Physical-Layer Security of 5G Wireless Networks for IoT: Challenges and Opportunities

Ning Wang, Pu Wang, Amir Alipour-Fanid, Long Jiao, and Kai Zeng, *Member, IEEE*

***Abstract*—The fifth generation (5G) wireless technologies serve as a key propellent to meet the increasing demands of the future Internet of Things (IoT) networks. For wireless communication security in 5G IoT networks, physical-layer security (PLS) has recently received growing interest. This paper aims to provide a comprehensive survey of the PLS techniques in 5G IoT communication systems. The investigation consists of four hierarchical parts. In the first part, we review the characteristics of 5G IoT under typical application scenarios. We then introduce the security threats from the 5G IoT physical-layer and categorize them according to the different purposes of the attacker. In the third part, we examine the 5G communication technologies in 5G IoT systems and discuss their challenges and opportunities when coping with physical-layer threats, including massive multiple-input-multiple-output (MIMO), millimeter wave (mmWave) communications, nonorthogonal multiple access (NOMA), full-duplex technology, energy harvesting (EH), visible light communication (VLC), and unmanned aerial vehicle (UAV) communications. Finally, we discuss open research problems and future works about PLS in the IoT system with technologies of 5G and beyond.**

***Index Terms*—5G communication, Internet of Things (IoT), network security, physical layer.**

I. Introduction

THE fifth generation (5G) communication technologies, such as millimeter wave (mmWave), massive multiple-input-multiple-output (MIMO), and nonorthogonal multiple access (NOMA), are the key enablers of many Internet of Things (IoT) applications [1], [2]. Since the IoT is penetrating in industry as well as our daily life, the security and privacy of 5G IoT wireless networks are of the utmost importance. Physical-layer security (PLS), which safeguards information by exploiting the intrinsic characteristics or principles of the communications medium, is a promising wireless security technique for IoT [3], [4].

PLS techniques can improve the security of 5G IoT networks from two main aspects. One aspect lies in the potential that PLS can help 5G IoT networks reduce the latency of authentication, especially in mobile scenarios. For example, in the Internet of Vehicles (IoV) and unmanned aerial vehicle (UAV) networks, the vehicle and UAV are highly dynamic and may randomly join or leave the network at any time [5]. Roaming in different base stations (BSs) or access points (APs) results in frequent authentication handovers, which may introduce large authentication overhead and affect communication performance. By exploring the radio frequency (RF) fingerprint, PLS is expected to offer an efficient and direct authentication which will help 5G IoT systems to simplify the handshake process and reduce the authentication latency [6]. Another benefit is that PLS schemes can be used as an additional level of protection cooperating with the existing security mechanisms so as to bring a highly effective safeguard for 5G IoT devices. In Industry 4.0 and massive IoT scenarios, an enormous number of smart devices across heterogeneous networks are connected [2]. In such massive and heterogeneous 5G IoT networks, achieving effective key distribution and management is challenging. As one of the PLS schemes, key generation achieved by using the randomness of wireless channels can relieve this burden [7]. In addition, based on information theory, the design of channel security capacity in PLS can be used to support wireless communication security without encryption and decryption.

Nevertheless, PLS technologies are facing both new challenges and opportunities when we consider the uniqueness of 5G technologies in IoT networks. On the one hand, new 5G wireless techniques bring some new physical-layer threats to 5G IoT applications. For example, massive MIMO needs to collect accurate channel state information (CSI) for selecting optimal beamforming. In the channel training phase, the channel estimation could be compromised by a pilot-contamination attacker, which can imitate and send the same pilot signals as that of legitimate users (LUs). As a result, the attacker could acquire an illegitimate advantage in the next communication phase [8]. Apart from massive MIMO, NOMA, which can improve spectral efficiency and facilitate massive connectivity for 5G IoT systems, is also subject to the pilot-contamination attack [9]. Since a NOMA transmitter can communicate with multiple LUs simultaneously in the same channel with perfect CSI, it could be more easily affected and distorted by the pilot-contamination attack. Worse still is that the detection and defense of pilot-contamination attacks become more challenging because of the superposed and complicated transmission signals in NOMA [10]. In addition, when an active attacker has the full-duplex capability, they will have more advantage

Manuscript received February 27, 2019; revised May 27, 2019; accepted June 21, 2019. Date of publication July 9, 2019; date of current version October 8, 2019. This work was supported in part by the National Science Foundation under Grant CNS-1619073. *(Corresponding author: Kai Zeng.)*

N. Wang, A. Alipour-Fanid, L. Jiao, and K. Zeng are with the Department of Electrical and Computer Engineering, George Mason University, Fairfax, VA 22030 USA (e-mail: nwang5@gmu.edu; aalipour@gmu.edu; ljiao@gmu.edu; kzeng2@gmu.edu).

P. Wang is with the Department of Electrical and Computer Engineering, George Mason University, Fairfax, VA 22030 USA, and also with the School of Cyber Engineering, Xidian University, Xi'an, China (e-mail: pwang20@gmu.edu).

Digital Object Identifier 10.1109/JIOT.2019.2927379

when launching eavesdropping or jamming in IoT wireless networks [11].

On the other hand, however, the special characteristics in 5G wireless communications provide PLS new opportunities to counter these physical-layer threats in IoT systems. In mmWave communications, high propagation loss and directionality can be used to counter spoofing attacks and eavesdropping attacks [12], and the unique communication properties of mmWave MIMO systems can enable an efficient pilot-contamination attack detection in 5G IoT networks [10], [13]. Additionally, 5G IoT devices with in-band full-duplex (IBFD) capability can also be exploited to thwart jamming attacks [14]. Other than these typical 5G technologies, the emerging wireless technologies with high potential in IoT networks, such as energy harvesting (EH), visible light communication (VLC), and UAV communications, are expected to provide new PLS solutions.

A. Contributions of the Survey

In this paper, we provide a comprehensive survey on the recent PLS research in 5G IoT networks. In particular, we first review the typical characteristics of 5G IoT networks and analyze their impacts on IoT security. Then the physical-layer threats in 5G IoT networks are categorized by different types of attackers, including eavesdropping, contamination, spoofing, and jamming. We survey the state-of-the-art works about PLS techniques to alleviate the physical-layer threats in 5G IoT networks, involving massive MIMO, NOMA, mmWave, full-duplex radio, EH, VLC, and UAV communications. Based on the presentation and analysis, we discuss the open issues and future research topics on PLS in 5G IoT.

It should be noted that there are existing survey papers on IoT security or PLS research [4], [15]–[18]. However, a comprehensive survey of PLS technologies in 5G IoT wireless communications is still missing, and that is the main contribution of this paper. The two most relevant works are [4] and [18]. While Hamamreh *et al.* [4] provided a survey of PLS technologies, this paper does not analyze the impact of 5G IoT communication technologies. Wu *et al.* [18] offered a survey of PLS for 5G communications, nevertheless, it does not thoroughly discuss IoT networks and other emerging wireless technologies of 5G and beyond, such as EH and VLC communications. In this survey, we provide a comprehensive and detailed overview of PLS in 5G IoT networks, involving typical scenarios, physical-layer threats, state-of-the-art techniques, limitations, and potential solutions.

B. Paper Organization

The rest of this paper is organized as follows. We first review the unique characteristics of 5G IoT networks in Section II, where the impact of 5G communications for IoT security is analyzed. Various physical-layer attackers with different purposes are investigated in Section III, in which the corresponding countermeasures and new scenarios under 5G IoT are discussed. We then survey PLS solutions for 5G IoT wireless communications in Section IV. Section V discusses the open issues and future research topics for PLS research under 5G IoT networks. The conclusion is given in Section VI. Table I lists the summary of abbreviations in this paper.

TABLE I
SUMMARY OF ABBREVIATIONS

Abbreviations	Notations
IoT	Internet of Things
NOMA	Non-orthogonal multiple access
WSNs	Wireless sensor networks
WBANs	Wireless body area networks
MIMO	Multiple input multiple output antenna
MmWave	Millimeter wave communication
PLS	Physical layer security
EH	Energy harvesting
VLC	Visible light communication
OAM	Orbital angular momentum
IoVs	Internet of vehicles
UAVs	Unmanned aerial vehicles
SIC	Successive interference cancellation
CSI	Channel state information
BS	Base station
SNR	Signal to noise ratio
AoA	Angle of arrival
AoD	Angle of departure
AN	Artificial noise
AF	Amplify-and-forward
PCA	Pilot contamination attack
AP	Access point
LU	Legitimate user
SC	Superimposition coding
PSK	Phase shift keying
IBFD	In-band full-duplex
AF	amplify-and-forward
LED	Light emitting diode
MISO	Multiple-input-single-output
LoS	Light-of-sight
MMTC	Massive machine-type-communication

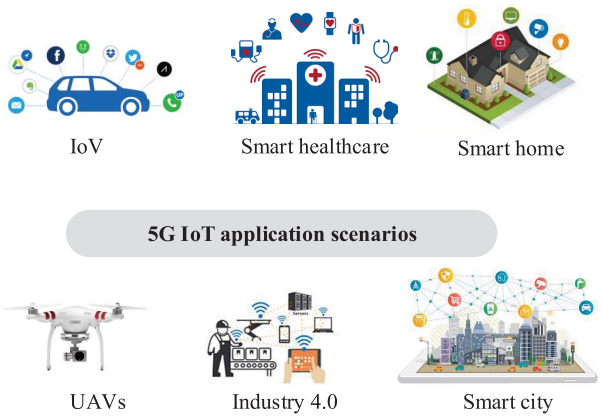


Fig. 1. Typical 5G IoT application scenarios.

II. CHARACTERISTICS OF 5G IOT NETWORKS

Compared with traditional IoT networks, 5G IoT networks have increasingly wide applications, such as IoV, smart

healthcare, smart home, smart city, UAVs, and Industry 4.0, as shown in Fig. 1. In this section, we discuss three typical characteristics of 5G IoT networks, where the traditional security mechanisms may not be suitable or efficient, but the PLS solution can provide possible solutions, concerning mobility, massive connection with resource constraint, and heterogeneous hierarchical architecture.

A. Mobility

In many application scenarios in 5G IoT networks, the mobility of devices is a prominent characteristic. For example, UAVs and IoVs are two typical 5G IoT applications, and they are playing a key role in intelligent traffic and smart city [19]. In contrast to communications with fixed infrastructures, IoT devices with varying speeds in IoV and UAVs may join or leave a proximal network without prior configuration [20]. If the IoT devices are fast-moving and continually switching between different BSs or APs, this will result in frequent authentication requests. Since the authentication process based on cryptography needs multiple handovers to perform key distribution and cryptographic protocol, current cryptographic authentication methods struggle to provide an efficient and concise solution, As a result, excessive authentication handovers could lead to the authentication delay beyond the latency tolerance of 5G services [7]. In contrast, by utilizing the inherent physical features, PLS methods are expected to help 5G IoT networks simplify the handshake process and reduce the authentication latency in mobile 5G IoT networks. For instance, RF fingerprinting technologies could provide a method of direct identification for the authentication process, and key-generation techniques based on a wireless channel can facilitate the key distribution.

B. Massive IoT With Resource Constraints

In many typical IoT applications, such as smart home, smart healthcare, and smart city, there are massive low-cost IoT devices which can make decisions autonomously based on information originating from sensors. These IoT devices with low end-to-end cost can efficiently access the Internet thanks to 5G communication technologies, such as NOMA, massive MIMO, and massive machine-type-communication (MMTC) [1], [2]. However, when facing a large number of these low-cost IoT devices, it is difficult to efficiently distribute and manage the secret key. Another difficulty is that with limited resource, the IoT devices cannot afford very complicated cryptography to maintain strong security [15]. Under these cases, these 5G IoT devices may be more easily compromised by malicious attackers. To address these issues, PLS schemes could offer effective and easy solutions to promote the security of such 5G IoT networks. For example, key-generation based on a wireless channel may expedite the key distribution for numerous IoT devices, and the design of security channel based on information theory can enhance the security performance without cryptographic schemes in 5G IoT.

C. Heterogeneous Hierarchical Architecture

Heterogeneous hierarchical architecture is also a noticeable characteristic of 5G IoT networks [21]. In Industry 4.0, IoT networks interconnect different devices and enable massive machine-to-machine (M2M) communication between heterogeneous devices without human intervention [2], [22], [23]. In general, these IoT devices always connect with each other with various power and computation capabilities at the different levels of the hierarchical architecture. However, how to effectively protect communication with heterogeneous hierarchical architecture is a largely open problem [24]. Based on physical-layer features, PLS solutions which are not influenced by the heterogeneous hierarchical architecture, are expected to offer an effective remedy to improve the security of such 5G IoT communication scenarios.

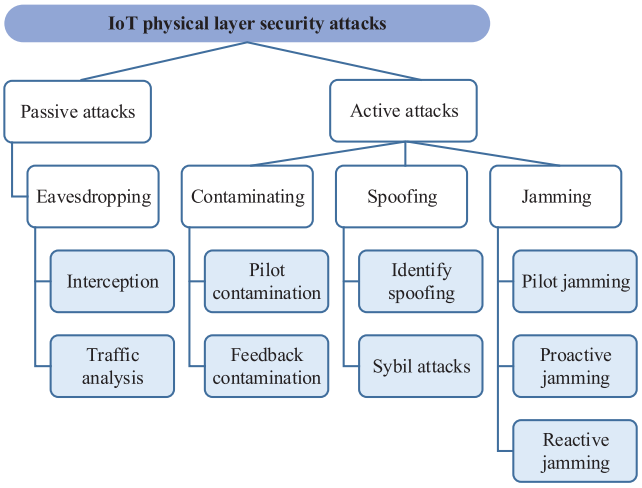


Fig. 2. Security threats in 5G IoT physical layer.

III. Physical-Layer Threats in 5G IoT

5G wireless communication technologies not only could open the door for physical-layer threats in IoT networks but can also provide new opportunities to mitigate the security risks. On the one hand, some new 5G wireless techniques could be more sensitive to existing physical-layer attacks. For example, massive MIMO and NOMA communications are very sensitive to pilot contamination attacks (PCAs). On the other hand, some physical-layer threats are curbed by 5G wireless communication technologies. For instance, beamforming in massive MIMO can be used to reduce the risk of eavesdropping.

In this section, we introduce the typical physical-layer threats in IoT networks, where the categorization is based on the different purposes of attackers, including eavesdropping, contaminating, spoofing, and jamming, as shown in Fig. 2. Furthermore, we will overview the corresponding PLS countermeasures and discuss the impact of 5G wireless technologies for these physical-layer threats.

A. Eavesdropping

Eavesdropping attackers attempt to intercept some confidential information. Since the attackers do not transmit any signal, it is hard for the legitimate transmitters or receivers to detect or locate the eavesdroppers. This physical-layer threat can be divided into two types based on the main manner of the attacker: 1) interception and 2) traffic analysis [25], [26].

1) *Interception:* Monitoring and eavesdropping are the most common attack on privacy for IoT devices. By snooping the nearby wireless environment, the attacker could easily discover legitimate communication. When the traffic conveys control information about the sensor network configuration, which contains potentially more detailed information than accessible through the location server, eavesdropping can act effectively against privacy protection [25].
2) *Traffic Analysis:* Critical information in legitimate communication may be encrypted by cryptographic algorithms. Under this case, the attacker is able to intercept the transmitted signal but cannot obtain the important contents. However, traffic analysis may be useful for tracking the communication patterns to facilitate other forms of attacks [26]. IoT devices' activities can potentially reveal enough information for enabling an attacker to cause malicious harm to the IoT networks.

1) PLS Strategies to Counter Eavesdropping: To counter eavesdropping attacks, the basic idea in PLS schemes is to create a channel security capacity between LUs, where the transmitter delivers a positive information rate (channel security capacity) to the legitimate receivers and ensures that the eavesdropper cannot obtain any information. Generally, there are two methods to achieve this channel security capacity, involving PLS based on artificial noise (AN) and PLS channel coding. The PLS using AN provides interference to the eavesdroppers to decrease the channel capacity of eavesdropping channels and improve the channel security capacity [27]. The PLS channel coding achieves this purpose by using the function of error correction in the channel coding, where the probability of the decoding error under the channel between the eavesdropper and LUs, will become higher than that of the channels between LUs. The existing PLS channel coding includes LDPS codes [28], polar codes [29], and lattice codes [30].

2) Under 5G IoT Networks: For 5G IoT networks, the potential of a PLS solution to this passive eavesdropping attack will be increased dramatically. Per the investigation in [8], resorting to massive MIMO technology, the received signal power at LUs could be several orders of magnitude larger than the received signal power at the eavesdropper. As a result, the channel security capacity offered by PLS schemes is close to the full transmission capacity of the LUs. Thus, if the passive eavesdropping attacker is not very close to the LUs, it is hard to obtain useful information from the legitimate communication under the massive MIMO scenario. Therefore, this physical-layer threat is curbed to a certain degree under 5G IoT networks with massive MIMO.

B. Contaminating

Contaminating attackers aim to contaminate the channel estimation phase and obtain illegitimate advantages in the next communication phase [31]. According to different channel estimation stages, this type of attacks can be divided into pilot and feedback contamination.

1) *Pilot Contamination:* In pilot contaminating attacks, a smart active attacker is assumed to have precise prior knowledge of pilot information [32]. During the channel training phase, the adversary can send the same pilot signals as that of LUs to confuse AP or BS. Hence, the AP or BS will make a wrong CSI estimation between itself and LUs. This wrong CSI information will in turn yield wrong precoding, beamforming, or successive interference cancellation (SIC) at the AP or BS.
2) *Feedback Contamination:* Existing 5G beam-training protocols, such as IEEE 802.11ad [33], are to find the optimal antenna steering. The best received probing frame is reported back so that the transmitter can select the corresponding beam for transmissions. Attackers can inject a forged feedback to force the transmitter to steer their beams to attackers other than the intended users. Even if the transmitter steers the beams in an unintended direction, it could cause a denial-of-service and prevent an association process in beam-training protocols [31].

1) PLS Strategies to Counter Contaminating: In general, physical-layer authentication (PLA) can be used to counter PCAs, including pilot-contamination attack detection and radio-frequency (RF)/hardware-based PLA. Existing pilot-contamination attack detections emphasize the detection by using special signals, such as pilots design [34] or beamformer design [35]. RF/hardware-based PLA is based on the fact that different wireless transceivers emit RF signals with unique features/patterns in analog and modulation domains, and these features can be explored to counter the contaminating attacks [6]. For feedback contamination attacks, a probability method was proposed in [31], where a sector sweep with authentication is presented to against feedback contamination attacks.

2) Under 5G IoT networks: In massive MIMO and NOMA communications, the beamforming design and SIC at BS/AP are based on the CSI which is estimated through pilot sequences. If the pilot signals are contaminated by attackers, the latter will gain more chances to eavesdrop on legitimate communication or significantly degrade the communication performance of LUs. While several methods have been proposed to detect this type of attack [34], [35], due to the complex pilot design and retransmission mechanisms, these methods are not desirable solutions for the low-cost 5G IoT devices. Meanwhile, there have not been many investigations on how to achieve an efficient RF/hardware-based PLA in 5G IoT networks. Hence, the contaminating attack is still a nontrivial physical-layer threat for 5G IoT networks.

C. Spoofing

Spoofing attackers attempt to join or corrupt legitimate communications by injecting some forged identity information. A spoofing attacker can transmit a deceiving signal with a higher power in the transmission phase between transceivers, or monitor the legitimate transmitter for sending a forged signal between two legitimate signals [36]. There are two typical spoofing attacks: 1) identity spoofing attacks and 2) Sybil attacks.

1) *Identity Spoofing:* Identity spoofing attacks are easy to launch in IoT networks. By using a fake identity such as the media access control (MAC) or Internet protocol (IP) address of the LU, an identity spoofing attacker can claim to be another legitimate IoT device. The attacker may gain illegal access to the IoT network and launch a more advanced attack, such as man-in-the-middle attacks and denial-of-service attacks [6].
2) *Sybil Attacks:* In the Sybil attack, a malicious node can impersonate other nodes or claim false identities, and the attacker may generate an arbitrary number of additional node identities, using only one physical device [37], [38]. In the presence of Sybil attacks, the IoT systems may generate wrong reports, and users may receive spam and lose their privacy [39].

1) PLS Strategies to Counter Spoofing: PLA is the main scheme to counter the spoofing attacks in PLS strategies [36]. Other than RF/hardware-based PLA, channel/location-based PLA techniques offer a way to detect identity spoofing or sybil attacks, where it can work even with coarse information, such as received signal strength (RSS). If an attacker is at a different location as the legitimate device, channel/location-based PLA techniques can efficiently detect it by examining the RSS fingerprint of the signals. Even in Sybil attacks, where an attacker can pretend to be multiple devices by transmitting packets using multiple identities, channel/location-based PLA techniques can efficiently detect this type of attack by recognizing that the received signals corresponding to different identities are eccentrically transmitted from the same location.

2) Under 5G IoT Networks: Resorting to 5G IoT wireless communication techniques, spoofing attackers can become smarter. For example, equipped with the full-duplex radio, the attacker can transmit fake identity information and monitor the victims at the same time. In this way, it can design the spoofing interval more intelligently. Conversely, LUs could also enjoy the benefits of 5G technologies to counter this physical-layer threat. For instance, beamforming technologies in massive MIMO and directionality in mmWave could be explored to curb the damage of spoofing attacks. Exploiting the unique features of 5G wireless technologies to achieve an effective solution for spoofing attacks is an interesting topic.

D. Jamming

The target of a jamming attacker is to block legitimate communications by noise [40]. For this purpose, the adversary could transfer radio signals continuously on a wireless channel to disrupt communication by decreasing the signal to noise ratio (SNR). This can lead to denial-of-service attacks at physical layer [41]. In general, jamming attacks can be divided into three types: 1) pilot jamming; 2) proactive jamming; and 3) reactive jamming.

1) *Pilot Jamming:* The pilot jamming attack can be viewed as a special case of jamming attacks launched during channel training phase [42]. Its purpose is to corrupt the legitimate communication even without the exact pilot sequences. Only possessing the prior knowledge of the pilot length and pilot sequence codebook, an adversary can launch a pilot jamming attack. This jamming attack can be very energy efficient since the attacker only needs to corrupt the pilot signals, not the entire communication.
2) *Proactive Jamming:* Proactive jamming attackers would send jamming or interfering signals whether the legitimate data communication is there or not [40], [43]. In order to save energy and toggle between the sleep phase and the jamming phase, attackers sporadically spread either arbitrary bits or normal packets into networks. This jamming type can be further classified into spot jamming, sweep jamming, barrage jamming, and deceptive jamming [40].
3) *Reactive Jamming:* The reactive jamming attackers can monitor the activity of the legitimate channel. If there is an activity, the adversary immediately sends out a random signal to collide with the existing signal on the channel [44].

1) PLS Strategies to Counter Jamming: Generally, PLS strategies to address jamming attacks include frequency-hopping spread spectrum, direct sequence spread spectrum, and ultrawide-band technology [40]. Meanwhile, these countermeasures to jamming attacks can be categorized in jamming detection techniques [45], reactive countermeasures [46], and proactive countermeasures [47]. The detection techniques cannot cope with jamming alone, but can instantly detect jamming attacks and provide valuable data to enhance jamming protection with other countermeasures. Reactive countermeasures enable reaction only upon the incident of a jamming attack sensed by the jamming detection. Moreover, the proactive countermeasures perform a continuous activity to counter jamming attack whatever the jamming is, and it will cost more energy than reactive countermeasures.

2) Under 5G IoT Networks: With regard to jamming attacks in 5G IoT networks, the full-duplex technique is an often considered 5G wireless technology. On one hand, a jamming attacker with a full-duplex radio is able to transmit interfering signals and listen to legitimate communication, simultaneously. On the other hand, the full-duplex LUs can also leverage the capability of full-duplex to counter jamming attacks. In addition, UAV communications can also be used to alleviate the traffic caused by jamming attacker [48]. More diverse jamming attacks and the corresponding countermeasures will be introduced in Section IV-D.

IV. PLS Solutions for 5G IoT Networks

In this section, we survey the recent research about 5G IoT PLS solutions with different wireless techniques of 5G and beyond, including massive MIMO, NOMA, mmWave, full-duplex radio, EH, VLC, and UAV communications.

A. Massive MIMO

As one of the core 5G technologies, massive MIMO has received huge attention on IoT research [49], [50]. Massive MIMO can provide manifold communication advantages based on beamforming, such as an array gain corresponding to the

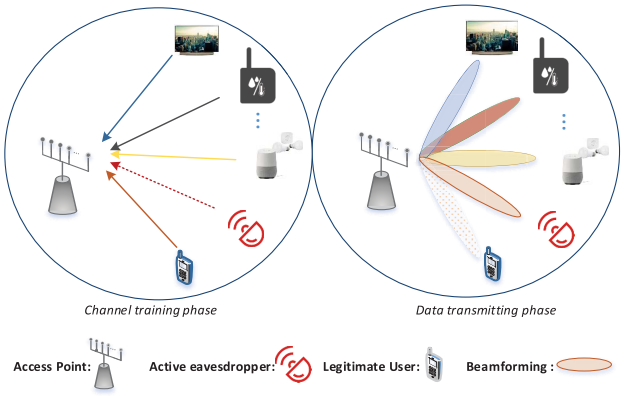


Fig. 3. PCA in wireless IoT systems under massive MIMO scenarios.

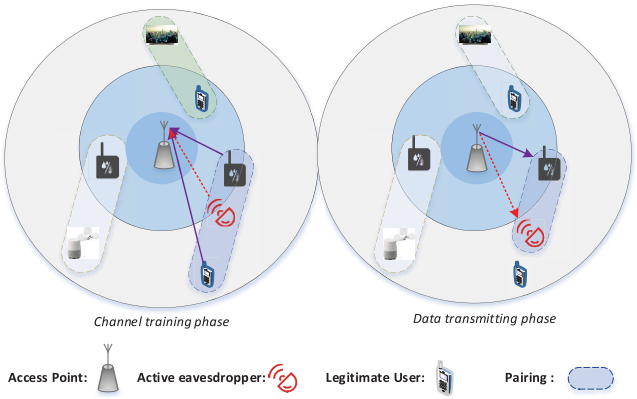


Fig. 4. PCA in IoT with NOMA scenario.

number of antennas, channel hardening, and nearly orthogonal channels [51]. Meanwhile, MIMO techniques for PLS are discussed in [52] and [53]. Kapetanovic *et al.* [8] investigated the passive eavesdropping and active attacks in massive MIMO. They presented that the potential of PLS against passive eavesdropping attacks in massive MIMO technique can be dramatically increased while facing serious threat under PCAs [32]. As shown in Fig. 3, an active attacker can send the same pilot sequence as LUs', and cover the legitimate pilot signals during the channel training phase. Thus, the active attacker has a greater chance to disturb the beamforming and degrade the channel gain at LUs while even improving the attacker's channel gain. Therefore, the PCA is a fatal physical-layer threat for massive MIMO communication.

Counter Physical-Layer Threats: In existing on PLS, several schemes have been proposed to counter the PCAs aforementioned in Section III-B. One is a random pilot scheme which introduces controllable randomness in pilot signals to detect this active attacker. There are mainly two variations: 1) random phase-shift keying (PSK) pilot and 2) random frequency shifts (CFO) pilot. Random PSK pilot is first proposed in [34] and an improved variation considering three or more observations is provided in [54]. First, an LU transmits a sequence of random PSK pilot symbols, which are chosen independently from an N-PSK constellation. Second, after obtaining these PSK symbols, AP detects the phase change between two symbols and estimates whether an active attacker exists over this period. If the received signals have valid PSK symbols, there is no active attacker detected, otherwise, an active attacker is detected. Another random pilot scheme is based on random frequency shifts [35]. An LU deliberately introduces multiple random frequency shifts when transmitting the pilot sequence. Then AP can detect whether there is an active attacker by calculating the autocorrelation matrix for the training phase. In addition, a special beamformer has been designed to detect the activity of pilot contamination attackers [54]. LU transmits a training signal to AP who uses this training signal to estimate the channel. In the next phase, AP establishes a specialized beamformer that ensures an agreed value of the received signal at LU approaching to 1, and transmits the signals to LU by using the same beamformer. If the attacker is active, the channel estimation in the second phase will inevitably be affected, i.e., the agreed value at LU will sharply decline under the case of active attackers.

The pilot retransmission scheme counters the jamming attack during the channel training phase [55]. First of all, AP establishes an achievable massive MIMO uplink rate for a single user with the presence of a pilot jamming attacker. By estimating the jamming pilot, AP decides whether LU needs to retransmit its pilot signal. The main idea and precondition lie in that the jamming attacker may have the prior knowledge of the pilot length and pilot sequence codebook, but lacks the knowledge of exact pilot sequence. Hence, by retransmitting the pilot sequence, AP can find a proper pilot sequence to minimize the pilot jamming to a certain degree, then mitigate the impact of jamming.

B. NOMA

Via nonorthogonal resource allocation, IoT with NOMA can improve spectral efficiency and achieve massive connectivity with low transmission latency and signaling cost [56]. It can be used in many IoT applications, from smart manufacturing to smart farming, where there are hordes of sensors and actuators [9]. More specifically, user pairing, i.e., assigning two users (near user and far user) to a single orthogonal resource block [57], is developed to trade off the complexity and efficiency. Superposed coding technology is applied to achieve the capability of superposing multiple signals into one orthogonal resource. Accordingly, to extract the corresponding information for separate LUs, SIC is used to eliminate the redundant signals based on the corresponding CSI. However, if the pilot sequence is falsified or distorted by PCAs, it is more likely to cause the failure of SIC or lead to confidential information leakage, as shown in Fig. 4.

Counter Physical-Layer Threats: The authors in [10] presented a new pilot contamination detection scheme, which can be applied in wireless IoT systems under NOMA communication scenarios. This scheme only relies on the signal processing at AP without requiring any additional signal design or change at LU (i.e., IoT device). By harnessing the sparseness and statistics of mmWave and massive MIMO virtual channel, two effective PCA detection schemes are proposed for tackling static and dynamic environments, respectively.

For the static environment, the problem of PCA detection is formulated as a binary hypothesis test of virtual channel sparseness. For the dynamic environment, the statistic of the peak in the virtual channel is leveraged to distinguish the contamination state from the normal state. A peak estimation algorithm and a machine learning-based detection scheme are proposed to achieve high detection performance. In addition, Liu *et al.* [58] investigated the secrecy performance of large-scale NOMA networks both for a single-antenna aided and a multiple-antenna assisted scenario at the BS. For the single-antenna scenario, the exact analytical expressions of the secrecy outage probability (SOP) of the selected pair of NOMA users are derived, when relying on channel ordering. Tian *et al.* [59] studied the secrecy sum rate optimization problem for the downlink MIMO NOMA system.

C. MmWave

MmWave, an important 5G communication technology, can improve the transmission in 5G IoT networks [60], [61], in which IoT devices can be connected by higher bandwidth communication channels [62]. Compared to micro-Wave, mmWave has various new characteristics such as blocking effect and highly directional transmissions, etc. [12]. Under these new characteristics of mmWave channels, the efficiency of traditional PLS techniques could be improved [10], [12]. Furthermore, the tiny wavelengths of mmWave allow for dozens to hundreds of antenna elements to be placed in an array on a relatively small physical platform. This can significantly support the application of massive MIMO and facilitate the integration of various 5G technologies. More than that, exploring the synthesis character of mmWave and other 5G technology in IoT systems is a very promising research direction.

Counter Physical-Layer Threats: The authors in [63] proposed to use new channel characteristics of mmWave, virtual angle of arrival (AoA) and angle of departure (AoD), to generate a shared secret key between two devices. Other than reciprocity, AoA and AoD of the virtual channel present sparsity and are efficient and robust against noise. The bit agreement ratio becomes higher when the number of antennas increases, along with higher key generation rates achieved per channel sounding. Wang *et al.* [12] investigated the secrecy performance of a mmWave cellular network. They proposed a systematic secrecy performance analysis approach for the mmWave cellular communication based on stochastic geometry framework and blockage model. A detailed secrecy performance analysis of both noise-limited and AN assisted mmWave communication was conducted. Vuppala *et al.* [64] studied the secrecy outage of mmWave networks under the impact of blockages. The authors used a network model that accounts for uncertainties both in node locations and blockages, to characterize the conditional connection outage probability and SOP of hybrid networks under multiple eavesdroppers. Xiao *et al.* [65] investigated the PLS solution of mmWave satellite communications, where the authors introduced a ray tracing-based mmWave satellite communication channel model, and show that the secrecy capacity in mmWave band widely depends on the richness of the RF environment.

D. Full-Duplex Radio

Full-duplex radio, i.e., IBFD [66], can simultaneously transmit and receive data signals with the same frequency band. Thus, based on the advantages offered by the features of full-duplex radio, it can bring IoT applications double ergodic capacity, reduce feedback delay, and end-to-end delay [66], as it did in the case of virtual reality (VR) and augmented reality (AR) [67], [68]. For PLS solutions, full-duplex is often used to counter to jamming attack under relay scenario [13]. Nonetheless, the unique characteristic of simultaneously transmitting and receiving signals at the same frequency band can also be explored to detect PCA [69]. As the technology matures gradually, full-duplex radio is expected to apply in many more wireless devices, which could further facilitate IoT applications.

Counter Physical-Layer Threats: The study of PLS solutions with full-duplex can be classified into four categorizations: 1) full-duplex receiver; 2) full-duplex transceiver; 3) full-duplex BS; and 4) full-duplex eavesdropper [18]. Zheng *et al.* [14] derived the SOP of a typical full-duplex receiver based on the stochastic geometry framework. The deployment of the full duplex receivers is optimized for the network-wide secrecy throughput maximization. Sun *et al.* [70] studied a more general system in the presence of multiple potential eavesdroppers, where a multiple-antenna full-duplex BS receives/transmits information from/to multiple single-antenna users. Wan *et al.* [71] maximized the secrecy sum rate of bidirectional full-duplex communication systems in the presence of a single-antenna eavesdropper under the sum transmit power constraint. Tang *et al.* [11] formulated the active eavesdropper problem into a hierarchical game theory problem, and the behaviors of the eavesdropper and LU seem like a leader and a follower.

E. EH

In the era of 5G and beyond, EH technique, i.e., simultaneous wireless information and power transfer (SWIPT) technology, can be of importance for 5G IoT networks, since wireless transceivers and sensors are usually constrained by energy [18]. The concept of SWIPT is that the RF signals can be simultaneously utilized to power multiple uses for EH and information decoding in a relatively long distance [72]. It becomes more attractive in IoT applications, notably in wireless body area networks (WBANs) and wireless sensor networks (WSNs), where it is inconvenient to replace or recharge the battery-limited devices [73]. Apart from providing noteworthy energy-efficient wireless communication, security and privacy is another crucial issue in the SWIPT system. These two separate objectives could bring new challenges for the designing phase of PLS in SWIPT enabled communication networks [74].

Counter Physical-Layer Threats: A handful of works have studied SWIPT for physical-layer security. Zhang and Liu [75] investigated the secrecy information decoding and power

transmission in downlink multiuser orthogonal frequency-division multiple access systems. They formulated an optimization problem to maximize the aggregated harvested energy of all users while satisfying the secrecy rate requirement of each user. In [76], with the help of SWIPT-enabled multiantenna amplify-and-forward (AF) relays, the secrecy capacity is maximized by jointly optimizing their cooperative beamforming with limitation of each relay's EH power constraints. The authors used AN to interfere with the eavesdropper for secrecy information nodes as well as to operate non-ID receivers as the primary source of EH [77]. All the techniques mentioned above are suitable for limited IoT devices without additional resource consumption.

Meanwhile, the SWIPT assisted communication with other 5G key technologies, such as mmWave and NOMA, is becoming a hot topic [78]. Security issues and possible solutions can vary in different types of SWIPT-enabled communication networks, with specific characteristics of these technologies. Nikoloska *et al.* [79] investigated the secrecy capacity of a point-to-point full-duplex wireless powered communication system in the presence of a passive eavesdropper. However, solid and comprehensive works about PLS and EH with 5G wireless technologies are still missing, whereas their specific features have not yet been exploited to improve the secrecy performance and harvested energy. For instance, the near NOMA users close to the source harvest energy and then can utilize the harvested energy to transmit AN signal to degrade the eavesdropping performance. Furthermore, the 3.5 GHz in low-frequency band and 28 GHz in a high-frequency band, possessing totally different channel propagation characteristics, will have a significant impact on the EH and secure information transmission.

F. VLC

VLC is an enabling technology that exploits the lighting infrastructures for short-range wireless communications. VLC communications benefit from the license-free light spectrum (high bandwidth), immunity to RF interference and high scalability [80]. Therefore, VLC has emerged as a great potential solution to support the 5G IoT with higher data rates, massive device connectivity, higher energy efficiency, lower traffic fees, and ultralow latency [81], [82]. Recent developments in the organic light emitting diode (LED) have enabled devices with high efficiency and brightness that can be used for data transmission as in conventional VLC systems [83]. Hence, VLC has been introduced either in replacement of, or complement to, existing RF networks, to support the indoor traffic demands in 5G IoT in which the amount of the connected devices to the Internet is increasing dramatically. Although VLC communication is more secure than traditional RF wireless communications due to the high directionality of laser beam, it could also be susceptible to optical tapping eavesdropping [84], [85].

Counter Physical-Layer Threats: Mostafa and Lampe [86] considered achievable secrecy rates of the multiple-input single-output (MISO) wiretap VLC channel. The VLC channel is modeled as a deterministic and real-valued Gaussian channel subject to amplitude constraints. If the eavesdropper's CSI is available to the transmitter, null-steering is utilized to cancel the eavesdroppers reception and fully secure the source-destination rate. While if without such information, AN can be added to the transmitted signal to jam the eavesdropper's reception and improve achievable secrecy rates. Mostafa and Lampe [85] investigated a scheme of enhancing the confidentiality of VLC links via physical-layer security techniques, where the lower and upper bounds on secrecy capacity of the amplitude-constrained Gaussian wiretap channel is given. Beamforming is leveraged to derive a closed-form lower bound on the secrecy capacity of the MISO channel. The work in [87] considered the VLC channel with orbital angular momentum (OAM) multiplexing under different atmospheric turbulence conditions. The authors presented the numerical simulation of the propagation of Laguerre–Gaussian beam over a turbulent LoS link. An information theoretic security analysis based on optical tapping scenarios is provided. The results show that even if adaptive optics are not used, a higher secrecy capacity can be achieved over conventional on–off keying VLC channels under certain channel conditions by using OAM multiplexing. Wang and Djordjevic [88] extended those studies by simulating the propagation of various orders of Bessel–Gaussian OAM beams under similar turbulence conditions and demonstrated higher secrecy capacity.

G. UAV Communications

UAVs have enormous potential in the public and civil domains, and UAV-aided communications also have emerged as an effective solution to provide large coverage and dynamic capacity for IoT applications [20]. It can be used for information dissemination, relaying and collection to/from the IoT devices because the low-altitude UAVs can be rapidly deployed as UAV-enabled BSs in 5G IoT systems with high mobility and fast deployment. Compared favorably with terrestrial systems, UAVs can overcome the propagation and blockage constraints due to terrain characteristics, especially for mmWave, and augment the coverage area by optimizing the UAVs' location (e.g., altitude) in the 3-D model [89]. For a start, Motlagh *et al.* [90] investigated UAV to provide 5G networks for the low-density population in rural and low-income zones. Feng *et al.* [91] utilized a multiantenna UAV, which follows a circular trajectory and hovers, to serve as a cluster of single antenna IoT devices. In addition, Khosravi *et al.* [92] concerned the performance of the UAV-assisted mmWave network for the 5G system in mobility-enabled urban environments by simulation and evaluation.

Counter Physical-Layer Threats: Security is a major concern that hinders the wide deployment of UAV-aided communication networks, thus a secure and efficient communication is a requirement for UAV communication [93], especially for the 3-D UAV-enabled mmWave networks. To guarantee perfect security, illegitimate users need to be prevented from eavesdropping any information intended to LUs. Existing security works have been considered to secure UAV-involved wireless communication at the physical layer [48], [94]–[99].

Liu and Kwak [95] analyzed the secrecy performance of UAV-aided relaying networks in which a best relaying pair is selected to convey the source message to the destination with various eavesdropping probabilities. Lu *et al.* [48] presented a UAV-aided 5G communication framework against jamming on a serving BS in 5G systems. The UAVs use reinforcement learning methods to choose the optimal relay policy for mobile devices within a heavily jammed BS. He *et al.* [100] also investigated a UAV-enabled mobile relaying system and aimed to optimize the transmission power of the source and the relay for maximizing the secrecy rate. Meanwhile, some works emphasize the features of high mobility and on-demand deployment to enhance security from the physical layer. Unlike the most existing literature on wireless PHY layer security only with ground nodes at fixed or quasi-static locations, these works [96], [97] exploited the high mobility of the UAVs to proactively establish favorable and degraded channels for the legitimate and eavesdropping links, respectively, via the trajectory design. Moreover, in a dual-UAV system, one UAV moves to communicate with multiple ground users while the other one flies to jam eavesdroppers on the ground. This strategy is applied to secure UAB-aided communication with optimization of UAVs trajectories and user communication scheduling [98].

For the key 5G wireless technologies, few relevant research investigates the PLS solution in the UAV networks yet. Khosravi *et al.* [92] analyzed the secrecy performance of 3-D UAV-enabled mmWave networks considering air-to-ground channel features (e.g., 3-D antenna gain), improved by using part of UAVs to send jamming signals, and used the matern hardcore point process to guarantee the safety distance among the randomly deployed UAV BSs. Another work investigated the secrecy rates of UAV-based mmWave communication network considering NOMA together with highly directional multiantenna and optimized a protected zone to enhance the secrecy [99]. However, the effects of new 5G wireless technologies, in the PLS for UAV networks, have not been solidly and comprehensively considered.

V. Open Issues and Future Topics

In this section, we discuss the open issues of existing PLS solutions for 5G IoT systems and future research directions.

A. Open Issues

In view of the unique characteristics of wireless 5G IoT systems, there are four major open issues in existing PLS solutions.

1) Existing methods do not sufficiently consider the low complexity profile of LUs (i.e., low-cost IoT devices) in wireless 5G IoT systems. Under the condition of limited hardware, low complexity, and severe energy constraints on many low-cost IoT devices, any signal processing requirements for LUs other than normal communication should be considered as an extra burden. A desirable PLS solution should not require any change in the low-cost IoT devices or introduce any extra processing or communication cost. Therefore, some mechanisms in existing methods, such as complex pilot design and retransmission, cannot be claimed as ideal solutions. On the other hand, we could allow certain extra signal processing or computation at AP or BS which usually has more resource and power.
2) PLA schemes based on the new features of 5G wireless technologies are still missing. There are lots of new physical-layer features in 5G IoT networks, such as high propagation loss and directionality in mmWave and superposed signals in NOMA. However, there are few studies to exploit these new features to achieve effective PLA schemes. Furthermore, the combination of different 5G techniques in 5G IoT networks may bring new synergy to inspire new physical-layer authentications.
3) It requires more PLS research on the new communication scenarios in 5G IoT networks. For instance, more research works are needed to design effective and efficient PLS schemes for practical UAV-involved networks with their unique features, such as mobility and unique air-to-ground channel characteristics (e.g., 3-D antenna beamforming). Furthermore, PLA schemes considering EH and VLC communications are still open.
4) Few studies have been done on the mobility of 5G IoT devices. Mobility will be an intrinsic feature in many wireless 5G IoT applications, such as smart transportation and UAV networks, etc. It will be very interesting to study the impact of mobility on physical-layer attacks on both attacker and defender sides. On the attacker side, the attacker may utilize mobility to find an optimal location to launch the attack or conduct the attack in a transient way in order to avoid detection. On the defender side, users may utilize mobility to move away from the attacking area or paring groups to reduce the possibility of being attacked. In addition, users may also need to consider the tradeoff between security and communication performance under the mobility scenario. Investigation on PLS solutions coping with the mobility in 5G IoT systems is largely open.

B. Future Research Topics

In this section, we discuss three promising future directions: 1) 5G characteristics synthesis; 2) attacking signal cancellation; and 3) 5G location-aware.

1) 5G Characteristics Synthesis: As the development of 5G communication, we can see that one trend of the 5G framework is to synthesize multiple technologies. For example, combining the advantages of massive MIMO and mmWave and coupling NOMA with full-duplex can further improve the spectrum efficiency. Therefore, we should revisit the physical-layer characteristics to achieve better PLS solutions. Rather than being confined to a certain physical-layer property in a single physical-layer technology, we should consider the comprehensive characteristics which are presented in the synthesis of multiple integrated technologies. For instance, under mmWave communications, the antenna space can be related to a virtual channel model through a spatial Fourier transform. Accounting for massive MIMO, this virtual channel model

will have many unique characteristics, such as sparsity and directionality, which can be utilized as new physical-layer features by PLS solutions. Considering an IoT system with low-cost and low-energy IoT devices, the model of the virtual channel can help a powerful AP or BS to distinguish different users, such as PCA detection in NOMA communications [10]. Hence, investigating the synthetic characteristics in 5G IoT wireless communication may bring some novel PLS solutions.

2) Attacking Signal Cancellation: Detecting active attacks in networks is just the first step to counter physical-layer threats. What we expect is that legitimate and secure communication can be achieved even under the active spoofing attacks. To this end, we have to cancel or remove the attacking influence as the attacks have been detected. Nevertheless, it is much more challenging to eliminate active attacks without disrupting legitimate communications. Here, we introduce a potential method by waveform design with location information. In the current various kinds of standard wireless protocols, the waveform has been given a canonical form. Nonetheless, under these regulatory forms, there is still a large design space to achieve some additional functionality. If location information is taken into account in the waveform design, it could be easier to identify whether the signals are from the same user. Afterward, we can design a corresponding filter mechanism at the receiving end to filter out any irrelevant signals, such as active eavesdroppers signals. Specifically, this location information should not be the real geographic information which will lead to a private information leakage. It is expected that such location information just shows the differences in LUs positions but cannot be mapped to the LUs real locations.

3) 5G Location-Aware Communications: To deal with the mobility of 5G IoT devices, 5G location-aware communications may be a potentially positive factor for PLS technologies [101]. 5G communication networks can afford sufficiently precise location information to benefit the network design and optimization. Naturally, the location distinguishability of transmitters could help 5G IoT networks to mitigate the risk of active attacks, where the users can effectively distinguish different users with the location information, which will be a powerful way to counter active attacks. In addition, IoT communication systems can utilize the location information in many ways, including distances, delays, velocities, angles, and predictable user behavior [101]. Besides, there are many potential characteristics of 5G technologies to achieve location-aware communication, such as the beamforming in massive MIMO and high directionality in mmWave. Therefore, how to achieve an efficient PLS solution by the fusion of 5G communication location information without violating personal privacy will be an interesting and important research direction.

VI. Conclusion

In this paper, we focused on the impact of 5G wireless technologies on physical-layer threats and PLS solutions in 5G IoT networks. We reviewed the characteristics and physical-layer threats in 5G IoT networks and categorized these threats with different attackers' purposes. We discussed the comprehensive PLS solutions in IoT networks with the wireless techniques of 5G and beyond. The open issues about the PLS for IoT within 5G framework were analyzed, and potential remedies and future research directions were introduced.

For the development of IoT, it is important to understand what are the associated physical-layer security threats as well as possible PLS solutions under the wide-ranging 5G wireless communication techniques. The main purpose of this paper is to analyze the security challenges and discuss the potential PLS solutions under the 5G IoT networks. We hope this paper can help to stimulate further research in this area.

References

[1] S. Li, L. Da Xu, and S. Zhao, "5G Internet of Things: A survey," *J. Ind. Inf. Integr.*, vol. 10, pp. 1–9, Jun. 2018.

[2] G. A. Akpakwu, B. J. Silva, G. P. Hancke, and A. M. Abu-Mahfouz, "A survey on 5G networks for the Internet of Things: Communication technologies and challenges," *IEEE Access*, vol. 6, pp. 3619–3647, 2018.

[3] D. Wang, B. Bai, W. Zhao, and Z. Han, "A survey of optimization approaches for wireless physical layer security," *IEEE Commun. Surveys Tuts.*, vol. 21, no. 2, pp. 1878–1911, 2nd Quart., 2019.

[4] J. M. Hamamreh, H. M. Furqan, and H. Arslan, "Classifications and applications of physical layer security techniques for confidentiality: A comprehensive survey," *IEEE Commun. Surveys Tuts.*, vol. 21, no. 2, pp. 1773–1828, 2nd Quart., 2018.

[5] K. M. Alam, M. Saini, and A. El Saddik, "Toward social Internet of Vehicles: Concept, architecture, and applications," *IEEE Access*, vol. 3, pp. 343–357, 2015.

[6] K. Zeng, K. Govindan, and P. Mohapatra, "Non-cryptographic authentication and identification in wireless networks [security and privacy in emerging wireless networks]," *IEEE Wireless Commun.*, vol. 17, no. 5, pp. 56–62, Oct. 2010.

[7] K. Zeng, "Physical layer key generation in wireless networks: Challenges and opportunities," *IEEE Commun. Mag.*, vol. 53, no. 6, pp. 33–39, Jun. 2015.

[8] D. Kapetanovic, G. Zheng, and F. Rusek, "Physical layer security for massive MIMO: An overview on passive eavesdropping and active attacks," *IEEE Commun. Mag.*, vol. 53, no. 6, pp. 21–27, Jun. 2015.

[9] Z.-G. Ding, M. Xu, Y. Chen, M.-G. Peng, and H. V. Poor, "Embracing non-orthogonalmultiple access in future wireless networks," *Front. Inf. Technol. Electron. Eng.*, vol. 19, no. 3, pp. 322–339, 2018.

[10] N. Wang, L. Jiao, and K. Zeng, "Pilot contamination attack detection for NOMA in mm-wave and massive MIMO 5G communication," in *Proc. IEEE Conf. Commun. Netw. Security (CNS)*, 2018, pp. 1–9.

[11] X. Tang, P. Ren, Y. Wang, and Z. Han, "Combating full-duplex active eavesdropper: A hierarchical game perspective," *IEEE Trans. Commun.*, vol. 65, no. 3, pp. 1379–1395, Mar. 2017.

[12] C. Wang and H.-M. Wang, "Physical layer security in millimeter wave cellular networks," *IEEE Trans. Wireless Commun.*, vol. 15, no. 8, pp. 5569–5585, Aug. 2016.

[13] G. Zheng, I. Krikidis, J. Li, A. P. Petropulu, and B. Ottersten, "Improving physical layer secrecy using full-duplex jamming receivers," *IEEE Trans. Signal Process.*, vol. 61, no. 20, pp. 4962–4974, Oct. 2013.

[14] T.-X. Zheng, H.-M. Wang, Q. Yang, and M. H. Lee, "Safeguarding decentralized wireless networks using full-duplex jamming receivers," *IEEE Trans. Wireless Commun.*, vol. 16, no. 1, pp. 278–292, Jan. 2017.

[15] Y. Yang, L. Wu, G. Yin, L. Li, and H. Zhao, "A survey on security and privacy issues in Internet-of-Things," *IEEE Internet Things J.*, vol. 4, no. 5, pp. 1250–1258, Oct. 2017.

[16] T. A. Ahanger and A. Aljumah, "Internet of Things: A comprehensive study of security issues and defense mechanisms," *IEEE Access*, vol. 7, pp. 11020–11028, 2018.

[17] M. A. M. Sadeeq, S. R. M. Zeebaree, R. Qashi, S. H. Ahmed, and K. Jacksi, "Internet of Things security: A survey," in *Proc. Int. Conf. Adv. Sci. Eng. (ICOASE)*, 2018, pp. 162–166.

[18] Y. Wu, A. Khisti, C. Xiao, G. Caire, K.-K. Wong, and X. Gao, "A survey of physical layer security techniques for 5G wireless networks and challenges ahead," *IEEE J. Sel. Areas Commun.*, vol. 36, no. 4, pp. 679–695, Apr. 2018.

[19] D. Kombate and Wanglina, "The Internet of Vehicles based on 5G communications," in *Proc. IEEE Int. Conf. Internet Things (iThings) IEEE Green Comput. Commun. (GreenCom) IEEE Cyber Phys. Soc. Comput. (CPSCom) IEEE Smart Data (SmartData)*, 2016, pp. 445–448.

[20] L. Gupta, R. Jain, and G. Vaszkun, "Survey of important issues in UAV communication networks," *IEEE Commun. Surveys Tuts.*, vol. 18, no. 2, pp. 1123–1152, 2nd Quart., 2016.

[21] M. Agiwal, A. Roy, and N. Saxena, "Next generation 5G wireless networks: A comprehensive survey," *IEEE Commun. Surveys Tuts.*, vol. 18, no. 3, pp. 1617–1655, 3rd Quart., 2016.

[22] S. Wang, J. Wan, D. Li, and C. Zhang, "Implementing smart factory of Industrie 4.0: An outlook," *Int. J. Distrib. Sensor Netw.*, vol. 12, no. 1, 2016, Art. no. 3159805.

[23] N. Yang, L. F. Wang, G. Geraci, M. Elkashlan, J. H. Yuan, and M. Di Renzo, "Safeguarding 5G wireless communication networks using physical layer security," *IEEE Commun. Mag.*, vol. 53, no. 4, pp. 20–27, Apr. 2015.

[24] X. Wang, P. Hao, and L. Hanzo, "Physical-layer authentication for wireless security enhancement: Current challenges and future developments," *IEEE Commun. Mag.*, vol. 54, no. 6, pp. 152–158, Jun. 2016.

[25] S. K. Singh, M. P. Singh, and D. K. Singh, "A survey on network security and attack defense mechanism for wireless sensor networks," *Int. J. Comput. Trends Technol.*, vol. 1, no. 2, pp. 9–17, 2011.

[26] Y.-S. Shiu, S. Y. Chang, H.-C. Wu, S. C.-H. Huang, and H.-H. Chen, "Physical layer security in wireless networks: A tutorial," *IEEE Wireless Commun.*, vol. 18, no. 2, pp. 66–74, Apr. 2011.

[27] N. Romero-Zurita, M. Ghogho, and D. McLernon, "Outage probability based power distribution between data and artificial noise for physical layer security," *IEEE Signal Process. Lett.*, vol. 19, no. 2, pp. 71–74, Feb. 2012.

[28] A. Thangaraj, S. Dihidar, A. R. Calderbank, S. W. McLaughlin, and J.-M. Merolla, "Applications of LDPC codes to the wiretap channel," *IEEE Trans. Inf. Theory*, vol. 53, no. 8, pp. 2933–2945, Aug. 2007.

[29] X. Liang, M. Zhang, and D. Han, "Security performance of polar codes in uv wireless communications," in *Proc. Asia Commun. Photon. Conf. (ACP)*, 2018, pp. 1–3.

[30] F. Oggier, P. Solé, and J.-C. Belfiore, "Lattice codes for the wiretap Gaussian channel: Construction and analysis," *IEEE Trans. Inf. Theory*, vol. 62, no. 10, pp. 5690–5708, Oct. 2016.

[31] D. Steinmetzer, S. Ahmad, N. Anagnostopoulos, M. Hollick, and S. Katzenbeisser, "Authenticating the sector sweep to protect against beam-stealing attacks in IEEE 802.11ad networks," in *Proc. 2nd ACM Workshop Millimeter Wave Netw. Sens. Syst.*, 2018, pp. 3–8.

[32] X. Zhou, B. Maham, and A. Hjorungnes, "Pilot contamination for active eavesdropping," *IEEE Trans. Wireless Commun.*, vol. 11, no. 3, pp. 903–907, Mar. 2012.

[33] T. Nitsche, C. Cordeiro, A. B. Flores, E. W. Knightly, E. Perahia, and J. C. Widmer, "IEEE 802.11ad: Directional 60 GHz communication for multi-gigabit-per-second Wi-Fi," *IEEE Commun. Mag.*, vol. 52, no. 12, pp. 132–141, Dec. 2014.

[34] D. Kapetanović, G. Zheng, K.-K. Wong, and B. Ottersten, "Detection of pilot contamination attack using random training and massive MIMO," in *Proc. IEEE 24th Int. Symp. Pers. Indoor Mobile Radio Commun. (PIMRC)*, 2013, pp. 13–18.

[35] W. Zhang, H. Lin, and R. Zhang, "Detection of pilot contamination attack based on uncoordinated frequency shifts," *IEEE Trans. Commun.*, vol. 66, no. 6, pp. 2658–2670, Jun. 2018.

[36] M. H. Yılmaz and H. Arslan, "A survey: Spoofing attacks in physical layer security," in *Proc. IEEE 40th Local Comput. Netw. Conf. Workshops (LCN Workshops)*, 2015, pp. 812–817.

[37] J. Newsome, E. Shi, D. Song, and A. Perrig, "The sybil attack in sensor networks: Analysis & defenses," in *Proc. 3rd Int. Symp. Inf. Process. Sensor Netw.*, 2004, pp. 259–268.

[38] L. Xiao, L. J. Greenstein, N. B. Mandayam, and W. Trappe, "Channel-based detection of sybil attacks in wireless networks," *IEEE Trans. Inf. Forensics Security*, vol. 4, no. 3, pp. 492–503, Sep. 2009.

[39] K. Zhang, X. Liang, R. Lu, and X. Shen, "Sybil attacks and their defenses in the Internet of Things," *IEEE Internet Things J.*, vol. 1, no. 5, pp. 372–383, Oct. 2014.

[40] A. Mpitziopoulos, D. Gavalas, C. Konstantopoulos, and G. Pantziou, "A survey on jamming attacks and countermeasures in WSNs," *IEEE Commun. Surveys Tuts.*, vol. 11, no. 4, pp. 42–56, 4th Quart., 2009.

[41] M. Dener, "Security analysis in wireless sensor networks," *Int. J. Distrib. Sensor Netw.*, vol. 10, no. 10, 2014, Art. no. 303501.

[42] T. C. Clancy, "Efficient ofdm denial: Pilot jamming and pilot nulling," in *Proc. IEEE Int. Conf. Commun. (ICC)*, 2011, pp. 1–5.

[43] H. Yang, M. Shi, Y. Xia, and P. Zhang, "Security research on wireless networked control systems subject to jamming attacks," *IEEE Trans. Cybern.*, vol. 49, no. 6, pp. 2022–2031, Jun. 2019.

[44] A. D. Wood, J. A. Stankovic, and G. Zhou, "Deejam: Defeating energy-efficient jamming in ieee 802.15.4-based wireless networks," in *Proc. 4th Annu. IEEE Commun. Soc. Conf. Sensor Mesh Ad Hoc Commun. Netw. (SECON)*, 2007, pp. 60–69.

[45] M. Li, I. Koutsopoulos, and R. Poovendran, "Optimal jamming attacks and network defense policies in wireless sensor networks," in *Proc. IEEE INFOCOM 26th IEEE Int. Conf. Comput. Commun.*, 2007, pp. 1307–1315.

[46] W. Xu, W. Trappe, and Y. Zhang, "Channel surfing: Defending wireless sensor networks from interference," in *Proc. 6th Int. Conf. Inf. Process. Sensor Netw.*, 2007, pp. 499–508.

[47] Y. W. Law, M. Palaniswami, L. V. Hoesel, J. Doumen, P. Hartel, and P. Havinga, "Energy-efficient link-layer jamming attacks against wireless sensor network MAC protocols," *ACM Trans. Sensor Netw.*, vol. 5, no. 1, p. 6, 2009.

[48] L. Xiao *et al.*, "UAV relay in VANETs against smart jamming with reinforcement learning," *IEEE Trans. Veh. Technol.*, vol. 67, no. 5, pp. 4087–4097, 2018.

[49] L. Lu, G. Y. Li, A. L. Swindlehurst, A. Ashikhmin, and R. Zhang, "An overview of massive MIMO: Benefits and challenges," *IEEE J. Sel. Topics Signal Process.*, vol. 8, no. 5, pp. 742–758, Oct. 2014.

[50] D. C. Araujo, T. Maksymyuk, A. L. de Almeida, T. Maciel, J. C. Mota, and M. Jo, "Massive MIMO: Survey and future research topics," *IET Commun.*, vol. 10, no. 15, pp. 1938–1946, Oct. 2016.

[51] K. Zheng, S. Ou, and X. Yin, "Massive MIMO channel models: A survey," *Int. J. Antennas Propag.*, vol. 2014, Mar. 2014, Art. no. 848071.

[52] X. Chen, D. W. K. Ng, W. H. Gerstacker, and H.-H. Chen, "A survey on multiple-antenna techniques for physical layer security," *IEEE Commun. Surveys Tuts.*, vol. 19, no. 2, pp. 1027–1053, 2nd Quart., 2017.

[53] J. Zhu, R. Schober, and V. K. Bhargava, "Secure transmission in multicell massive MIMO systems," *IEEE Trans. Wireless Commun.*, vol. 13, no. 9, pp. 4766–4781, Sep. 2014.

[54] D. Kapetanovic, A. Al-Nahari, A. Stojanovic, and F. Rusek, "Detection of active eavesdroppers in massive MIMO," in *Proc. IEEE 25th Annu. Int. Symp. Pers. Indoor. Mobile Radio Commun. (PIMRC)*, 2014, pp. 585–589.

[55] T. T. Do, H. Q. Ngo, T. Q. Duong, T. J. Oechtering, and M. Skoglund, "Massive MIMO pilot retransmission strategies for robustification against jamming," *IEEE Wireless Commun. Lett.*, vol. 6, no. 1, pp. 58–61, Feb. 2017.

[56] Z. G. Ding, X. F. Lei, G. K. Karagiannidis, R. Schober, J. H. Yuan, and V. K. Bhargava, "A survey on non-orthogonal multiple access for 5G networks: Research challenges and future trends," *IEEE J. Sel. Areas Commun.*, vol. 35, no. 10, pp. 2181–2195, Oct. 2017.

[57] Z. Ding, P. Fan, and H. V. Poor, "Impact of user pairing on 5G nonorthogonal multiple-access downlink transmissions," *IEEE Trans. Veh. Technol.*, vol. 65, no. 8, pp. 6010–6023, Aug. 2016.

[58] Y. Liu, Z. Qin, M. Elkashlan, Y. Gao, and L. Hanzo, "Enhancing the physical layer security of non-orthogonal multiple access in large-scale networks," *IEEE Trans. Wireless Commun.*, vol. 16, no. 3, pp. 1656–1672, Mar. 2017.

[59] M. Tian, Q. Zhang, S. Zhao, Q. Li, and J. Qin, "Secrecy sum rate optimization for downlink MIMO nonorthogonal multiple access systems," *IEEE Signal Process. Lett.*, vol. 24, no. 8, pp. 1113–1117, Aug. 2017.

[60] T. S. Rappaport *et al.*, "Millimeter wave mobile communications for 5G cellular: It will work!" *IEEE Access*, vol. 1, pp. 335–349, 2013.

[61] Y. Niu, Y. Li, D. Jin, L. Su, and A. Vasilakos, "A survey of millimeter wave (mmWave) communications for 5G: Opportunities and challenges," in *Computer Science-Networking and Internet Architecture*. New York, NY, USA: Springer, Apr. 2015.

[62] R. W. Heath, N. González-Prelcic, S. Rangan, W. Roh, and A. M. Sayeed, "An overview of signal processing techniques for millimeter wave MIMO systems," *IEEE J. Sel. Topics. Signal Process.*, vol. 10, no. 3, pp. 436–453, Apr. 2016.

[63] L. Jiao, J. Tang, and K. Zeng, "Physical layer key generation using virtual AoA and AoD of mmwave massive MIMO channel," in *Proc. IEEE Conf. Commun. Netw. Security (CNS)*, 2018, pp. 1–9.

[64] S. Vuppala, S. Biswas, and T. Ratnarajah, "An analysis on secure communication in millimeter/micro-wave hybrid networks," *IEEE Trans. Commun.*, vol. 64, no. 8, pp. 3507–3519, Aug. 2016.

[65] K. Xiao, S. Zhang, K. Michel, and C. Li, "Study of physical layer security in mmwave satellite networks," in *Proc. IEEE Int. Conf. Commun. (ICC)*, 2018, pp. 1–6.

[66] D. Kim, H. Lee, and D. Hong, "A survey of in-band full-duplex transmission: From the perspective of PHY and MAC layers," *IEEE Commun. Surveys Tuts.*, vol. 17, no. 4, pp. 2017–2046, 4th Quart., 2015.

[67] O. Abari, D. Bharadia, A. Duffield, and D. Katabi, "Enabling high-quality untethered virtual reality," in *Proc. NSDI*, 2017, pp. 531–544.

[68] D. Bharadia and S. Katti, "FastForward: Fast and constructive full duplex relays," *ACM SIGCOMM Comput. Commun. Rev.*, vol. 44, no. 4, pp. 199–210, 2015.

[69] J. Prakash, J. Wang, and J. Lee, "Detection of pilot contamination attack with full-duplex receiver," in *Proc. Int. Tech. Conf. Circuits Syst. Comput. Commun. (ITC-CSCC)*, Seoul, South Korea, Jun. 2015, pp. 54–55.

[70] Y. Sun, D. W. K. Ng, J. Zhu, and R. Schober, "Multi-objective optimization for robust power efficient and secure full-duplex wireless communication systems," *IEEE Trans. Wireless Commun.*, vol. 15, no. 8, pp. 5511–5526, Aug. 2016.

[71] Y. Wan, Q. Li, Q. Zhang, and J. Qin, "Optimal and suboptimal full-duplex secure beamforming designs for MISO two-way communications," *IEEE Wireless Commun. Lett.*, vol. 4, no. 5, pp. 493–496, Oct. 2015.

[72] X. Lu, P. Wang, D. Niyato, D. I. Kim, and Z. Han, "Wireless networks with RF energy harvesting: A contemporary survey," *IEEE Commun. Surveys Tuts.*, vol. 17, no. 2, pp. 757–789, 2nd Quart., 2015.

[73] Z. Ding, I. Krikidis, B. Sharif, and H. V. Poor, "Wireless information and power transfer in cooperative networks with spatially random relays," *IEEE Trans. Wireless Commun.*, vol. 13, no. 8, pp. 4440–4453, Aug. 2014.

[74] L. Wang, K.-K. Wong, S. Jin, G. Zheng, and R. W. Heath, "A new look at physical layer security, caching, and wireless energy harvesting for heterogeneous ultra-dense networks," *IEEE Commun. Mag.*, vol. 56, no. 6, pp. 49–55, Jun. 2018.

[75] M. Zhang and Y. Liu, "Energy harvesting for physical-layer security in OFDMA networks," *IEEE Trans. Inf. Forensics Security*, vol. 11, no. 1, pp. 154–162, Jan. 2016.

[76] A. Salem, K. A. Hamdi, and K. M. Rabie, "Physical layer security with RF energy harvesting in AF multi-antenna relaying networks," *IEEE Trans. Commun.*, vol. 64, no. 7, pp. 3025–3038, Jul. 2016.

[77] L. Liu, R. Zhang, and K.-C. Chua, "Secrecy wireless information and power transfer with MISO beamforming," *IEEE Trans. Signal Process.*, vol. 62, no. 7, pp. 1850–1863, Apr. 2014.

[78] D. Zhai, R. Zhang, J. Du, Z. Ding, and F. R. Yu, "Simultaneous wireless information and power transfer at 5G new frequencies: Channel measurement and network design," *IEEE J. Sel. Areas Commun.*, vol. 37, no. 1, pp. 171–186, Jan. 2019.

[79] I. Nikoloska, N. Zlatanov, and Z. Hadzi-Velkov, "Capacity of a full-duplex wirelessly powered communication system with self-interference and processing cost," *IEEE Trans. Wireless Commun.*, vol. 17, no. 11, pp. 7648–7660, 2018.

[80] Z. N. Chaleshtori, P. Chvojka, S. Zvanovec, Z. Ghassemlooy, and P. A. Haigh, "A survey on recent advances in organic visible light communications," in *Proc. 11th Int. Symp. Commun. Syst. Netw. Digit. Signal Process. (CSNDSP)*, 2018, pp. 1–6.

[81] L. U. Khan, "Visible light communication: Applications, architecture, standardization and research challenges," *Digit. Commun. Netw.*, vol. 3, no. 2, pp. 78–88, 2017.

[82] P. H. Pathak, X. Feng, P. Hu, and P. Mohapatra, "Visible light communication, networking, and sensing: A survey, potential and challenges," *IEEE Commun. Surveys Tuts.*, vol. 17, no. 4, pp. 2047–2077, 4th Quart., 2015.

[83] Z. Ghassemlooy, L. N. Alves, S. Zvanovec, and M.-A. Khalighi, *Visible Light Communications: Theory and Applications*. Boca Raton, FL, USA: CRC Press, 2017.

[84] F. J. Lopez-Martinez, G. Gomez, and J. M. Garrido-Balsells, "Physical-layer security in free-space optical communications," *IEEE Photon. J.*, vol. 7, no. 2, pp. 1–14, Apr. 2015.

[85] A. Mostafa and L. Lampe, "Physical-layer security for MISO visible light communication channels," *IEEE J. Sel. Areas Commun.*, vol. 33, no. 9, pp. 1806–1818, Sep. 2015.

[86] A. Mostafa and L. Lampe, "Physical-layer security for indoor visible light communications," in *Proc. IEEE Int. Conf. Commun. (ICC)*, 2014, pp. 3342–3347.

[87] X. Sun and I. B. Djordjevic, "Physical-layer security in orbital angular momentum multiplexing free-space optical communications," *IEEE Photon. J.*, vol. 8, no. 1, pp. 1–10, Feb. 2016.

[88] T.-L. Wang and I. B. Djordjevic, "Physical-layer security in free-space optical communications using bessel-Gaussian beams," in *Proc. IEEE Photon. Conf. (IPC)*, 2018, pp. 1–2.

[89] A. Al-Hourani, S. Kandeepan, and S. Lardner, "Optimal lap altitude for maximum coverage," *IEEE Wireless Commun. Lett.*, vol. 3, no. 6, pp. 569–572, Dec. 2014.

[90] N. H. Motlagh, M. Bagaa, and T. Taleb, "UAV-based IoT platform: A crowd surveillance use case," *IEEE Commun. Mag.*, vol. 55, no. 2, pp. 128–134, Feb. 2017.

[91] W. Feng, J. Wang, Y. Chen, X. Wang, N. Ge, and J. Lu, "UAV-aided MIMO communications for 5G Internet of Things," *IEEE Internet Things J.*, vol. 6, no. 2, pp. 1731–1740, Apr. 2019.

[92] Z. Khosravi, M. Gerasimenko, S. Andreev, and Y. Koucheryavy, "Performance evaluation of UAV-assisted mmWave operation in mobility-enabled urban deployments," in *Proc. TSP*, Jul. 2018, pp. 1–5.

[93] Y. Zeng and R. Zhang, "Energy-efficient UAV communication with trajectory optimization," *IEEE Trans. Wireless Commun.*, vol. 16, no. 6, pp. 3747–3760, Jun. 2017.

[94] Q. Wang, Z. Chen, W. Mei, and J. Fang, "Improving physical layer security using UAV-enabled mobile relaying," *IEEE Wireless Commun. Lett.*, vol. 6, no. 3, pp. 310–313, Jun. 2017.

[95] H. Liu and K. S. Kwak, "Secrecy outage probability of UAV-aided selective relaying networks," in *Proc. ICUFN*, Jun. 2017, pp. 24–29.

[96] G. Zhang, Q. Wu, M. Cui, and R. Zhang, "Securing UAV communications via trajectory optimization," in *Proc. IEEE Glob. Commun. Conf. (GLOBECOM)*, 2017, pp. 1–6.

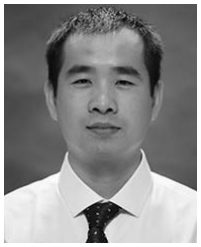
[97] Q. Wu, Y. Zeng, and R. Zhang, "Joint trajectory and communication design for multi-UAV enabled wireless networks," *IEEE Trans. Wireless Commun.*, vol. 17, no. 3, pp. 2109–2121, Mar. 2018.

[98] Y. Cai, F. Cui, Q. Shi, M. Zhao, and G. Y. Li, "Dual-UAV enabled secure communications: Joint trajectory design and user scheduling," *IEEE J. Sel. Areas Commun.*, vol. 36, no. 9, pp. 1972–1985, Sep. 2018.

[99] N. Rupasinghe *et al.*, "Enhancing physical layer security for NOMA transmission in mmWave drone networks," in *Proc. IEEE 52nd Asilomar Conf. Signals Syst. Comput.*, Oct. 2018.

[100] Y. He *et al.*, "Deep reinforcement learning-based optimization for cache-enabled opportunistic interference alignment wireless networks," *IEEE Trans. Veh. Technol.*, vol. 66, no. 11, pp. 10433–10445, Nov. 2017.

[101] R. Di Taranto, S. Muppirisetty, R. Raulefs, D. Slock, T. Svensson, and H. Wymeersch, "Location-aware communications for 5G networks: How location information can improve scalability, latency, and robustness of 5G," *IEEE Signal Process. Mag.*, vol. 31, no. 6, pp. 102–112, Nov. 2014.



Ning Wang received the Ph.D. degree in information and communication engineering from the Beijing University of Post and Telecommunication, Beijing, China, in 2017.

He is currently a Post-Doctoral Scholar with the Electrical and Computer Engineering Department, George Mason University, Fairfax, VA, USA. He was an Engineer with Huaxin Post and Telecommunications Consulting Design Company, Ltd., Hangzhou, from 2012 to 2013. His current research interests include physical layer security, machine learning, device identification, and RF fingerprinting.

Pu Wang received the B.S. degree in telecommunications engineering from Xidian University, Xi'an, China, in 2014, where he is currently pursuing the Ph.D. degree in cyber engineering.

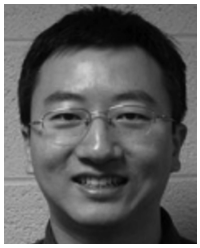
He is currently a visiting Ph.D. student with George Mason University, Fairfax, VA, USA. His current research interests include backscatter communication, wireless information and power transfer, and physical layer security.

Amir Alipour-Fanid received the B.S. degree in electrical engineering-power from the Islamic Azad University of Ardabil, Ardabil, Iran, in 2005, and the M.S. degree in electrical engineering-communication from the University of Tabriz, Tabriz, Iran, in 2008. He is currently pursuing the Ph.D. degree with the Electrical and Computer Engineering Department, George Mason University, Fairfax, VA, USA.

His current research interests include machine learning applications in security and privacy of cyber-physical systems, Internet of Things, vehicle-to-vehicle communication, and 5G and wireless networks.

Long Jiao received the B.Sc. degree in information security from Xidian University, Xi'an, China, in 2016. He is currently pursuing the Ph.D. degree with George Mason University, Fairfax, VA, USA.

He has been with George Mason University since 2016. His current research interests include 5G physical layer security, mmWave communication, mmWave HetNet, and deep learning.



Kai Zeng (M'08) received the Ph.D. degree in electrical and computer engineering from Worcester Polytechnic Institute (WPI), Worcester, MA, USA, in 2008.

He was a Post-Doctoral Scholar with the Department of Computer Science, University of California at Davis (UCD), Davis, CA, USA, from 2008 to 2011. He was an Assistant Professor with the Department of Computer and Information Science, University of Michigan–Dearborn, Dearborn, MI, USA, from 2011 to 2014. He is currently an Associate Professor with the Department of Electrical and Computer Engineering, Cyber Security Engineering, and the Department of Computer Science, George Mason University, Fairfax, VA, USA. His current research interests include cyber-physical system security and privacy, 5G physical layer security, network forensics, and spectrum sharing networks.

Dr. Zeng was a recipient of the U.S. National Science Foundation Faculty Early Career Development (CAREER) Award in 2012, the Excellence in Post-Doctoral Research Award from UCD in 2011, and the Sigma Xi Outstanding Ph.D. Dissertation Award from WPI in 2008. He is an Editor of the IEEE TRANSACTIONS ON INFORMATION FORENSICS AND SECURITY, the IEEE TRANSACTIONS ON WIRELESS COMMUNICATIONS, and the IEEE TRANSACTIONS ON COGNITIVE COMMUNICATIONS AND NETWORKING.