Preface: Security and safety in physical layer systems

Aiqun Hu 1,* , Liang Jin 2, Xiangyun Zhou 3, Feng Shu 4, and Xiangwei Zhou 5

1 State Key Laboratory of Mobile Communications, Southeast University, Nanjing 210096, China
2 National Digital Switching System Engineering & Technological R&D Center, Zhengzhou 450002, China
3 School of Engineering, Australian National University, Canberra 2601, Australia
4 School of Information and Communication Engineering, Hainan University, Haikou Hainan 570100, China
5 Division of Electrical and Computer Engineering, Louisiana State University, Baton Rouge 70803, USA

Received: 17 January 2024 / Accepted: 18 January 2024 / Published online: 31 January 2024


This special topic mainly focuses on the progress of physical-layer security (PLS) technologies and their potential applications for the future beyond fifth-generation (B5G) and sixth-generation (6G) networks. The tremendous growth in connectivity and the ubiquity of wireless communications have resulted in an unprecedented awareness of the importance of security and privacy. Achieving secure and trusted communications is vital for future intelligent connected applications, especially life-critical vehicle-to-everything (V2X) applications. However, the heterogeneous, dynamic and decentralized architecture of these networks leads to difficulties for cryptographic key management and distribution. By exploiting the physical characteristics of devices, wireless channels and noise, PLS offers reliable solutions against eavesdropper attacks as complementary approaches to cryptographic techniques.

This special topic includes 8 papers, covering three main research directions of PLS, i.e., authentication, confidentiality, and malicious node detection. The strength of features and properties of the PHY layer are well studied for different security purposes. These papers are written by experts and scholars in relevant fields around the world and indicate the authors’ insights into the topics of physical layer security model, mechanism and applications in B5G and 6G networks, along with the inherent advantages of some cutting-edge technologies. The detail information is provided as follows:

In the survey “Radio frequency fingerprint identification for internet of things: a survey [1]”, the authors introduced related definitions of RFFI and details of each stage in the identification process, namely signal preprocessing, RFF feature extraction, further processing, and RFFI. Furthermore, a novel framework is established from the perspective of closed set and open set problems, and the related state-of-the-art methodologies are investigated, including approaches based on traditional machine learning, deep learning, and generative models. Additionally, they highlighted the challenges faced by RFF and pointed out that the universal RFF and the application of interpretable neural networks are promising subsequent research directions in this field.

In the survey “Securing NextG networks with physical-layer key generation: a survey [2]” the authors introduced the advantages of (PKG) techniques compared to traditional upper-layer based encryption schemes, its principles, and relevant research advancements. In some highly regarded emerging technologies and network scenarios, such as massive multiple-input multiple-output (MIMO), reconfigurable...
intelligent surfaces (RISs), artificial intelligence (AI) enabled networks, integrated space-air-ground networks, and quantum communication, the author analyzed the role of PKG, the challenges it faces, and the future research directions.

In “Exploration of transferable deep learning-aided radio frequency fingerprint identification systems [3]”, two transferable RFFI protocols are proposed leveraging the concept of transfer learning. Most deep learning-based RFFI systems require the collection of a great number of labelled signals for training, which is time-consuming and not ideal. Moreover, the long time required to train a neural network from scratch is also a challenge. The proposed protocols aim to address the aforementioned issues. The experimental results show that both the proposed RFFI protocols can achieve classification accuracy higher than 90% when transferred to a new IoT network, and require no more than five signals per device under test (DUT).

In the paper “Topology-based Multi-jammer Localization in Wireless Networks [4]”, the authors built a wide range of defense strategies to alleviate jamming attacks in wireless communication networks by focusing on the identification and exploitation of the jammers’ position. In the study, a framework that can partition network topology into clusters and can estimate the positions of multiple jammers even when their jamming areas are overlapping was developed. The experiments on a multi-hop network setup using MicaZ sensor nodes performed real-time collection of network topology changes under jamming and results demonstrated the proposed approach can localize multiple attackers efficiently.

In the paper “Covert communication in relay and RIS networks [5]”, the authors proposed a hybrid relay-reflecting intelligent surface (HR-RIS)-assisted strategy to enhance the performance of covert communications. Covert communication aims to prevent the warden from detecting the presence of communications. Different from conventional methods, the proposed HR-RIS is composed of active components and passive components, which means that it simultaneously possesses the functions of both a relay and a RIS. By jointly designing the transmit power at Alice and relay/reflection coefficients of the HR-RIS subject to the covertness and other constraints, the covert rate at Bob is maximized. The numerical results demonstrated that the proposed scheme significantly outperforms the conventional IRS/RIS-aided covert communication schemes in terms of covert rate by using a small number of active elements.

In the paper “The technology of radio frequency fingerprint identification based on deep learning for 5G application [6]”, the authors constructed a comprehensive link-level simulation platform tailored for 5G scenarios to expedite the integration of RFFI within 5G networks. The platform emulates various device impairments. A plausibility analysis was executed. Then, the impact of transmitter impairments, deep neural networks (DNNs), and channel effects on RFF performance was assessed. The result shows that under a signal-to-noise ratio (SNR) of 15 dB, the deep learning approach can accurately classify 100 User Equipment (UEs) with an accuracy rate of 91%.

In the paper “Optimization for UAV-assisted simultaneous transmission and reception communications in the existence of malicious jammers [7]”, the authors studied an unmanned aerial vehicle (UAV)-assisted communication system, where the UAV is dispatched to implement simultaneous transmission and reception (STR) in the existence of multiple malicious jammers. In frequency band-division-duplex (FDD) scheme, the bandwidth is divided into two portions which are used for transmitting information and receiving information, respectively. In time-fraction (TF) scheme, a fraction of a time slot is used for the downlink and the remaining for the uplink. By optimizing the UAV three-dimensional (3D) trajectory and resource allocation for each scheme, the worst-case throughput is maximized.

In the paper “A physical layer secret key consistency enhancement scheme using constellation decision information [8]”, the authors pointed out that existing schemes in secret key generation based on wireless channel (WC-SKG) only use pilot symbols for channel estimation, which may result in low secret key generation rate (SKGR) and incomplete utilization of received signal power. A consistency enhancement algorithm based on constellation decision information (CEA-CDI) was proposed to address the issue. By making soft decisions on the received data symbols, the influence of the channel is preserved for each symbol. The simulation results demonstrate that compared to the initial channel estimation, the proposed algorithm enhance performance by approximately 16 dB.

There are yet some open directions and challenges in this field, e.g., physical-layer key generation in static or poor scattering environments, radio frequency fingerprint identification in fast-moving environment and smart malicious nodes launching various attacks. The future research directions include but not limited to AI/ML-empowered PLS solutions, cross-layer security, energy-efficient PLS optimization,
content-aware PLS design, integration with PHY layer’s cutting-edge technologies such as RIS, NOMA, JCAS, BS communications, VLC, and THz communications, etc. Through this special topic, we hope to foster an exchange of research results, experiences, and products in the physical layer security domain from both theoretical and practical perspectives. Finally, we thank all the authors, editors and referees for their contributions and support to this special topic.

References