doi: 10.1109/OJVT.2022.3229064.

[A2] S. S. Yılmaz, B. Özbek, and R. Mumtaz, "Delay minimization for massive MIMO based cooperative mobile edge computing system with secure offloading," *IEEE Open J. Veh. Technol.*, vol. 4, pp. 149–161, 2023, doi: 10.1109/OJVT.2022.3226565.

[A3] M. Abdrabou and T. A. Gulliver, "Authentication for satellite communication systems using physical characteristics," *IEEE Open J. Veh. Technol.*, vol. 4, pp. 48–60, 2023, doi: 10.1109/OJVT.2022.3218609.

[A4] E. Erdogan, O. B. Yahia, G. K. Kurt, and H. Yanikomeroglu, "Optical HAPS eavesdropping in vertical heterogeneous networks," *IEEE Open J. Veh. Technol.*, vol. 4, pp. 208–216, 2023, doi: 10.1109/OJVT.2022.3232272.

[A5] O. Y. Al-Jarrah, K. E. Haloui, M. Dianati, and C. Maple, "A novel detection approach of unknown cyber-attacks for intra-vehicle networks using recurrence plots and neural networks," *IEEE Open J. Veh. Technol.*, vol. 4, pp. 271–280, 2023, doi: 10.1109/OJVT.2023.3237802.

[A6] D. T. Uysal, P. D. Yoo, and K. Taha, "Data-driven malware detection for 6G networks: A survey from the perspective of continuous learning and explainability via visualisation," *IEEE Open J. Veh. Technol.*, vol. 4, pp. 61–71, 2023, doi: 10.1109/OJVT.2022.3219898.

[A7] Y. Shi, Y. E. Sagduyu, T. Erpek, and M. C. Gursoy, "How to attack and defend nextG radio access network slicing with reinforcement learning," *IEEE Open J. Veh. Technol.*, vol. 4, pp. 181–192, 2023, doi: 10.1109/OJVT.2022.3229229.

[A8] T. Q. Duong, J. A. Ansere, B. Narottama, V. Sharma, O. A. Dobre, and H. Shin, "Quantum-inspired machine learning for 6G: Fundamentals, security, resource allocations, challenges, and future research directions," *IEEE Open J. Veh. Technol.*, vol. 3, pp. 375–387, 2022, doi: 10.1109/OJVT.2022.3202876.

[A9] A. Aldahmani, B. Ouni, T. Lestable, and M. Debbah, "Cyber-security of embedded IoTs in smart homes: Challenges, requirements, countermeasures, and trends," *IEEE Open J. Veh. Technol.*, vol. 4, pp. 281–292, 2023, doi: 10.1109/OJVT.2023.3234069.

[A10] M. Gheisari et al., "An agile privacy-preservation solution for IoT-based smart city using different distributions," *IEEE Open J. Veh. Technol.*, vol. 4, pp. 356–362, 2023, doi: 10.1109/OJVT.2023.3243226.

LINA MOHJAZI (Senior Member, IEEE) received the B.Sc. (Hons.) degree in electrical and electronic engineering from the United Arab Emirates University, Al-Ain, UAE, in 2008 (Full Scholarship), the M.Sc. degree in electrical and electronic engineering from Khalifa University, Abu Dhabi, UAE, in 2012 (Full Scholarship), and the Ph.D. degree in electrical and electronic engineering from the University of Surrey, Guildford, U.K., in 2018. She is currently a Lecturer of autonomous systems and connectivity with the James Watt School of Engineering, University of Glasgow, Glasgow, U.K. She has co-authored more than 40 research papers in international high-impact journals and highly-rated conferences as well as book chapters. Her research interests include green and sustainable wireless communications, IoT's, machine learning, Big Data analytics, energy efficiency, fundamental performance limits, and beyond 5G and its applications. Dr. Mohjazi is a Fellow of the Women's Engineering Society, and a Senior member of the IEEE Women in Engineering and IEEE Vehicular Technology Society. She is currently an Associate Editor for IEEE Communications Letters and IEEE OPEN Journal of the Communications Society. Dr. Mohjazi was a technical program committee member and a session chair of several IEEE flagship conferences. She actively participates in organizing IEEE conferences and workshops. Dr. Mohjazi is endorsed as a U.K. Exceptional Talent by the Royal Academy of Engineering, U.K. She was also the recipient of multiple teaching awards and the IEEE GPECOM 2022 best paper presentation award. She is an Affiliate Member of Mohammed Bin Rashid Academy of Scientists, UAE.

LINA BARIAH (Senior Member, IEEE) received the M.Sc. and Ph.D. degrees in communications engineering from Khalifa University, Abu Dhabi, UAE, in 2015 and 2018, respectively. She was a Visiting Researcher with the Department of Systems and Computer Engineering, Carleton University, Ottawa, ON, Canada, in 2019, and an Affiliate Research Fellow with the James Watt School of Engineering, University of Glasgow, Glasgow, U.K. She is currently a Senior Researcher with the Technology Innovation Institute, an Adjunct Professor with Khalifa University, and an Adjunct Research Professor with Western University, London, ON, Canada. Dr. Bariah is a Senior Member of the IEEE Communications Society, IEEE Vehicular Technology Society, and IEEE Women in Engineering. She is currently an Associate Editor for the IEEE Communication Letters and IEEE Open Journal of the Communications Society, and an Area Editor of *Physical Communication* (Elsevier). She is a Guest Editor of *IEEE Network Magazine*, *IEEE Communication Magazine*, and *RS Open Journal on Innovative Communication Technologies* (RS-OJICT). She was a technical program committee member of a number of IEEE conferences, such as ICC and Globecom. She is also organizing/chairing a number of workshops. She is a Session Chair and an active reviewer for numerous IEEE conferences and journals.

SAMI MUHAIDAT (Senior Member, IEEE) received the Ph.D. degree in electrical and computer engineering from the University of Waterloo, Waterloo, ON, Canada, in 2006. From 2007 to 2008, he was an NSERC Postdoctoral Fellow with the Department of Electrical and Computer Engineering, University of Toronto, ON, Canada. From 2008 to 2012, he was an Assistant Professor at the School of Engineering Science, Simon Fraser University, Burnaby, BC, Canada. He is currently a Professor with Khalifa University and an Adjunct Professor with Carleton University, Ottawa, ON, Canada. His research interests include advanced digital signal processing techniques for wireless communications, intelligent surfaces, MIMO, optical communications, massive multiple access techniques, backscatter communications, and machine learning for communications. He is currently an Area Editor of the IEEE Transactions on Communications, Guest Editor of the IEEE Network "Native Artificial Intelligence in Integrated Terrestrial and Non-Terrestrial Networks in 6G" special issue, and the Guest Editor of the IEEE Open Journal of Vehicular Technology "Recent Advances in Security and Privacy for 6G Networks" special section. He was a Senior Editor and Editor of the IEEE Communications Letters, Editor of IEEE Transactions on Communications, and an Associate Editor for IEEE Transactions on Vehicular Technology.

XIANFU LEI (Member, IEEE) received the Ph.D. degree from Southwest Jiaotong University, Chengdu, China, in 2012. He is currently a Full Professor with the School of Information Science and Technology with Southwest Jiaotong University. From 2012 to 2014, he was a Research Fellow with the Department of Electrical and Computer Engineering, Utah State University, Logan, UT, USA. His research interests include 5G/6G networks, cooperative and energy harvesting networks, and physical-layer security. He is currently the Area Editor of the IEEE COMMUNICATIONS LETTERS and Editor of IEEE TRANSACTIONS ON COMMUNICATIONS and IEEE WIRELESS COMMUNICATIONS LETTERS. From 2014 to 2019, he was the Senior/Associate Editor for IEEE COMMUNICATIONS LETTERS He was also symposium/track chairs for major IEEE conferences. He was the recipient of the Best Paper Award at IEEE/CIC ICCC'20, Best Paper Award at WCSP'18, WCSP 10-Year Anniversary Excellent Paper Award, IEEE Communications Letters Exemplary Editor Award, and Natural Science Award of China Institute of Communications in 2019.

ABDALLAH SHAMI (Senior Member, IEEE) is currently the Acting Associate Dean Research and a Professor with the ECE Department, Western University, Ontario, ON, Canada. His research interests include the area of future networks, network automation and smart systems. He is/was an Associate Editor for IEEE TRANSACTIONS ON MOBILE COMPUTING, IEEE INTERNET OF THINGS JOURNAL, and IEEE COMMUNICATIONS TUTORIALS AND SURVEY. He was the elected Chair of the IEEE Communications Society Technical Committee on Communications Software and IEEE London Ontario Section Chair.