Invited Paper

Physical layer security for terahertz band communication： emerging technologies and the future trends

Yuqian He, Hongqi Zhang, Prem Narayan Choubey and Xianbin Yu [*]
College of Information Science and Electronic Engineering, Zhejiang University, Hangzhou 310027, China
[*] Email: xyu@zju.edu.cn

(Received December 2022)

Abstract: Terahertz (THz) band communications are envisioned as a key technology for 6G and beyond. For wireless communication security in THz band, physical-layer security (PLS) has recently received growing interest. This paper aims to provide a comprehensive survey of the PLS techniques in THz communication systems. The investigation consists of three hierarchical parts. Firstly, we introduce the emerging security threats arising from the THz physical-layer and compare them with the traditional security threats. Then, three newly-proposed PLS solutions in THz band are highlighted, which match the features of THz link well and are expected to be applied in the near future, including photonics-based frequency hopping (FH), intelligent reflecting surfaces (IRS) secure beamforming and security signal processing. At last, we discuss their challenges and propose different interesting areas that can be opted as future research directions.

Keywords: THz communications; Physical layer security; Beam scattering; Artificial noise

doi:

1. Introduction

By 2030, the 6th Generation (6G) of the wireless communication is expected to land, which should exceed the data traffic rate above 100’s of Gbps [1]. As a promising candidate to enable high-speed wireless communications, the THz band (0.1-10 *THz*) has attracted extensive attention owing to its advantages of high carrier frequency and large available bandwidth. Due to the rapid development of transceiver architectures, THz wireless transmissions providing over 100 *Gbps* or even 1 *Tbps* have been demonstrated recently in laboratories and in field environments [2-6], which has brought THz communication closer to reality. However, high-speed THz communication is also accompanied with a great information security risk. Without any precautions, a third illegal party can also intercept information over 100 *Gbps* or 1 *Tbps* equally, which may cause disaster especially in some sensitive applications such as the transmission of military secrets.

Traditional networks rely heavily on the cryptographic technology to address security issues at upper-layer protocol stack, which is not suitable for future THz networks [7, 8]. From point-to-point communication perspective, current THz transceivers often comprise relatively complex and precise terahertz circuits, such as UTC-PD in optical domain [9] or the high-speed mixer in electric domain [10]. Therefore, adding expensive and complex encryption-based system using complicated algorithms will undoubtedly burden the THz transceiver furtherly, which may stop the pace of large-scale application of THz communication. Besides, in future THz transmission, intelligent eavesdroppers may possess powerful computational devices, such as quantum computers with unbounded computing capabilities [11], which can unlock encryption and decryption keys with ease and jeopardize existing systems based on cryptography. From network perspective, future THz network are based on decentralized architectures [8, 12], which means users are free to join or leave the access points (APs) anytime. In this case, encryption-based handshake process may introduce large authentication overhead and increase the latency.

Different from the conventional cryptographic approaches, PLS exploits the physical properties of wireless medium including interference, noise, and fading to improve the security and therefore ensures a keyless secure data transmission [13-15]. Compared to cryptographic methods, the advantages of PLS techniques for THz communication are threefold. Firstly, PLS technology only adopts the simple signal processing algorithms and hence simplifies THz transceiver configuration compared to encryption-based techniques. Besides, keyless transmission also avoids the potential threat from powerful computational devices. Secondly, by using the fingerprint from devices or the wireless channel, PLS is expected to offer an efficient and direct authentication which will help THz network to simplify the handshake process and reduce the authentication latency [16, 17]. Thirdly, some applications of THz communication provide perfect stages for PLS. For example, multi-hop scheme is usually used to combat the distance limitation of the THz propagation, where secure relay selection technique can be adopted to improve secrecy [18, 19]. Besides, large bandwidth THz communication is also suitable for spread spectrum techniques to establish a secure communication link against jamming or eavesdropping [20].

The study of traditional PLS methods and high-speed THz communication have both achieved fruitful results in the past decades. Meanwhile, PLS methods match the characteristic of future

THz application well as mentioned above. However, as a new research topic, it is still challenging to apply the PLS methods in THz applications. Specifically, THz communication has the two of the most unique features: high directivity [21] and intrinsic frequency-selectivity [22]. How to design PLS strategies that well match two features remains an open problem. In this article, we present a comprehensive review of the PLS techniques for THz wireless communication. The objective of this article is to highlight the unique features of THz communication in PLS and discuss the future research directions so that PLS can be fully utilized in THz wireless communication.

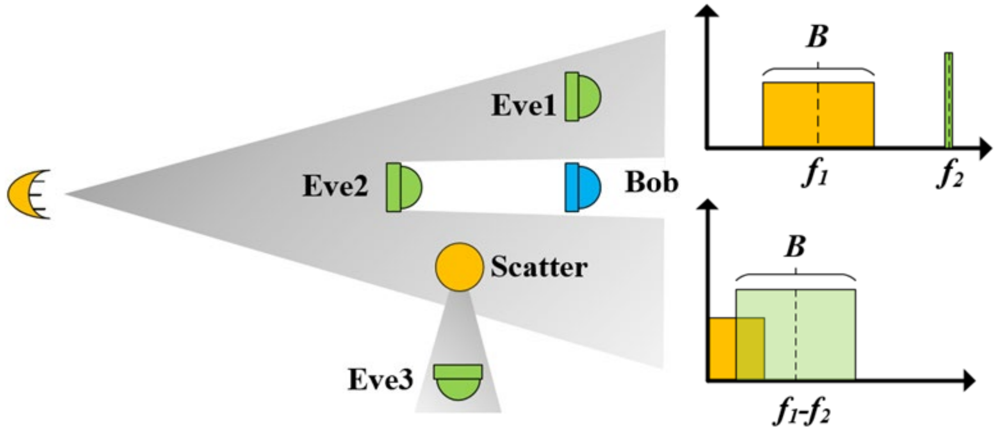
The rest of the paper is organized as follows. In Section 2, we introduce various physical-layer attackers in THz band and distinguish them from traditional ones. In Section 3, we analyze the emerging PLS solutions that are well suited to the unique features of THz link. In Section 4, we discuss the challenge in existing PLS solutions and point out the future directions. Finally, we give a brief conclusion in Section 5.

2. Physical-layer threat in THz communication

The potential of THz communications for enhancing information security has attracted great attention due to its high directivity and high path loss. However, the probability of successful attack still exists [23, 24]. Due to unique features of THz link, such as the adoption of noncoherent measurement, new threats are arising. In this section, we introduce the emerging physical-layer threats in THz band and compare them with the traditional methods, including eavesdropping, jamming and spoofing.

A. Eavesdropping

Due to the broadcast nature of wireless channel, attackers are able to eavesdrop confidential information. Eavesdropping attackers can be classified as active eavesdroppers [25] and passive eavesdroppers [26]. The transmitter (Alice) can design the signal and compute the secrecy capacity precisely since the channel state information (CSI) of active eavesdroppers is available. However, active eavesdroppers may spoil the transmission through jamming or the pilot contamination, simultaneously [27]. Passive eavesdroppers intercept information without raising an alarm, so their CSIs are not obtained by transmitters. For the active or passive attackers, the capable eavesdroppers can acquire the CSI of the main channel, which will mitigate the effective measures of Alice or disable them completely [28, 29]. In some cases, multiple-eavesdroppers scene should be taken into account, where the eavesdroppers can overhear the communication together with and without centralized processing [30, 31]. For example, in a cellular network, all the users who don't communicate with base station (BS) can be regarded as eavesdroppers.



(a) (b)

Fig. 1 (a) Three different eavesdropping attackers (Eve) in THz band. (b) The 'beating jamming' in THz band. The upper and bottom pictures show the spectrum before and after the detection. The yellow color represents original data while the green jamming signal.

To resist eavesdropping, the basic concept in PLS methods is to create a positive security capacity, where the legitimate user gets better signal quality compared to the malicious eavesdroppers in terms of the signal-to-noise ratio (SNR). Generally speaking, there are three methods in PLS to improve security: artificial noise (AN) techniques [32, 33], beamforming-based techniques [34] and diversity-based techniques [35]. The AN-based techniques inject AN into the null space of the legal channel so that only SNR of the illegal receiver is degraded by the AN, while the legal receiver remains unchanged. The beamforming-based techniques achieves the purpose by steering the information signal in a certain direction towards the legal receiver, so that the eavesdropper (Eve) only gets weak signal or pure noise while Bob gets the best channel through selection from precoding matrix for all the transmit antennas or a better channel compared to Eve. Different from the previous two, diversity-based techniques can enhance the information security without any additional power or CSI of Eve, through choosing the optimal antenna, relays or users.

Contrary to the traditional wireless links, THz band communications should be based on highly-directive narrow beams, which brings inherent advantages to the PLS. Nevertheless, Eves can still intercept information. In general, there are two types of attackers: Eve inside the THz beam [36, 37] and Eve outside the THz beam [23]. As shown in Fig.1(a), for Eve inside the beam

(Eve1), although the main lobe of the THz beam is highly-directive, footprint is much wider than the dimensions of the receiver [38] (Assuming a divergence angle of 4 degree, the beam radius for a 100 *m* link distance, which has already been achieved in the experiment, is 7 *m*). Therefore, Eve can put itself at the footprint of the beam or somewhere without blocking the main lobe. In another case (Eve2), Eve puts itself at the center of the main beam directly to capture the message, which may cause a shadow on receiver and raise an alarm. However, the THz beams are naturally prone to blockage by other normal objects like building walls, vehicles, furniture, and even human bodies. So, the receiver cannot distinguish if the shadow is caused by the surrounding environment or the malicious eavesdroppers. For Eve outside the beam (Eve3), attackers can put a tiny passive object, like a metal cup or a mobile phone, inside the narrow beam to scatter THz electromagnetic waves. By this mean, the Eve outside can capture the message without raising an alarm.

B. Jamming

Jamming is defined as the emission of electromagnetic waves by an illegal external source, in order to destroy the reception of a legitimate user. A key point to distinguish jamming and interference is whether it is intentional or not. Here, we classify different jamming techniques into two types: single-tone jamming and the barrage jamming [39]. Single-tone jamming can be very efficient and energy-saving if the target frequency is known. However, it could be easily avoided by changing the target frequency. Different from single-tone jamming, barrage jamming can cover a large bandwidth at the same time and hence leaves a little chance for the legal transceiver to escape. However, as bandwidth increases, the emission of the signals drains the energy fast. It is noted that the strategies of attackers are flexible no matter single-tone and barrage jamming. They can change the jamming frequencies over time using different pattern and select a proper time slot to work or sleep [15].

Jamming methodologies and countermeasures evolve as the carrier frequencies move to THz band [24]. Indeed, the highly-directive beams bring more robustness against jamming attack as the jammer needs to accurately aim at the main lobe of receiver to implement a successful attack. However, the large bandwidth, another characteristic of THz communication, brings new challenges in two aspects. Firstly, in order to achieve larger bandwidth, the photonic systems are more attractive contrary to the electronic one [40]. However, if photonic approach is adopted, malicious attackers may utilize the electronic system, which has much more transmitter power [41], to jam the receiver. Secondly, the 'beating jamming', as shown in Fig.1(b), can be utilized to bring attackers additional degree of freedom. The THz communication usually adopt noncoherent measurement [42, 24], where the jamming frequency is different from the carrier frequency before noncoherent detection and hence minimize the possibility of alarming Alice and Bob to the presence of attackers.

C. Spoofing

Spoofing attackers can deceive communications parties and gain access to confidential information by forging MAC identity information. The attackers can perform spoofing at the time gap when transmitter stops transmitting the signal, or, replace the transmitter simply in the phase of transmission by using higher power [43]. In general, there are two kinds of spoofing attacks: identity spoofing attacks [44] and Sybil attacks [45]. Identity spoofing allow the attackers to impersonate another legal node by stealing the legal MAC address. In this way, the attackers can intercept confidential message and carry out a more aggressive attack, such as man-in-the-middle attacks. In the Sybil attack, with only one physical devices, an attacker can claim the multiple identities. Therefore, many resources of the network are occupied and the users may receive spam and lose their privacy.

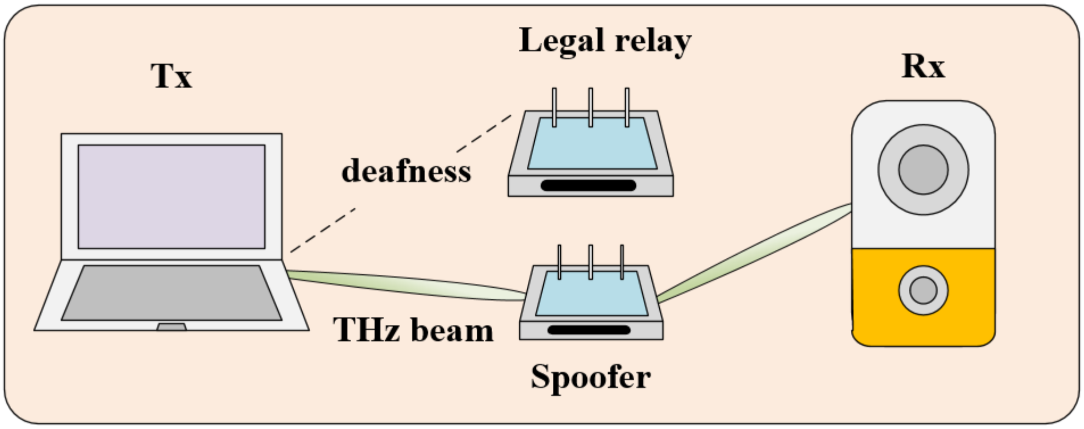


Fig. 2 The man in the middle attack in THz band.

In THz MAC network, the need for high-gain directional antennas leads to the deafness problem [47, 48], as shown in Fig.2. Because one node has no information about the location of the other node, an exhaustive beam direction search is usually used at both transceivers in order to find each other. This search process provides a new opportunity for spoofing attack, since attackers don’t have to wait for the time gap or use higher power any more as mentioned before. The attackers only need to find the beam direction of receiver and forge a legal MAC address. We note that any user movement can destroy the maintenance of the link. Besides, as shown in Fig.2, multi-hop relays may be extensively adopted in THz network to extend the coverage [18, 19], which creates a good environment for man-in-the-middle attacks if attackers can steal the MAC address of the relay. Last but not the least, the spoofing attack is hard to be detected in THz network. Traditional location-based and channel-based detection methods may not work [43]. The density of access point (AP) in THz band is much higher than that in lower frequency band [49]. Therefore, it is more challenging for receivers to distinguish the attacker from AP, and a strong correlation between the main channel and the illegal channel also makes the channel-based detection methods efficacy lower. To the best of our knowledge, there are no studies on how to develop an effective PLS for THz networks. Hence, the spoofing attack is still a nontrivial physical-layer threat.

3. Countermeasures

In this section, we survey the recent researches about THz PLS solutions in order to tackle the new physical-layer threats highlighted in the previous section, including photonics-based frequency hopping (FH), intelligent reflecting surfaces (IRS) secure beamforming and security signal processing.

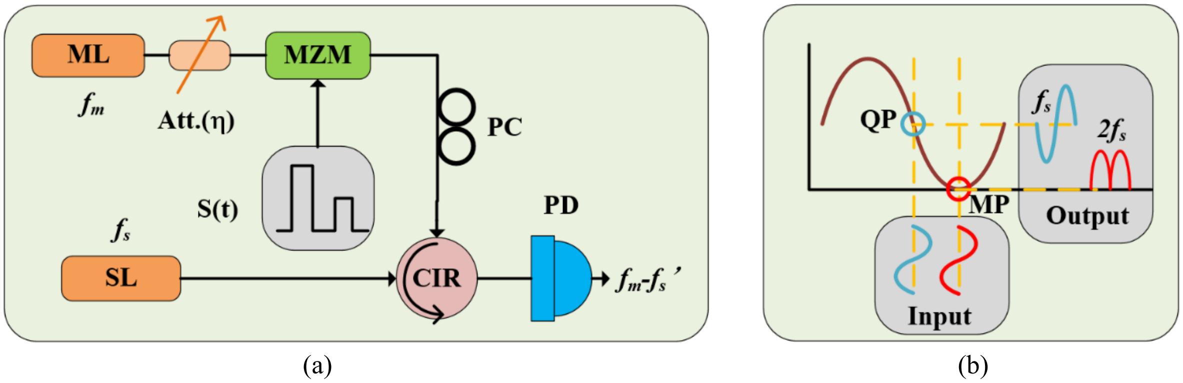


Fig. 3 (a) Schematic diagram of the period-one dynamic-based frequency-hopping system. (b) Transmission characteristics of the DD-MZM at quadrature (QP) and minimum (MP) biasing points.

A. Photonics-based frequency hopping

The FH systems can mitigate the effects of inter-symbol interference and jamming and therefore have been widely implemented in some applications such as Bluetooth and the military strategy. However, the bandwidth of today's electronic-based FH systems are limited to several *GHz*, and the hopping speeding is confined to milliseconds, which weakens its ability against jamming and eavesdropping. Conversely, photonics-based FH systems have larger hopping bandwidth and roughly 10^3-10^6 times faster hopping speed compared to the electronic-based methods [50]. Although photonics-based THz communications system are more prone to jamming attack due to the relative low power, they are able to tune the THz frequency over a broad spectral range to escape from the unique ‘beating jamming’ attack in THz band.

There are mainly two types of photonics-based FH carrier generation schemes: photonics-based frequency synthesizer with ultrafast frequency switching ability [51, 52] and photonics-based switch for fast switching of pre-generated frequencies [53, 54]. In the former scheme, as shown in Fig.3(a), period-one dynamics-based FH system is adopted in [51] to generate different frequency. A master laser (ML) at $f_{\rm M}$ modulated by a hopping code sequence *S(t)* is launched to a slave laser (SL) $f_{\rm S}$ by an optical circulator (CIR). Due to the effect of injection locking and the change of refractive index by light power, the SL lases at both $f_{\rm M}$ and $f_{\rm S}$’ finally. Therefore, the output RF frequency ($f_{\rm M}$ - $f_{\rm S}$’) can be controlled by adjusting the power of the modulated ML. In the latter scheme, pockels effect of dual-drive Mach–Zehnder (DD-MZM) is adopted in [53] to achieve a faster FH speed. A reference signal $f_{\rm S}$ with amplitude V_0 and a hopping sequence *S(t)* with amplitude V_s are both injected into the two arms of DD-MZM. Therefore, the transmission function of the proposed system can be given by:

$$T = \frac{1}{2} + \cos\left[\frac{\pi(V_0 \cos(2\pi f_S t) - V_s S(t) - V_{DC})}{V_\pi}\right],$$

where V_π is half wave voltage of the DD-MZM and V_{DC} is DC bias difference between the two arms. As shown in Fig.3(b), if the input V_{DC} is at the quadrature point (QP) of DD-MZM, the output RF is $f_{\rm S,}$ while V_{DC} at the minimum point (MP) the output is $2f_{\rm S}$. Thus, by changing *S(t)* to let the DD-MZM work at the MP or QP, a FH system ($f_{\rm S}$/$2f_{\rm S}$) can be achieved.

A recent study in THz band utilizes two distributed feedback laser (DFB) to generate a linear FH system against single/multi-tone jamming attack [20], where a microprocessor-based laser controller is adopted to control the frequency of DFB. By comparing the ‘input frequency’ with the ‘estimated frequency’, they find increasing the scanning rate declines frequency tunable range significantly. With a fixed decision threshold, a non return zero (NRZ) signal of 6Gbps in 1.75 *m* distance has been achieved in a THz FH communication system with different scanning rates. They find higher scanning rate corresponds to smaller BER, as the frequency hopping at a higher scanning rate containing the frequencies window of the lower BER. This study sets an example for the other future FH system to fight against the single/multitone jamming in an incoherent THz communication.

B. IRS secure beamforming

Recently, intelligent reflecting surfaces (IRS) have gotten a lot of attention in THz communications owing to their huge potentials in extending the transmission distance and overcoming the non-line-of-sight (NLoS) transmission problems. On the other hand, the IRS technology can also be used to improve the secrecy performance of THz communication.

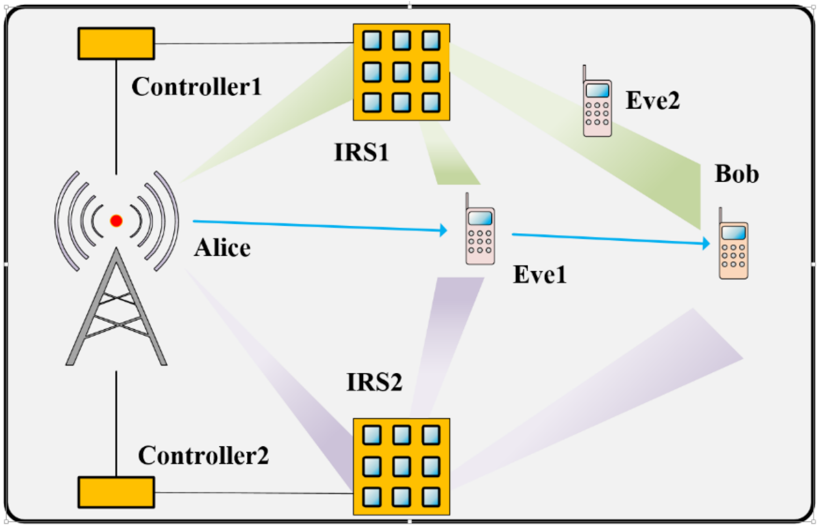


Fig. 4 A multipath IRS-assisted THz wiretap system.

In THz link, the channel of the eavesdropper communication link is often highly correlated with the legal channel, and the SNR of eavesdropper is usually better than Bob. Therefore, traditional PLS such as beamforming may not work. In this case, we can add another THz link to the original line-of-sight (LOS) link [55, 56], as shown in Fig.4, whichapplies IRS as a relay node, to decorrelate the Bob's and Eve's channel since the IRS-Eve link and IRS-Bob link are independent from each other. It is noteworthy if Eve is located between IRS and Bob (Eve2), the legal channel will also be independent from illegal channel since there are always at least two paths between Alice and Bob. By effectively controlling the phase shifts of the IRS's reflecting elements, the reflected signal is added increasingly towards Bob while decreasingly to Eve, both leading to improved secrecy performance for the legal receiver. It is first proved in [57] that active beamforming design at transmitter is independent of passive reflecting beamforming at IRS.

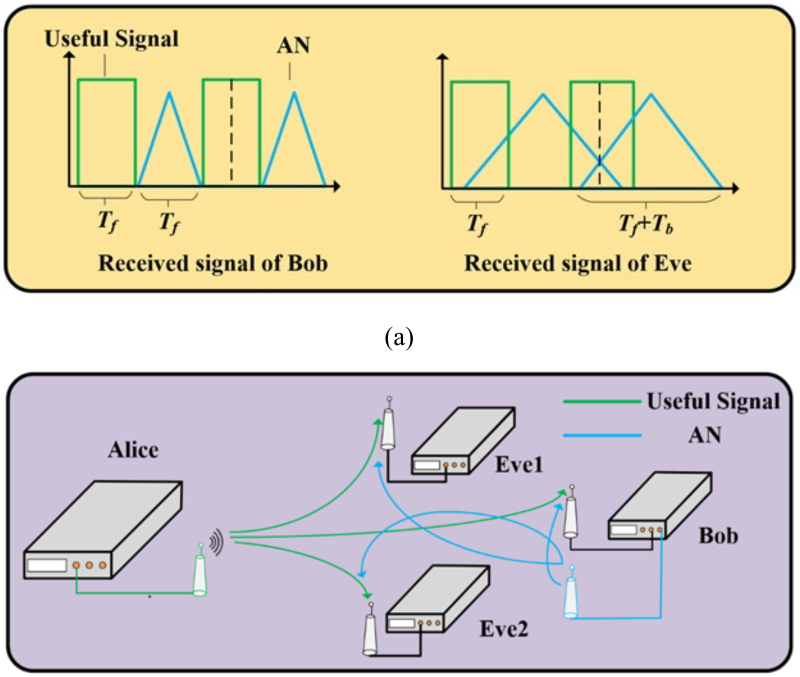
The above studies use only one IRS to improve the secrecy performance. However, a recent study indicates THz communication can be further enhanced by utilizing *multiple propagation paths* between Alice and Bob [58]. The probability of interception by eavesdropper decreases drastically as the number of paths increases. One way to achieve *multiple propagation paths* is to share the secret message via several AP. Nevertheless, the message sharing among different THz

APs significantly increases system overhead thanks to the synchronization problem. Therefore, the authors don’t explicitly propose using IRS to realize the purpose, and the multiple IRS technology with only one AP should be the most appropriate method to achieve *multiple propagation paths* in THz communication, as shown in Fig4. The message is encoded so that the receiver can only decode the message when it receives all the shares from *multiple propagation paths*.

The above works in [55-58] either assume eavesdropper does not block the THz link or assume a perfect CSI of eavesdropper can be obtained. In reality, eavesdroppers may pretend to be some stationary and mobile objects such as building walls, vehicles which cast a shadow on receiver, as shown in Fig.1(a). Moreover, the CSI of eavesdroppers can hardly to be obtained perfectly thanks to their passive behaviors. Therefore, the study in [37] investigates a multi-IRS secure transmission strategy in THz systems with imperfect CSI of eavesdroppers, where an eavesdropper placed within the range of THz beams can both intercept and block the confidential messages. A joint optimization problem of beamforming for the BS and IRS is proposed and a robust secure scheme is adopted to counter the adverse effects of multiple blocking eavesdroppers.

C. Security signal processing

Besides IRS, another method to keep secret transmission when Eve’s channel is better than Bob’s channel is to use AN. The AN has been first proposed in [32] and then been studied widely and thoroughly in many works over the past decades, such as unmanned aerial vehicles (UAVs) [59], non-orthogonal multiple access (NOMA) [60] and visible light communication (VLC) [61]. In THz band, the null space of Bob’s channel may disappear due to the LOS link, which causes the failure of AN [62]. Recently, in [36], the authors use a molecular absorption aided scheme to achieve AN technology with a full-duplex (FD) mode, as shown in Fig5(a). The receiver transmits AN and receives useful signal simultaneously. Instead of mixing the AN and the useful signal as a whole, the proposed scheme puts each of the AN pulse between the two the useful signals pulse. On the one hand, the AN will not interfere with the Bob’s useful signal since the transmission distance is very short due to the full-duplex mode of Bob. On the other hand, by well designing the carrier frequency, the AN to Eve will undergo a temporal broadening effect (TBE) caused by the frequency-selectivity of molecular absorption. Therefore, the AN at Eve will overlap with the useful signal and cause interference, as shown in Fig 5(b). Instead of utilizing the traditional high-complexity techniques [63], this study avoids the self-interference problem of FD mode by a proper signal detection design.



(a)

(b)

Fig. 5 (a) Proposed THz AN security model where AN is transmitted on the receiver side. (b) Illustration of the received signal on both Bob's and Eve's side.

Although AN technology guarantees the secret transmission of message, the malicious eavesdroppers can still become aware of the existence of the transceivers. In some cases, users want to transmit message covertly. For example, soldiers want to hide their location in the battle field. Therefore, convert communication has been proposed to leave no chance for adversary to detect the transmission. In [64], the authors have found LoS covert communication in THz band is impossible because attackers can simply place a receiver in the narrow beam. However, by adopting the NLoS link, i.e., the reflection or diffuse scattering from a rough surface, the covert communication can still be implemented successfully. This study puts the THz communication in an IoT network so that each IoT devices will cause interference to the receiver. The attacker could adopt omnidirectional antenna if he doesn't know any information about the NLoS link. However, omnidirectional antenna will experience more interference from other IoT devices and therefore give attacker a dilemma of how to select the type of antenna.

The above study suits for the case when the attacker is located between Alice and Bob. However, a recent study shows that covert communication can be achieved in LoS link when the attacker is located behind Bob [65]. The authors propose a distance-adaptive absorption peak modulation (DA-APM) method to increase signal covertness. The main idea is to dynamically modulate signals on the molecular absorption peaks in THz spectrum. Specifically, the authors choose from [66] designed a multi-wideband waveform and select the frequency bands with proper molecular absorption coefficients. As a result, it is demonstrated that the maximum distance Eves can percept signal is shrunk by approximately 60% when transmit power is 10*dBm* and a minimal data rate of 5*Gbps* is attained which can not be achieved in traditional random spectrum selection.

4. Challenges and future direction

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

A. Imperfect channel

To design the state-of-the-art PLS techniques with enhanced secrecy performance, CSI is one of the most important channel features that helps in obtaining information about both the receiver's and interceptor's channel. In the aforementioned technologies, the IRS method assume global CSI is known by the BS/IRS, including the CSI of eavesdropper. Notably, although the study in [37] has discussed the effect of imperfect CSI of eavesdropper, they assume the main channel is perfectly known by BS which would also cause a performance degradation. In AN method and covert communication, exact CSI influenced by the molecular absorption should also be known by the transceiver so that absorption peak can be selected for the design of waveform. However, it is not possible to get the perfect CSI in practice due to the delay, feedback quantization error, estimation error, and user's mobility [62]. As a result, performance of the secrecy technique, does not give even near-satisfactory results. It will be of great benefit to study the effect of imperfect CSI and conduct field experiments for the sake of verifying the efficiency of various physical-layer security in THz band [13].

Another challenge comes from the highly-directive of THz link. The channel of an eavesdropper within the LoS direction is highly correlated with the legal channel. Therefore, the available PLS techniques based on AN generation, direction modulation, beamforming, linear and non-linear precoding techniques, and the others mentioned above, all go in vain. Although the IRS and FD-based AN generation methods are proposed to solve the problem, they both have their own drawbacks. The IRS method is originally used for circumvent obstacles which increases the coverage range, especially in some indoor scenarios. Therefore, in those scenarios where IRS technology in not essential, such as, the highly-directive THz backhaul links between two high buildings where obstacles have seldom been seen, the IRS-based PLS technology may lose their value. The FD-based AN generation method also reduce the baud rate intentionally by inserting AN signal between two useful signals. Moreover, these two methods can not defend attack when eavesdroppers are just near the receiver, because the main channel and the illegal channel are almost exactly the same. Hence, there is a huge requirement of coming up with new PLS techniques that can give secure environment in LoS case.

One way to avoid 'perfect CSI assumption' and 'LoS link problem' is to utilize the device-based features. Device-based methods have been widely adopted in physical-layer authentication [67, 68]. For example, phase noise and carrier frequency offset determined by the imperfections of local oscillators, power amplification or the I/Q imbalance — determined by the transceiver. All these features can be used to achieve the physical-layer authentication, since a pair device produced by the same process would own different hardware characteristic. A recent study in [17] shows that devices features can also be applied to physical-layer key generation. By exchanging the stimulus, each transceiver gets the information of both the channel and the circuit characteristics on the other side. In this manner, symmetric information is formed at both sides to generate the encryption keys. The attacker would find it difficult to distinguish the circuit characteristics from channel characteristics by evaluating the signals it received.

In THz communication, device-based features can also be deemed as another physical-layer resources. As the bandwidth increases in THz band, the device impairments caused by frequency-selective behavior such as ripples and the tilt in gain and group delay can be deemed as a substitute to the frequency-selective channel. Compared to the traditional 'spatial channel', the 'device-based channel' has advantages of uniqueness and robustness. One can always find the differences between attacker's and receiver's device. Besides, this the uniqueness is easy to estimate since the fixed device is different from the changeable channel, where CSI is hard to estimate.

B. Intelligent attacker

In future THz communication, as the diversity and intensity of security attacks should grow gradually, the attackers may employ artificial intelligence (AI) to break through the security limit [62]. In [69], the eavesdropper also decides an optimal jamming power in accordance with its observation of the strategy of the transmitter. Meanwhile, a physical layer switch strategy between half-duplex (HD) mode and FD mode can also be utilized by an intelligent eavesdropper to decrease the secrecy rate according to its location and self-interference.

As a countermeasure, transceivers can also introduce the AI to fight against jamming or eavesdropping. In [70], the authors adopt a single-agent reinforcement learning (RL) communications scheme against jamming attacks, where a sweeping jammer is assumed to move across the entire wideband spectrum. The proposed Q-learning anti-jamming protocol will select the idle frequency bands with the longest uninterrupted time once getting jammed. In [71], the authors investigate a multiple channel anti-jamming scene with one secondary user (SU) and *m* jammers, with each constrained to occupy one channel during each iteration. The Q-learning methods are adopted to improve the successful transmission and reduce the loss value for getting jammed under different types of attackers. The experiments show the proposed Q-learning in [71] achieves 80% successful transmission while achieving only 75% in [70]. This is because the latter method implements FH before getting jammed. In [72], the authors use the deep Q-network (DQN), one type's method of deep learning (DL), in the underwater acoustic networks (UANs) to decide the best optimal power allocation against smart jamming attackers.

Besides jamming, the AI can also be utilized against eavesdropping. In [73], authors use AI together with AN technique to degrade the eavesdropper's performance. In the scheme, both transceivers have two antennas with one antenna to achieve normal communication and the other to implement AN and artificial interference transmission. The error performance of Eve, even with an advantageous position, can still be significantly degraded.

The AI can improve the performance of THz communication in many aspects, for example, achieving the optimal energy-efficient beamforming variables with post-massive multiple-input multiple-output (PM-MIMO), selecting the optimal precoding variables in THz transceiver and choosing the flexible spectrum management framework for THz/mmWave communication [74]. However, only a few works investigate the positive effect of AI on THz PLS. Applying AI to enhance PLS of THz link is a very interesting topic such as using RL or DL to estimate the CSI of receiver and attacker.

C. Network design

At present, network security design in THz communication is at the initial stage. There are three potential challenges existing in the field of THz PLS from the perspective of network. Firstly, specific PLS technologies for THz network security are waiting to be invented. The existing PLS methods including FH, IRS, AN and covert communication are only designed for point-to-point communication which does not resolve the secure problems in upper-layer, e.g., spoofing. Although covert communication can hide the existence of transceivers and avoid spoofing attackers to some extent, the malicious attackers can discover their existence through other way, especially in some scenes such as indoor T-WLAN. Therefore, it is of great interest to build new authentication technology that matches the unique features of THz network well. Secondly, there is lack of joint security optimization methods for the whole THz network consisting of physical-layer, the MAC-layer, the network-layer, the transport-layer, and the application-layer. For example, in order to meet the authenticity requirements, the existing wireless networks may utilize multiple authentication methods to keep different layers secure separately [75]. Although the employment of multiple separate authentication mechanisms at different protocol layers improves the security level of wireless networks, these methods are potentially inefficient with the huge expense of a complexity and the latency [13]. It is estimated that the cross-layer security design will advance the THz network security with a reduced overhead. Thirdly, in existing wireless network, the security and throughput are designed individually in order to be maximized, which is however potentially suboptimal for future THz network [76]. Different types of services have totally different security requirements. For example, the ordinary web browsing service calls for a much lower security level than different online payment. So, there is no need to pay too many resources to improve the security of web browsing. Another example is that increasing the source's transmit power which can improve the throughput of the main link, but it may also increase the risk of successful eavesdropping. Therefore, in order to achieve secure and high-rate THz communication, it is necessary to investigate the joint optimization of security and throughput of THz network.

5. Conclusion

In this survey, we have focused on the impact of physical-layer threats and PLS solutions in THz communication. We have reviewed the characteristics and physical-layer threats in THz link and categorized these threats with different attackers' purposes. We have discussed the emerging PLS solutions in THz band and pointed out their unique advantages over the traditional PLS technology. In addition, we have discussed numerous challenges that are being faced in practically implementing these existing PLS techniques, and also proposed potential remedies that can be selected as future research topics.

It is noted that the THz PLS technology is still at its infancy. With the rapid advancement of THz communication thanks to breakthrough in semiconductor technologies, more security problem in THz band will be exposed and more PLS solutions will be proposed in the future. The main purpose of this paper is to analyze the unique features of THz link and discuss the potential PLS solutions for future THz communication. We hope this paper can help stimulating further researches in this area.

References

[1] Elayan H, Amin O, Shihada B, et al. "Terahertz band: The last piece of RF spectrum puzzle for communication systems". *IEEE Open Journal of the Communications Society*, 1:1-32(2019).

[2] Jia S, Pang X, Ozolins O, et al. “0.4 THz photonic-wireless link with 106 Gb/s single channel bitrate[J]”. *Journal of Lightwave Technology*, 36(2): 610-616(2018).

[3] Zhang J, Zhu M, Lei M, et al. “Real-time demonstration of 103.125-Gbps fiber–THz–fiber 2× 2 MIMO transparent transmission at 360–430 GHz based on photonics[J]”. *Optics Letters*, 47(5): 1214-1217(2022).

[4] Zhang H, Zhang L, Wang S, et al. “Tbit/s multi-dimensional multiplexing THz-over-fiber for 6G wireless communication[J]”. *Journal of Lightwave Technology*, 39(18): 5783-5790(2021).

[5] Wang S, Lu Z, Li W, et al. “26.8-m THz wireless transmission of probabilistic shaping 16-QAM-OFDM signals[J]”. *APL photonics*, 5(5): 056105(2020).

[6] Harter T, Füllner C, Kemal J N, et al. “Generalized Kramers–Kronig receiver for coherent terahertz communications[J]”. *Nature Photonics*, 14(10): 601-606(2020).

[7] Cacciapuoti A S, Sankhe K, Caleffi M, et al. “Beyond 5G: THz-based medium access protocol for mobile heterogeneous networks[J]”. *IEEE Communications Magazine*, 56(6): 110-115(2018).

[8] Yang P, Xiao Y, Xiao M, et al. “6G wireless communications: Vision and potential techniques[J]”. *IEEE network*, 33(4): 70-75(2019).

[9] Chao E, Xiong B, Sun C, et al. “D-Band MUTC Photodiodes With Flat Frequency Response[J]”. *IEEE Journal of Selected Topics in Quantum Electronics*, 28(2): 1-8(2021).

[10] Wang C, Yu J, Li X, et al. “Fiber-THz-Fiber Link for THz Signal Transmission[J]”. *IEEE Photonics Journal*, PP(2):1-1(2018).

[11] Sanenga A, Mapunda G A, Jacob T M L, et al. “An overview of key technologies in physical layer security[J]”. *Entropy*, 22(11): 1261(2020).

[12] Sun L, Du Q. “Physical layer security with its applications in 5G networks: A review[J]”. *China communications*, 14(12): 1-14(2017).

[13] Zou Y, Zhu J, Wang X, et al. “A survey on wireless security: Technical challenges, recent advances, and future trends[J]”. *Proceedings of the IEEE*, 104(9): 1727-1765(2016).

[14] Liu Y, Chen H H, Wang L. “Physical layer security for next generation wireless networks: Theories,

technologies, and challenges[J]". *IEEE Communications Surveys & Tutorials*, 19(1): 347-376(2016).

[15] Wang N, Wang P, Alipour-Fanid A, et al. "Physical-layer security of 5G wireless networks for IoT: Challenges and opportunities[J]". *IEEE Internet of Things Journal*, 6(5): 8169-8181(2019).

[16] Xie N, Li Z, Tan H. "A survey of physical-layer authentication in wireless communications[J]". *IEEE Communications Surveys & Tutorials*, 23(1): 282-310(2020).

[17] Ramabadran P, Afanasyev P, Malone D, et al. "A novel physical layer authentication with PAPR reduction based on channel and hardware frequency responses[J]". *IEEE Transactions on Circuits and Systems I: Regular Papers*, 67(2): 526-539(2019).

[18] Mir T, Waqas M, Mir U, et al. "Hybrid precoding design for two-way relay-assisted terahertz massive MIMO systems[J]". *IEEE Access,* 8: 222660-222671(2020).

[19] Huang C, Yang Z, Alexandropoulos G C, et al. "Multi-hop RIS-empowered terahertz communications: A DRL-based hybrid beamforming design[J]". *IEEE Journal on Selected Areas in Communications*, 39(6): 1663-1677(2021).

[20] Nallappan K, Skorobogatiy M. "Photonics based frequency hopping spread spectrum system for secure terahertz communications[J]". *Optics Express*, 30(15): 27028-27047(2022).

[21] Boulogeorgos A A A, Jornet J M, Alexiou A. "Directional terahertz communication systems for 6g: Fact check: A quantitative look[J]". *IEEE Vehicular Technology Magazine*, 16(4): 68-77(2021).

[22] Han C, Bicen A O, Akyildiz I F. "Multi-ray channel modeling and wideband characterization for wireless communications in the terahertz band[J]". *IEEE Transactions on Wireless Communications*, 14(5): 2402-2412(2014).

[23] Ma J, Shrestha R, Adelberg J, et al. "Security and eavesdropping in terahertz wireless links[J]". *Nature*, 563(7729): 89-93(2018).

[24] Shrestha R, Guerboukha H, Fang Z, et al. "Jamming a terahertz wireless link[J]". *Nature Communications*, 13(1): 1-9(2022).

[25] Liu C, Lee J, Quek T Q S. "Safeguarding UAV communications against full-duplex active eavesdropper[J]". *IEEE Transactions on Wireless Communications*, 18(6): 2919-2931(2019).

[26] Kim M, Hwang E, Kim J N. "Analysis of eavesdropping attack in mmWave-based WPANs with directional antennas[J]". *Wireless Networks*, 23(2): 355-369(2017).

[27] Zhou X, Maham B, Hjorungnes A. "Pilot contamination for active eavesdropping[J]". *IEEE Transactions on Wireless Communications*, 11(3): 903-907(2012).

[28] Yang Y, Jiao B. "Artificial-noise strategy for single-antenna systems over multi-path fading channels[C]"//2015 International Wireless Communications and Mobile Computing Conference (IWCMC). IEEE, 2015: 96-

101(2015).

[29] Zhang M, Liu Y, Zhang R. “Artificial noise aided secrecy information and power transfer in OFDMA systems[J]”. *IEEE Transactions on Wireless Communications*, 15(4): 3085-3096(2016).

[30] Zhou X, Ganti R K, Andrews J G. “Secure wireless network connectivity with multi-antenna transmission[J]”. *IEEE Transactions on Wireless Communications*, 10(2): 425-430(2010).

[31] Zheng T X, Wang H M, Yuan J, et al. “Multi-antenna transmission with artificial noise against randomly distributed eavesdroppers[J]”. *IEEE Transactions on Communications*, 63(11): 4347-4362(2015).

[32] Goel S, Negi R. “Guaranteeing secrecy using artificial noise[J]”. *IEEE transactions on wireless communications*, 7(6): 2180-2189(2008).

[33] Zhou X, McKay M R. “Secure transmission with artificial noise over fading channels: Achievable rate and optimal power allocation[J]”. *IEEE Transactions on Vehicular Technology*, 59(8): 3831-3842(2010).

[34] Nghia N T, Tuan H D, Duong T Q, et al. “MIMO beamforming for secure and energy-efficient wireless communication[J]”. *IEEE Signal Processing Letters*, 24(2): 236-239(2017).

[35] Zou Y, Zhu J, Wang X, et al. “Improving physical-layer security in wireless communications using diversity techniques[J]”. *IEEE Network*, 29(1): 42-48(2015).

[36] Gao W, Han C, Chen Z. “DNN-powered SIC-free receiver artificial noise aided terahertz secure communications with randomly distributed eavesdroppers[J]”. *IEEE Transactions on Wireless Communications*, 21(1): 563-576(2021).

[37] Qiao J, Zhang C, Dong A, et al. “Securing Intelligent Reflecting Surface Assisted Terahertz Systems[J]”. *IEEE Transactions on Vehicular Technology*, 71(8): 8519-8533(2022).

[38] Wu H, Kang D, Ding J, et al. “Secrecy performance analysis in the FSO communication system considering different eavesdropping scenarios[J]”. *Optics Express*, 30(23): 41028-41047(2022).

[39] Aref M A, Jayaweera S K, Yepez E. “Survey on cognitive anti-jamming communications[J] ”. *IET Communications*, 14(18): 3110-3127(2020).

[40] Horst Y, Blatter T, Kulmer L, et al. “Transparent Optical-THz-Optical Link at 240/192 Gbit/s Over 5/115 m Enabled by Plasmonics[J]”. *Journal of Lightwave Technology*, 40(6): 1690-1697(2022).

[41] Siles J V, Cooper K B, Lee C, et al. “A new generation of room-temperature frequency-multiplied sources with up to 10× higher output power in the 160-GHz–1.6-THz range[J]”. *IEEE Transactions on Terahertz Science and Technology*, 8(6): 596-604(2018).

[42] Qiao M, Zhang L, Wang S, et al. “60 Gbit/s PAM-4 wireless transmission in the 310 GHz band with nonlinearity tolerant signal processing[J]”. *Optics Communications*, 492: 126988(2021).

[43] Yılmaz M H, Arslan H. “A survey: Spoofing attacks in physical layer security[C]//2015 IEEE 40th Local

Computer Networks Conference Workshops (LCN Workshops)". IEEE, 812-817(2015).

[44] Zeng K, Govindan K, Mohapatra P. "Non-cryptographic authentication and identification in wireless networks [security and privacy in emerging wireless networks[J]". IEEE Wireless Communications, 17(5): 56-62(2010).

[45] Xiao L, Greenstein L J, Mandayam N B, et al. "Channel-based detection of sybil attacks in wireless networks[J]". *IEEE Transactions on Information Forensics and Security*, 4(3): 492-503(2009).

[46] Zhou W, Marshall A, Gu Q. A novel classification scheme for 802.11 WLAN active attacking traffic patterns[C]//IEEE Wireless Communications and Networking Conference, 2006. WCNC 2006. IEEE, 2: 623-628(2006).

[47] Han C, Zhang X, Wang X. "On medium access control schemes for wireless networks in the millimeter-wave and terahertz bands[J]". *Nano Communication Networks*, 19: 67-80(2019).

[48] Xia Q, Jornet J M. "Expedited neighbor discovery in directional terahertz communication networks enhanced by antenna side-lobe information[J]". *IEEE Transactions on Vehicular Technology*, 68(8): 7804-7814(2019).

[49] Wu Y, Kokkoniemi J, Han C, et al. "Interference and coverage analysis for terahertz networks with indoor blockage effects and line-of-sight access point association[J]". *IEEE Transactions on Wireless Communications*, 20(3): 1472-1486(2020).

[50] Liu Q, Fok M P. "Ultrafast and wideband microwave photonic frequency-hopping systems: A review[J]". *Applied Sciences*, 10(2): 521(2020).

[51] Zhou P, Zhang F, Ye X, et al. "Flexible frequency-hopping microwave generation by dynamic control of optically injected semiconductor laser[J]". *IEEE Photonics Journal*, 8(6): 1-9(2016).

[52] Tseng C H, Hung Y H, Hwang S K. "Frequency-modulated continuous-wave microwave generation using stabilized period-one nonlinear dynamics of semiconductor lasers[J]". *Optics Letters*, 44(13): 3334-3337(2019).

[53] Chen Y. "High-speed and wideband frequency-hopping microwave signal generation via switching the bias point of an optical modulator[J]". *IEEE Photonics Journal*, 10(1): 1-7(2018).

[54] Ge J, Feng H, Scott G, et al. "High-speed tunable microwave photonic notch filter based on phase modulator incorporated Lyot filter[J]". *Optics letters*, 40(1): 48-51(2015).

[55] Cui M, Zhang G, Zhang R. "Secure wireless communication via intelligent reflecting surface[J]". *IEEE Wireless Communications Letters*, 8(5): 1410-1414(2019).

[56] Ning B, Chen Z, Chen W, et al. Improving security of THz communication with intelligent reflecting surface[C]//2019 IEEE Globecom Workshops (GC Wkshps). IEEE, 1-6(2019).

[57] Qiao J, Alouini M S. "Secure transmission for intelligent reflecting surface-assisted mmWave and terahertz systems[J]". *IEEE Wireless Communications Letters*, 9(10): 1743-1747(2020).

[58] Petrov V, Moltchanov D, Jornet J M, et al. Exploiting multipath terahertz communications for physical layer

security in beyond 5G networks[C]//IEEE INFOCOM 2019-IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS). IEEE, 865-872(2019).

[59] Maeng S J, Yapıcı Y, Güvenç İ, et al. “Precoder Design for Physical-Layer Security and Authentication in Massive MIMO UAV Communications[J]”. *IEEE Transactions on Vehicular Technology,* 71(3): 2949-2964(2022).

[60] Wang W, Liu X, Tang J, et al. “Beamforming and jamming optimization for IRS-aided secure NOMA networks[J]”. *IEEE Transactions on Wireless Communications*, 21(3): 1557-1569(2021).

[61] Yang F, Zhang K, Zhai Y, et al. “Artificial noise design in time domain for indoor SISO DCO-OFDM VLC wiretap systems[J]”. *Journal of Lightwave Technology*, 39(20): 6450-6458(2021).

[62] Irram F, Ali M, Naeem M, et al. “Physical layer security for beyond 5G/6G networks: Emerging technologies and future directions[J]”. *Journal of Network and Computer Applications*, 103431(2022).

[63] Yan S, Zhou X, Yang N, et al. “Secret channel training to enhance physical layer security with a full-duplex receiver[J]”. *IEEE Transactions on Information Forensics and Security*, 13(11): 2788-2800(2018).

[64] Liu Z, Liu J, Zeng Y, et al. “Covert wireless communication in IoT network: From AWGN channel to THz band[J]”. *IEEE Internet of Things Journal*, 7(4): 3378-3388(2020).

[65] Gao W, Chen Y, Han C, et al. “Distance-adaptive absorption peak modulation (DA-APM) for terahertz covert communications[J]”. *IEEE Transactions on Wireless Communications*, 20(3): 2064-2077(2020).

[66] Gao W, Chen Y, Han C, et al. Distance-adaptive absorption-peak hopping (DA-APH) modulation for terahertz covert communications[C]//2019 IEEE Global Communications Conference (GLOBECOM). IEEE, 1-6(2019).

[67] Pitarokoilis A, Björnson E, Larsson E G. “ML detection in phase noise impaired SIMO channels with uplink training[J]”. *IEEE Transactions on communications*, 64(1): 223-235(2015).

[68] Polak A C, Dolatshahi S, Goeckel D L. “Identifying wireless users via transmitter imperfections[J]”. *IEEE Journal on selected areas in communications*, 29(7): 1469-1479(2011).

[69] Huang W, Chen W, Bai B, et al. Physical layer security game with full-duplex proactive eavesdropper[C]//2016 IEEE Global Conference on Signal and Information Processing (GlobalSIP). IEEE, 992-996(2016).

[70] Machuzak S, Jayaweera S K. Reinforcement learning based anti-jamming with wideband autonomous cognitive radios[C]//2016 IEEE/CIC International Conference on Communications in China (ICCC). IEEE, 1-5(2016).

[71] Wu Y, Wang B, Liu K J R, et al. “Anti-jamming games in multi-channel cognitive radio networks[J]”. *IEEE journal on selected areas in communications*, 30(1): 4-15(2011).

[72] Xiao L, Wan X, Su W, et al. “Anti-jamming underwater transmission with mobility and learning[J]”. *IEEE Communications Letters*, 22(3): 542-545(2018).

[73] Goekceli S, Cepheli O, Basaran S T, et al. How effective is the artificial noise? Real-time analysis of a PHY

security scenario[C]//2017 IEEE Globecom Workshops (GC Wkshps). IEEE, 1-7(2017).

[74] Yang H, Alphones A, Xiong Z, et al. “Artificial-intelligence-enabled intelligent 6G networks[J]”. *IEEE Network*, 34(6): 272-280(2020).

[75] Kolias C, Kambourakis G, Gritzalis S. “Attacks and countermeasures on 802.16: Analysis and assessment[J]”. *IEEE Communications Surveys & Tutorials*, 15(1): 487-514(2012).

[76] Zou Y, Wang X, Shen W, et al. “Security versus reliability analysis of opportunistic relaying[J]”. *IEEE Transactions on Vehicular Technology*, 63(6): 2653-2661(2013).