Special Issue on
Recent Advances in Security and Privacy for 6G Networks

Scope

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, includes 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 the 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 (AI), 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 communciation systems. The scope of this special issue is to promote research in the development of efficient and novel security and privacy designs and enabling techniques to address the underlying fundamental and practical challenges. More specifically, this special issue will bring together leading researchers from both industry and academia to present their views on the current trends and challenges, addressing various concerns related to security and privacy in future wireless networks.

Topics

Topics of interest include, but are not limited to:

- Advanced physical layer security techniques and standards.
- Potential threats and attacks in 6G networks.
- AI-enabled security mechanisms.
- Secrecy analysis and enhancement in security for 6G networks.
- Secure optical wireless communications (OWC).
- Security and privacy in HetNets.
- Blockchain-empowered security schemes in 6G networks.
- Technological advancements for secure aerial networks.
- Advanced privacy and security mechanisms for vehicular networks.

- Efficient security schemes for satellite communications.
- Efficient security mechanisms for integrated terrestrial and non-terrestrial networks.
- Reconfigurable intelligent surface-empowered physical layer security approaches.
- Enhanced security mechanisms for massive-MIMO, NOMA, and RSMA.
- Secure terahertz (THz) and millimeter-wave (mmWave) wireless communications.
- Security and privacy solutions for internet-of-things (IoT) systems.
- Practical testbeds, experimental results, demonstrators.
- Enhancements in secure beamforming, coding and modulation techniques.
- Secure offloading in mobile-edge computing.
- Energy efficient secure mechanisms for simultaneous wireless information and power transfer (SWIPT) and backscatter communications (BackCom).

Important Dates

Manuscript submission: September 15, 2022
First review notification: October 30, 2022
Revised manuscript due: November 30, 2022
Final editorial decision: December 15, 2022
Final manuscript due: December 30, 2022
Publication date: 4th Quarter 2022

Guest Editors

Lina Mohjazi
University of Glasgow, UK (l.mohjazi@ieee.org)
Lina Bariah
KU C2PS, Khalifa University, UAE/University at Albany, SUNY, USA (lina.bariah@ieee.org)
Sami Muhaidat
KU C2PS, Khalifa University, UAE (muhaidat@ieee.org)
Xianfu Lei
Southwest Jiaotong University, China (xflei@swjtu.edu.cn)
Abdallah Shami
Western University, Canada (abdallah.shami@uwo.ca)