Wireless Communications and Mobile Computing

WILEY | Hindawi

Special Issue on

Safeguarding 5G Networks through Physical Layer Security Technologies

CALL FOR PAPERS

5G wireless networks are expected to support massive user connections and exponentially increasing wireless services, which makes information security unprecedentedly important. As an emerging network security solution, physical layer security (PLS) takes advantage of the intrinsic characteristics of wireless channels, such as noise, interference, and fading, to degrade the received signal qualities at the malicious users, and achieves keyless secure transmission via signal design and signal processing approaches. Compared with the traditional cryptographic methods at upper layers of the protocol stack, PLS has the following technical advantages. First, PLS does not depend on encryption/decryption operations, thus avoiding the difficulty of distributing and managing secret keys in large-scale heterogeneous 5G networks. Second, by using PLS approaches, adaptive signal design and resource allocation can be implemented based on the varying channel conditions, thereby providing flexible security levels and realizing user-centric security guarantees. Third, PLS often requires relatively simple signal processing operations, which translates into minor additional overheads.

In the past few years, the research on PLS has generated a large body of literature, with the topics ranging from information-theoretical studies to practical scheme design. However, it is still challenging to develop innovative PLS solutions that well match the unique features of 5G networks. First, most of the existing PLS schemes only exploit the characteristics of wireless channels (i.e., link-level properties including noise, fading, and interference) but underappreciate the significance of characteristics of wireless networks (i.e., network-level properties such as feedback, cooperation, competition, and cognition among users) in security enhancement. Second, the PLS techniques developed so far mainly focus on the optimization of the secrecy rate or secrecy outage performance. Yet, 5G is expected to support various application scenarios and diverse wireless services. Different types of services have totally different quality-of-service (QoS) requirements, which implies that the PLS protocols should jointly consider various aspects of user demands, including reliability, delay, throughput, and secrecy as well. Third, the existing PLS solutions often unilaterally pursue the system performance optimization without taking into account the limitations in the available resources of practical devices. In 5G-enabled IoT communications, low-cost machine-type devices have very simple functionalities and very limited power, storage, and processing capabilities. Therefore, most of the existing PLS solutions cannot be directly applied in IoT applications.

The aim of this special issue is to provide a venue to publish innovative PLS solutions that address the aforementioned challenges faced by 5G security. Original research articles as well as review articles from both academia and industry are welcome.

Potential topics include but are not limited to the following:

- Information-theoretic fundamentals for PLS
- Advanced signal design and coding techniques for enhanced security
- PHY authentication techniques in 5G
- CSI-based key generation and PHY encryption algorithm design
- Secure transmission techniques in massive MIMO and millimeter wave communications
- Security threats and countermeasures in full-duplex communications
- Privacy and security in D2D/M2M communications
- Transmission secrecy in ultradense heterogeneous networks
- Security provisioning for NOMA
- PLS techniques in 5G-enabled IoT
- PLS for 5G networks with energy harvesting and wireless power transfer
- Cross-layer security approaches
- Analysis of the tradeoffs among secrecy, capacity, delay, energy efficiency, and QoS
- Novel PLS performance metrics
- Random matrix approaches and other mathematical tools for PLS
- Testbed development for the evaluation of PLS solutions

Authors can submit their manuscripts through the Manuscript Tracking System at https://mts.hindawi.com/submit/journals/wcmc/snplt/.

Papers are published upon acceptance, regardless of the Special Issue publication date.

Lead Guest Editor
Li Sun, Xi'an Jiaotong University, Xi'an, China
lisun@mail.xjtu.edu.cn

Guest Editors
Kamel Tourki, Huawei France Research Center, Boulogne-Billancourt, France
kamel.tourki@gmail.com

Yafei Hou, Okayama University, Okayama, Japan
yfhou@okayama-u.ac.jp

Lu Wei, University of Michigan-Dearborn, Dearborn, USA
luwe@umich.edu

Submission Deadline
Friday, 29 June 2018

Publication Date
November 2018