Security and Safety, Vol. 1, 2022007 (2022)
https://doi.org/10.1051/sands/2022007
sands.edpsciences.org

Review

Open Access

Information Network

Physical layer security techniques for data transmission for future wireless networks

Weiping Shi[1], Xinyi Jiang[1], Jinsong Hu[2,*], Abdeldime Mohamed Salih Abdelgader[4], Yin Teng[1], Yang Wang[1], Hangjia He[1], Rongen Dong[3], Feng Shu[1,3 *], and Jiangzhou Wang[5]

[1] *School of Electronic and Optical Engineering, Nanjing University of Science and Technology, Nanjing 210094, China*
[2] *College of Physics and Information Engineering, Fuzhou University, Fujian 350116, China*
[3] *School of Information and Communication Engineering, Hainan University, Haikou 570228, China*
[4] *Karary University, Khartoum 12304, Sudan*
[5] *School of Engineering, University of Kent, Canterbury CT2 7NT, UK*

Received: 28 December 2021 / Revised: 31 March 2022 / Accepted: 13 April 2022 / Published online: 22 July 2022

Abstract The broadcast nature of wireless communication systems makes wireless transmission extremely susceptible to eavesdropping and even malicious interference. Physical layer security technology can effectively protect the private information sent by the transmitter from being listened to by illegal eavesdroppers, thus ensuring the privacy and security of communication between the transmitter and legitimate users. Thus, the main design goal of physical layer security is to increase the performance difference between the link of the legitimate receiver and that of the eavesdropper using well-designed transmission schemes. The development of mobile communication presents new challenges to physical layer security research. This paper provides a survey of the physical layer security research on various promising mobile technologies from secure key generation and keyless techniques, including secure key generation, directional modulation (DM), spatial modulation (SM), covert communication, and intelligent reflecting surface (IRS)-aided communication. Finally, the future topics and the unresolved technical challenges are presented in physical layer security for mobile communications.

Keywords Physical layer security, Key generation, DM, SM, Covert communication, IRS

Citation Shi W, Jiang X and Hu J et al. Physical layer security techniques for data transmission for future wireless networks. Security and Safety 2022; **1**: 2022007. https://doi.org/10.1051/sands/2022007

1 Introduction

Wireless mobile communications have been developing very fast [1–5]. Fifth generation (5G) mobile systems have been started to be deployed worldwide. Due to the broadcast nature of wireless media, information security has been a critical issue in wireless communication. The traditional method of addressing communication security is to adopt the secret key encryption. The secure transmission of private data is achieved by designing various encryption algorithms in the upper protocol stack. However, cryptography is of computational security and its security level depends on the hardness of the underlying mathematical problem it employs. Once an effective method is developed to solve its mathematical problem, the security of the encryption method will be seriously compromised [6]. The physical layer (PHY) is

[*] Corresponding author (email: jinsong.hu@fzu.edu.cn (Jinsong Hu); shufeng0101@163.com (Feng Shu))

the lowest one in the Open System Interconnect (OSI) model of computer and communication networks. PHY deals with hardware specifications, encoding and signalling, data transmission and reception, and finally topology and physical network design [7].

PHY security technology has become an effective solution to the wireless communication security problem. As shown in Figure 1, the transmitter (*i.e.*, Alice) sends a confidential message to the legitimate receiver (*i.e.*, Bob), while the eavesdropper (*i.e.*, Eve) receives the signal and intends to decode it. The key idea of PHY security technology is to exploit the inherent propagation characteristics of wireless channels (such as the difference between the main channel and the eavesdropping channel, randomness, and reciprocity) from the perspective of information theory, and to improve the amount of mutual information between the transmitter and the desired user at the PHY while reducing the amount of information in the eavesdropping channel through a rational design of the transmit signal. Compared with traditional encryption technology, PHY security technology has the following notable features and advantages. First, PHY security includes not only secure key generation techniques but also keyless techniques (*i.e.*, no encryption and decryption operations are required). Second, PHY security techniques can take advantage of the time-varying and random nature of wireless channels.

The PHY security technology can effectively protect the content of private messages sent by the transmitter from being eavesdropped by illegal Eves [8] and protect the behavior of signal transmission from being detected or the presence of the user from being discovered by a surveillant [9]. Specifically, the key generation-based PHY security technology mainly relies on the reciprocity and randomness of the wireless channel to generate channel keys, ensuring that legitimate users can dynamically generate the corresponding keys under the observation of the transceiver link [10]. The study of keyless PHY security techniques originated from the Wyners Wire-tap wireless communication eavesdropping channel model, which shows that when Eve's channel is the degenerate channel of the legitimate receiver, there is some way to maximize the transmission rate from the sender to the legitimate receiver without giving away any information to Eve. This eavesdropping channel model has been extended to broadcast Gaussian channels [11, 12]. In particular, signal processing techniques are employed to design reasonable beamforming or power allocation strategies from the transmitter's perspective to improve the security performance of wireless communication systems [13]. Based on the above advantages, solving the communication security problem from the PHY has aroused widespread concern. The authors in [14] studied the secure transmission of private information on Gaussian channels, and proved that expanding the difference between the main channel and the eavesdropping channel can achieve low probability interception and low probability detection for Eves. Wang *et al.* [15] further researched the keyless PHY secure transmission technology over fading channels. The use of multiple antennas can add additional degrees of freedom and further improve the security performance of the wireless network [16, 17]. In addition, by generating random artificial noise (AN) at the transmitter to interfere with Eves, the security of the system can be further improved [18]. Currently, scenarios where Eves exist are considered in various wireless communication systems.

The basic PHY security techniques have been summarized comprehensively in the literature [6–8, 13, 19]. However, firstly, the published papers only provided a basic summary of PHY security on basic transmission content, and did not address the case of transmission behavior subject to detection. Secondly, the published papers did not conclude the current emerging intelligent reflecting surface (IRS) which can greatly improves the PHY security performance. Also, we review the latest literature on directional modulation (DM) and secure spatial modulation (SM). Therefore, as a complement to the existing surveys, we focus on the following areas.

Specifically, secure key generation technology is an encryption method that uses the random characteristics of the physical channel of wireless transmission to generate a key and combines it with traditional upper layer encryption mechanisms to achieve security. It places no restrictions on the eavesdropping party's computing power, eliminating the dangers present in traditional wireless key negotiation, allowing independent key generation and extraction, providing unconditional security, and circumventing the risks of pre-distributed keys [10]. The difficulty lies in designing a key sequence that reflects the uniqueness, reciprocity, and randomness of the channel to ensure that the two communicating parties in a legitimate channel can identify the key sequence accurately and unambiguously [20]. Keyless PHY security does not need to generate keys. Advanced signal processing techniques such as antenna selection, beamforming, relay selection, and cooperative jamming are used to increase the transmission difference between legitimate and eavesdropping links so as to enhance the secure transmission capability of the

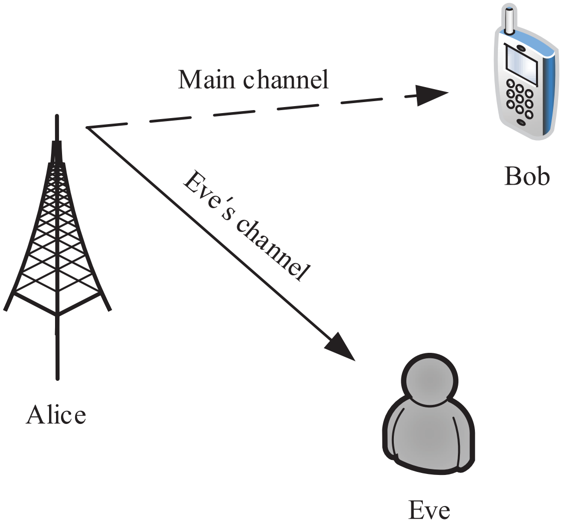

Figure 1. A three-node secure communication model

system. For keyless PHY security, firstly, satellite communications, marine communications, mmWave communications, and unmanned aerial vehicle (UAV) networks have been widely used in current 5G networks, and their communication channels are mainly dominated by line-of-sight (LoS) components; DM is very suitable for LoS channels to achieve a strong directive transmission because it can guarantee secure transmission in the desired direction while distorting the constellation diagram in all other directions [21]. Secondly, for the conventional multiple-input multiple-output (MIMO) technology, the large number of radio frequency (RF) chains leads to high system energy consumption, while SM provides a low-cost, low-energy, and high-performance communication technology. SM also uses antenna sequences and modulation symbols to transmit bit information, which reduces the design complexity of transmitters and receivers and reduces the RF link overhead. Therefore, SM has become a promising technology for MIMO systems because of its ability to address security problems in many scenarios by protecting the content of the message [22]. It is worth noting that the behavior of the transmission itself exposes the connection between the parties involved in that communication process, which can trigger further investigation and attacks. The task of covert communication is to protect the behavior of wireless transmissions, thereby reducing the probability that a watcher will discover the communication behavior in a wireless network. It achieves a higher level of security than cryptography and traditional PHY security techniques [9]. Moreover, with the development of sixth generation (6G) research, it is realized that the key issues facing future wireless communication will be the high cost of hardware, the high complexity of wireless communication networks, and the increasing energy consumption. IRS is the key technology that has received the most attention in 6G research due to its low cost, low energy consumption, and programmable nature [23]. Thus, SM and DM are used to protect the privacy of the transmitted content, covert communication protects the transmitted behavior, and IRS is introduced to further improve the security of the system while reducing the cost.

Considering the potential of PHY security for mobile communications, the opportunities and challenges of how to achieve high levels of security at the PHY deserve more attention from the research community. There are several approaches to achieve security using PHY, such as pre-processing scheme [24, 25], coding [26], key generation and exchange [20, 27–29], artificial noise scheme [30], game theoretic schemes [31], signal processing, and cooperation communications. The purpose of this paper is to provide a summary of the latest PHY security research results for key future wireless network technologies. As shown in Figure 2, we will focus on the following five aspects of PHY security technologies.

(1) Secure key generation: Key generation is an essential part of cryptosystems. For symmetric key cryptosystems, the two legitimate parties should agree on a common key to complete the authentication, privacy, and integrity services. However, key distribution is one of the challenging problems

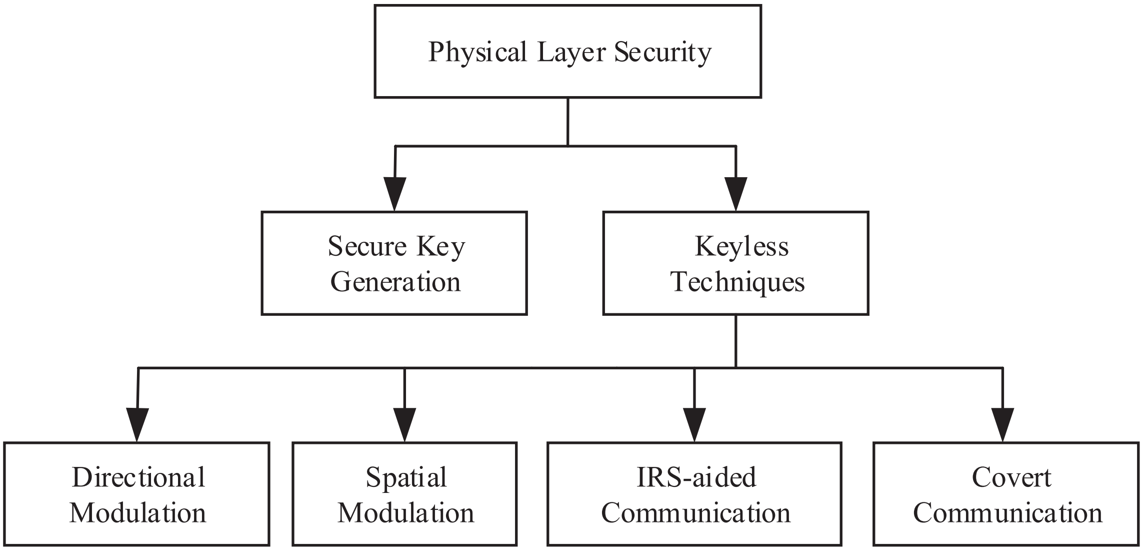

Figure 2. An illustration of PHY security

of these services. Moreover, ordinary key generation techniques require much effort in terms of complexity and acceptable secrecy. This work investigates the ongoing efforts for using PHY security for key generation and key sharing for security solutions in wireless communications.

(2) Directional modulation (DM): The DM technique using phased arrays sends information along the direction of the desired receiver, making the constellation diagram of the received signal in the desired receiver direction the same as that of the baseband modulated signal, while the constellation diagram of the received signal in the undesired direction will be distorted, thus ensuring the safe transmission of information.

(3) Spatial modulation (SM): SM is a new MIMO antenna transmission technique, which plays an effective balance between hardware overhead and transmission rate. Because it makes full use of the channel index information to transmit more bit streams, it enhances the spectral efficiency of the system without increasing the costly RF links. Since both antenna index and modulation symbols in SM networks carry private information, interception of either of them may result in leakage of confidential information. In other words, compared with MIMO communication, the SM network has serious communication security risks. Therefore, it is strategically important to utilize PHY security technology to provide security for SM systems.

(4) Covert communication: In covert communication, when the transmitter transmits a message to the receiver, it is guaranteed that the probability that the illegal watcher can detect the transmission is small enough. Covert transmission technique, as an important secure transmission technique, aims to hide the transmission behavior of the transmitter. Compared to PHY security techniques that aim to prevent the transmitted content from being overheard by Eves, covert communication techniques can achieve a higher level of communication security.

(5) Intelligent reflecting surface (IRS)-aided communication: An IRS is an artificial surface made of electromagnetic material and composed of a large number of passive reflective units. By configuring these reflective units to act on the phase shift and amplitude of the incident signal, fine-grained three-dimensional beamforming can be achieved, which can be used to improve channel quality, enhance received power, and extend the communication distance. IRS transforms the traditional uncontrollable and random wireless communication environment into a programmable and relatively deterministic transmission space, and plays an active role in the signal transmission process. By introducing IRS into the security system, the security of the system can be further enhanced.

The rest of this paper can be outlined as follows. We first discuss secure key generation in Section 2, then DM and SM techniques on PHY security in Sections 3 and 4, respectively. Section 5 focuses on the covert communication, and Section 6 summarizes the security in IRS-aided wireless communication systems. Finally, conclusions are drawn in Section 7.

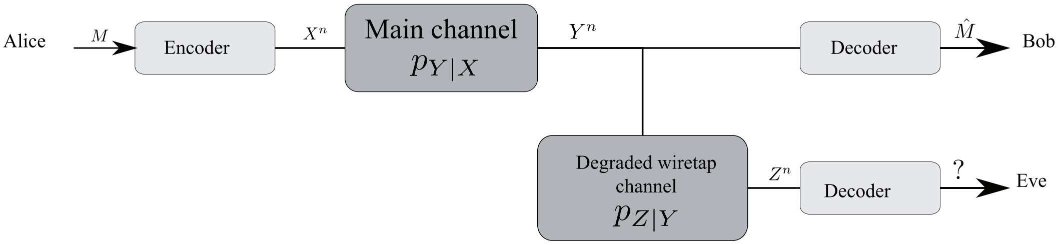

Figure 3. A simple PHY security using degraded wiretap model

2 Secure key generation

In communication systems, the authentication, confidentiality, and privacy services are usually handled in the upper layers using private-key and public-key cryptosystems. Nowadays, many researches from information theory, signal processing, and cryptography suggest that there is much security to be gained by accounting for the imperfections of the PHY when designing secure systems. Ordinarily, asymmetric key cryptosystems are the most common methods for distributing a secret key in many wireless communication systems [20]. Asymmetric key cryptosystems consume significant amounts of computing resources, bandwidth, and power; thus it might not be available in specific wireless scenarios such as in vehicle ad-hoc networks (VANETs) [7, 27], mobile ad-hoc networks (MANET) [27, 32], and wireless sensor networks (WSNs) [33]. Public key system limitations have motivated many researchers to develop alternative approaches. Quantum cryptography is one of these attempts, which uses the quantum theory laws for sharing a secret key [34]. It has been involved in some applications [35], nonetheless, the researches are still in their initial stages and excessively expensive. PHY security solutions can be implemented using channel properties without involving traditional secret key mechanism. Such research results can be utilized to generate secret keys in a cost efficient way without sacrificing much communication capacity.

2.1 Key extraction techniques

The key generation techniques using the PHY can be generally categorized into keyless security and secret key-based security. Keyless security-aided transmission and secret key agreement fall under the umbrella of PHY security, which achieves security by exploiting the unpredictable characteristics of the random channel. Most of secure communication models have not considered the physical reality of communication channels [28, 36], particularly, the degradation of signals because of fading or noise. This observation naturally introduced a more realistic communication model, now known as the wiretap channel, where noise in the main channel and eavesdropper's channel was explicitly introduced.

Wiretap channel model, which is usually referred to as the keyless security, transmits data without any encryption and generation of a common key. To illustrate how secrecy could be possible over a noisy channel without any encryption mechanism, a degraded additive white Gaussian noise (AWGN) wiretap channel is considered, as shown in Figure 3. The degraded wiretap channel [Alice-Eve] has lower signal-to-noise ratio (SNR) than the main channel [Alice-Bob]. Consequently, for a given binary constellation employed by Alice and Bob, the bit error rate (BER) for the main channel is lower than the BER for the wiretap channel. Consider that the difference is large enough so that after decoding of the repeated symbols sent by Alice, Bob is able to identify a unique symbol, while Eve can only see a cloud of points all over the constellation, which would make her unable to decode the sent symbol. This is one of the simplest examples of exploiting a physical layer advantage to securely transmit information between two parties without involving a key distribution technique. Despite the advantage in this scheme, the choice of the constellation by Alice and Bob depends on their knowledge about the channel state information (CSI) of the wiretap channel, which is one of the main challenges in the field of PHY security. PHY secrecy research usually considers complete, partial, or no knowledge of CSI [29, 37, 38].

There are two models of secret key agreement: channel model-based and source model-based. Both models include a two-way authenticated public channel with no rate limitation, unless stated otherwise. The channel model-based key agreement follows a similar concept to the wiretap channel model, but there are some differences.

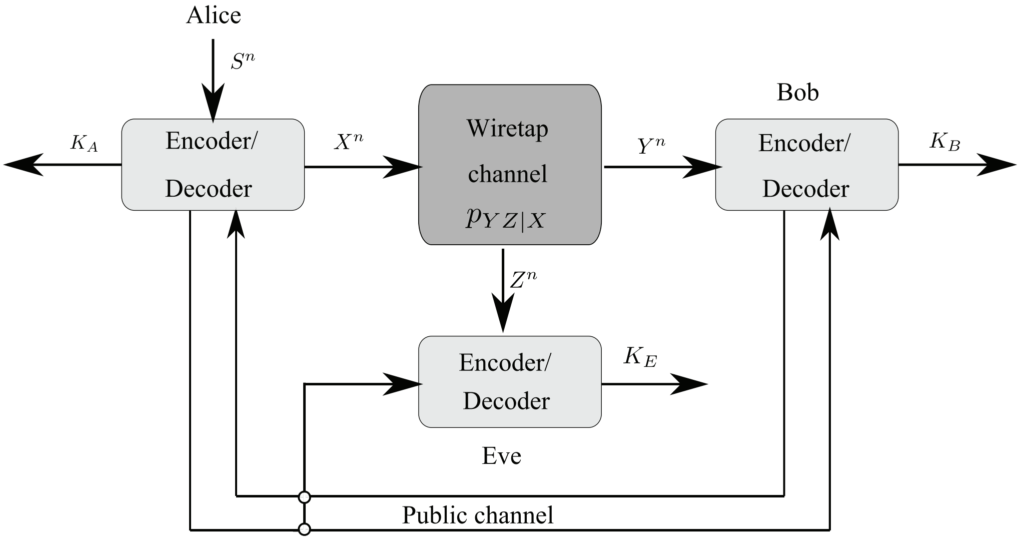

Figure 4. Secret key agreement channel model

The channel model-based key agreement securely transmits keys from Alice to Bob, and agrees on the same key via a two-way public channel [37–40]. It consists of transmission strategies that leverage the wireless channel as a medium to convey secret information. This model is an extension of the wiretap channel. There exists a two-way, noiseless, public, and side channel of unlimited capacity. This model is introduced to analyze the effect of feedback on secret communications. In this model, Alice sends a random sequence X^n over a discrete memory-less channel (DMC) defined by $P(YZ|X)$, Bob and Eve observe outputs Y^n and Z^n as shown in Figure 4. Indeed, the wiretap channel (characterized by $P(YZ|X)$) is a particular case of common information (characterized by $P(XYZ) = P(YZ|X)P(X)$) when Alice chooses $P(X)$ and generates n independent, identically distributed (i.i.d) random realizations according to $P(X)$ [37–40].

Legitimate party can communicate over a public, authenticated, two-way side-channel of unlimited capacity. The supposition that the channel is public allows Eve to intercept all messages sent over the channel, so that the channel does not establish a source of secrecy. However, the assumption that the channel is authenticated prevents the intruder from interfering the messages. The objective is for the legitimate parties Alice and Bob to exchange n symbols over the noisy channel and to transmit messages, denoted by F, over the public channel, so that they eventually agree on the same secret key K. If there exists a sequence of key generation policies with an increasing number of symbols transmitted in the noisy channel, a secret-key rate R is accomplished, satisfying the following three requirements. Firstly, with high probability, legitimate parties reliably agree on the same key. Secondly, the secret key is uniformly distributed, in order to be used for cryptographic applications. Thirdly, the key is secret with respect to eavesdropper, who observes the noisy signals and the public messages.

The addition of a public authenticated channel does not underestimate the problem, because it is not a resource for secrecy. The only resource for secrecy leftovers is the noisy communication channel. Contrasting the wiretap channel model, the channel model for secret-key sharing allows for two-way communication and feedback. Feedback turns out to be an essential ingredient for secret key generation. In addition, the key K is not a traditional message because its value needs to be fixed at the beginning of a secret-key agreement strategy. This allows the key to be generated interactively based on the observations and messages of all legitimate parties, and to be processed with non-invertible functions. This differs with the wiretap channel model in which the secret message from the sender must be received unchanged. Moreover, secret-key generation strategies are extremely sophisticated. There are some other possible methods to improve the key generation security at the transmitter side. For instance, the sender party can make some noise when transmitting the message. However, it requires much efforts from the receiver to correctly detect and estimate the information. The common challenge of both channel model-based key agreement and keyless security solutions is the practical implementation.

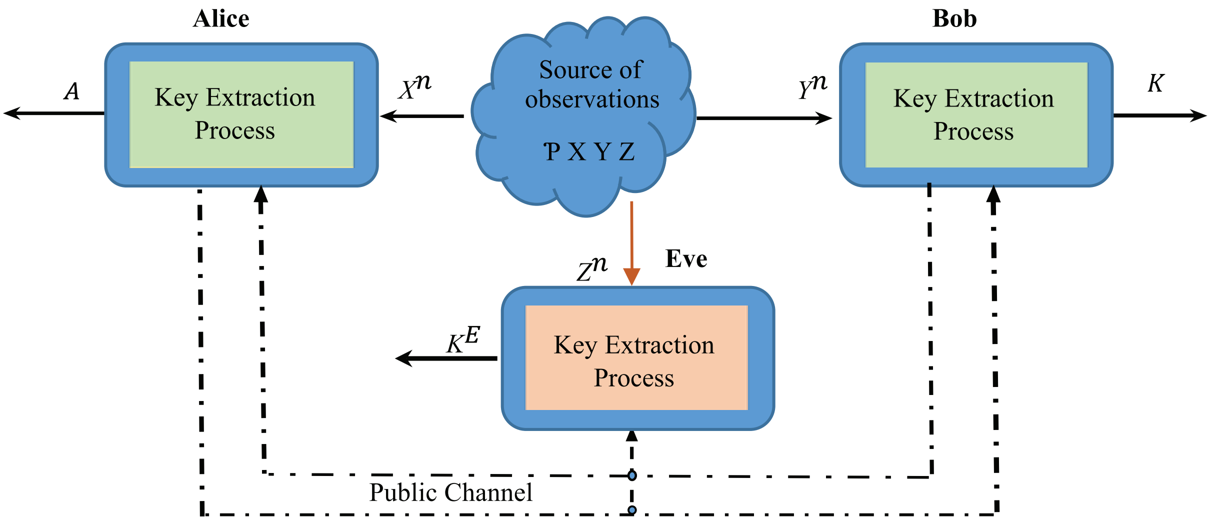

Figure 5. Secret key agreement source model

The source model-based secret key agreement works in a different manner. It generates the keys from the wireless channel between Alice and Bob rather than transmitting the keys, which is termed as key generation from wireless channels. It considers the wireless channel as a source of random information and not as a transmission support. Legitimate party only has to agree on a key based on common randomness observations instead of transmitting a particular message. The source model assumes the existence of a discrete memory-less source (DMS) defined by $P(XYZ)$ with components $(X^n; Y^n; Z^n)$ observed by Alice, Bob, and Eve, respectively, as shown in Figure 5.

Assume that two legitimate terminals want to agree on a key while preventing Eve from knowing anything about it, but a random guess. When legitimate parties are not collocated, signals observed at outputs of the main channel and eavesdropper's channel are usually different. Natural discrepancies are caused by physical phenomena. For wireless communications, the most notable effects are noise, fading, and path-loss [29, 34]. The source model of key generation involves two legitimate users, Alice and Bob, and a passive eavesdropper, Eve. Alice, Bob, and Eve acquire channel observations $X^n = [x^1(A), x^2(A), \dots, x^n(A)]$, $Y^n = [y^1(B), y^2(B), \dots, y^n(B)]$, and $Z^n = [z^1(E), z^2(E), \dots, z^n(E)]$, respectively [40]. These observations are the main inputs for the key extraction process, which is used to agree upon the same key between legitimate parties. For legitimate parties, these observations are theoretically equal, while those observed by Eve are totally different.

To establish a shared secret key, legitimate users measure the variations of the wireless channel by transmitting probes to each other and measuring the received signal strength (RSS) values of the probes. Legitimate parties should ideally measure the RSS values at the same coherence time to get identical readings. However, typical commercial wireless transceivers are half duplex; they cannot exchange the signals at the same time. Thus, they must measure the radio channel in one direction at a time. However, as long as the time between two directional channel measurements is within the channel coherence time, they will attain identical readings. General speaking, the secret key sharing is achieved using four stages which are channel probing, quantization, information reconciliation, and privacy amplification as shown in Figure 6 [27]. As channel coherence time is very short, and the bandwidth and capacity in some communication systems are very limited, the drop ratio should be greatly reduced. Therefore, some approach uses a quantization method to extract the secret key that increases the range and amount of quantization levels [20, 41].

Recently, channel state has been widely used to extract a secret key [42, 43]. In this context, Abdelgader and Wu exploited the physical characteristics of the wireless channel to provide secrecy for transmissions and key sharing mechanism appropriate for VANET [20]. Many efforts and comprehensive reviews in this context have been tackled and summarized in [44–47]. In particular, Mathur *et al.* in [42] proposed a level-crossing key extraction algorithm that preserves only one bit from m successive 1s or 0s and drops other redundant $m-1$ bits. However, it achieved low match rate while reducing the secrecy rate. To solve

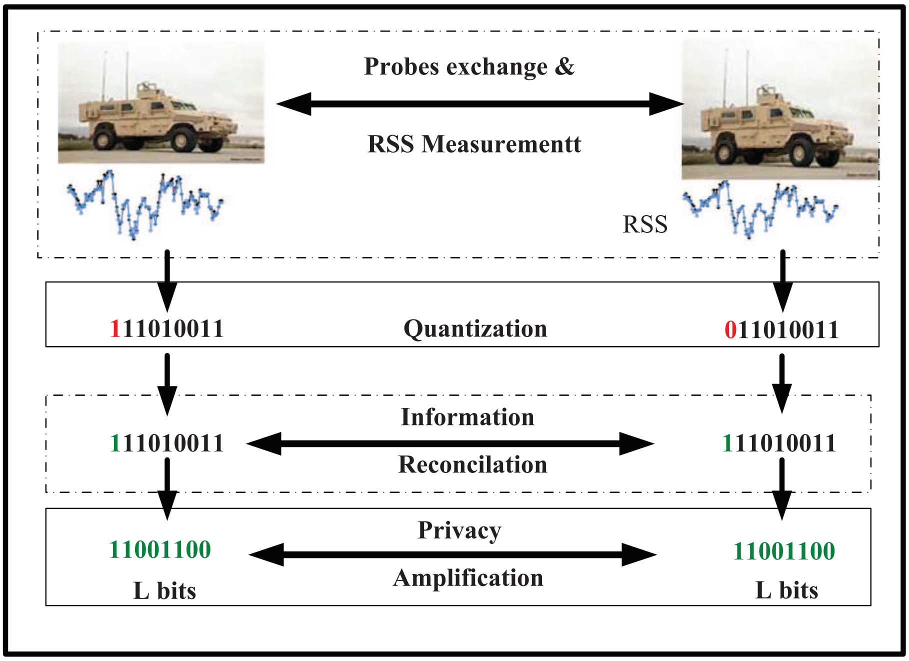

Figure 6. Key sharing process [27]

this problem, Zhu *et al.* applied canonical correlation analysis to obtain the optimal weight coefficient of the sliding smoothing filter in order to improve the correlation of the measurements of transceivers and accelerate the bit generation rate [48]. Also, to solve the secrecy rate and dependency issue in the extracted key, Abdelgader *et al.* employed two orders of Markov chain to scramble the extracted bits and increase randomness [27], while an adaptive secret bit generation scheme was proposed in [36], which is an improved version of the scheme [42].

Different from the Mathur quantizer, the measurements in [27] were divided into multiple blocks, and the quantizer extracted a bit from each measurement of each block, and it depended on further steps to eliminate the effects of correlated bits. Furthermore, another paper also introduced an adaptive secret multi-bit key generation scheme using the Gray code, which not only improved the secret rate but also increased the bit mismatch rate. Abdelgader and Ali *et al.* [20, 41] put forward the RSS-based high-bit rate, consistent, and random key extraction for VANETs scenarios. Exactly, for perfect mismatch rate, it used an inconsistency removal method to remove the inconsistent measurements between the two communication parties. This scheme was able to achieve near zero-bit mismatch rate with low secret bit rate. Afterwards, they solved the secret rate degradation by proposing a multilevel quantization approach, which reuses each RSS many times.

Many types of research employed the RSS for extracting the shared secret key. However, other parameters related to the channel response between the three parties can be used for extracting the secret key for the legitimate parties without giving useful information to the intruder party. The channel response between the two legitimate parties is typical and totally different from that between legitimate parties and the intruder. This fact concludes that there are three different channel responses H_{AB}, H_{AE}, and H_{BE} which are matrices containing many parameters [49]. Therefore, one can investigate and search these parameters and develop a model for extracting a secret key from it.

Finally, it is important to note that the key generation using PHY has been widely used in vehicular networks and is very promising to be employed in other types of wireless communication networks such as Internet of things (IoT), machine to machine (M2M), MANET, and WSN suitable for mobiles, drones, and helicopter networks. It is also worth mentioning that the PHY-based extracted keys are usually appropriate for solving the key distribution problem of symmetric key cryptosystems and can replace public (asymmetric) cryptosystem solutions in the near future owing to the complexity and the bulk amount of data generated by public key solutions. It is also important to note that the key generation methods based on PHY security are much suitable and have a high rate of success in wireless mobile communication systems, owing to the possibility and presence of Doppler shift, fading, multipath, noise, and interference, which create a fine venue for acceptable randomness to the generated secret key.

2.2 PHY security limitations and possible attacks

The PHY security solutions may have many limitations. It is also vulnerable to several ordinary security attacks, such as attack against privacy, authentication, and integrity. In this context, denial of service (DOS) is a common security attack, which is performed by causing malicious action or deliberate failure of nodes. It can be performed through consuming the resources of the victim system, by transferring bulk amounts of unwanted information and hence denying the victim from accessing the resources and service of the communication system. PHY security solutions for wireless communication systems are widely susceptible to this kind of attacks.

Brute force attack is also a possible attack when applying PHY security solutions, because some channel measurements which are as a part of the security system, such as the key agreement, can be predicted and discovered using a Brute force attack. The good news is that, most of the PHY security solutions are suitable for limited resource computational capability communication systems. This means that the Brute force attack in these systems has very limited probabilities.

One of the common attacks in wireless communication systems is the jamming attack. Flow jamming attack (FJA) is one of the most intelligent attacks because the jamming devices are located in such a way that the amount of flow to be jammed in the wireless system is greatly maximized while the power used to jam the flow is minimum [2, 16]. This attack has a great chance when PHY security solutions are applied. The FJA can have a great influence on the probing stage during the key generation process. FJA and its model are considered as a linear programming. One of the key areas of research that tackles the jamming attack is to find scheduling algorithms for collecting real-time data about the data flow in the communication system during a FJA. The scheduling problem aims at finding a value that maximizes the use of multiple channels to filter the packet with interference and channel parameter constraints.

When extracting secret key using RSS, the RSS reading and the level fine tuning values, such as mean and standard deviation, are general statistical values, which can be predicted by the attacker. Therefore, to ensure that an attacker cannot use his knowledge about the distance between legitimate users to predict some parts of the key, the mean RSS value is dropped out of the measured RSS in many solutions, because it can be an expected function of distance. Future key generation solutions based on PHY should find a trade-off between reducing the drop ratio and closing the security vulnerability accordingly.

2.3 Future challenges

Future PHY key generation solutions should take care of decreasing the mismatch rate and increasing the secrecy and entropy rate while reducing the number of probes and the amount of the exchanged data between the two legitimate parties. Future approaches should evaluate their robustness of key extraction results using the secrecy rate, entropy rate, mismatch rate, and drop ratio as assessment metrics. More research is needed in terms of secrecy capacity, quantization techniques, information reconciliation with less information exchange and robust results, and high entropy rate privacy amplification approaches. Besides, a challenging scenario arises when using PHY security to extract keys where the link between Bob and Alice is not a direct communication channel. For example, when two parties communicate through an entrusted relay. It is worth noting that much research is required to determine which type of key generation method is suitable for a particular communication security system.

3 PHY security of DM

In recent years, as one of the key technologies of PHY wireless transmission, DM has been a research hotspot in the field of PHY security. DM technology realizes the directionality of signal transmission by optimizing the design of beamforming and adding AN to the transmitted signal. Using this technology can not only accurately and efficiently transmit information to desired users, but also achieve signal

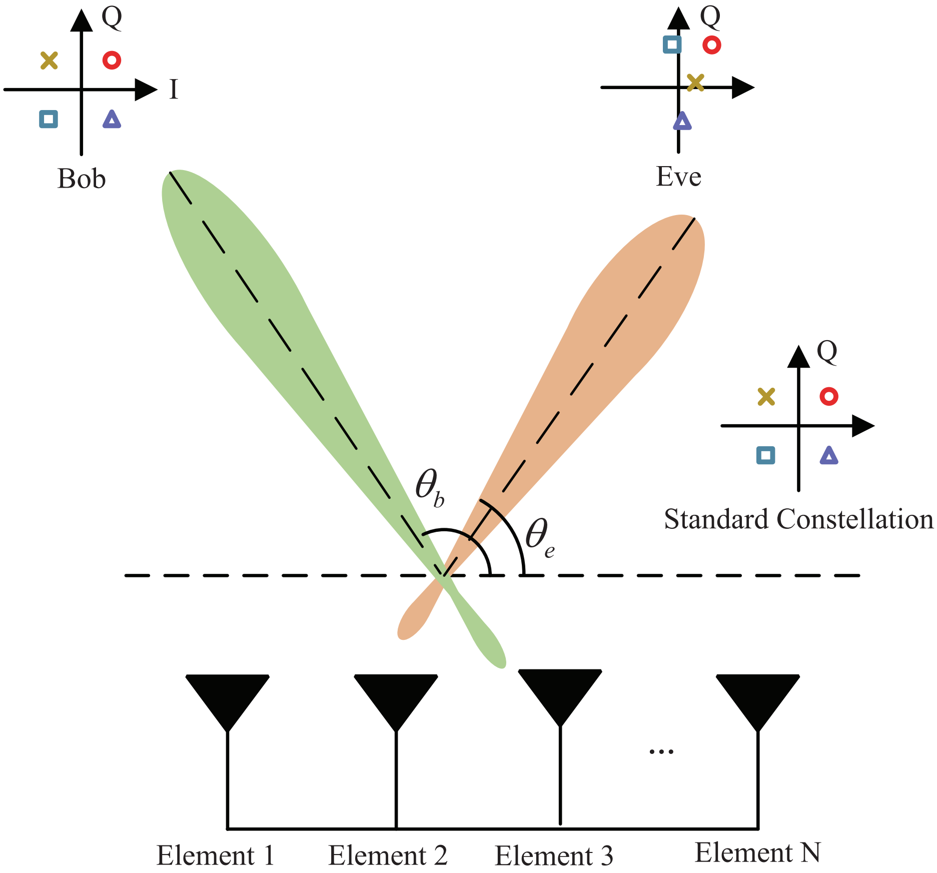

Figure 7. Schematic diagram of DM network

constellation distortion in undesired directions by designing AN projection matrix to transmit AN to undesired directions. Different from traditional PHY security technologies, DM is mainly suitable for fading-free Gauss white noise channels. When the distance and direction of the transmitter and receiver are known, the channel steering vector has static stability.

In Figure 7, a schematic diagram is given to show the basic idea of DM. The system consists of three nodes: a multi-antenna transmitter (Alice), a desired user (Bob) and an eavesdropper (Eve). Using the AN technology and the null space projection (NSP) criterion, the AN is projected into the null space of the desired direction channel, that is, it does not affect the desired user so that the expected receiver can easily decode useful information. At the same time, since AN makes it difficult for Eve to observe the changing law of the signal constellation diagram, Eve cannot correctly decode confidential messages (CMs). In this system, M independent data streams are sent to M desired receiver directions, respectively, with $\{x_m\}_{m=1}^{M}$, and the direction angles are $\{\theta_{d1}, \theta_{d2}, \ldots, \theta_{dM}\}$. In addition, it is assumed that there are J eavesdropping directions, which are $\{\theta_{u1}, \theta_{u2}, \ldots, \theta_{uJ}\}$. Let the kth symbol modulating of the mth user be x_{mk}, and $\mathbb{E}[x_{mk}^{*}x_{mk}] = 1$. The transmitter simultaneously transmits the useful signal and artificial noise at the transmitting end, and the transmission vector of the kth symbol is denoted as

$$\mathbf{s}_k = \beta_1\sqrt{P_s}\sum_{m=1}^{M}\mathbf{v}_m x_{mk} + \beta_2\sqrt{P_A}\mathbf{W}\mathbf{z}, \tag{1}$$

where P_s is the total transmit power, β_1 and β_2 are the power allocation parameters of CMs and AN, and $\beta_1^2 + \beta_2^2 = 1$. $\mathbf{v}_m \in \mathbb{C}^{N\times 1}$ denotes the transmit beamforming vector of the mth CM, and $\mathbf{W} \in \mathbb{C}^{N\times N}$ is the projection matrix for controlling AN to the undesired direction, where $\mathbf{v}_m^H\mathbf{v}_m = 1$. In addition, $\mathbf{z} \in \mathbb{C}^{N\times 1}$ denotes the AN vector with complex Gaussian distribution, *i.e.*, $\mathbf{z} \sim \mathcal{CN}(0, \mathbf{I}_N)$. The signal data stream $\mathbf{s}$ is transmitted through the wireless channel, and the kth data received along the direction angle θ is expressed as

$$y_k(\theta) = \mathbf{h}^H(\theta)\mathbf{s}_k + w_k, \tag{2}$$

where w_k is the complex AWGN vector, distributed as $w_k \sim \mathcal{CN}(0, \sigma_{w_k}^2)$. The normalized steering vector $\mathbf{h}(\theta)$ is

$$\mathbf{h}(\theta) = \frac{1}{\sqrt{N}}[e^{j2\pi\Psi_\theta(1)}, \ldots, e^{j2\pi\Psi_\theta(n)}, \ldots, e^{j2\pi\Psi_\theta(N)}]^T, \tag{3}$$

where the phase function $\Psi_\theta(n)$ is defined as

$$\Psi_\theta(n) \triangleq -\left(n - \frac{N+1}{2}\right)\frac{d\cos\theta}{\lambda}, \quad n = 1, \ldots, N, \tag{4}$$

where θ is the direction of arrival or departure, n is the index of antenna, d represents the element spacing in the transmit antenna array, and λ is the wavelength.

As an advanced PHY security transmission technology, DM combines beamforming technology and artificial noise to further improve the security performance of communication systems. Different from the traditional beamforming technology, the DM technology can realize the directivity of the signal, ensure the safe transmission of the signal in the desired direction, and interfere with the constellation of the signal in the undesired direction at the same time. However, different from the conventional MIMO system, DM is only suitable for the LoS channels due to its effect of gathering AN to Bob in mulitpath channels. Its main advantage is its directive property, which may improve the physical-layer security and achieve a high energy efficiency. Its main disadvantages are as follows: (a) Alice with transmit antennas only transmits one confidential message stream (CBS) towards Bob with multiple receiver antennas due to the rank-one property of the channel matrix from Alice and Bob in line-of-propagation channel; (b) The effect of gathering AN towards Bob will significantly degrade the SR performance of Bob. Although DM is only suitable to the line-of-propagation channels, it still has several potential future applications such as deep space channel, satellite communication channel, UAV communication channel, and even the future 6G mmWave and THz channels.

3.1 Realization method of DM

DM can be divided into two categories: one is based on the combination of RF and components, and the other is implemented by designing algorithms for baseband signals. Babakhani *et al.* [50] introduced a near-field direct antenna modulation (NFDAM) technology, which modulates the far-field radiation signal through the time-varying electromagnetic boundary conditions of the antennas near-field. This enables the transmitter to send information depending on the direction so as to achieve a safe transmission effect. Daly and Bernhard [51] proposed a DM technique based on phased array generation. By correctly phase shifting each element, the amplitude and phase required by each symbol in the digital modulation scheme are generated in a given direction. The disadvantage of this technology is that it only considers the signal constellation in the desired direction and ignores the consideration of the distortion of the constellation in the undesired direction. Therefore, Daly *et al.* [52] designed a phased array-based PHY secure transmission technology on the basis of [51]. They found through experiments that the DM transmitter creates a narrower low error rate area around the desired direction, while continuing to maintain a high error rate in the sidelobe area. Daly and Bernhard [21] then used an array with pattern reconfigurable elements to switch elements for each symbol, thereby generating a digitally modulated signal in the desired direction, and used this reconfigurable array to demonstrate the improvement of DM in terms of safety performance. Unlike traditional transmitters that excite the same antenna, Hong *et al.* [53] proposed a dual-beam DM technology for PHY security communications, which used in-phase and quadrature baseband signals to excite two different antennas. In [54], the DM network with a time-modulated phased arrays was proposed, which can synthesize multicarrier DM symbols for PHY security.

According to the concept of orthogonal AN in information theory, Ding and Fusco applied orthogonal vector technology to DM in [55]. By adding orthogonal AN signals at the baseband, the signal constellation in the undesired direction is distorted, causing Eves to be unable to decipher CMs according to the changing law of the signal constellation. At the same time, the orthogonal AN is projected into the null space (NS) of the channel steering vector of the desired direction, thereby eliminating the influence of AN on the signal received by desired users. Ding and Fusco [56] further proposed an orthogonal vector method for DM transmitter to synthesize multiple beams on the basis of [55]. Ding and Fusco [57] showed that when the non-cooperative receivers are placed separately, the DM system can be regarded as a MIMO system operating in free space. By transmitting AN that is orthogonal to the useful information, the security performance of the DM system is thereby improved.

3.2 Robust beamforming and DOA measurement for DM secure system

In actual application scenarios, there will be errors in the measured angle, which will affect the expected user reception performance and reduce the security of wireless transmission. However, in the above research, the direction angle is assumed to be the ideal known information, thus further studies on systems with imperfect information of direction angle are needed. Hu *et al.* [58] designed a robust DM synthesis technique based on the principle of minimum mean square error (MMSE) in view of the uncertainty of the estimated direction angle, which improves the bit error rate (BER) performance of the system by minimizing the constellation distortion in the desired direction. Shu *et al.* [59] considered a multi-beam broadcast DM scenario with an imperfect desired direction. Shu *et al.* [59] designed beamforming by minimizing information leakage in the eavesdropping direction, and maximizing the expected average received signal-to-interference-to-noise ratio (SINR) of the user end to design a projection matrix of AN, so as to achieve the robustness of CM transmission in the wireless communication system. Shu *et al.* [60] considerd the MIMO system with direction of arrival (DOA) measurement error, and proposed a robust beamforming scheme based on the combination of main lobe integration and leakage, which transmits independent and parallel private data streams to multiple legitimate users at the same time, thereby realizing the stable and safe transmission of CMs in the DM system. Shu *et al.* further designed a low-complexity scheme in [61] that can accurately and safely transmit CMs to desired users through the joint use of AN, phase alignment, orthogonal frequency division multiplexing (OFDM) technology, and DM random subcarrier selection technology.

In addition, there is a key technology in the DM field, DOA estimation technology, which combines information of different frequencies to obtain the best DOA. Hung and Kaveh [62] characterized the specific structure of the focus matrix to avoid focus loss, and the focus matrix is preferably a unitary matrix, which has an important impact on the statistical characteristics of DOA estimation. In [63], the data were robustly preprocessed through the weighted average of the signal subspace and the enhanced design of the focus matrix. Ng *et al.* [64] proposed a wideband structure for processing array signals, and estimated the order and DOA through the Bayesian method and the reversible jumping Markov chain Monte Carlo process.

3.3 Future challenges

In wireless communication, the scattering of electromagnetic waves caused by the atmosphere and the reflection or diffraction of the electromagnetic waves created by the surrounding buildings and other surface objects will cause multipath propagation of radio signals. In practice, due to the lack of cooperation between Alice and Eve, the CSI may be imperfect. For DM, if the directional angle from Alice to Eve is available, AN can be forced to its direction by beamforming. Once Eve communicates with its data center, Alice or Bob may estimate its directional angle. The basic idea of multiple parallel transmissions can be extended to the scenario of imperfect CSI. In our view, the joint optimization problem will become harder to address due to the imperfect CSI constraint.

The PHY security technology provides a guarantee for the security of wireless communication, and its future research still faces many problems. For example, the problem of secure transmission of DM in the multipath environment, the problem of information theory, and the key technology of precise wireless communication under the impact of two-dimensional (distance and direction angle) factors and its robustness under the condition of estimation error. In the multi-user scenario, from the perspective of information theory, the problem of the security capacity region of the multi-user system and the asymptotic upper bound of the secrecy rate sum can be further studied.

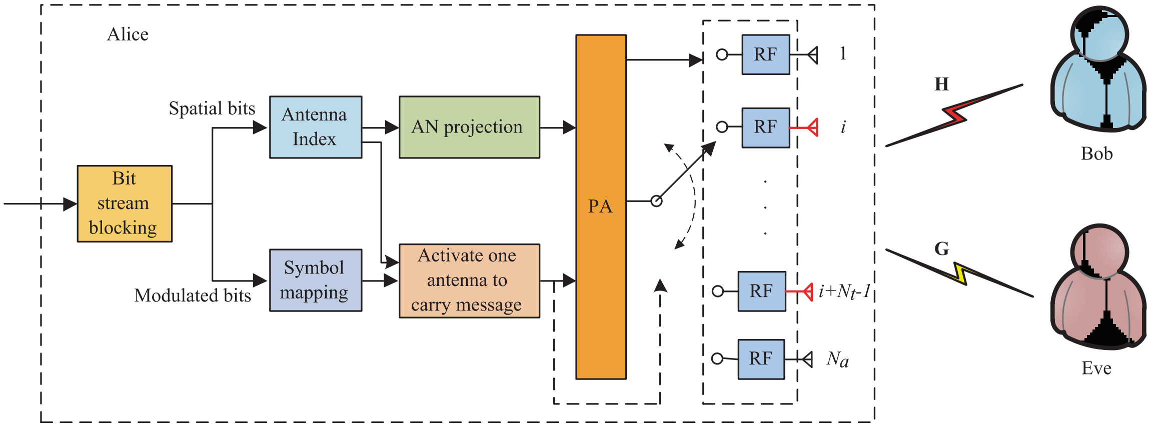

Figure 8. Schematic diagram of SSM network

4 PHY security of SM

As one of the derivatives in the context of MIMO techniques, SM is becoming a hot research area. Its basic idea is using both the transmit antenna index and the modulated symbol to convey messages, which improves the spectrum efficiency and reduces the cost of RF chain [22]. SM technology belongs to a special MIMO technology which only needs a RF chain to activate one antenna among multiple antennas to send information, which can reduce hardware cost and avoid inter-antenna interference and synchronization problems. Accordingly, in SM system, we consider the finite input which is more realistic. However, SM utilizes a very limited number of RF chains when compared to the transmit antennas (TAs) present in the spatial-constellation. Due to this, the estimation of the channel gains of all TAs simultaneously is not possible. Moreover, the number of TAs must be a power of 2, whereas in generalized SM (GSM), an arbitrary number of antennas can be utilized. As for the application scenario, the basic idea of SM is using both the transmit antenna index and modulated symbol to convey messages, which indicates its advantage in higher data rate scenario. Moreover, as SM can reduce the complexity of the design of transmitter and receiver, SM performs well in massive MIMO scenario. On the other hand, the broadcast nature of the wireless communication incurs that the desired receiver is vulnerable to hostile users, thus establishing a set of systematically secure transmission strategies becomes an imperative demand. In this section, we review the crucial transmission strategies of the PHY security under the typical SM system and hybrid SM system, respectively.

4.1 Typical SM system

A typical SM system has been shown in Figure 8. In this figure, four important tools including transmit antenna selection (TAS), AN projection, power allocation (PA), and receive beamformer at the desired receiver are fully employed to achieve a high-performance secure SM (SSM).

In Figure 8, the transmitter (Alice) is equipped with N_a TAs. Without loss of generality, N_a is not a power of two, thus N_t out of N_a TAs should be selected for mapping binary bits to the antenna index. Accordingly, the signals observed at Bob and Eve can be, respectively, formulated as follows:

$$\mathbf{y}_b = \beta_1\sqrt{P_s}\mathbf{H}_b\mathbf{T}_k\mathbf{e}_n s_m + \beta_2\sqrt{P_s}\mathbf{H}_b\mathbf{T}_k\mathbf{P}_{\mathrm{AN}}\mathbf{n} + \mathbf{n}_b, \tag{5}$$

$$\mathbf{y}_e = \beta_1\sqrt{P_s}\mathbf{H}_e\mathbf{T}_k\mathbf{e}_n s_m + \beta_2\sqrt{P_s}\mathbf{H}_e\mathbf{T}_k\mathbf{P}_{\mathrm{AN}}\mathbf{n} + \mathbf{n}_e, \tag{6}$$

where $\mathbf{H}_b$ and $\mathbf{H}_e$ are the channel gain matrices of the desired and eavesdropping channels, respectively. $\mathbf{T}_k$ is the TAS matrix. $\mathbf{n}_b$ and $\mathbf{n}_e$ denote the complex additive white Gaussian noise vectors.

The security of the SM system is characterized by evaluating average secrecy rate (SR) which is formulated as

$$\bar{R}_s = \mathbb{E}_{\mathbf{H}_b,\mathbf{H}_e}\left[I\left(\mathbf{e}_n, s_m; \mathbf{y}_b\right) - I\left(\mathbf{e}_n, s_m; \mathbf{y}_e\right)\right]^+, \tag{7}$$

where $I\left(\mathbf{e}_n, s_m; \mathbf{y}_g\right)$ stands for the mutual information of Bob and Eve, which is expressed as

$$I\left(\mathbf{e}_n, s_m; \mathbf{y}_g\right) = \log_2 N_t M - \frac{1}{N_t M} \times \sum_{i=1}^{N_t M} \mathbb{E}_{\mathbf{n}_g} \left\{ \log_2 \sum_{j=1}^{N_t M} \exp\left(-\left\| \beta_1 \sqrt{P_s} \mathbf{H}_g \mathbf{T}_k \left(\mathbf{e}_n s_m - \mathbf{e}_i s_j \right) + \mathbf{n}_g \right\|^2 + \left\| \mathbf{n}_g \right\|^2 \right) \right\}, \quad (8)$$

where g stands for b or e. Appropriately selecting out an active antenna group is capable of improving the security performance of SM systems. The authors in [65] proposed two TAS methods: capacity-optimized antenna selection (COAS) and Euclidean distance-optimized antenna selection (EDAS) which focused on improving bit-error rate performance. In [66], the authors generalized EDAS method to the secure SM system and proposed the maximizing signal-to-leakage-plus-noise ratio (Max-SLNR) TAS strategy, where the Max-SLNR scheme achieved a higher secrecy rate (SR) performance with a lower complexity. However, Max-SLNR method does not directly maximize the secrecy rate of the SSM system. To overcome the above disadvantage, the authors in [67] proposed two low-complexity TAS methods for maximizing SR by analyzing the asymptotic performance of SR when SNR approaches 0 and ∞. Furthermore, a compromise solution that suits for the whole SNR region was further devised, which has the capability of achieving a close SR performance when compared with the exhaustive search (ES) method. When a rough CSI of Eve's channel is obtained, the authors in [68] proposed a simulated-annealing-mechanism-based TAS scheme which obtained excellent SR profit.

By reasonably generating Gaussian AN at the transmitter, the detection of Eve can be deteriorated, so as to further improve the security performance of the system [69]. Wang *et al.* [70] projected AN onto the null-space of the desired channel to interfere with an unknown Eve. Although NSP scheme ensures the high security performance in high SNR region, the beamformer design for AN has not been further explored to improve the security performance of SSM. The authors in [68] proposed a novel ratio optimization algorithm which reduced computational overhead and achieved near-optimal safety performance.

As the total power is constrained, elaborately splitting the power allocated to the CM and allocated to the AN has a great impact on improving the SR performance. In [71] and [72], the approximation of SR based on cut-off rate was invoked to substitute the non-closed SR expression for secure SM systems. Using the approximation as the objection function, the authors in [71] proposed a gradient-based PA method which approached the optimal PA method based on ES. In [72], a novel criterion that maximizes the ratio of Bob's SLNR and of Eve's AN-to-leakage plus noise ratio (ANLNR) was conceived which was close to the optimal PA factor and also reduced some computational complexity. To further reduce the computational complexity and approach the optimal SR performance, the authors in [73] proposed a deep-neural-network (DNN)-based PA strategy whose key idea was to treat the input and output of ES algorithm as an unknown nonlinear mapping and used a DNN to approximate it.

Consider a SSM system with a full-duplex (FD) malicious attacker (Mallory), where Mallory works on FD mode, eavesdropping from Alice and transmitting jamming to Bob simultaneously. A game-theoretic approach was adopted in [74] to deal with a combination of passive eavesdropping and active attacks. The authors in [75] proposed three effective receiver beamformers with low complexity to eliminate jamming and improve SR.

4.2 Hybrid SM system

When the number of TAs tends to be large, the circuit cost and complexity will become a burden on the fully digital SSM. To address this problem, hybrid SM was proposed and fully investigated where the total antenna array was divided into multiple transmit antenna subarrays with each subarray being connected to a single RF chain. As for hybrid SSM, two effective tools including the precoder and transmit antenna subarray selection are used to achieve a high security SSM.

In [76], the authors proposed a semi-definite relaxation based alternating minimization (SDR-AltMin) algorithm to jointly design the digital and analog precoders. In [77], the authors generalized SDR-AltMin algorithm to the hybrid SSM system, and proposed two precoders which maximized approximate SR (ASR) based on the gradient method and alternating direction method of multipliers, respectively.

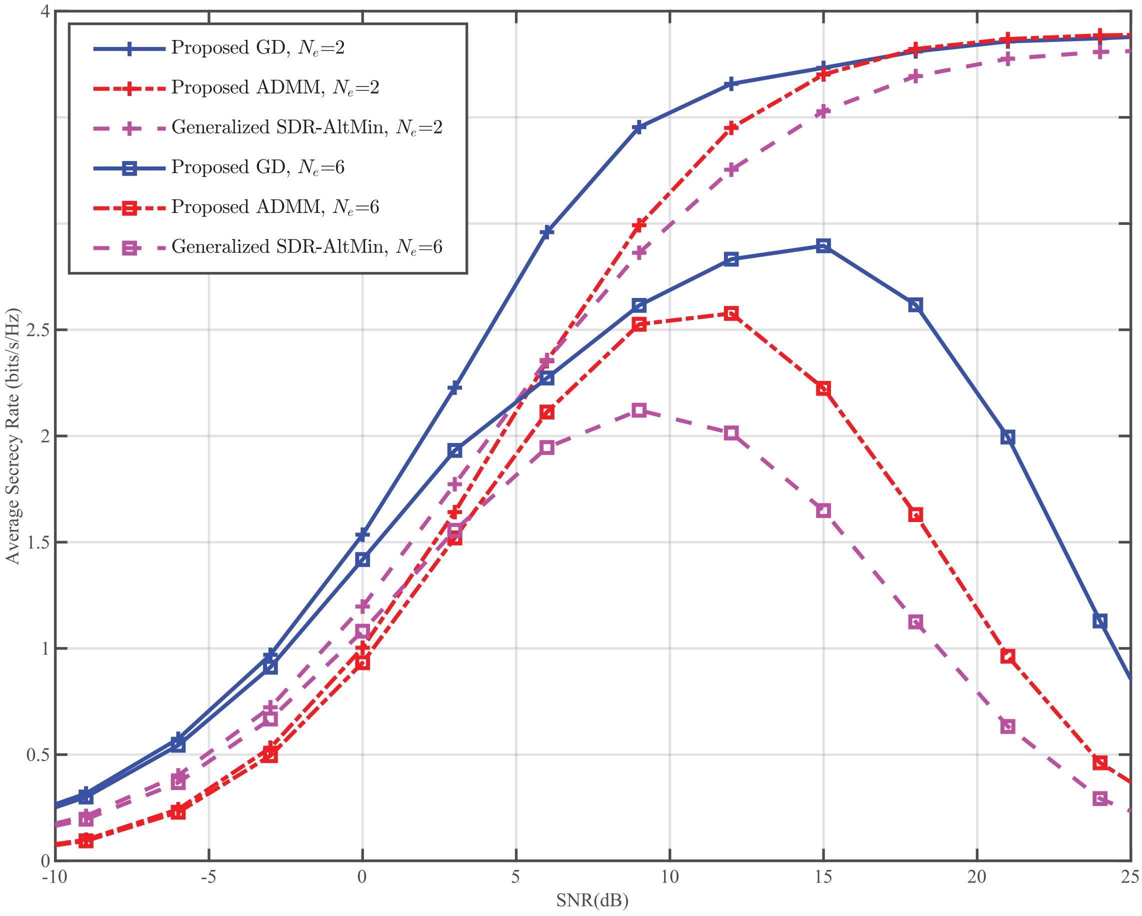

Figure 9. Comparison of SR performance of various precoders in [77]

Figure 9 shows that the two proposed methods in [77] harvested a higher SR performance than the generalized SDR-AltMin method. For hybrid generalized SSM systems, the authors in [78] proposed a novel algorithm to separately optimize the analog precoder and the digital precoder to maximize SR. As the objective function is non-concave, the authors conceived a pair of concave objective functions to optimize the analog precoder and digital precoder.

As the number of RF chains is not a power of two, there exists the transmit antenna subarray selection problem. The authors in [77] proposed two low-complexity transmit antenna subarray selection (TASS) methods, named maximizing eigenvalue (Max-EV) and maximizing product of signal-to-interference-plus-noise ratio and artificial noise-to-signal-plus-noise ratio (Max-P-SINR-ANSNR), which performed better than the generalized Max-SLNR method. The above studies mainly analyzed the system secrecy performance under the Rayleigh fading channel, and the application of the hybrid precoding algorithm to AN-aided mmWave GSM system was studied in [79], where the AN-aided mmWave GSM system adopting Gram-Schmidt precoding was proposed, which can obtain a more satisfactory system secrecy capacity compared with the SDR-AltMin in [76].

4.3 Future challenges

(1) The existing research on SM was based on the Rayleigh fading model. How to extend the SM system to other types of fading channels is very important for the practical application and deployment of SM. In addition, how to construct the security optimization problem in the relevant channel environment is worth pondering.

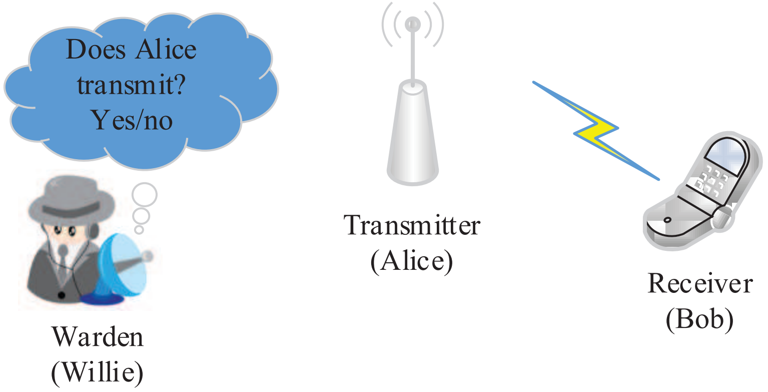

Figure 10. System model for covert communication

(2) Since there is no closed expression of SR, it is a primary task to find a closed form to replace the original expression of SR. Although there are some approximate expressions, the specific performance differences are not clear. This is because communication configuration, modulation mode, and channel model all have a potential impact on the secrecy rate. Therefore, performance analysis based on SM system needs to be further followed up to meet the next communication deployment requirements.

(3) As another important indicator of communication security, the research of secure interrupt probability in the field of finite input is scarce. Therefore, the analysis of SM system security interrupt probability is an important performance standard for the next step.

5 Covert communication

While most information-theoretic security studies to date have revolved around the issues of protecting the content of information, the growing concern around mass communication surveillance programs has reignited interest in investigating the covertness of communications, also known as low probability of detection (LPD) [80], in which covertness requires that the communication remains undetectable from a watchful adversary, named warden. The concept of covert communication has shown tremendous research value and application value [81, 82]. The warden in covert communication and eavesdropper in traditional PHY security represent two types of threats in wireless communication, respectively. Specially, the covert communication considers the external attackers, *e.g.*, warden, which act as the surveillant for detecting the signal transmission and discovering the presence of the user. On the other hand, the eavesdropper may be internal attackers, *e.g.*, eavesdropper, which aim to decode the confidential information. Therefore, there are some scenarios where both types of attacks do exist concurrently, *e.g.*, some military and governmental applications. Therefore, the secure transmission schemes reviewed in this work aim at protecting the confidential information from being decoded at the internal attackers (eavesdropper) and detected at the external attackers (warden).

Specifically, the covert communication scenario is shown in Figure 10, where a transmitter (Alice) tries to send messages to a receiver (Bob) covertly under the supervision of a warden (Willie), who is detecting whether Alice is communicating with Bob or not. It means that Willie faces a binary hypothesis testing problem. The null hypothesis $\mathcal{H}_0$ states that Alice did not transmit while the alternative hypothesis $\mathcal{H}_1$ states that Alice did transmit, sending covert information to Bob. $\mathcal{D}_0$ and $\mathcal{D}_1$ represent the binary decisions that Alice transmits or not, respectively. We define the probability of false alarm $\mathbb{P}_{\text{FA}} \triangleq \mathbb{P}(\mathcal{D}_1|\mathcal{H}_0)$ (or Type I error) as the probability that Willie makes a decision in favor of the alternative hypothesis, while the null hypothesis is true. Similarly, the probability of miss detection $\mathbb{P}_{\text{MD}} \triangleq \mathbb{P}(\mathcal{D}_0|\mathcal{H}_1)$ (or Type II error) is defined as the probability of Willie making a decision in favor of the null hypothesis, while the alternative hypothesis is true. The detection error probability at Willie is the sum of Type I error and Type II error. Therefore, the optimal test is to minimize the detection error probability $\xi = \mathbb{P}_{\text{FA}} + \mathbb{P}_{\text{MD}}$. We have a lower bound on ξ according to the Pinsker's inequality [83], which provides us with a theoretical basis for the following analysis and is given by

$$\xi \geq 1 - \sqrt{\frac{1}{2}\mathcal{D}(\mathbb{P}_0||\mathbb{P}_1)}, \tag{9}$$

where $\mathcal{D}(\mathbb{P}_0||\mathbb{P}_1)$ is the Kullback–Leibler (KL) divergence from $\mathbb{P}_0$ to $\mathbb{P}_1$, $\mathbb{P}_0$ and $\mathbb{P}_1$ are the likelihood functions under $\mathcal{H}_0$ and $\mathcal{H}_1$, respectively. In the following, we present a review of literature considering the covertness constraint in terms of detection error probability or Kullback–Leibler (KL) divergence for achieving covert communication, where KL divergence is a statistical distance of how one probability distribution of null hypothesis is different from another probability distribution of the alternative hypothesis. The transmitter (Alice) possesses sensitive information that needs to be sent to the legitimate receiver (Bob), while the warden (Willie) listens to the communication environment and tries to detect any covert transmission from Alice to Bob with some probable existed uncertainties. These uncertainties can be formed from Willie's receiver noise power, imperfect channel knowledge, finite blocklength, and interference from other network users or artificial noise.

In the following, we present a review of literature considering the covertness constraint in terms of detection error probability or Kullback–Leibler (KL) divergence for achieving covert communication, where KL divergence is a statistical distance of how one probability distribution of null hypothesis is different from another probability distribution of the alternative hypothesis.

5.1 Covert communication with relay

The ultimate goal of covert communication is to achieve shadow wireless networks. Preliminary results toward this goal have been achieved in the context of relay networks. Covert communication with the aid of relay was analyzed in [9, 84–86]. The scenario investigated in [9] is that there is a source node which attempts to transmit information to a destination node via a relay node. The relay node receives a message from a source node and then attempts to retransmit the source's original message in addition to its own covert message to the destination without the source node detecting the covert transmission. This work presents two schemes (rate-control and power-control) for evaluating the probability that the covert criteria are satisfied.

In [84], the authors studied covert communications with a self-sustained relay over Rayleigh fading channels, where the relay harvests extra energy from the source to transmit covert message to destination by employing a more powerful energy harvester with a higher conversion efficiency factor, while the source is to detect the covert communication. The work aims to find the maximum throughput, given a certain level of covertness for two energy harvesting schemes, time switching and power splitting. Covert communication with a positive rate was shown to be possible in the transmission from a relay node to a destination when the source is uncertain regarding the forwarding strategy of the relay node.

Two relay selection schemes (*i.e.*, random selection and superior-link selection) in multiple relays-assisted Internet of things (IoT) systems were proposed in [85], where the source needed to transmit two types of messages with/without covert requirement. The numerical results showed that the superior-link selection scheme has significant improvement in terms of covert capacity when compared to the random selection under the same transmission power at the source. The routing of information in covert wireless networks with multiple relay nodes and multiple wardens under additive white Gaussian noise (AWGN)channels has been considered in [86], where the algorithms were developed to find the path with the maximum throughput and the path with minimum end-to-end delay when considering a single key and the case of independent keys at the intermediate nodes.

5.2 Covert communication with full-duplex

In the covert communication, there is always a trade-off between the throughput and covertness. Using a full-duplex receiver offers a two-fold benefit for the covert communication relative to generating AN by a separate and independent jammer. Firstly, it enables a higher degree of control over the transmitted AN signals (*e.g.*, its power), thus causing further deliberate confusion at the warden. Secondly, the cutting-edge self-interference cancellation techniques can be adopted to provide higher data rates for covert communications with the full-duplex receiver. In [87], the transmitter Alice aims to send message at a fixed rate to a legitimate receiver Bob over a fading wireless channel, while the whole communication is under the surveillance of the warden Willie. Operating at the full-duplex mode, Bob can receive information from Alice and also simultaneously inject interference to confuse Willie over the same channel, which can increase the detection error probability at Willie. On the other hand, it can also decrease covert throughput due to the effect of self-interference at Bob. Based on these discussions, the trade-off between the achievable rate, the transmission power, and covertness criterion that is the probability of error minimized over all prior distributions of the fading channel was investigated.

The aforementioned studies in the literature mainly focus on how to hide the wireless transmission action rather than the transmitter itself, since there is some prior information that can indicate the existence of the transmitter. To achieve a higher level covert communication, the transmitter itself also should be hidden from the warden. Taking advantage of the full-duplex and channel inversion power control (CIPC), the work aims to hide the transmitter by removing the requirement on channel state information (CSI) [88]. For the CIPC schemes adopted in this work, the transmitter varies its transmitted signal power as per the channel from itself to the receiver so that the received power of the covert information signal is a fixed value. Therefore, neither Bob nor Willie knows the corresponding CSI perfectly, since Alice does not transmit any pilot signal at all. Meanwhile, the full-duplex receiver can further confuse the detection of Willie.

Ultra-reliable and low-latency communications (URLLC) is envisioned to support mission critical applications with stringent requirements of latency and reliability, where the codeword is required to be short, *e.g.*, the order of 100 channel uses. Specifically, with the aid of the full-duplex receiver, the authors in [89] showed that transmitting AN with a fixed power is still helpful in covert communication with finite blocklength, since in a limited time period the warden cannot exactly learn its received power. The blocklength has a significant impact on the detection performance at Willie and the maximal achievable rate of the channel from Alice to Bob (*i.e.*, the maximal achievable rate decreases as blocklength decreases for a fixed decoding error probability).

5.3 Covert communication with UAV

For the static covert communication network, the positions of the three participants (Alice, Bob, and Willie) are fixed. The UAV-assisted communication networks enable the participants to realize more flexible deployments in covert communication [90]. UAV can establish LoS wireless links for air-ground communications, which provides significant performance improvement over the conventional non-line-of-sight (NLoS) terrestrial communications. In some scenarios, the covert rate can be effectively improved by exploiting the mobility of UAV while the detection by Willie will become easier due to the component of LoS channel.

In [91], a UAV acted as a mobile relay to enhance covert transmission by dynamically adjusting its trajectory and transmit power. Specifically, the authors formulated an optimization problem that maximizes the average covert transmission rate subject to the transmission outage probability constraint at Bob, covertness constraint at Willie as well as the UAV's mobility constraint and transmit power constraint. Such a joint optimization problem is generally difficult to tackle directly due to the non-convex constraints. To solve this optimization problem, the authors first transformed the intractable transmission outage probability constraint into a deterministic form using the conservative approximation and then applied the first-order restrictive approximation to transform the optimization problem into a convex form, which is mathematically tractable. A multi-hop relaying strategy (*e.g.*, the number of hops, transmit power) was optimized to maximize the throughput against the surveillance of a UAV warden in [92]. The beam sweeping-based detection of a UAV's transmission by a terrestrial warden with multiple antennas was investigated in [93], where Pinsker's inequality and Kullback–Leibler divergence were adopted to derive the detection error probability.

In the aforementioned studies, the UAV's trajectory designs with the optimization for some parameters may suffer from several limitations. For example, the objective function or constraints in the optimization problems are non-convex and difficult to be tackled. Against this background, the deep reinforcement learning (DRL) has been serving as an efficient solution to handle the decision-making issue due to its essential traits, *i.e.*, learning dynamically from the real world. Motivated by the superiorities of DRL, we

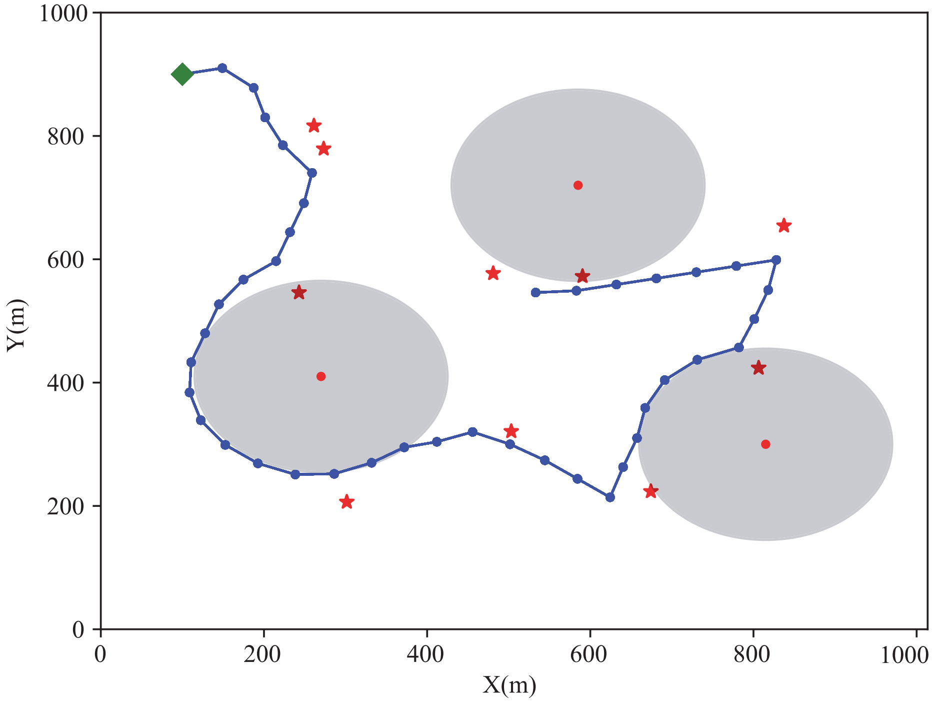

Figure 11. The UAV's optimized trajectory

intend to address the non-convex problem for considering covert data dissemination with UAV, where UAV intends to transmit the covert data to some legitimate receivers (Bobs) under the surveillance by some wardens (Willies). Specially, a twin-delayed deep deterministic policy gradient-based covert data dissemination (TD3-CDD) algorithm is proposed to minimize the time of covert data dissemination by jointly optimizing the UAV's trajectory and Bobs' schedule. In detail, we first determined the covertness constraint explicitly by analyzing the detection performance at each Willie. Then, we formulated an optimization problem to minimize the total time for data dissemination subject to the covertness constraint and other practical constraints, *e.g.*, the UAV's mobility constraints. By applying the deep reinforcement learning approach, an efficient algorithm named TD3-CDD is developed to solve the optimization problem.

In Figure 11, we plot the optimized UAV's trajectory achieved by our proposed TD3-CDD scheme. where the locations of Bobs are indicated by "⋆", the green diamond indicates the initial position of the UAV, the central locations of Willies are indicated by "●" and the shaded area indicates the surveillance area of each Willie. In this figure, the UAV is able to sequentially visit all Bobs while avoiding each Willie's surveillance. Figure 12 shows the average time for each Bob to complete the data reception achieved by our TD3-CDD scheme and the benchmark scheme (*e.g.*, UAV's flight trajectory of keeping away from Willies without optimization). In this figure, as expected, we observe that the TD3-CDD scheme takes less time than the benchmark scheme to complete the data transmission to all Bobs.

5.4 Future challenges

The scenarios considered in this work have focused on a single-hop communication between Alice and Bob. However, due to low transmit power of Alice, the communication range in covert scenarios is essentially reduced, and in many applications where the end-to-end distance is large, multi-hop communications become essential, effectively increasing the communication distance. The tradeoff between the communication distance of hops and number of hops in achieving a long-distance covert communication has not been analyzed before, although an initial study on multi-hop covert communications was presented in [86]. It is not yet clear whether more small distance hops or a few large distance hops are better to achieve

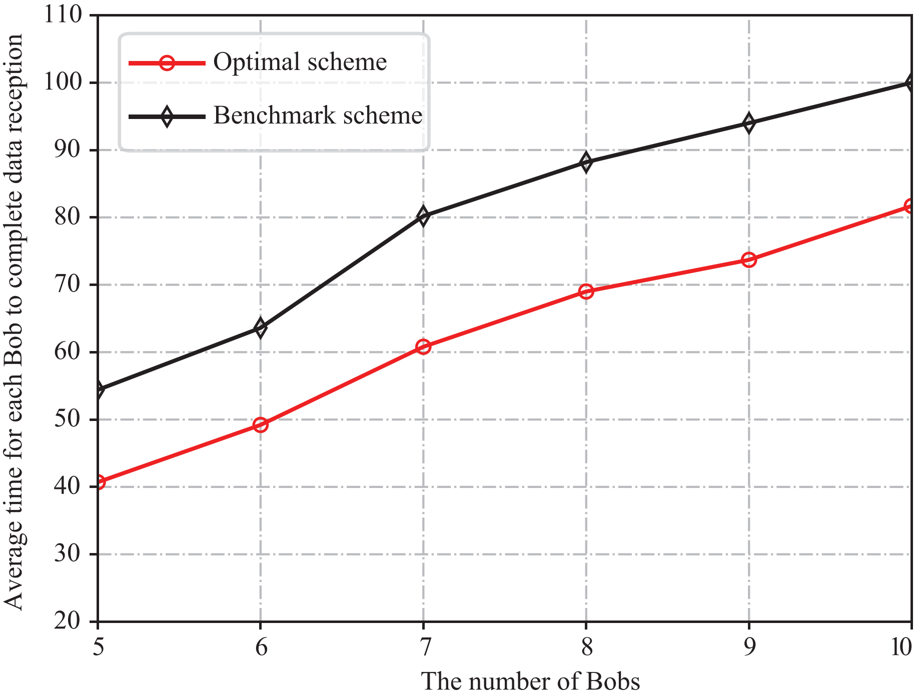

Figure 12. Average time for each Bob to complete data reception achieved by our TD3-CDD scheme and the benchmark scheme

a higher covertness. An interesting research direction is to design an adaptive strategy of mode selection between amplify-and-forward (AF) and decode-and-forward (DF) modes for each nodes in multi-hop covert communication.

6 IRS-aided PHY security

Due to the significant increase in the number of wireless communication devices, various novel technologies have been proposed in the literature to improve the spectrum and energy efficiencies, as well as the security and reliability of wireless communication systems. Future wireless networks are expected to support high (energy and spectrum) efficiency, security, reliability, and flexible design for emerging applications of 6G and beyond. Relentless efforts have been made in research and development of wireless communications to achieve this goal. However, overall progress has been relatively sluggish due to the fact that traditional wireless communication designers have focused only on the transmitter and receiver sides, while treating the wireless communication environment as an uncontrollable factor. Recently, IRS has been considered as a promising new technology for the next-generation wireless communications, which can reconfigure the wireless propagation environment via controlling reflection with software [23]. Specifically, an IRS composes a large number of low-cost passive reflecting elements, each of which can induce a phase change to the incident signal independently. By smartly adjusting the phase shift of the reflecting elements, the IRS-reflected signals and signals from other paths can be combined constructively to enhance the desired signal power or destructively to suppress undesired signals such as co-channel interference, which thus significantly improves the communication performance. IRS is particularly suitable for indoor applications with high density of users (such as stadium, shopping mall, exhibition center, airport.). For PHY security, when the distance from Eve to Alice is smaller than the distance from the legitimate user to Alice, or when Eve is in the same direction as the legitimate user, IRS can be deployed near Eve, and the signal reflected by IRS can be tuned to cancel out the (non-IRS-reflected) signal from Alice at Eve, thus effectively reducing the information leakage.

The main advantage of having IRS in a communication system is the capability to execute passive beamforming, which can be done at the midpoint of the channel, unlike the traditional active beamforming

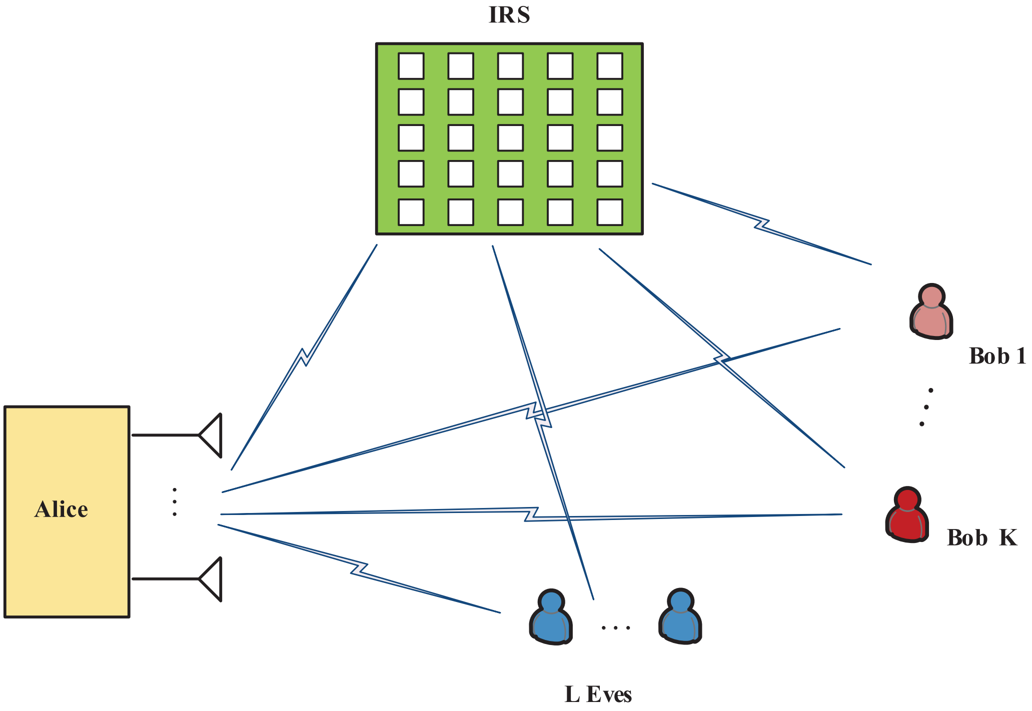

Figure 13. An IRS-aided secure multi-user communication system

at Alice. This additional degree of freedom has been shown to improve system performance in several metrics, including PHY security, which is entirely dependent on the ability of the system to precisely direct the signal beam to the expected path (or eliminate it). In addition, the coverage area can be further increased with the assistance of IRS. However, the employment of IRS increases the complexity of the system. For example, in PHY security applications, traditional active beamforming is optimized in order to maintain the confidentiality of the system. In contrast, the presence of IRS in the system requires joint optimization of active and passive beamforming, and the performance of the system depends greatly on the quality of the acquired CSI. Moreover, under the far-field propagation assumption, the communication channel of the IRS link suffers from a dual path loss, the so-called product-distance path loss model, which needs to be compensated in the link budget or by increasing the number of reflective elements. A typical IRS-aided MISO multi-user secure system is shown in Figure 13. The introduction of IRS in the system can increase the achievable rate of legitimate users (*i.e.*, Bobs) while suppressing the achievable rate of illegal users (*i.e.*, Eves), ultimately improving the security performance of the system. Hence, IRS can be used for strengthening the system security under the wiretap channel, especially when the channel of the eavesdropping communication link is stronger than that of the legitimate link. In particular, by denoting the reflecting coefficient matrix of the IRS as $\mathbf{\Theta} = \mathrm{diag}[\mathbf{e}^{j\theta_1}, \ldots, \mathbf{e}^{j\theta_N}]$, and the transmit beamforming at the BS as $\mathbf{x} = \sum_{k=1}^{K} \mathbf{w}_k s_k$, the achievable SR of user k is

$$R_{s,k} = \log_2\left(1 + \frac{\left(\mathbf{h}_{ib,k}^H \mathbf{\Theta}\mathbf{G} + \mathbf{h}_{ab,j}^H\right)\mathbf{w}_k}{\sum_{j\neq k}\left(\mathbf{h}_{ib,k}^H \mathbf{\Theta}\mathbf{G} + \mathbf{h}_{ab,j}^H\right)\mathbf{w}_j + \sigma_k^2}\right) - \log_2\left(1 + \frac{\left(\mathbf{h}_{ie,l}^H \mathbf{\Theta}\mathbf{G} + \mathbf{h}_{ae,l}^H\right)\mathbf{w}_k}{\sum_{j\neq k}\left(\mathbf{h}_{ie,l}^H \mathbf{\Theta}\mathbf{G} + \mathbf{h}_{ae,l}^H\right)\mathbf{w}_j + \sigma_e^2}\right), \tag{10}$$

where $\mathbf{G}$, $\mathbf{h}_{ib,k}$, $\mathbf{h}_{ab,k}$, $\mathbf{h}_{ie,l}$, and $\mathbf{h}_{ae,l}$ are the channels from Alice to the IRS, from the IRS to user k, from Alice to user k, from the IRS to Eve l, and from Alice to Eve l, respectively. Notice that unlike the traditional model that contains only direct paths, the IRS is introduced with the addition of reflected paths, *i.e.*, terms that contain $\mathbf{\Theta}$. In the optimization process, we optimize not only the active beamforming $\mathbf{w}_k$ at Alice but also the phase shift matrix $\mathbf{\Theta}$ of the IRS, *i.e.*, passive beamforming.

6.1 IRS-aided MISO/SISO secure systems

Many recent studies have utilized IRS to secure the PHY of wireless communications. The authors in [94–96] investigated an IRS-aided secure wireless system where a multi-antenna transmitter communicates with a single-antenna receiver in the presence of an Eve. In [94–96], the SR was maximized by jointly optimizing the transmit beamforming and the IRS phase shifts. Specifically, the authors in [94] proposed an alternating optimization (AO) algorithm to design two variables alternately, in which the optimal solution to the transmit beamforming was computed directly and the IRS phase shifts were optimized by using semidefinite relaxation (SDR) method. In [95], the transmit beamforming and the IRS phase shifts were also optimized in an alternating manner. In each iteration, the solution to the transmit beamforming was achieved in closed form, while a semi-closed form solution to the IRS phase shifts was obtained by adopting the Majorization-Minimization (MM) algorithm. The element-wise block coordinate descent (BCD) and AO-MM algorithms were developed for solving the problem efficiently in [96]. Furthermore, the authors in [97] investigated a minimum-SR maximization problem in a secure IRS-aided multiuser multiple-input single-output (MISO) broadcast system with multiple Eves. The problem was successfully solved by applying the path-following algorithm and AO technique in an iterative manner. Moreover, two suboptimal algorithms with closed-form solutions were developed to further reduce the computational complexity.

To further enhance the security, the AN is designed to disturb Eve. In [98], AN was firstly considered in an IRS-aided secure communication system. Specifically, the achievable SR of the system was maximized by jointly optimizing the transmit beamforming with AN and IRS phase shifts. An efficient algorithm based on AO was developed to solve the problem sub-optimally. The authors in [99] considered the resource allocation design in an IRS-aided multiuser MISO communication system. Aiming to maximize the system sum SR, the beamforming vectors, AN covariance matrix at the BS and phase shift matrix at the IRS were jointly optimized by applying AO, SDR and manifold optimization. The authors in [100] investigated a secure IRS-aided multigroup multicast MISO communication system to minimize the transmit power subject to the SR constraints. First, an SDR-based AO algorithm was proposed and a high-quality solution was obtained. Then, to reduce the high computation complexity, a low-complexity AO algorithm based on second-order cone programming (SOCP) was presented. Simulation result indicates that these designs can guarantee reliable secure communication with the aid of IRS as shown in Figure 14. Moreover, secure IRS-aided simultaneous wireless information and power transfer (SWIPT) system were studied in [101]. To maximize the harvested power of energy harvesting receiver (EHR), the secure transmit beamforming at Alice and phase shifts at the IRS were optimized subject to the SR and the reflecting phase shifts at the IRS constraints. The SDR and the low-complexity AO algorithms were proposed, and the harvested power with the help of IRS approximately double that of the existing method without IRS. All of the above literature showed that the inclusion of IRS in the protection of private content achieves a significant increase in the secrecy rate of the system. To investigate the effect of IRS in covert communication systems, [102] studied IRS-assisted covert wireless communications, and proved that the perfect covertness can be achieved if the channel quality of the reflected path is higher than that of the direct path. This also demonstrated that IRSs are also effective in protecting transmission behavior. A brief summary of the above work is given in Table 1, where MISOSE refers to multiple-input single-output single-antenna Eve, and MISOME refers to multiple-input single-output multiple-antenna Eve.

6.2 IRS-aided MIMO secure systems

Recently, the introduction of IRS in MIMO system to enhance the security has also made effective progress. Dong and Wang [103] and Jiang *et al.* [104] studied an IRS-aided secure MIMO communication system, where a base station (BS) equipped with multiple antennas communicates with a multi-antenna receiver in the presence of a multi-antenna Eve. Particularly, the joint design of the transmit covariance at the BS and the phase shift coefficients at the IRS was considered to maximize the SR. In [103], the barrier, Newton and backtracking line search methods were used to search for global optimal transmit covariance, while the MM algorithm was applied to obtain the local optimal phase shift coefficients. In [104], the successive convex approximation (SCA)-based algorithm was used to solve the optimization

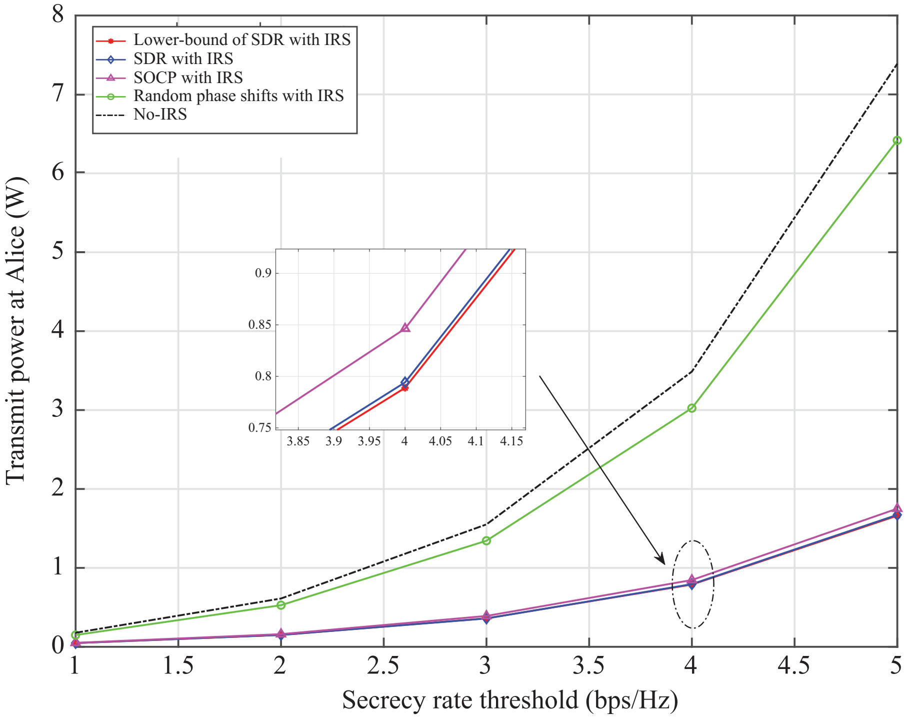

Figure 14. Transmit power at Alice *versus* SR [100]

Table 1. IRS-aided MISO/SISO secure systems

Paper	System model	AN	Objective
[94]	MISOSE Single-user	No AN	Maximize the system secrecy rate
[95]	MISOME Single-user	No AN	Maximize the system secrecy rate
[96]	MISOSE Single-user	No AN	Maximize the system secrecy rate
[97]	MISOSE Multi-user	No AN	Maximize minimum secrecy rate
[98]	MISOSE Single-user	Add AN	Maximize the system secrecy rate
[99]	MISOSE Multi-user	Add AN	Maximize the system secrecy rate
[100]	MISOSE Multi-user	Add AN	Minimize the transmit power
[101]	MISOSE SWIPT	No AN	Maximize the harvested power of energy harvesting receiver
[102]	SISO covert communication	No AN	Maximize the received SNR at user

of the transmit covariance. For the design of the phase shift coefficients, the closed-form solution of each phase shift coefficient was individually provided in an alternating way while fixing other phase shift coefficients. Hong *et al.* [105] considered an AN-aided secure MIMO communication system assisted by an IRS. With the aim for maximizing the SR, the BCD algorithm was exploited to alternately optimize the variables. Specifically, the optimal transmit covariance and AN covariance matrix were derived in a semi-closed form by applying the Lagrangian multiplier method, and the optimal phase shifts were obtained in closed form by utilizing the MM algorithm. An IRS-aided secure DM-MIMO system was studied in [106]. Two confidential bit streams transmitted from Alice to Bob, different from the conventional DM where Alice only transmits single CBS to Bob. This paper demonstrates that the IRS significantly enhanced the SR of DM. Hehao and Ni [107] studied a secure IRS-aided MIMO-SWIPT, where the information receiver (IR) and energy receiver (ER) are all equipped with multiple antennas, and the ER is regarded as a potential Eve. To address the SR maximization problem, an inexact BCD-based algorithm was proposed, in which the unit modulus and harvested energy constraints were solved by applying the penalty MM and complex circle manifold methods.

6.3 Robust IRS-aided secure system

The above contributions are obtained under the assumption that perfect CSI is available at Alice. However, obtaining perfect CSI is ideal, so it is necessary to consider robust security performance of the system. The authors in [108–110] investigated the robust transmission design in an IRS-aided secrecy system, where the CSI of Eves' channels is not perfectly known. Particularly, a robust secure beamforming problem was formulated to maximize the worst case of SR in [108]. By replacing the wiretap channels with a weighted combination of discrete samples and then using SDR technique, an efficient AO algorithm was proposed to solve the optimization problem sub-optimally. In [109], the authors considered a scenario where two IRSs are deployed to improve the sum SR of multiple single-antenna legitimate receivers in the presence of multiple multi-antenna Eves. Considering the imperfection of the CSI of Eves' channels, a robust non-convex optimization problem was proposed. Then the design of the transmit covariance, AN covariance matrix, and IRS phase shifts was handled by adopting AO, SCA, and SDR methods. In [110], the authors first considered the statistical CSI error model and the imperfect cascaded channels of Alice-IRS-EVE in IRS-aided secure communications. Then an outage-constrained power minimization problem was formulated. To solve it, the Bernstein-type inequality was exploited to tackle the outage rate probability constraints, and then a sub-optimal algorithm based on AO, the penalty-based and SDR methods were utilized to optimize the variables alternately.

6.4 Future challenges

To ensure the confidentiality of wireless communication, simultaneous control of transmissions from Alice and reflections at the IRSs can be an effective solution. Some simulation results verified the overall SR enhancement of the IRS-assisted system compared with the conventional system. However, there are still some challenges, open problems and new research directions.

(1) CSI Acquisition: In practice, due to the lack of cooperation between Alice/IRS and Eve, the CSI may be imperfect. The acquisition of perfect CSI in PHY security is a challenging task. It is mainly manifested in the following aspects. First, it is especially difficult to obtain the CSI associated with Eve due to the hidden nature of Eves. However, the CSI of Eves is known in the scenario where Eves are also active users in the system but untrusted by Bobs. In this case, the CSI can be achieved by modern adaptive system design, where channels are estimated at Bob and Eve and sent back to Alice. Second, in IRS-assisted security systems, because of the limited signal processing capability at the IRS, the perfect CSI of IRS-links is difficult to obtain. Depending on whether the IRS is equipped with an RF link, there are two ways to obtain the CSI. When each element of the IRS is equipped with a low-power receiver RF chain for channel estimation, the channels related to AP-IRS/IRS-user links can be estimated at the IRS based on their training signals. To reduce the computational overhead, the elements of the IRS could be divided into subarrays based on the rows or columns. Each sub-array is equipped with one receiver RF chain for channel estimation. If there are no receiver RF chains at the elements of the IRS, channel estimation becomes very challenging because the elements have no dedicated signal processing capability. One practical method for IRS channel estimation is to employ an ON/OFF-based IRS reflection pattern (element-by-element of IRS is set ON or all elements of IRS are switched ON).

(2) Deployment and design of IRS: The physical design of IRSs including the number, distribution, and geometry of RISs and the impact of IRS deployment on PHY security may be an interesting direction of research but is not well explored in the literature. In addition, the impact of a different number of RIS elements and their distribution on PHY security needs to be further explored. The positioning accuracy of the IRS-assisted system depends to a large extent on the location of the IRS. Therefore, it is important to find the optimal physical design and the placement to enhance IRS-assisted PHY security. In scenarios where no eavesdropper is present, it has been demonstrated that the user's achievable rate can be maximized when the IRS is close to the transmitter or receiver. However, there is no clear conclusion on the location of the IRS when there is an eavesdropper in the system or when there is a monitor present.

7 Conclusion

The development of future wireless technologies such as secure key generation technique, DM/SM technology, covert communication, and IRS has brought new security challenges to future networks. Designing effective and secure transmission schemes for future wireless communications that exploit the propagation properties of radio channels in the PHY has recently attracted extensive research interest. This paper reviewed the currently popular PHY secure communication techniques from both theoretical and technical perspectives. We investigated the confidentiality issues of PHY security technologies from secure key generation, DM, SM, covert communication, and IRS. We also discussed potential challenges in PHY security and point out some possible future research directions.

Conflict of Interest

The authors declare that they have no conflict of interest.

Data Availability

No data are associated with this article.

Authors' Contributions

Weiping Shi mainly surveyed the IRS-aided PHY security and the future challenges about the IRS-aided systems. Xinyi Jiang mainly surveyed the typical SM systems and the hybrid SM systems. Jinsong Hu mainly surveyed the covert communication with relay, the covert communication with full-duplex, and the covert communication with UAV. Abdeldime M. S. Abdelgader mainly surveyed the key extraction techniques, PHY security limitations, and possible attacks. Yin Teng mainly surveyed the realization method of DM and robust beamforming and DOA measurement for DM Secure System. Yang Wang mainly surveyed the robust IRS-aided physical secure. Hangjia He mainly surveyed the future challenges about the PHY security DM systems. Rongen Dong improved the readability of the paper by grammatical modification and polishing. Feng Shu and Jiangzhou Wang designed the whole frame of the paper and the whole structure of the paper.

Acknowledgements

We thank the anonymous reviewers for their helpful comments.

Funding

This work was supported in part by the National Natural Science Foundation of China (Nos. 62071234, 62071289, 61972093, and 62001116), the Hainan Province Science and Technology Special Fund (ZDKJ2021022), the Scientific Research Fund Project of Hainan University under Grant KYQD(ZR)-21008, the National Key R&D Program of China under Grant 2018YFB180110, and the Natural Science Foundation of Fujian Province under Grant 2020J05106.

References

[1] Zhu H and Wang J. Chunk-based resource allocation in OFDMA systems – Part I: Chunk allocation. IEEE Trans Commun 2009; **57**: 2734–44.
[2] Zhu H and Wang J. Chunk-based resource allocation in OFDMA systems – Part II: Joint chunk, power and bit allocation. IEEE Trans Commun 2012; **60**: 499–509.
[3] Wang J, Zhu H and Gomes N. Distributed antenna systems for mobile communications in high speed trains. IEEE J Sel Areas Commun 2012; **30**: 675–83.
[4] Zhou Y, Wang J and Sawahashi M. Downlink transmission of broadband OFCDM systems – Part I: Hybrid detection. IEEE Trans Commun 2005, **53**: 718–29.
[5] Zhou Y, Liu H and Pan Z et al. Two-stage cooperative multicast transmission with optimized power consumption and guaranteed coverage. IEEE J Sel Areas Commun 2014; **32**: 274–84.
[6] Wu Y, Khisti A and Xiao C et al. A survey of PHY security techniques for 5G wireless networks and challenges ahead. IEEE J Sel Areas Commun 2018; **36**: 679–95.
[7] Abdeldime MA and Wu L. The physical layer of the IEEE 802.11p wave communication standard: The specifications and challenges. In: Proc. World Congr. Eng. Comput. Sci. (WCECS), **Vol. 2**, San Francisco, CA, USA, Oct. 2014, 22–4.
[8] Chen X, Ng DWK and Gerstacker WH et al. A survey on multiple-antenna techniques for PHY security. IEEE Commun Surv Tutor 2017; **19**: 1027–53.
[9] Hu J, Yan S and Zhou X et al. Covert communication achieved by a greedy relay in wireless networks. IEEE Trans Wirel Commun 2018; **17**: 4766–79.
[10] Chou TH, Draper SC and Sayeed AM et al. Secret key generation from sparse wireless channels: Ergodic capacity and secrecy outage. IEEE J Sel Areas Commun 2013; **31**: 1751–64.
[11] Csiszar I and Korner J. Broadcast channels with confidential messages. IEEE Trans Inf Theory 1978; **24**: 339–48.
[12] Leung-Yan-Cheong S and Hellman M. The Gaussian wire-tap channel. IEEE Trans Inf Theory 1978; **24**: 451–6.
[13] Wang D, Bai B and Zhao W et al. A survey of optimization approaches for wireless PHY security. IEEE Commun Surv Tutor 2019; **21**: 1878–911.

[14] Leung-Yan-Cheong S and Hellman M. The Gaussian wire-tap channel. IEEE Trans Inf Theory 1978; **24**: 451–6.

[15] Wang X, Tao M and Mo J et al. Power and subcarrier allocation for physical-layer security in OFDM-based broadband wireless networks. IEEE Trans Inf Forensics Secur 2011; **61**: 693–702.

[16] Ng DWK, Lo ES and Schober R. Energy-efficient resource allocation for secure OFDM systems. IEEE Trans Veh Technol 2012; **61**: 2572–85.

[17] Jeong C, Kim I-M. Optimal power allocation for secure multicarrier relay systems. IEEE Trans Signal Process 2011; **59**: 5428–42.

[18] Goel S and Negi R. Guaranteeing secrecy using artificial noise. IEEE Trans Wirel Commun 2008; **7**: 2180–89.

[19] Hamamreh JM, Furqan HM and Arslan H. Classifications and applications of physical layer security techniques for confidentiality: A comprehensive survey. IEEE Commun Surv Tutor 2018; **21**: 1773–828.

[20] Abdelgader AMS and Wu L. A secret key extraction technique applied in vehicular networks. In: Proc. IEEE 17th Int. Conf. Comput. Sci. Eng., 2014, 1396-1403.

[21] Daly MP and Bernhard JT. Beamsteering in pattern reconfigurable arrays using directional modulation. IEEE Trans Antennas Propag 2010; **58**: 2259–65.

[22] Mesleh RY, Haas H and Sinanovic S et al. Spatial modulation. IEEE Trans Veh Technol 2008; **57**: 2228–41.

[23] Wu Q and Zhang R. Towards smart and reconfigurable environment: Intelligent reflecting surface aided wireless network. IEEE Commun Mag 2020; **58**: 106–12.

[24] Yuliana M. A simple secret key generation by using a combination of pre-processing method with a multilevel quantization. Entropy 2019; **21**: 192.

[25] Kim Y-S, Kim J-H and Kim S-H. A secure information transmission scheme with a secret key based on polar coding. IEEE Commun Lett 2014; **18**: 937–40.

[26] Bhatia J and Shah B. Review on various security threats & solutions and network coding based security approach for VANET. Int J Adv Eng Technol 2013; **6**: 361.

[27] Abdelgader AMS, Feng S and Wu L. Exploiting the randomness inherent of the channel for secret key sharing in vehicular communications. Int J Intell Transp Syst Res 2018; **16**: 39–50.

[28] Premnath SN, Croft J and Patwari N et al. Efficient high-rate secret key extraction in wireless sensor networks using collaboration. ACM Trans Sens Netw (TOSN) 2014; **11**: 1–32.

[29] Mukherjee A, Fakoorian SA and Huang J et al. Principles of physical layer security in multiuser wireless networks: A survey. IEEE Commun Surv Tutor 2014; **16**: 1550–73.

[30] Gong C, Yue X and Zhang Z et al. Enhancing physical layer security with artificial noise in large-scale NOMA networks. IEEE Trans Veh Technol 2021; **70**: 2349–61.

[31] Wang Y, Yu FR and Tang H et al. A mean field game theoretic approach for security enhancements in mobile ad hoc networks. IEEE Trans Wirel Commun 2014; **13**: 1616–27.

[32] Bang AO and Ramteke PL. MANET: History, challenges and applications. Int J Appl Innov Eng Manag (IJAIEM) 2013; **2**: 249–51.

[33] Xu J, Liu W and Lang F et al. Distance measurement model based on RSSI in WSN. Wirel Sens Netw 2010; **28**: 606–11.

[34] Bennett CH, Bessette F and Brassard G et al. Experimental quantum cryptography. J Cryptol 1992; **5**: 3–28.

[35] Greenemeier L. Election Fix? Switzerland Tests Quantum Cryptography. Scientific American, Swiss, 2007.

[36] Jana S, Premnath SN and Clark M et al. On the effectiveness of secret key extraction from wireless signal strength in real environments. In: Proc. ACM MobiCom, Beijing, China, **Vol. 12**, 2009, 321–32.

[37] Maurer U and Wolf S. Secret-key agreement over unauthenticated public channels Part I. Definitions and a completeness result. IEEE Trans Inf Theory 2003; **49**: 822–31.

[38] Lai L, Liang Y and Poor H. Key agreement over wireless fading channels with an active attacker. In: Proc. 48th Allerton Conf. Communication, Control, Computing, Monticello, IL, Sept. 2010, 1391–96.

[39] Mukherjee A, Fakoorian SA and Huang J et al. Principles of physical layer security in multiuser wireless networks: A survey. IEEE Commun Surv Tutor 2014; **16**: 1550–73.

[40] Zhang J, Li G and Marshall A et al. A new frontier for IoT security emerging from three decades of key generation relying on wireless channels. IEEE Access 2020; **8**: 138406–46.

[41] Ali IAI, Weibin Z and Zeng Z et al. An Adaptive Lossly Quantization Technique for Key Extraction Applied in Vehicular Communication. Wireless Personal Communications 2022: 1–17.

[42] Mathur S, Trappe W and Mandayam N et al. Radio-telepathy: Extracting a secret key from an unauthenticated wireless channel. In: Proc. 14th Annu. Int. Conf. Mobile Comput. Netw., San Francisco, CA, USA, Sept. 2008, 128–39.

[43] Abdelgader AMS Wu L and Jakalan A et al. BER analysis of OFDM communication in VANET. J Netw 2016; **11**: 69–79.

[44] Rezki Z, Zorgui M and Alomair B et al. Secret key agreement: Fundamental limits and practical challenges. IEEE Wirel Commun 2017; 24: 72–9.

[45] Zhang J, Duong TQ and Marshall A et al. Key generation from wireless channels: A review. IEEE Access 2016; **4**: 614–26.

[46] Zhang J, Li G and Marshall A et al. A new frontier for IoT security emerging from three decades of key generation relying on wireless channels. IEEE Access 2020; **8**: 138406–46.

[47] Zeng K. Physical layer key generation in wireless networks: Challenges and opportunities. IEEE Commun Mag 2015; **53**: 33–9.

[48] Zhu X, Xu F and Novak E et al. Using wireless link dynamics to extract a secret key in vehicular scenarios. IEEE Trans Mob Comput 2016; **16**: 2065–78.

[49] Shu F, Abdelgader AMS and Wu L et al. On channel estimation in vehicular networks. IET Commun 2016; **11**: 142–9.

[50] Babakhani A, Rutledge DB and Hajimiri A. Transmitter architectures based on near-field direct antenna modulation. IEEE J Solid-State Circ 2008; **43**: 2674–92.

[51] Daly MP and Bernhard JT. Directional modulation technique for phased arrays. IEEE Trans Antennas Propag 2009; **57**: 2633–40.

[52] Daly MP, Daly EL and Bernhard JT. Demonstration of directional modulation using a phased array. IEEE Trans Antennas Propag 2010; **58**: 1545–50.

[53] Hong T, Song MZ and Liu Y. Dual-beam directional modulation technique for physical-layer secure communication. IEEE Antennas Wirel Propag Lett 2011; **10**: 1417–20.

[54] Huang G, Ding Y and Ouyang S. Multicarrier directional modulation symbol synthesis using time-modulated phased arrays. IEEE Antennas Wirel Propag Lett 2021; **20**: 567–71.

[55] Ding Y and Fusco VF. A vector approach for the analysis and synthesis of directional modulation transmitters. IEEE Trans. Antennas Propag 2014; **62**: 361–70.

[56] Ding Y and Fusco V. Orthogonal vector approach for synthesis of multi-beam directional modulation transmitters. IEEE Antennas Wirel Propag Lett 2015; **14**: 1330–3.

[57] Ding Y and Fusco VF. MIMO-inspired synthesis of directional modulation systems. IEEE Antennas Wirel Propag Lett 2016; **15**: 580–4.

[58] Hu J, Shu F and Li J. Robust synthesis method for secure directional modulation with imperfect direction angle. IEEE Commun Lett 2016; **20**: 1084–7.

[59] Shu F, Wu X and Li J et al. Robust synthesis scheme for secure multi-beam directional modulation in broadcasting systems. IEEE Access 2016; **4**: 6614–23.

[60] Shu F, Zhu W and Zhou X et al. Robust secure transmission of using main-lobe-integration-based leakage beamforming in directional modulation MU-MIMO systems. IEEE Syst J 2018; **12**: 3775–85.

[61] Shu F, Wu X and Hu J et al. Secure and precise wireless transmission for random-subcarrier-selection-based directional modulation transmit antenna array. IEEE J Sel Areas Commun 2018; **36**: 890–904.

[62] Hung H and Kaveh M. Focussing matrices for coherent signal-subspace processing. IEEE Trans Acoust Speech Signal Process 1988; **36**: 1272–81.

[63] di Claudio ED and Parisi R. WAVES: weighted average of signal subspaces for robust wideband direction finding. IEEE Trans Signal Process 2001; **49**: 2179–91.

[64] Ng W, Reilly JP and Kirubarajan T, et al. Wideband array signal processing using MCMC methods. IEEE Trans Signal Process 2005; **53**: 411–26.

[65] Rajashekar R, Hari K and Hanzo L. Antenna selection in spatial modulation systems. IEEE Commun Lett 2013; **17**: 521–4.

[66] Shu F, Wang Z and Chen R et al. Two high-performance schemes of transmit antenna selection for secure spatial modulation. IEEE Trans Veh Technol 2018; **67**: 8969–73.

[67] Xia G, Shu F and Zhang Y et al. Antenna selection method of maximizing secrecy rate for green secure spatial modulation. IEEE Trans Green Commun Net 2019; **3**: 288–301.

[68] Xia G, Lin Y and Liu T et al. Transmit antenna selection and beamformer design for secure spatial modulation with rough CSI of Eve. IEEE Trans Wirel Commun 2020; **19**: 4643–56.

[69] Goel S and Negi R. Guaranteeing secrecy using artificial noise. IEEE Trans Wirel Commun 2008; **7**: 2180–9.

[70] Wang L, Bashar S and Wei Y et al. Secrecy enhancement analysis against unknown eavesdropping in spatial modulation. IEEE Commun Lett 2015; **19**: 1351–4.

[71] Shu F, Liu X and Xia G et al. High-performance power allocation strategies for secure spatial modulation. IEEE Trans Veh Technol 2019; **68**: 5164–8.

[72] Xia G, Jia L and Qian Y et al. Power allocation strategies for secure spatial modulation. IEEE Syst J 2019; **13**: 3869–72.

[73] Shu F, Liu L and Yang L et al. Spatial modulation: An attractive secure solution to future wireless network, 2021. https://arxiv.org/abs/2103.04051.

[74] Choi J. Full-duplexing jamming attack for active eavesdropping. In: 2016 6th ICITCS, 2016, 1–5.

[75] Jiang X, Liu X and Chen R et al. Efficient receive beamformers for secure spatial modulation against a malicious full-duplex attacker with eavesdropping ability. IEEE Trans Veh Technol 2021; **70**: 1962–6.

[76] Yu X, Shen JC and Zhang J et al. Alternating minimization algorithms for hybrid precoding in millimeter wave MIMO systems. IEEE J Sel Topics Signal Process 2016; **10**: 485–500.

[77] Shu F, Jiang X and Liu X et al. Precoding and transmit antenna subarray selection for secure hybrid spatial modulation. IEEE Trans Wirel Commun 2021; **20**: 1903–17.

[78] Xia G, Lin Y and Zhou X et al. Hybrid precoding design for secure generalized spatial modulation with finite-alphabet inputs. IEEE Trans Commun 2021; **69**: 2570–84.

[79] Yang P and Qiu X. Hybrid precoding aided secure generalized spatial modulation in millimeter wave MIMO systems. IEEE Commun Lett 2021; **25**: 397–401.

[80] Weeks GD, Townsend JK and Freebersyer JA. A method and metric for quantitatively defining low probability of detection. In: Proc. IEEE Military Commun. Conf. (MILCOM), **Vol. 3**, Dublin, Ireland, Oct. 1998, 821–6.

[81] Bash BA, Goeckel D and Towsley D. Hiding information in noise: Fundamental limits of covert wireless communication. IEEE Commun Mag 2015; **53**: 26–31.

[82] Yan S, Zhou X and Hu J et al. Low probability of detection communication: Opportunities and challenges. IEEE Wirel Commun 2019; **26**: 19–25.

[83] Bash BA, Goeckel D and Towsley D. Limits of reliable communication with low probability of detection on AWGN channels. IEEE J Sel Areas Commun 2013; **31**: 1921–30.

[84] Hu J, Yan S and Shu F et al. Covert transmission with a self-sustained relay. IEEE Trans Wirel Commun 2019; **18**: 4089–102.

[85] Gao C, Yang B and Jiang X et al. Covert communication in relay-assisted IoT systems. IEEE Internet Things J 2021; **8**: 6313–23.

[86] Sheikholeslami A, Ghaderi M and Towsley D et al. Multi-hop routing in covert wireless networks. IEEE Trans Wirel Commun 2018; **17**: 3656–69.

[87] Shahzad K, Zhou X and Yan S et al. Achieving covert wireless communications using a full-duplex receiver. IEEE Trans Wirel Commun 2018; **17**: 8517–30.

[88] Hu J, Yan S and Zhou X et al. Covert wireless communications with channel inversion power control in Rayleigh fading. IEEE Trans Veh Technol 2019; **68**: 12135–49.

[89] Shu F, Xu T and Hu J et al. Delay-constrained covert communications with a full-duplex receiver. IEEE Wirel Commun Lett 2019; **8**: 813–6.

[90] Jiang X, Chen X and Tang J et al. Covert communication in UAV-assisted air-ground networks. IEEE Wirel Commun 2021; **28**: 190–7.

[91] Zhou X, Yan S and Hu J et al. Joint optimization of a UAV's trajectory and transmit power for covert communications. IEEE Trans Signal Process 2019; **67**: 4276–90.

[92] Wang H-M, Zhang Y and Zhang X et al. Secrecy and covert communications against UAV surveillance via multi-hop networks. IEEE Trans Commun 2020; **68**: 389–401.

[93] Hu J, Wu Y and Chen R et al. Optimal detection of UAV's transmission with beam sweeping in covert wireless networks. IEEE Trans Veh Technol 2020; **69**: 1080–5.

[94] Cui M, Zhang G and Zhang R. Secure wireless communication via intelligent reflecting surface. IEEE Wirel Commun Lett 2019; **8**: 1410–4.

[95] Shen H, Xu W and Gong S et al. Secrecy rate maximization for intelligent reflecting surface assisted multi-antenna communications. IEEE Commun Lett 2019; **23**: 1488–92.

[96] Yu X, Xu D and Schober R. Enabling secure wireless communications via intelligent reflecting surfaces. In: Proc. IEEE Global Commun. Conf. (GLOBECOM), Waikoloa, HI, USA, 2019, 1–6.

[97] Chen J, Liang Y-C and Pei Y et al. Intelligent reflecting surface: A programmable wireless environment for physical layer security. IEEE Access 2019; **7**: 82599–612.

[98] Guan X, Wu Q and Zhang R. Intelligent reflecting surface assisted secrecy communication: Is artificial noise helpful or not? IEEE Wirel Commun Lett 2020; **9**: 778–82.

[99] Xu D, Yu X and Sun Y et al. Resource allocation for secure IRS-assisted multiuser MISO systems. In: IEEE Globecom Workshops (GC Wkshps), 2019, 1–6.

[100] Shi W, Li J and Xia G et al. Secure multigroup multicast communication systems via intelligent reflecting surface. China Commun 2021; **18**: 39–51.

[101] Shi W, Zhou X and Jia L et al. Enhanced secure wireless information and power transfer via intelligent reflecting surface. IEEE Commun Lett 2020; **25**: 1084–8.

[102] Zhou X, Yan S and Wu Q et al. Intelligent reflecting surface (IRS)-aided covert wireless communications with delay constraint. IEEE Trans Wirel Commun 2022; **21**: 532–47.

[103] Dong L, Wang H-M. Secure MIMO transmission via intelligent reflecting surface. IEEE Wirel Commun Lett 2020; **9**: 787–90.

[104] Jiang W, Zhang Y and Wu J et al. Intelligent reflecting surface assisted secure wireless communications with multiple-transmit and multiple-receive antennas. IEEE Access 2020; **8**: 86659–73.

[105] Hong S, Pan C and Ren H et al. Artificial-noise-aided secure MIMO wireless communications via intelligent reflecting surface. IEEE Trans Commun 2020; **68**: 7851–66.

[106] Shu F, Teng Y and Li J et al. Enhanced secrecy rate maximization for directional modulation networks via IRS. IEEE Trans Commun 2021; **69**: 8388–401.

[107] Hehao N and Ni L. Intelligent reflect surface aided secure transmission in MIMO channel with SWIPT. IEEE Access 2020; **8**: 192132–40.

[108] Lu X, Yang W and Guan X et al. Robust and secure beamforming for intelligent reflecting surface aided mmWave MISO systems. IEEE Wirel Commun Lett 2020; **9**: 2068–72.

[109] Yu X, Xu D and Sun Y et al. Robust and secure wireless communications via intelligent reflecting surfaces. IEEE J Sel Areas Commun 2020; **38**: 2637–52.

[110] Hong S, Pan C and Ren H et al. Robust transmission design for intelligent reflecting surface-aided secure communication systems with imperfect cascaded CSI. IEEE Trans Wirel Commun 2020; **20**: 2487–501.

Weiping Shi received her M.S. degree from the Chongqing University of Posts and Telecommunications, China, in 2014. She is currently pursuing her Ph.D. degree from the School of Electronic and Optical Engineering, Nanjing University of Science and Technology, China. Her research interests include IRS-aided wireless communication, wireless energy transmission, and physical layer security.

Xinyi Jiang received her B.S. and M.S. degrees from Nanjing University of Science and Technology, Nanjing, China, in 2019 and 2022, respectively. Her research interests include wireless communications, physical layer security, and spatial modulation system.

Jinsong Hu received his B.S. degree and Ph.D. degree from the School of Electronic and Optical Engineering, Nanjing University of Science and Technology, Nanjing, China in 2013 and 2018, respectively. From 2017 to 2018, he was a Visiting Ph.D. Student at the Research School of Engineering, Australian National University, Canberra, ACT, Australia. He is an associate professor at the College of Physics and Information Engineering, Fuzhou University, Fuzhou, China. He served as a TPC member for the IEEE ICC2020/2019. His research interests include array signal processing, covert communications, and physical layer security.

Abdeldime Mohamed Salih Abdelgader got his B.S. degree from Sudan University of Science and Technology, Khartoum, Sudan, in 2000, M.S. degree from Karary University, Omdurman, Sudan in 2003, and Ph.D. from Southeast University, Nanjing, China in 2016. From 2003 to 2019, he worked at Karary University as a Lecturer in the Department of Electrical and Computer Engineering. During this period besides the regular research and teaching activities he provided more than 50 short courses that are related to communication systems and computer networks. Moreover, he is consultant for many IT companies in Sudan. Since 2019 till now, he is an associate professor at Karary University, Khartoum, Sudan. He has many publications and academic contributions in the field of Information security and communication engineering. Besides academic degrees, he has many certificates such as CCNA, CCNA sec, CCNP, the Sudanese Engineering Society Award, *etc.* His research interest is related to information security, mobile communication, and the physical layer of the vehicular networks.

Yin Teng received her B.S. degree from Zijin College at Nanjing University of Science and Technology, China, in 2019, and her M.S. degree from Nanjing University of Science and Technology, Nanjing, China, in 2022. Her research interests include wireless communication, physical layer security, and directional modulation networks.

Yang Wang received his B.S. and M.S. degrees from Nanjing University of Science and Technology, Nanjing, China, in 2019 and 2022, respectively. His research interests include wireless communications, physical layer security, and spatial modulation system.

Hangjia He received her B.S. degree from the Nanjing University of Science and Technology, China, in 2020. She is currently working toward her M.S. degree in the School of Electronic and Optical Engineering, Nanjing University of Science and Technology, Nanjing, China. Her research interests include wireless communication and signal processing.

Rongen Dong is currently pursuing her Ph.D. degree from the School of Information and Communication Engineering, Hainan University, China. Her research interests include wireless communication, signal processing, and mobile networks.

Feng Shu received his Ph.D., M.S., and B.S. degrees from the Southeast University, Nanjing, in 2002, XiDian University, Xi'an, China, in 1997, and Fuyang Teaching College, Fuyang, China, in 1994, respectively. From Sept. 2009 to Sept. 2010, he was a visiting post-doctor at the University of Texas at Dallas. From Oct. 2005 to Nov. 2020, he was with the School of Electronic and Optical Engineering, Nanjing University of Science and Technology, Nanjing, China. Since Dec. 2020, he has been with the school of information and communication engineering, Hainan University, Haikou, where he is currently a Professor and supervisor of Ph.D. and graduate students. He was awarded the Leading-talent Plan of Hainan Province, Mingjian Scholar Chair Professor and Fujian hundred-talent plan in Fujian Province. His research interests include wireless networks, wireless location, and array signal processing.

Jiangzhou Wang (Fellow, IEEE) has been a professor since 2005 at the University of Kent, UK. He has published over 400 papers and 4 books in the areas of wireless communications. Professor Wang is a Fellow of the Royal Academy of Engineering, UK, Fellow of the IEEE, and Fellow of the IET. He was a recipient of the Best Paper Award from the IEEE GLOBECOM2012. He was an IEEE Distinguished Lecturer from 2013 to 2014. He was the Technical Program Chair of the 2019 IEEE International Conference on Communications (ICC2019), Shanghai, the Executive Chair of the IEEE ICC2015, London, and the Technical Program Chair of the IEEE WCNC2013.