Physical Layer Security for MmWave Communications: Challenges and Solutions

HE Miao, LI Xiangman, NI Jianbing

(Department of Electrical and Computer Engineering, Queen's University, Kingston, Ontario K7L 3N6, Canada)

DOI: 10.12142/ZTECOM.202204006

https://kns.cnki.net/kcms/detail/34.1294.TN.20221206.1501.001.html, published online December 7, 2022

Manuscript received: 2022-09-11

Abstract: The mmWave communication is a promising technique to enable human commutation and a large number of machine-type communications of massive data from various non-cellphone devices like Internet of Things (IoT) devices, autonomous vehicles and remotely controlled robots. For this reason, information security, in terms of the confidentiality, integrity and availability (CIA), becomes more important in the mmWave communication than ever since. The physical layer security (PLS), which is based on the information theory and focuses on the secrecy capacity of the wiretap channel model, is a cost effective and scalable technique to protect the CIA, compared with the traditional cryptographic techniques. In this paper, the theory foundation of PLS is briefly introduced together with the typical PLS performance metrics secrecy rate and outage probability. Then, the most typical PLS techniques for mmWave are introduced, analyzed and compared, which are classified into three major categories of directional modulation (DM), artificial noise (AN), and directional precoding (DPC). Finally, several mmWave PLS research problems are briefly discussed, including the low-complexity DM weight vector codebook construction, impact of phase shifter (PS) with finite precision on PLS, and DM-based communications for multiple target receivers.

Keywords: mmWave communication; physical layer security; phased array; directional modulation

Citation (IEEE Format): M. He, X. M. Li, and J. B. Ni, "Physical layer security for mmwave communications: challenges and solutions," *ZTE Communications*, vol. 20, no. 4, pp. 41 – 51, Dec. 2022. doi: 10.12142/ZTECOM.202204006.

1 Introduction

The millimeter-wave (mmWave) communication employs high frequencies (30 – 300 GHz) as the carrier frequencies. With the advantage of high carrier frequencies, mmWave communication has much wider available spectrum than that of sub-6 GHz communication. It can provide high data transmission rates with wide spectrum bandwidths[1]. According to the Frequency Range 2 (FR2) defined in the 5G New Radio (NR)[2], the minimum channel spectrum bandwidth defined for FR2 is 50 MHz and the maximum is 400 MHz. With such wide spectrum bandwidths, the mmWave band 5G network can achieve the data transmission rate up to 1.8 Gbit/s[3]. In addition, due to the millimeter-level short wave length of mmWave, the physical dimension of antennas for an mmWave communication device can be greatly reduced. Hundreds to thousands of antenna elements can be integrated as a phased array on the device to enable narrow beamforming[4]. Therefore, mmWave wireless communication is one of the key technologies in 5G NR for 5G mobile networks[5 – 6] that can significantly increase the data transmission rate over small and densely populated areas. It is also expected to be applied in the 6G mobile network, which can support the future growing network applications in the Internet of Things (IoT), the Vehicle-to-everything (V2X), etc.[7 – 8]

Despite the appealing characteristics and applications, the mmWave communications are vulnerable to eavesdropping due to the open nature of the wireless medium[8 – 10]. Eavesdroppers may intercept the communication[10] by residing in the transmitting beam. Such vulnerability threats the confidentiality of some sensitive information, such as financial data, electronic media and medical records. To minimize the risk of sensitive information leakage from mmWave communications, preserving the secrecy is essential in the design and implementation of the mmWave communication system[8, 11].

The traditional cryptography technique is an effective tool to protect the information security. However, traditional cryptography techniques can hardly meet the new requirements of the mmWave communication security. First, traditional cryptography techniques are all based on the mathematical computation complex problem and the secret key. Proper key management is essential to ensure the security. The huge device density and highly dynamic environment make it extremely difficult to design a safe key management protocol for traditional cryptography-based security schemes[12 – 13]. Second, traditional cryptography-based algorithms, especially asymmetric cryptography algorithms, require significant computation resource. Many devices in mmWave communication scenarios, especially in the 5G network, are IoT devices. For the reason of cost control, these devices are typically built with very limited computational capabilities in terms of the CPU speed, storage size and power supply. Performing the traditional high-computation-cost cryptography algorithm on these resource limited devices may not only deteriorate the individual device life span but also result in poor performance[12, 14]. Lastly, a trusted third party is always required for system initialization and key management in the security scheme based on traditional cryptography. For security reasons, the trusted third party is typically remotely centralized. The dependence on a centralized third party limits the application within a centralized model, which limits the scalability of the mmWave communication, such as the supporting of up to one million devices in per square km[15–16] in 5G networks. And the frequent interactions with the remote party will cause additional delay and increase the system overhead.

Thus, physical layer security (PLS), which is based on the information theory and focuses on the secrecy capacity of the wiretap channel model, gains much attention from academia and industry. While applying to the mmWave communication security, the PLS techniques have significant advantages compared to the traditional cryptography techniques[15, 17]. First, the PLS technique is based on the information theory fundamentals, instead of computational complexity. It greatly reduces the burden on the devices to run the traditional heavy cryptography algorithms[18]. While naturally having good support on lightweight devices with limited computational and power resources, the PLS techniques can still protect the information security in the mmWave communication, even with the existence of powerful computational eavesdroppers[15]. Second, the PLS technique does not rely on the centralized trusted third party for system initialization and key management. The future network with mmWave communications may be with highly dynamic access[17], which means that any device may join or leave the network at any time, especially under mobile scenarios with the Internet of Vehicles (IoV) and unmanned aerial vehicles (UAV). The PLS technique can perform secure data transmission or user authentication directly without the time-consuming system setup. It not only significantly lowers the complexity of system management to lower the implementation cost, but also greatly reduces the latency with lower communication overhead.

In this paper, we first give a brief introduction to the theoretical foundation of PLS together with the typical PLS performance metrics secrecy rate and outage probability. Then, we introduce, analyze and compare the typical PLS techniques for mmWave, which are classified into three major categories of directional modulation (DM), artificial noise (AN), and directional precoding (DPC). Several schemes based on these techniques are discussed in detail to reveal each technique's advantages and constraints in the mmWave environment. Finally, we propose several future mmWave PLS research problems including low-complexity DM weight vector codebook construction, impact of phase shifter (PS) with finite precision on PLS, and DM-based communication for multiple target receivers. The definitions of frequently used acronyms are presented in Table 1.

▼Table 1. Summary of Acronyms

Acronym	Definition
ADC	analog-to-digital converter
AN	artificial noise
BS	base station
CE	constant envelope
CJ	cooperative jamming
CSI	channel state information
DAC	digital-to-analog converter
DM	directional modulation
DMC	discrete memoryless channel
DPC	directional precoding
IoT	Internet of Things
IoV	Internet of Vehicles
LOS	line-of-sight
LTE	Long-Term Evolution
MIMO	multiple-input and multiple-output
MISO	multiple-input single-output
OFDM	orthogonal frequency-division multiplexing
OTP	one time pad
PA	power amplifier
PAPR	peak to average power ratio
PLS	physical layer security
PS	phase shifter
QPSK	quadratic phase shift keying
RF	radio frequency
SNR	signal-to-noise ratio
UAV	unmanned aerial vehicle
ULA	uniform linear array

2 Theoretical Background for Physical Layer Security

The theoretical foundation of traditional cryptography is the number theory and abstract algebra. Different from traditional cryptography, the theoretical foundation of the PLS technique is the information theory. By minimizing eavesdroppers' channel capacity with the PLS techniques, information privacy can be preserved at a certain security level. Based on the definition of a channel, the PLS techniques can be classified into two major categories: one is the coding technique aiming at coding channels and the other is the signal processing technique aiming at modulation channels. In this section, we introduce the information theory related concepts in the PLS and review the wiretap channel and several performance evaluation metrics on PLS.

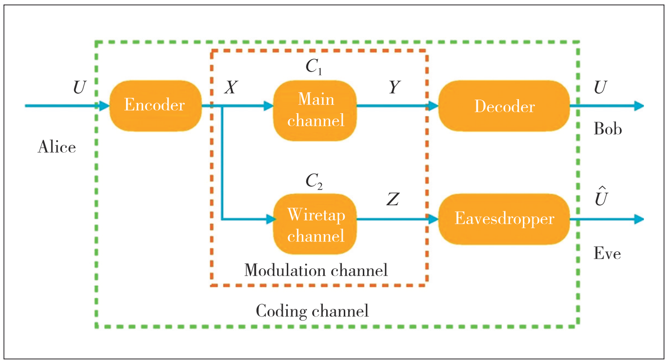
2.1 Perfect Security

Information security has been a topic in human history for thousands of years. The earliest known use of cryptography is found in the wall of a tomb from the Old Kingdom of Egypt circa 1900 BC[18]. Until the 1940s, information security in communications was first mathematically analyzed from the view of information theory by Claude Shannon. The concept of information-theoretically secure communication or "perfect security" was also introduced[19]. Perfect security means that the ciphertext gives absolutely no additional information about the plaintext. Shannon has proved that perfect security can be achieved with the one-time pad (OTP) even against adversaries with infinite computational power. Perfect security aims to protect the confidentiality of the information. While confidentiality is perfectly protected, integrity and availability can also be protected at a certain level.

2.2 Physical Layer Security

To achieve perfect security in communications from the view of information theory, there are extremely strict restrictions on the OTP. The OTP must be the same size as, or longer than, the message to be sent. The OTP must be pre-shared in a secure channel. The OTP can only be used once. These strong restrictions make perfect security only available to be implemented in very limited applications with extremely high costs. In most communications, the required security level does not have to achieve perfect security. On the other hand, the information security techniques should be scalable and affordable for daily use. For these reasons, an acceptable weaker level of information security known as PLS was defined in the wiretap channel model by WYNER in the 1970s[20]. Similar to perfect security, the PLS also focuses on the protection of information confidentiality.

In the wiretap channel model, three parties are defined, as shown in Fig. 1. They are Alice, Bob and Eve. Alice wants to send the message with particular information to Bob as private as possible. Eve eavesdrops the message from Alice to Bob and tries to get the information as much as possible. There are two channels in the model. One is between Alice and Bob (legitimate channel). The other is between Alice and Eve (wiretap channel). Due to the randomness of the physical medium (noise, interference, fading, etc.), differences between these two channels exist. The PLS techniques take advantage of these differences to make the channel from Alice to Bob statistically better than that from Alice to Eve. Thus, the channel capacity between Alice and Bob is higher than the wiretap channel between Alice and Eve. If the data rate from Alice is lower than that of the legitimate channel capacity but higher than the wiretap channel capacity, reliable communication could be achieved in the legitimate channel but not in the wiretap channel. In this way, information confidentiality can be preserved between Alice and Bob.



▲**Figure 1. Wiretap model**

To measure the secrecy of PLS techniques, several performance metrics have been introduced in information theoretic terms. Among all the metrics, secrecy capacity and outage probably are the most accepted.

2.3 Secrecy Capacity

Secrecy capacity characterizes the maximal rate to meet two requirements in wiretap channels. One requirement is that Bob can reliably get the information in the message sent from Alice through legitimate channels. The other requirement is that Eve cannot get any information in the message sent from Alice through wiretap channel. For discrete memoryless channels (DMC), WYNER first introduced the secrecy capacity for the case of degraded channels[20] as

$$C_s = \sup_{p(X)} \{ I(X;Y) - I(X;Y) \}, \tag{1}$$

where X is the input of information source, and Y and Z are the output of legitimate receiver and eavesdropper, respectively. X, Y and Z form a Markov chain $X \rightarrow Y \rightarrow Z$. The wiretap channel model for PLS in discrete memoryless channels can be extended to models in wireless channels[21]. Gaussian wiretap channel is widely accepted for PLS in wireless channels. It has linear time-invariant multiplicative links with additive white Gaussian noise. Thus, at interval i , the transmitted signal by Alice is X_i , and the received signals by Bob and Eve are $Y_{B,i}$ and $Y_{E,i}$, respectively. They can be expressed as

$$Y_{B,i} = h_B X_i + N_{B,i}, \tag{2}$$

$$Y_{E,i} = h_E X_i + N_{E,i}. \tag{3}$$

Here h_B and h_E are the channel gains for the legitimate channel and wiretap channel, respectively. $N_{B,i}$ and $N_{E,i}$ are the additive Gaussian noises. They are independent of the transmitted signal with zero means and variances σ_B^2 and σ_E^2, respectively. With the average transmit power constraint of P, the secrecy capacity can be expressed as

$$C_s = \frac{1}{2}\log\left(1 + \frac{P\left|h_B\right|^2}{\sigma_B^2}\right) - \frac{1}{2}\log\left(1 + \frac{P\left|h_E\right|^2}{\sigma_E^2}\right). \tag{4}$$

Note that the secrecy capacity in the Gaussian wiretap channel is equal to the difference between the legitimate channel's Shannon capacity C_M and the eavesdropper channel's Shannon capacity C_E, which can be formed as

$$C_s = C_M - C_E, \tag{5}$$

$$C_M = \frac{1}{2}\log\left(1 + \frac{P\left|h_B\right|^2}{\sigma_B^2}\right), \tag{6}$$

$$C_E = \frac{1}{2}\log\left(1 + \frac{P\left|h_E\right|^2}{\sigma_E^2}\right). \tag{7}$$

As a result, it can be concluded that secure communication is possible if and only if the legitimate channel is better than the wiretap channel, which is $\left|h_B^2\right|/\sigma_B^2 > \left|h_E^2\right|/\sigma_E^2$.

2.4 Secrecy Capacity

Another well-accepted PLS performance metric for the Gaussian wiretap channel is the secrecy outage probability introduced by BLOCH et al.[22] The secrecy outage is the event of instantaneous secrecy capacity C_S lower than the target secrecy rate R_S, which is $\{C_S < R_S\}$. The secrecy outage event will trigger the suspending of transmission. Thus, the outage probability is defined as

$$P_{\text{out}}(R_s) = P\{C_S < R_S\}. \tag{8}$$

3 Physical Layer Security Techniques Under MmWave Channel

The mmWave is the spectrum from 30 GHz to 300 GHz. It is receiving lots of interest from academia, industry and government due to the limited available spectrum in sub-6 GHz bands and the advantage of gigabit-per-second data rates in mmWave[6, 23–24]. The hardware constraints, channel model and array size for mmWave are quite different from those for the spectrum below 6 GHz at which the carrier frequencies of most consumer wireless systems operate[4]. First, more analog-to-digital converters with higher resolution are required for mmWave, due to the higher frequency and bandwidth channel. Partitioning the operations into analog and digital domains for signal processing is a possible solution to these hardware constraints. In addition, the propagation environment has a different effect on the channel model because of the smaller wavelength of mmWave signals. Lastly, the array size for mmWave communications could be large, benefitting from the shorter wavelength of the mmWave. This section briefly surveys most recent research work in the PLS topics on DM, AN and DPC.

3.1 Directional Modulation

The DM is a technology that transmits digitally encoded signals to a specific direction while scrambling the other directions' constellations of the same signal at the same time[25]. In this way, confidential communications can be achieved between the transmitter and the designated receiver in the desired spatial direction.

The concept of DM was first introduced to phased arrays by DALY et al.[25] In DALY et al.'s scheme[25], the controlled radio frequency (RF) level analog PSs are added to each antenna of the phased array. By changing the phase weighting through the PSs at the symbol rate, a desired constellation is produced in the intended direction, while deliberately distorting the constellations in other directions. In addition, DALY et al. also implemented the proposed technique with a four-element patch array in Ref. [26]. In the implemented scheme, the genetic algorithm is employed to get the phase shift value of each antenna in order to achieve DM for the quadratic phase shift keying (QPSK) signal. However, DALY et al.'s scheme does not take the characteristics of different channels into account. The calculation of phase values with a genetic algorithm is time-consuming for a large-scale array. Many of the subsequent DM-based PLS schemes[27–31] are investigated for sub-6 GHz channels.

However, DALY et al.'s scheme[25] may be not suitable for the mmWave band system, which has the following characteristics. First, the small carrier wavelength of mmWave makes the implementation of large antenna arrays possible. The high pathloss of the mmWave band signal could be compensated with the high beamforming gain from the large array size[32]. On the other hand, the larger array size increases the complexity of the design for PLS schemes. Second, the larger array size highlights the importance of system structure simplification due to the hardware cost constraint[4]. Specifically, the RF chain cost is the dominant factor in the mmWave system with a large array size[33]. Minimizing the number of RF chains can reduce the hardware cost and power consumption, which are key factors to support massive machine-type communication between resource constraints devices, especially IoT devices. Third, the scattering and multi-paths in the mmWave band are sparse. The propagation channel in the mmWave band, which is highly directional, has large path loss and very few multi-paths[34]. The majority of multipath components is determined by the line-of-sight (LOS) components[35]. Thus, spatial sparsity commonly existing in mmWave channels poses new challenges and opportunities in designing efficient PLS schemes.

By taking advantage of the larger array size of the mmWave system, VALLIAPPAN et al. proposed a low-complexity DM scheme named Antenna Subset Modulation (ASM)[36]. In

VALLIAPPAN's scheme, the array radiation pattern is modulated at the symbol rate to achieve DM. Only a subset of all the array antennas is used for transmission. The antenna subset used for transmission will change with the symbol rate. The subset for each symbol interval is selected from all subsets with the same number of the active antennas at random. As a result, randomness will be added to the constellations in all directions except the intended one.

VALLIAPPAN et al.'s ASM considers and takes the advantages of the large array size characteristic of mmWave system. The design of the constellation in ASM is much simpler. It only requires phase shifts or switching combinations to produce an expected modulation symbol for the user in the target direction. It is quite different from other previous DM techniques such as those in Refs. [26, 37 – 38], which typically run optimization algorithms to obtain the correct set of weights. Because only the inter-antenna phase shift needs to be changed, it opens a new era for the DM application in PLS for the mmWave channel. However, ASM restricts the modulation type to phase modulation only. In addition, many of the antennas remain idle, especially when the RF chain size is much smaller than that of the antenna number. Furthermore, the switching speed must be the same as the data rates, which increases the hardware cost.

Based on VALLIAPPAN et al.'s scheme[38], ALOTAIBI et al. proposed a similar scheme named Switched Phase Array (SPA)[39]. SPA modifies the ASM. In SPA, only one antenna is changed to be off to generate the constellation distortion in undesired directions. Thus, the system complexity is reduced while increasing the active antenna numbers used for transmission with higher gain in the main lobe. In addition, SPA can support both phase modulation and amplitude modulation and cause both phase and amplitude distortion in the undesired direction.

VALLIAPPAN et al.'s ASM[38] and ALOTAIBI et al.'s SPA[39] use the on-off switches to change the beamforming weight vector, which results in the scrambled constellation in the undesired direction. In their schemes, the beamforming weights are all binary. Neither ASM nor SPA takes full advantage of the full value range of beamforming weights to increase the difficulty for eavesdroppers to get the information. In addition, idle antennas exist in both ASM and SPA. The idle antennas neither contribute to the data transmission in the target direction nor generate the interference in the undesired direction. Motivated by the mentioned point, HONG et al. proposed a novel programmable weight phased array (PWPA) scheme[40]. PWPA has a conventional phased-array architecture with a programmable power amplifier used to change the antenna weight element amplitude. Based on the idea of PWPA, HONG et al.[40] proposed an antenna subset transmission scheme with inverted antennas named Inverted Antenna Subset Transmission (IAST) first. In IAST, several antennas are selected to transmit with inverted signals, which is different from the on-off mechanism in ASM and SPA. IAST not only scrambles the constellation but also generates more AN than conventional schemes in the undesired directions.

In recent years, some new DM-based schemes were proposed to address challenges in new scenarios such as Cybertwin and reconfigurable intelligent surface (RIS). HE et al.[41] proposed a low-complexity phased-array PLS scheme for the mmWave communication in Cybertwin-driven V2X scenarios. Similar to the typical DM-based approach, a lightweight swap-based transmitting weight vector is utilized to periodically update the transmitting weight. An efficient algorithm based on the bisection method is also introduced to quickly obtain the initial weight vector at a low computational cost. YE et al.[42] considers that the additionally introduced beam to align to the RIS may cause high sidelobe, which has a significantly negative impact on the discrete optimization in antenna subset selection. To address such a challenge introduced by the RIS, a low sidelobe beamforming approach to enable DM-based PLS in RIS communication networks is proposed, by using a novel cross-entropy iterative method.

3.2 Artificial Noise

For PLS, the security capacity, one of the important performance metrics, is a function of the received signal SNR of legitimate receivers and eavesdroppers in the wireless Gaussian channel. For wireless channels, the received signal power will decrease with the increase of the distance between the transmitter and receiver. For this reason, it is possible that the eavesdropper may be placed in an undesired direction with a much closer distance to the transmitter. Even though the eavesdropper is in the lower order sidelobe of the transmitter beam, the received signal power of the eavesdropper may be still high enough to get an acceptable SNR due to the much smaller power fade of a shorter distance. As a result, the security capacity will be seriously deteriorated in this scenario.

To address this problem, a properly designed AN is added to the transmitted signal in order to degrade the SNR of the received signal by the eavesdropper. The concept of AN was first introduced by GOEL et al.[43] The application of AN in the PLS has been studied in a number of works since then. ASHISH et al. showed that the AN transmission can be secrecy capacity-achieving at high SNR for the multi-input, single-output, multi-eavesdropper (MISOME) wiretap channel, if the eavesdropper's channel knowledge is known by the transmitter[44]. This conclusion indicates that the AN is an effective technique for the PLS under certain conditions. ASHISH et al.'s work lays a solid theoretical foundation for AN-based physical layer security schemes. An optimal power allocation scheme that balanced the message and the AN transmission[45] was then studied for fading MIMO channels by ZHOU et al. Since then, a considerable number of studies have been conducted for AN-based PLS schemes.

However, most of the proposed schemes[43 – 49] focus on the sub-6 GHz channel. They neither take the hardware and cost constraints of the mmWave system into account, nor make use of the characteristics of the mmWave to additionally enhance the security. ZHAO et al. proposed a scheme named Phase-Only Zero Forcing (PZF) for secret communications[50], by using the AN technique for the mmWave channel. In the proposed scheme, ZHAO et al. fully considered the hardware cost constraints of the massive antenna system for mmWave. Specifically, each RF chain in the array is associated with an analog beamforming vector. All elements' magnitudes must be constants, but they can have arbitrary phases. This constraint comes for two reasons. First, the full digital array with a digital beamforming vector requires each RF chain to be equipped with both the digital-to-analog converter (DAC) and analog-to-digital converter (ADC). Due to the large array size of mmWave systems, which could be tens or even hundreds, the hardware cost of a full digital array system will be extremely high[51–52]. Second, the constant magnitude weight has a lower peak-to-average power ratio (PAPR), which means the signal can be amplified with more affordable non-linear power amplifier (PA) with higher efficiency. Compared to expensive linear power PA, the non-linear power PA is more scalable for the mmWave system with a large array size[4, 53].

ZHAO et al.'s main idea is to find a beamforming vector for AN transmitting in the null space of the legitimate receiver's channel. Inspired by ZHAO et al.'s idea, XU et al. proposed a secure massive MIMO communication scheme[54] by taking advantage of the null-space of the user channel, which is constructed by the DACs with lower resolution. By projecting the AN into the null space of the legitimate receiver's channel with proper power allocation between low-resolution or high-resolution DACs, the PLS can be achieved. Specifically, XU et al. derived a closed-form SNR threshold to improve the secrecy rate. The threshold determines the choice between the DACs with low resolution or high resolution. A DAC quantization model is developed to support the analysis of the asymptotic achievable secrecy rate. In addition, XU et al. investigated secure communications over sparse mm-Wave massive MIMO channels. With consideration of the spatial sparsity of a legitimate user's channel, XU et al. proposed a secure communication scheme in Ref. [55]. Through a limited number of RF chains, the information data are precoded onto dominant angle components of the sparse channel. The AN is broadcast to the nondominant angles. Thus, only the eavesdroppers will be interfered with a high probability. With two defined statistical measures of the channel sparsity, XU et al. analytically characterized its impact on the secrecy rate. Analysis shows that a significant improvement in the secrecy rate is achieved, due to the uncertainty introduced by the unknown channel sparsity for the eavesdropper.

ELTAYEB et al. investigated the mmWave PLS in vehicular communication systems and proposed two AN-based schemes[56] for vehicular mmWave communication systems. By utilizing multiple antennas with a single RF chain, the first scheme implements the transmission of symbols to a target direction, while AN is sent in non-receiver directions. The second design uses multiple antennas with a few RF chains to transmit information symbols to a target user, while opportunistically injecting artificial noise in controlled directions. The purpose is to reduce interference in vehicular environments.

JU et al. comprehensively studied the secure transmissions in the mmWave decode-and-forward (DF) relay system[57]. They investigated the optimal parameter design for the DF relay system under the same codeword transmission (SCT) scheme and the different codeword transmission (DCT) schemes. JU et al. derived the closed-form expressions for the secrecy outage probability and connection probability. Then a solution to the secrecy throughput maximization problem was given. Based on this work, JU et al. performed extensive experiments to investigate practical secure transmission problems for mmWave communication systems[58]. They analyzed the vulnerability of existing defenses in practice and found that the existing defenses in Refs. [36] and [56] had vulnerabilities, because they might have impractical hardware requirements or still be vulnerable against multiple colluding eavesdroppers. Finally, JU et al. proposed the artificial noise hopping (ANH) with minimal hardware complexity to effectively enhance the security.

LIN et al. investigated the scenario of a 5G cellular network coexisting with a satellite network in Ref. [59]. By employing a ULA at the base station (BS) and assuming the imperfect angle-of-arrival-based channel state information (CSI) of multiple eavesdroppers (Eves) is known, a constrained optimization problem is formulated. Under the constraints that are the transmit power of BS and the interference threshold of the satellite earth station, the achievable secrecy rate of the cellular user under the worst case can be maximized.

LIN et al. proposed two robust beamforming methods to solve the complex optimization problem, in the case of either coordinated or uncoordinated Eves. They also investigated the secure communication of a cognitive satellite terrestrial network with the software-defined architecture in Ref. [60]. In LIN's scheme, the interference from the terrestrial network can be regarded as a green source to enhance the physical-layer security for the satellite network. With this assumption, a constrained joint optimization problem is formulated to minimize the total transmit power. The optimization satisfies both the terrestrial users' quality-of-service requirement and the satellite users' secrecy rate requirements.

Different from many schemes focusing on protecting the downlink transmission, XU et al.[61] proposed a scheme to protect the uplink transmission for the massive MIMO system with AN-based approaches. By optimizing the power allocation between AN and data symbols, the maximum secrecy rate can be formulated.

3.3 Directional Precoding

The DPC is commonly used in the MIMO system to improve system performance by forming the beam in certain directions, which can concentrate the power in those directions. It can be also used in the PLS to protect the secrecy of the legitimate receiver, by adding additional constraints for the power leaking to the undesired directions. A lot of PLS schemes based on DPC[62–67] have been proposed. However, most of them are designed for the sub-6 GHz environment. There is no special consideration for the characteristics of the mmWave environment, especially the large array size and hardware constraints.

To support the PLS under both multiple legitimate receivers and multiple eavesdroppers, HUANG et al. proposed a constant envelope (CE) hybrid precoding scheme (CEP)[68]. A unified CE hybrid precoding framework is introduced for the sub-connected digital and analog hybrid mmWave system to protect communication secrecy. By solving an optimization problem, the qualities of target users' received constellations are guaranteed. It minimizes the power leaked to the possible eavesdroppers. To address the high hardware cost issue with the large array size mmWave system, HUANG et al. applied two measures in the proposed scheme. First, a digital and analog hybrid MIMO architecture with a much reduced number of RF chains is adopted to reduce the high hardware cost and energy consumption of mmWave RF chains. Second, only the CE signal with low PAPR, which can be amplified with high power efficiency but low-cost non-linear PA, is transmitted through the array.

CHEN et al. investigated a novel hybrid beamforming design[62] to jointly optimize the data precoding and the AN power fraction selection in the massive MIMO system. To solve the non-convex secrecy rate maximization problem for hybrid precoder design, CHEN et al. separated the design for analog and digital precoders. The analog precoder was used to maximize corresponding channel gain in the analog data precoder design. In the digital data precoder design, an iterative algorithm was proposed for the optimal design with the removed non-convex codebook constraint.

LI et al. systematically investigated the impact of low-resolution PS on hybrid beamforming under various scenarios[63–71]. Specifically, for a wideband mmWave multiple-input and multiple-output orthogonal frequency-division multiplexing (MIMO-OFDM) system, LI et al. introduced a novel hybrid beamforming architecture[63] with varying antenna subarrays and efficient low-resolution PSs. The performance loss due to the employment of practical low-resolution PSs can be mitigated with the multiple-antenna diversity, which comes from the dynamic connection for each RF chain to a non-overlapping antenna subarray with the help of a switch network and PSs. For the architecture of dynamic hybrid beamforming, they jointly designed the hybrid precoder and combiner to maximize the average spectral efficiency. However, they did not consider the impact of low-resolution PSs on PLS.

3.4 Other PLS Schemes

The principle of AN techniques is to send jamming signals to degrade the eavesdropper channel capacity in order to improve the secrecy capacity of the legitimate channel. The jamming signal may be sent from the main transmitter or other friendly users. In this way, the main transmitter can work with other friendly receivers to cooperatively degrade the eavesdropper channel capacity. This technique is called cooperative jamming (CJ), which was first introduced by DONG et al.[72]

HU et al. investigated cooperative secret communications in wireless networks with multiple passive eavesdroppers, without the knowledge of legitimate users' perfect CSI but only eavesdroppers' statistical CSI. The secrecy beamforming with AN and CJ are explored to enhance secrecy[73]. The closed-form secrecy outage probability expression is derived. HU et al. concluded the condition that a positive secrecy rate could be achievable. Finally, a secure transmission with AN and CJ design, which maximizes the secrecy outage probability with a constrained secrecy rate, is proposed.

Motivated by HU's work, SONG et al. proposed an enhanced scheme with weaker CSI assumptions[74]. In SONG et al.'s scheme, only the knowledge of the statistic CSI of illegitimate channels and the imperfect CSI of legitimate channels are known. They derived the optimal power allocation ratio between the information-bearing signal and the AN signal in order to maximize the secrecy rate. Under the statistic CSI of illegitimate channels and the imperfect CSI of legitimate channels, the optimal power allocation, which balances the information bearing signal and the AN signal, is derived to achieve the max secrecy rate.

The mmWave PLS in UAV is another hot topic with significant attention in recent years. LI et al. investigated a secure communication system[75], which considers the smart attack from another UAV besides the legitimate UAVs. LI et al. also considered the practical cases in communications. The first is that the limited number of pilot signals may exist for channel estimation. The second is that the receiver side's channel estimation may be imperfect. To address the problems brought by the imperfect channel estimation and smart attackers who choose different kinds of attacks on the basis of the continuously changing channel environments, LI et al. used the non-cooperative game theory to derive a Q-learning-based power control algorithm, which obtains an adaptive policy for the transmitter. MA et al. investigated the secure mmWave communications assisted by multiple UAV-enabled relays, together with eavesdroppers[76], under the model of randomly distributed eavesdroppers on the ground. With the models of 3D-antenna gain and stochastic geometry, the characteristics of air-to-ground channels are considered for deriving the closed form expressions of secrecy outage probability based opportunistic relay selection. It is demonstrated that the secrecy improves when the relay density increases. For mmWave MIMO-

OFDM systems with dynamic subarray (DS), SUN et al. proposed a machine learning based hybrid precoding scheme[77]. The scheme presents a shared agglomerative hierarchical clustering (shared-AHC) algorithm for DS grouping to improve spectral efficiency (SE) performance.

3.5 Comparison

The techniques for mmWave PLS can be classified into three categories based on their technical patterns: DM, AN and DPC. Their characteristics are summarized in Table 2.

▼Table 2. Cost and power efficiency comparison of mmWave physical layer security (PLS) techniques

Category	Hardware Cost	Computation Cost	Power Efficiency
DM	Medium	Depend	High
AN	Low	Medium	Low
DPC	High	High	High

AN: artificial noise DPC: directional precoding
DM: directional modulation

Specifically, the DM technique depends on the weight vector codebook. It achieves PLS by randomly selecting the vector from the codebook. The computation cost to get the codebook may be either low or high depending on the scheme and codebook size. If the scheme randomly selects the antenna subset just as what the scheme ASM does, there is only a very tiny computation cost. On the other hand, if the sechem, like Polygon, constructs the codebook with an infinite size, the computation cost may be high. The other two techniques are different from the DM technique, which are usually based on optimized weight vector results under certain security constraints. The optimization calculation may be quite complex. However, once getting the results, the weight vector will normally not change at the symbol rate. Thus, high-speed switch is not required as that in DM-based schemes.

A detailed comparison of the typical mmWave PLS schemes is shown in Table 3. Different schemes with different advantages and shortcomings are suitable for different scenarios. The subset array scheme[36] utilizes the characteristic of the large array size of the mmWave system to enable PLS. However, it is only suitable for single path scenarios. The polygon scheme[39] can work under a multiple-path scenario with a different approach. It should be noticed that current DM-based mmWave PLS schemes only support single-target receiver scenarios. It significantly constrains its application in massive machine-type communication scenarios, where multiple target receivers usually exist. To support multiple Bobs, the AN approach is usually adopted, but it comes with the cost of low power efficiency, which may be not friendly to mobile devices. In addition, the AN-based scheme proposed in Ref. [50] requires the CSI on both Bob and Eve. It may be not practical to meet such the condition, since Eve may not be exposed. The DPC-based scheme in Ref. [68] can work for multiple Bobs and multiple Eves at a high cost on both hardware and computational resource.

4 Future Research Problems

In this section, we discuss three future research problems for the PLS-based mmWave environment.

4.1 Low Complexity Directional Modulation Weight Vector Codebook Construction

The DM-based PLS schemes rely on randomly selecting the weight vector from the codebook. The codebook must be constructed before the actual transmission. However, the codebook is highly related to the target receiver's relative direction to the transmitter. Once the relative direction between the transmitter and the target receiver changes, the whole codebook has to be reconstructed. For current DM-based PLS schemes[36, 39, 40, 46], although the hardware cost has been minimized by adopting various techniques such as constant envelope, on-off switch and subarray, the algorithms for codebook construction all still suffer high complexity and high time consumption. This fact makes these schemes hardly adapt to highly dynamic scenarios with frequent and quick relative direction changes, such as vehicle networks and UAV networks, which require the codebook to be reconstructed within a short time. Since mobility is an important feature of the massive machine-type communication scenario, the DM PLS scheme with low complexity codebook construction algorithm is preferred. Motivated by this demand, the research will be conducted on reducing the DM codebook construction algorithm complexity. One of the challenges is how to maintain the PLS while reducing the codebook construction computation cost. Another challenge is how to balance the hardware cost and the codebook construction algorithm complexity.

▼Table 3. Property comparison of mmWave physical layer security (PLS) schemes

MmWave PLS Technique	Category	Bob	Eve	Bob Antenna	Eve Antenna	CSI	Propagation
Subset array[36]	DM	Single	Multiple	Single	Single	Bob only	Single path
Polygon[39]	DM	Single	Multiple	Single	Single	Bob only	Multiple path
PZF[50]	AN	Multiple	Single	Single	Multiple	Both	Single path
CEP[68]	DPC	Multiple	Multiple	Single	Single	Both	Single path

AN: artificial noise CSI: channel state information DPC: directional precoding PZF: Phase-Only Zero Forcing
CEP: constant envelope (CE) hybrid precoding scheme DM: directional modulation PLS: physical layer security

4.2 Impact of Phase Shifter with Finite Precision on PLS

For the DM-based mmWave PLS schemes, the PS is a critical component to change the weight vector in order to achieve PLS. However, similar to all other hardware, the PS cannot ideally operate as it is expected in the theory. The actual shift phase value may be different from the expected value due to the limited precision of the hardware. It causes a truncation error in the PS. The effect of the truncation error of the PS can hardly be ignored. A dynamic antenna subarray approach in Ref. [63] is introduced to mitigate the performance loss due to the employment of practical low-resolution PSs. However, this approach only focuses on the communication performance enhancement of the target receiver. Its motivation does not come from the view of PLS. The impact of low-resolution PSs on the PLS performance has not been fully investigated. Thus, many opening questions need to be addressed and researched for the impact of finite precision PS on the PLS. How to describe and measure the truncation error in DM-based PLS schemes? Is there any possibility to take advantage of the truncation error to construct new DM-based PLS schemes? These questions pose both opportunities and challenges to the DM-based mmWave PLS schemes.

4.3 Multiple Target Receivers Supported Direction Modulation

Most of the DM-based PLS schemes for mmWave can only support one target receiver, by placing the target receiver in the main lobe. It limits the application to massive machine-type communication scenarios such as IoT device networks, which often require multicast communications to multiple target receivers. The scheme in Ref. [31] provides a multiple target receiver supported DM approach by utilizing the retrodirective array antenna. However, the retrodirective array antenna suffers serious performance degrading under the mmWave band[78]. The hardware cost will also increase dramatically by implementing the retrodirective array antenna with a large array size. The IoT device network with a large number of devices can hardly afford such a high cost. Thus, this approach is not suitable for the massive machine-type communication under mmWave. The approaches in Refs. [79 – 81] provide multi-beam DM solutions to supporting multiple target receivers. However, they do not consider the fact that multiple target receivers may locate in the same direction with different ranges to the transmitter in practical scenarios. Thus, the multi-beam solution cannot fully adapt to the multiple target receiver scenarios. Motivated by the demand on multiple target user support in the massive machine-type communication, the research for multiple target user supported DM will be conducted. The major challenge is how to distinguish different target receivers in both the angular domain and range domain, while protecting their PLS.

5 Conclusions

In this paper, we introduce the concept of PLS together with its importance to the mmWave 5G network, and discuss the typical PLS techniques including DM, AN and DPC. By literature reviewing the PLS schemes based on each PLS technique in detail, we summary the advantages and constraints of the DM, AN and directional precoding technique for the mmWave PLS. Finally, we propose several future research problems on mmWave PLS. Specifically, the multiple target receivers supported DM and the impact of PS with finite precision on PLS have not been fully investigated for the mmWave PLS. The computation cost for DM weight vector codebook construction is still too high to make the DM-based PLS solution adapt to highly dynamic massive machine-type communication scenarios. It is expected to draw more attention and efforts to addressing these interesting open problems in PLS-based mmWave communications.

References

[1] XIAO M, MUMTAZ S, HUANG Y M, et al. Millimeter wave communications for future mobile networks [J]. IEEE journal on selected areas in communications, 2017, 35(9): 1909 – 1935. DOI: 10.1109/JSAC.2017.2719924

[2] 3GPP. NR; User Equipment (UE) radio transmission and reception; Part 2: Range 2 Standalone: 3GPP TS 38.101-2 version 16.3.1 [S]. 2020

[3] DOLCOURT J. We tested 5G speeds across the globe [EB/OL]. [2022-03-31]. https://www. cnet. com/features/we-ran-5g-speed-tests-on-verizon-at-t-ee-and-moreheres-what-we-found

[4] HEATH R W, GONZÁLEZ-PRELCIC N, RANGAN S, et al. An overview of signal processing techniques for millimeter wave MIMO systems [J]. IEEE journal of selected topics in signal processing, 2016, 10(3): 436 – 453. DOI: 10.1109/JSTSP.2016.2523924

[5] BOCCARDI F, HEATH R W, LOZANO A, et al. Five disruptive technology directions for 5G [J]. IEEE communications magazine, 2014, 52(2):74 – 80. DOI: 10.1109/MCOM.2014.6736746

[6] ROH W, SEOL J Y, PARK J, et al. Millimeter-wave beamforming as an enabling technology for 5G cellular communications: theoretical feasibility and prototype results [J]. IEEE communications magazine, 2014, 52(2): 106 – 113. DOI: 10.1109/mcom.2014.6736750

[7] YU Q, REN J, FU Y J, et al. Cybertwin: An origin of next generation network architecture [J]. IEEE wireless communications, 2019, 26(6): 111 – 117. DOI: 10.1109/MWC.001.1900184

[8] YANG N, WANG L F, GERACI G, et al. Safeguarding 5G wireless communication networks using physical layer security [J]. IEEE communications magazine, 2015, 53(4): 20 – 27. DOI: 10.1109/MCOM.2015.7081071

[9] WANG L F, ELKASHLAN M, DUONG T Q, et al. Secure communication in cellular networks: The benefits of millimeter wave mobile broadband [C]//IEEE 15th International Workshop on Signal Processing Advances in Wireless Communications (SPAWC). IEEE, 2014: 115 – 119. DOI: 10.1109/SPAWC.2014.6941328

[10] ZHU Y X, WANG L F, WONG K K, et al. Secure communications in millimeter wave ad hoc networks [J]. IEEE transactions on wireless communications, 2017, 16(5): 3205 – 3217. DOI: 10.1109/TWC.2017.2676087

[11] WANG C, WANG H M. Physical layer security in millimeter wave cellular networks [J]. IEEE transactions on wireless communications, 2016, 15(8): 5569 – 5585. DOI: 10.1109/TWC.2016.2562010

[12] MUKHERJEE A, FAKOORIAN S A A, HUANG J, et al. Principles of physical layer security in multiuser wireless networks: a survey [J]. IEEE communications surveys & tutorials, 2014, 16(3): 1550 – 1573. DOI: 10.1109/SURV.2014.012314.00178

[13] ALAM K M, SAINI M, SADDIK A E. Toward social Internet of vehicles: concept, architecture, and applications [J]. IEEE access, 2015, 3: 343 – 357. DOI: 10.1109/ACCESS.2015.2416657

[14] ZENG K. Physical layer key generation in wireless networks: challenges and opportunities [J]. IEEE communications magazine, 2015, 53(6): 33 – 39. DOI: 10.1109/MCOM.2015.7120014

[15] WU Y P, KHISTI A, XIAO C S, et al. A survey of physical layer security techniques for 5G wireless networks and challenges ahead [J]. IEEE journal on selected areas in communications, 2018, 36(4): 679 – 695. DOI: 10.1109/JSAC.2018.2825560

[16] ZHENG T X, WANG H M, YANG Q, et al. Safeguarding decentralized wireless networks using full-duplex jamming receivers [J]. IEEE transactions on wireless communications, 2017, 16(1): 278 – 292. DOI: 10.1109/TWC.2016.2622689

[17] WANG N, WANG P, ALIPOUR-FANID A, et al. Physical-layer security of 5G wireless networks for IoT: challenges and opportunities [J]. IEEE Internet of Things journal, 2019, 6(5): 8169 – 8181. DOI: 10.1109/JIOT.2019.2927379

[18] DAVIES D. A brief history of cryptography [J]. Information security technical report, 1997, 2(2): 14 – 17. DOI: 10.1016/s1363-4127(97)81323-4

[19] SHANNON C E. A mathematical theory of cryptography [J]. Mathematical theory of cryptography, 1945

[20] WYNER A D. The wire-tap channel [J]. The bell system technical journal, 1975, 54(8): 1355 – 1387. DOI: 10.1002/j.1538-7305.1975.tb02040.x

[21] LEUNG-YAN-CHEONG S, HELLMAN M. The Gaussian wire-tap channel [J]. IEEE transactions on information theory, 1978, 24(4): 451 – 456. DOI: 10.1109/TIT.1978.1055917

[22] BLOCH M, BARROS J, RODRIGUES M R D, et al. Wireless information-theoretic security [J]. IEEE transactions on information theory, 2008, 54(6): 2515 – 2534. DOI: 10.1109/TIT.2008.921908

[23] PI Z Y, KHAN F. An introduction to millimeter-wave mobile broadband systems [J]. IEEE communications magazine, 2011, 49(6): 101 – 107. 10.1109/MCOM.2011.5783993

[24] AKDENIZ M R, LIU Y P, SAMIMI M K, et al. Millimeter wave channel modeling and cellular capacity evaluation [J]. IEEE journal on selected areas in communications, 2014, 32(6): 1164 – 1179. DOI: 10.1109/jsac.2014.2328154

[25] DING Y, FUSCO V F. A vector approach for the analysis and synthesis of directional modulation transmitters [J]. IEEE transactions on antennas and propagation, 2014, 62(1): 361 – 370. DOI: 10.1109/TAP.2013.2287001

[26] DALY M P, BERNHARD J T. Directional modulation technique for phased arrays [J]. IEEE transactions on antennas and propagation, 2009, 57(9): 2633 – 2640. DOI: 10.1109/TAP.2009.2027047

[27] DALY M P, DALY E L, BERNHARD J T. Demonstration of directional modulation using a phased array [J]. IEEE transactions on antennas and propagation, 2010, 58(5): 1545 – 1550. DOI: 10.1109/TAP.2010.2044357

[28] DING Y, FUSCO V F. Constraining directional modulation transmitter radiation patterns [J]. IET microwaves, antennas & propagation, 2014, 8(15): 1408 – 1415. DOI: 10.1049/iet-map.2014.0042

[29] DING Y, FUSCO V F. MIMO-inspired synthesis of directional modulation systems [J]. IEEE antennas and wireless propagation letters, 2016, 15: 580 – 584. DOI: 10.1109/LAWP.2015.2459752

[30] DING Y, FUSCO V, CHEPALA A. Circular directional modulation transmitter array [J]. IET microwaves, antennas & propagation, 2017, 11(13): 1909 – 1917. DOI: 10.1049/iet-map.2016.1140

[31] DING Y, FUSCO V. A synthesis-free directional modulation transmitter using retrodirective array [J]. IEEE journal of selected topics in signal processing, 2017, 11(2): 428 – 441. DOI: 10.1109/JSTSP.2016.2605066

[32] CHEN X M, NG D W K, GERSTACKER W H, et al. A survey on multiple-antenna techniques for physical layer security [J]. IEEE communications surveys & tutorials, 2017, 19(2): 1027 – 1053. DOI: 10.1109/COMST.2016.2633387

[33] ZHU J, WANG N, BHARGAVA V K. Per-antenna constant envelope precoding for secure transmission in large-scale MISO systems [C]//IEEE/CIC International Conference on Communications in China (ICCC). IEEE, 2016: 1 – 6. DOI: 10.1109/ICCChina.2015.7448727

[34] LEE G, SUNG Y, KOUNTOURIS M. On the performance of random beamforming in sparse millimeter wave channels [J]. IEEE journal of selected topics in signal processing, 2016, 10(3): 560 – 575. DOI: 10.1109/JSTSP.2016.2524999

[35] XU H, KUKSHYA V, RAPPAPORT T S. Spatial and temporal characteristics of 60-GHz indoor channels [J]. IEEE journal on selected areas in communications, 2006, 20(3): 620 – 630. DOI: 10.1109/49.995521

[36] VALLIAPPAN N, LOZANO A, HEATH R W. Antenna subset modulation for secure millimeter-wave wireless communication [J]. IEEE transactions on communications, 2013, 61(8): 3231 – 3245. DOI: 10.1109/TCOMM.2013.061013.120459

[37] BABAKHANI A, RUTLEDGE D B, HAJIMIRI A. A near-field modulation technique using antenna reflector switching [C]//IEEE International Solid-State Circuits Conference—Digest of Technical Papers. IEEE, 2009: 188 – 189+605. DOI: 10.1109/ISSCC.2008.4523120

[38] MADIHIAN M, DESCLOS L, MARUHASHI K, et al. A high-speed resonance-type FET transceiver switch for millimeter-wave band wireless network [C]//26th European Microwave Conference. IEEE, 2007: 941 – 944. DOI: 10.1109/EUMA.1996.337731

[39] ALOTAIBI N N, HAMDI K A. Switched phased-array transmission architecture for secure millimeter-wave wireless communication [J]. IEEE transactions on communications, 2016, 64(3): 1303 – 1312. DOI: 10.1109/TCOMM.2016.2519403

[40] HONG Y Q, JING X J, GAO H. Programmable weight phased-array transmission for secure millimeter-wave wireless communications [J]. IEEE journal of selected topics in signal processing, 2018, 12(2): 399 – 413. DOI: 10.1109/JSTSP.2018.2822048

[41] HE M, NI J B, HE Y Y, et al. Low-complexity phased-array physical layer security in millimeter-wave communication for cybertwin-driven V2X applications [J]. IEEE transactions on vehicular technology, 2022, 71(5): 4573 – 4583. DOI: 10.1109/TVT.2021.3138702

[42] YE N, ZHUO X R, LI J G, et al. Secure directional modulation in RIS-aided networks: a low-sidelobe hybrid beamforming approach [J]. IEEE wireless communications letters, 2022, 11(8): 1753 – 1757. DOI: 10.1109/LWC.2022.3180931

[43] GOEL S, NEGI R. Guaranteeing secrecy using artificial noise [J]. IEEE transactions on wireless communications, 2008, 7(6): 2180 – 2189. DOI: 10.1109/TWC.2008.060848

[44] KHISTI A, WORNELL G W. Secure transmission with multiple antennas I: the MISOME wiretap channel [J]. IEEE transactions on information theory, 2010, 56(7): 3088 – 3104. DOI: 10.1109/tit.2010.2048445

[45] ZHOU X Y, MCKAY M R. Secure transmission with artificial noise over fading channels: achievable rate and optimal power allocation [J]. IEEE transactions on vehicular technology, 2010, 59(8): 3831 – 3842. DOI: 10.1109/TVT.2010.2059057

[46] ZHANG X, MCKAY M R, ZHOU X Y, et al. Artificial-noise-aided secure multi-antenna transmission with limited feedback [J]. IEEE transactions on wireless communications, 2015, 14(5): 2742 – 2754. DOI: 10.1109/TWC.2015.2391261

[47] WANG H M, WANG C, NG D W K. Artificial noise assisted secure transmission under training and feedback [J]. IEEE transactions on signal processing, 2015, 63(23): 6285 – 6298. DOI: 10.1109/TSP.2015.2465301

[48] WU Y P, SCHOBER R, NG D W K, et al. Secure massive MIMO transmission with an active eavesdropper [J]. IEEE transactions on information theory, 2016, 62(7): 3880 – 3900. DOI: 10.1109/TIT.2016.2569118

[49] DO T T, NGO H Q, DUONG T Q, et al. Massive MIMO pilot retransmission strategies for robustification against jamming [J]. IEEE wireless communications letters, 2017, 6(1): 58 – 61. DOI: 10.1109/LWC.2016.2631163

[50] ZHAO W Y, LEE S H, KHISTI A. Phase-only zero forcing for secure communication with multiple antennas [J]. IEEE journal of selected topics in signal processing, 2016, 10(8): 1334 – 1345. DOI: 10.1109/JSTSP.2016.2611483

[51] SOHRABI F, YU W. Hybrid digital and analog beamforming design for large-scale antenna arrays [J]. IEEE journal of selected topics in signal processing, 2016, 10(3): 501 – 513. DOI: 10.1109/JSTSP.2016.2520912

[52] DOAN C H, EMAMI S, SOBEL D A, et al. Design considerations for 60 GHz CMOS radios [J]. IEEE communications magazine, 2004, 42(12): 132 – 140. DOI: 10.1109/MCOM.2004.1367565

[53] RUSEK F, PERSSON D, LAU B K, et al. Scaling up MIMO: opportunities and challenges with very large arrays [J]. IEEE signal processing magazine, 2013, 30(1): 40 – 60. DOI: 10.1109/MSP.2011.2178495
[54] XU J D, XU W, ZHU J, et al. Secure massive MIMO communication with low-resolution DACs [J]. IEEE transactions on communications, 2019, 67(5): 3265 – 3278. DOI: 10.1109/TCOMM.2019.2895023
[55] XU J D, XU W, NG D W K, et al. Secure communication for spatially sparse millimeter-wave massive MIMO channels via hybrid precoding [J]. IEEE transactions on communications, 2020, 68(2): 887 – 901. DOI: 10.1109/TCOMM.2019.2954517
[56] ELTAYEB M E, CHOI J, AL-NAFFOURI T Y, et al. Enhancing secrecy with multiantenna transmission in millimeter wave vehicular communication systems [J]. IEEE transactions on vehicular technology, 2017, 66(9): 8139 – 8151. DOI: 10.1109/TVT.2017.2681965
[57] JU Y, WANG H Y, PEI Q Q, et al. Physical layer security in millimeter wave DF relay systems [J]. IEEE transactions on wireless communications, 2019, 18(12): 5719 – 5733. DOI: 10.1109/TWC.2019.2938757
[58] JU Y, ZHU Y Z, WANG H M, et al. Artificial noise hopping: a practical secure transmission technique with experimental analysis for millimeter wave systems [J]. IEEE systems journal, 2020, 14(4): 5121 – 5132. DOI: 10.1109/JSYST.2020.2976852
[59] LIN Z, LIN M, WANG J B, et al. Robust secure beamforming for 5G cellular networks coexisting with satellite networks [J]. IEEE journal on selected areas in communications, 2018, 36(4): 932 – 945. DOI: 10.1109/JSAC.2018.2824760
[60] LIN M, LIN Z, ZHU W P, et al. Joint beamforming for secure communication in cognitive satellite terrestrial networks [J]. IEEE journal on selected areas in communications, 2018, 36(5): 1017 – 1029. DOI: 10.1109/JSAC.2018.2832819
[61] XU W Y, LI B, TAO L L, et al. Artificial noise assisted secure transmission for uplink of massive MIMO systems [J]. IEEE transactions on vehicular technology, 2021, 70(7): 6750 – 6762. DOI: 10.1109/TVT.2021.3081803
[62] CHEN W R, CHEN Z, NING B Y, et al. Artificial noise aided hybrid precoding design for secure mmWave MIMO system [C]//Proceedings of 2019 IEEE Global Communications Conference (GLOBECOM). ACM, 2019: 1 – 6. DOI: 10.1109/GLOBECOM38437.2019.9013417
[63] LI H Y, LI M, LIU Q, et al. Dynamic hybrid beamforming with low-resolution PSs for wideband mmWave MIMO-OFDM systems [J]. IEEE journal on selected areas in communications, 2020, 38(9): 2168 – 2181. DOI: 10.1109/JSAC.2020.3000878
[64] TIAN X W, WANG Z H, LI H Y, et al. Secure hybrid beamforming with low-resolution phase shifters in mmWave MIMO systems [C]//Proceedings of 2019 IEEE Global Communications Conference (GLOBECOM). IEEE, 2020: 1 – 6. DOI: 10.1109/GLOBECOM38437.2019.9013333
[65] LI H Y, LIU R, LI M, et al. FP-based hybrid precoding with dynamic subarrays and low-resolution PSs [C]//11th International Conference on Wireless Communications and Signal Processing (WCSP). IEEE, 2019: 1 – 6. DOI: 10.1109/WCSP.2019.8928111
[66] LI H Y, LIU Q, WANG Z H, et al. Joint antenna selection and analog precoder design with low-resolution phase shifters [J]. IEEE transactions on vehicular technology, 2019, 68(1): 967 – 971. DOI: 10.1109/TVT.2018.2879083
[67] LIU R, LI H Y, GUO Y Q, et al. Hybrid beamformer design with low-resolution phase shifters in MU-MISO SWIPT systems [C]//Proceedings of 2018 10th International Conference on Wireless Communications and Signal Processing (WCSP). IEEE, 2018: 1 – 6. DOI: 10.1109/WCSP.2018.8555694
[68] HUANG Y M, ZHANG J J, XIAO M. Constant envelope hybrid precoding for directional millimeter-wave communications [J]. IEEE journal on selected areas in communications, 2018, 36(4): 845 – 859. DOI: 10.1109/JSAC.2018.2825820
[69] LI H Y, LI M, LIU Q. Hybrid beamforming with dynamic subarrays and low-resolution PSs for mmWave MU-MISO systems [J]. IEEE transactions on communications, 2020, 68(1): 602 – 614. DOI: 10.1109/TCOMM.2019.2950905
[70] WANG Z H, LI M, LI H Y, et al. Hybrid beamforming with one-bit quantized phase shifters in mmWave MIMO systems [C]//Proceedings of 2018 IEEE International Conference on Communications (ICC). IEEE, 2018: 1 – 6. DOI: 10.1109/ICC.2018.8422249
[71] LI H Y, LIU Q, WANG Z H, et al. Transmit antenna selection and analog beamforming with low-resolution phase shifters in mmWave MISO systems [J]. IEEE communications letters, 2018, 22(9): 1878 – 1881. DOI: 10.1109/LCOMM.2018.2852304
[72] DONG L, HAN Z, PETROPULU A P, et al. Improving wireless physical layer security via cooperating relays [J]. IEEE transactions on signal processing, 2010, 58(3): 1875 – 1888. DOI: 10.1109/TSP.2009.2038412
[73] HU L, WEN H, WU B, et al. Cooperative-jamming-aided secrecy enhancement in wireless networks with passive eavesdroppers [J]. IEEE transactions on vehicular technology, 2018, 67(3): 2108 – 2117. DOI: 10.1109/TVT.2017.2744660
[74] SONG H H, WEN H, HU L, et al. Secure cooperative transmission with imperfect channel state information based on BPNN [J]. IEEE transactions on vehicular technology, 2018, 67(11): 10482 – 10491. DOI: 10.1109/TVT.2018.2849364
[75] LI C, XU Y, XIA J J, et al. Protecting secure communication under UAV smart attack with imperfect channel estimation [J]. IEEE access, 2018, 6: 76395 – 76401. DOI: 10.1109/ACCESS.2018.2880979
[76] MA R Q, YANG W W, ZHANG Y, et al. Secure mmWave communication using UAV-enabled relay and cooperative jammer [J]. IEEE access, 2019, 7: 119729 – 119741. DOI: 10.1109/ACCESS.2019.2933231
[77] SUN Y W, GAO Z, WANG H, et al. Machine learning based hybrid precoding for mmWave MIMO-OFDM with dynamic subarray [C]//IEEE Globecom Workshops (GC Wkshps). IEEE, 2019: 1 – 6. DOI: 10.1109/GLOCOMW.2018.8644321
[78] ALI A A M, EL-SHAARAWY H B, AUBERT H. Millimeter-wave substrate integrated waveguide passive van atta reflector array [J]. IEEE transactions on antennas and propagation, 2013, 61(3): 1465 – 1470. DOI: 10.1109/TAP.2012.2228622
[79] DING Y, FUSCO V. Orthogonal vector approach for synthesis of multi-beam directional modulation transmitters [J]. IEEE antennas and wireless propagation letters, 2015, 14: 1330 – 1333. DOI: 10.1109/LAWP.2015.2404818
[80] HONG T, SONG M Z, LIU Y. Dual-beam directional modulation technique for physical-layer secure communication [J]. IEEE antennas and wireless propagation letters, 2011, 10: 1417 – 1420. DOI: 10.1109/LAWP.2011.2178384
[81] SHI H Z, TENNANT A. Simultaneous, multichannel, spatially directive data transmission using direct antenna modulation [J]. IEEE transactions on antennas and propagation, 2014, 62(1): 403 – 410. DOI: 10.1109/TAP.2013.2287284

Biographies

HE Miao received his BE degree from Zhejiang University, China and MASc degree from the University of Waterloo, Canada, respectively. He is currently pursuing his PhD degree with the Department of Electrical and Computer Engineering, Queen's University, Canada. His research interests include signal processing, applied cryptography and information security, with current focus on beamforming using large antenna arrays and physical layer security in millimeter-wave wireless communications.

LI Xiangman received her BE degree from the Department of Electrical and Computer Engineering, Queen's University, Canada. She is currently pursuing the MASc degree with the Department of Electrical and Computer Engineering, Queen's University. Her research interests include machine learning security, secure data trading, and Blockchain Technology.

NI Jianbing (jianbing.ni@queensu.ca) is currently an assistant professor with the Department of Electrical and Computer Engineering and a member of the Ingenuity Labs Research Institute, Queen's University, Canada. He received his PhD degree in electrical and computer engineering from University of Waterloo, Canada in 2018. His research interests are applied cryptography, wireless and mobile network security, edge computing security, machine learning security, and blockchain technology. He received the Best Paper Awards from IEEE MASS 2018, IEEE ICC 2018, IEEE GLOBECOM 2017, EAI SECURECOMM 2016, etc., and the Best Paper Award from *IEEE Transactions on Mobile Computing*. He is serving as the associate editor of *IEEE Systems Journal* and *ACM Distributed Ledger Technologies: Research and Practice*.