photonics

MDPI

Review

Physical Layer Security Techniques for Terahertz Communications Above 100 GHz: A Review

Shenghong Ye *, Ming Che, Yuya Mikami and Kazutoshi Kato

Graduate School of Information Science and Electrical Engineering, Kyushu University, Fukuoka 819-0395, Japan; che.ming.677@m.kyushu-u.ac.jp (M.C.); mikami@ed.kyushu-u.ac.jp (Y.M.); kato@ed.kyushu-u.ac.jp (K.K.)
* Correspondence: ye.shenghong.983@s.kyushu-u.ac.jp; Tel.: +81-92-802-3753

Abstract

Terahertz (THz) communication above 100 GHz is widely recognized as a key enabler for sixth-generation (6G) networks because of its ultra-broad bandwidth and strong directionality. Meanwhile, the rapid evolution of artificial intelligence has considerably weakened conventional cryptographic methods at the network layer, making THz physical layer security increasingly critical. THz links are inherently susceptible to jamming and eavesdropping, which calls for dedicated security mechanisms that integrate physical structures with advanced signal processing. This review summarizes recent advances in two complementary directions. The first addresses signal domain strategies, including frequency hopping spread spectrum techniques, channel modeling, and artificial noise injection, to strengthen confidentiality and robustness against intentional interference. The second focuses on spatial domain strategies, where intelligent reflecting surfaces and beam steering architectures leverage topological diversity to reduce interception risks. This review also discusses the practical challenges these techniques may face in future 6G scenarios and identifies potential directions for further research.

Keywords: terahertz communication; 6G; physical layer security

1. Introduction

The terahertz (THz) band, spanning from 100 GHz to 10 THz, possesses vast bandwidth resources and is considered a strategic key technology for sixth-generation (6G) communication following millimeter-wave (mmW) [1–3]. This area has attracted extensive and in-depth research worldwide. THz band signals possess short wavelengths, and consequently, the corresponding transceivers offer the advantages of high integration and miniaturization. Methods for generating THz signals are categorized into electronics-based and photonics-based approaches. Currently, electronics-based methods utilizing frequency multiplier chains are the standard used to up-convert microwave signals. This method can generate high output power, overcoming obstructions caused by strong atmospheric and water absorption in outdoor environments for long-distance transmission [4]. Conversely, photonics-based methods, which mix two optical signals and down-convert them to the THz band, feature lower phase noise and are thus well suited for high-order modulation schemes [5]. Moreover, photonics-based approaches can be seamlessly integrated with widely deployed optical fiber networks, which facilitates low-cost and rapid deployment [6,7]. In the last few years, THz hardware for wireless communications has evolved into a more complete ecosystem, including highly integrated transceiver front-ends and on-chip links [8–11], high-power and ultra-wideband THz sources together with broadband

Check for updates

Received: 11 December 2025
Revised: 24 December 2025
Accepted: 25 December 2025
Published: 31 December 2025

Copyright: © 2025 by the authors. Licensee MDPI, Basel, Switzerland. This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license.

antenna components [12–15], and large-aperture programmable structures for dynamic beam and propagation control [16,17]. These advances collectively push wireless links around and beyond the 100 Gbit/s regime from purely theoretical projections toward experimental reality. Notably, photonics-aided technologies have recently achieved remarkable milestones in both capacity and distance. In terms of capacity, broadband transmission and multi-user multiple-input multiple-output (MIMO) technologies have pushed data rates beyond 500 Gb/s [18–20]. Simultaneously, transmission ranges have successfully extended from laboratory scales to outdoor kilometer-level links, laying a solid physical foundation for future 6G deployment [21,22].

The rapid development of THz communication technology, characterized by its advantages in having high capacity and long-distance transmission, is poised for practical deployment in several key scenarios:

- Outdoor Long-Distance Scenarios: THz links can serve as wireless fiber extenders to interconnect base stations or buildings over distances of several hundred meters, establishing high-capacity, private wireless links with exceptional directionality. Moreover, vehicles exchange sensor data in high-mobility scenarios. When deployed in stadiums, these links facilitate the real-time broadcasting of mega-scale sporting events, enabling ultra-high-definition video transmission and immersive virtual reality (VR) broadcasting. Furthermore, they are instrumental in establishing temporary high-capacity networks for multi-unmanned aerial vehicle (multi-UAV) and multi-person collaboration during large-scale disaster relief operations.
- Indoor Short-Distance Scenarios: In these environments, high-speed THz links enable users to instantaneously exchange massive files at close range, such as facilitating the real-time collaborative editing of complex 3D engineering models. The technology also supports critical applications like telesurgery that demand high-resolution data transmission with ultra-low latency. Moreover, the ultra-large capacity of THz bands offers a robust solution for scenarios requiring temporary access points with surging traffic demands, such as establishing temporary indoor local area networks (LANs) for large-scale exhibitions and crowded commercial events.

So far, real-time THz communication systems have demonstrated the powerful capabilities and promising vision of THz technology through practical high-resolution video transmission. For instance, Kamiura et al. showcased real-time 4K video transmission using on–off keying (OOK) modulation [23]. Webber et al. further advanced this by demonstrating real-time 8K video transmission, also employing OOK modulation [24]. However, these aforementioned transmissions were limited to indoor scenarios. Then, Liu et al. successfully extended the 8K video transmission distance to 1.26 km with 16-quadrature amplitude modulation orthogonal frequency division multiplexing (16QAM-OFDM) [25]. This system was practically applied in the broadcasting of large-scale sporting events.

These exciting achievements are poised to initiate a wave of translating THz technology from academic research to practical applications. International standardization efforts focusing on THz technology, as evidenced by IEEE 802.15.3 standards [26], have also begun to encompass THz operation specifications from 100 GHz to 300 GHz [27].

However, as the data capacity of THz communication increases, the security challenges faced by the THz channel are also becoming increasingly severe. Especially with the development of artificial intelligence (AI) and quantum computing, communication links protected by conventional computational cryptography are becoming vulnerable. Against this backdrop, THz physical layer security (PLS) technology has garnered significant attention, particularly in the last five years, where a large amount of cutting-edge research has emerged.

Figure 1 illustrates the table of contents (TOC) graphic for this review. To provide a systematic overview, this review classifies the various THz PLS methods into two major types based on the primary physical domain in which the security mechanism operates. The first type, signal-based techniques, focuses on manipulating the waveform properties in the frequency or power domains to confuse potential adversaries. This category includes frequency hopping (FH), environment-adaptive propagation, and noise masking. The second type, spatial-based techniques, exploits the high directionality and propagation geometry of THz waves to physically restrict information leakage. This category covers reconfigurable intelligent surfaces (RIS), secure beamforming, and wavefront hopping.

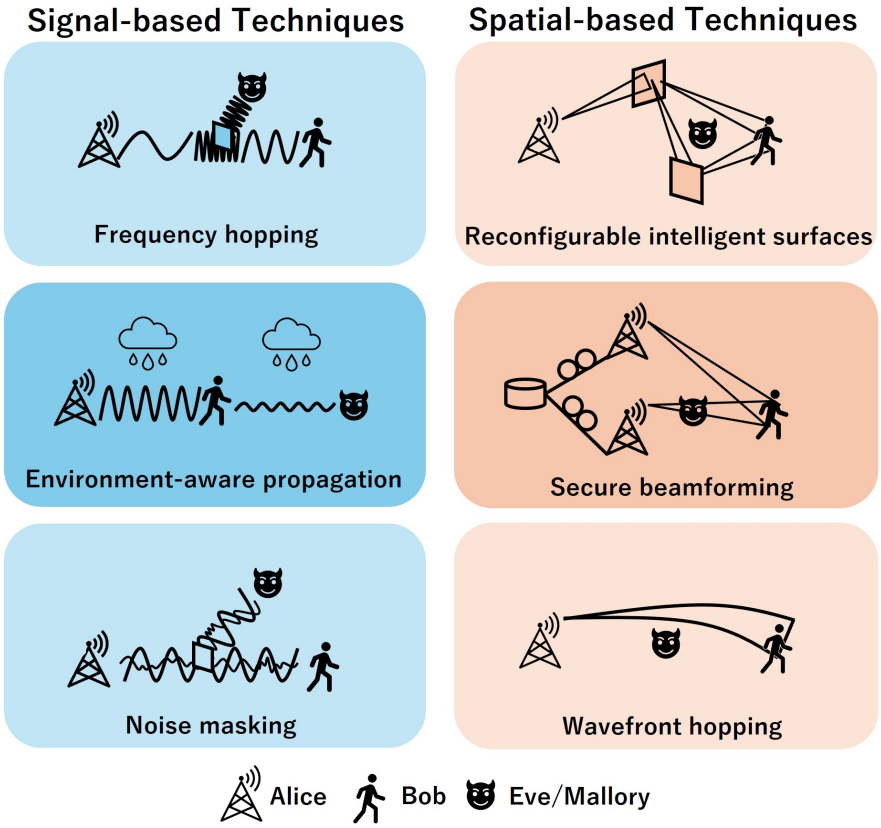


Figure 1. Table of contents for THz PLS technologies.

The remainder of this paper is organized as follows. Section 1 introduces the threat types faced in THz wireless communication. Section 2 introduces the three categories within the first major type, signal-based techniques. Section 3 introduces the three categories within the second major type, spatial-based techniques. Section 4 provides a supplementary discussion of other PLS methods not included in these two major types. Finally, Section 5 provides the conclusion.

2. Threats in THz Communication

THz is generally considered to offer enhanced security compared to microwave and mmW. This perceived security enhancement is attributed to its physical characteristics, such as high directionality and narrow beam width, which significantly reduce the risk of information leakage. However, several studies have revealed the potential threats in the THz band. This section introduces two significant threats faced by THz communication: eavesdropping and jamming. Subsequent sections will then introduce PLS techniques, focusing on their effectiveness in countering these two threats.

2.1. Eavesdropping

Wireless communication is unavoidably exposed to public free space. This exposure provides opportunities for eavesdroppers (Eves) to intercept the signal. Ma et al. revealed that highly directional beams do not guarantee complete protection against eavesdropping [28]. Eves can place an object between the transmitter (Alice) and the receiver (Bob), which causes the radiation to scatter toward an Eve's location. To quantify the effectiveness of eavesdropping attacks, Ma et al. defined the parameter blockage as

$$b = 1 - \frac{\mathrm{SNR}_{\mathrm{Bob}}^{\mathrm{object}}}{\mathrm{SNR}_{\mathrm{Bob}}^{\mathrm{no\ object}}}, \tag{1}$$

and normalized secrecy capacity (SC), as:

$$\bar{c}_s = \frac{\log(1+\mathrm{SNR}_{\mathrm{Bob}}) - \log(1+\mathrm{SNR}_{\mathrm{Eve}})}{\log(1+\mathrm{SNR}_{\mathrm{Bob}})}, \tag{2}$$

where parameter b represents the degree of blockage to the THz path caused by the scatterer, and parameter $\bar{c}_s$ indicates whether Eve has achieved effective eavesdropping by obtaining a signal-to-noise ratio (SNR) comparable to Bob's. Only analyzing $\bar{c}_s$ is misleading. Eve might place a large object to obtain a very low $\bar{c}_s$, indicating highly effective eavesdropping. However, this action would result in a very high b value, leading to immediate detection by Bob. Therefore, both parameters must be analyzed simultaneously. The scenario where both b and $\bar{c}_s$ are simultaneously low poses the most significant threat.

Ma et al. also experimentally demonstrated using metal cylindrical pipes, square planar metal reflectors, and a beam splitter as scatterers with low b and $\bar{c}_s$ [28]. Additionally, scatterers can be placed on the beam's central axis or off-axis for low b. For example, in the outdoor scenario illustrated in Figure 2a, a wireless fiber-THz bridge link between buildings spans a long distance. A drone equipped with a scatterer could invade the THz path, directing the information to the Eve's location. In an indoor situation, as illustrated in Figure 2b, metal cylindrical pipes and square planar metal reflectors can be easily replaced by common items, such as mugs, vacuum flasks, and laptops. Doeker et al. practically evaluated the eavesdropping capabilities of these three object types in an office scenario [29]. The vacuum flask features the lowest $\bar{c}_s$, maintaining this low value regardless of whether the object is placed in line-of-sight (LOS) or non-LOS (NLOS). Taleb et al. further studied the scattering characterization of 50 common building materials, such as glass, stone, and plastics. Although this study did not directly address eavesdropping applications, it revealed the diversity of scatterer choices and the potential for high eavesdropping risks [30]. Li et al. identified the eavesdropping threats in THz NLOS communication scenarios that utilize metallic wavy surfaces (MWSs). An MWS scatters the input THz signal into multiple high-intensity lobes. While only one lobe is directed at Bob, the remaining lobes provide Eves with multiple exploitable, high-quality eavesdropping points [31]. This threat persists even when the MWS is concealed by common indoor materials like wallpaper, curtains, or wall plaster [32]. The vulnerability also extends to outdoor environments. Li et al. simulated rain scenarios and demonstrated that neither raindrops in the transmission path nor raindrops adhering to the MWS prevent eavesdropping. Eves can find a specific surface rotation angle that achieves a low b and $\bar{c}_s$ [33]. All these studies indicate that THz eavesdropping threats are everywhere in daily life. Therefore, anti-eavesdropping techniques in PLS are an urgent research topic.

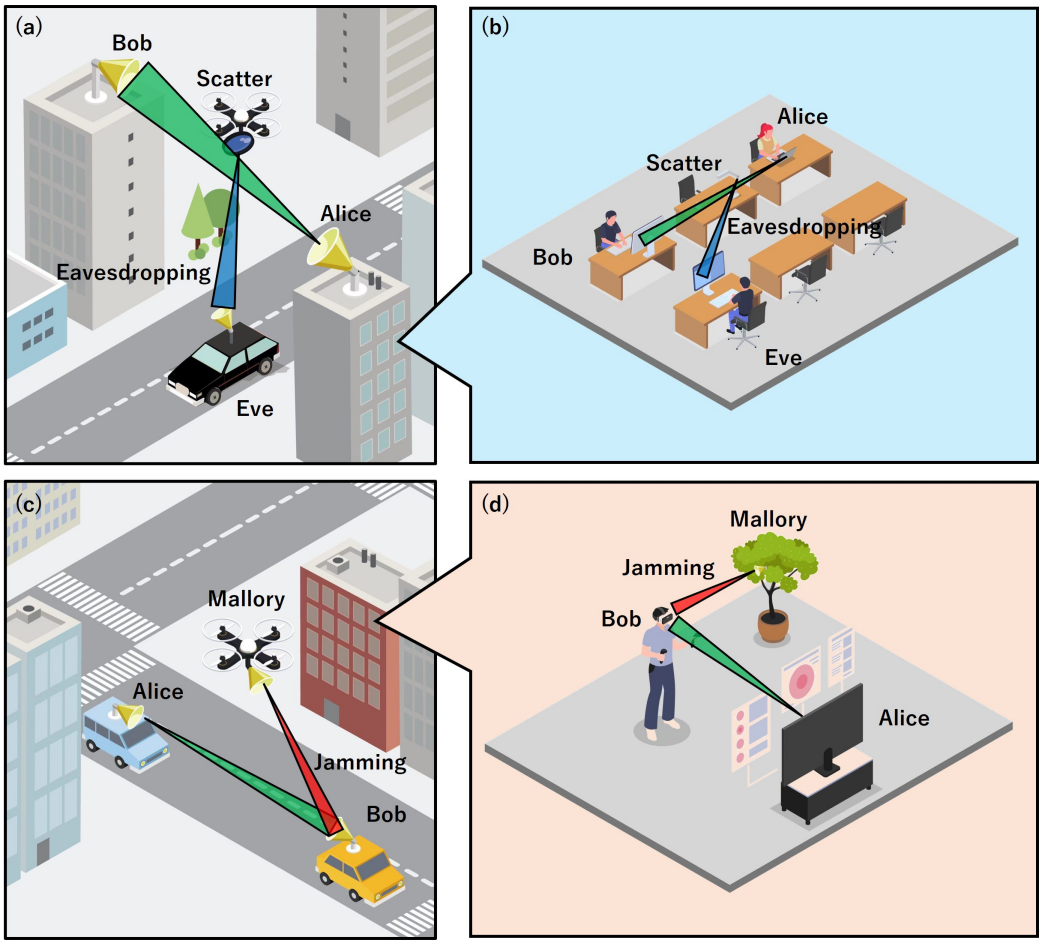


Figure 2. Typical situations of THz threats. (**a**) Outdoor eavesdropping. (**b**) Indoor eavesdropping. (**c**) Outdoor jamming. (**d**) Indoor jamming.

2.2. Jamming

In addition to the information leakage threat from eavesdropping, Shrestha et al. also pointed out a threat aimed at completely destroying the link, known as jamming. Unlike the interference risk present in multi-user scenarios, jamming is more intentional [34]. Figure 2c illustrates a possible outdoor jamming scenario. In this case, the jammer (Mallory) does not attack the THz path between the communicating vehicles. Instead, Mallory directly attacks Bob's receiving antenna, achieving jamming by overwhelming the original signal or by transmitting erroneous signals. The indoor jamming scenario shown in Figure 2d also presents a significant disruptive threat. This threat is primarily because Bob, the legitimate user, is in an exposed position. In contrast, Mallory operates from a concealed location and can access or leave the network at will, making the attack highly threatening. Shrestha et al. also defined a parameter to quantitatively evaluate the severity of the jamming threat, the jamming efficiency e_j, as follows [34]:

$$e_j = \frac{\log \mathrm{BER}_{\mathrm{Unjammed}} - \log \mathrm{BER}_{\mathrm{Jammed}}}{\log \mathrm{BER}_{\mathrm{Unjammed}} - \log \mathrm{BER}_{\mathrm{Limit}}}. \tag{3}$$

This parameter is similar to $\bar{c}_s$ but uses bit error rate (BER) instead of SNR, making it more practical for engineering purposes. The chosen value of $\mathrm{BER}_{\mathrm{Limit}}$ is also based on the stringency of the system under test, which is typically set to the standard forward error correction (FEC) limit of 10^{-3} [34]. A higher e_j value indicates that the attack from Mallory is more effective, and a value of 1 signifies a completely destructive attack.

Priyadarshani et al. classified multiple possible jammer types based on Mallory's timing characteristics and interaction methods with Alice and Bob. The first type is the proactive jammer [35]. This jammer actively transmits high-power noise or spoofing information to jam Bob continuously. Alternatively, it may randomly start and stop its jamming transmissions to conserve energy, as continuous jamming would cost significant power. An active jammer generally succeeds by transmitting a jamming signal that is the same frequency as Alice. This appears difficult to achieve in the ultra-wide THz band. However, beat jamming can possess a much wider frequency range for successful jamming in THz non-coherent communication. Although Mallory's beat jamming emits the same single-tone jamming signal as a basic proactive jammer, the attack mechanism is different. Nallappan et al. pointed out that beat jamming is achieved as long as the frequency difference between its signal and the legitimate carrier frequency is less than the output bandwidth of the THz non-coherent receiver [36]. This proximity in frequency causes mixing and generates an unwanted beat signal, which successfully jams the link. Shrestha et al. also pointed out that a proactive jammer transmitting spoofing information can achieve modulated jamming. This is because the modulated signal will be retained in the baseband by a THz non-coherent receiver, regardless of whether the transmission carrier frequency matches. Another type identified by Priyadarshani et al. is advanced jammers, such as the follow-on jammer. The follow-on jammer can continuously monitor the channel, following Alice as she switches to new frequencies. The scattering objects used for eavesdropping, discussed in Section 2.1, can thus assist a follow-on jammer in obtaining the correct frequency information of the legitimate link.

The high data rate of THz communication means that information loss from jamming, even over extremely short durations, can be substantial. This will severely impact critical applications that rely on THz communication as a backbone, such as autonomous driving and telesurgery. Therefore, the development of anti-jamming techniques is just as indispensable as anti-eavesdropping techniques.

3. Signal-Based PLS Techniques

3.1. Frequency Hopping (FH)

FH is a classic PLS technique. It achieves secure communication by rapidly and pseudo-randomly changing the carrier frequency across a predetermined hopping code of frequency carriers [37]. Alice and Bob share a secret hopping code to maintain synchronization, while Eves or Mallorys cannot predict the next hop frequency carrier. This provides strong anti-eavesdropping and anti-jamming capabilities. FH is already mature and commercially used in Bluetooth and WiFi. The THz band, however, possesses a vast bandwidth range. This forces jammers to guess within an enormous frequency space, making the security enhancement provided by FH even more significant. However, implementing FH in the THz band faces severe challenges. While electronics-based methods offer advantages in output power, their hopping range is constrained by frequency multipliers, so is limited to several tens of GHz. In contrast, photonics-based THz generation technology, based on the principle of photomixing, has become the preferred solution for achieving wideband THz FH. In this scheme, two lasers with optical frequencies f_1 and f_2 are photomixed on a photodetector, such as a uni-traveling carrier photodiode (UTC-PD). This generates a THz carrier with a frequency of $f_{THz} = |f_1 - f_2|$.

To theoretically analyze the anti-jamming capability of FH against single-tone attacks in THz non-coherent systems, we assume Alice transmits a modulated signal with amplitude A_A and center frequency f_A, while the Mallory launches an attack using a high-power single-tone THz signal at frequency f_M with amplitude A_M. These two THz signals are mixed and square-law-detected at Bob. The ideal noise-free output signal is expressed as

$$U_B = |A_A u_A(t) \cos(2\pi f_A t + \phi_A) + A_M \cos(2\pi f_M t + \phi_M)|^2. \quad (4)$$

In a non-coherent system, phase information ϕ_A and ϕ_M, as well as the direct current components, can be ignored. Therefore, the detected signal simplifies to

$$U_B = \frac{A_A^2 u_A(t)^2}{2} + A_A A_M u_A(t) \cos(2\pi \Delta f t), \quad (5)$$

where $\Delta f = f_A - f_M$ represents the frequency difference between Alice and Mallory. The second term in Equation (5), $A_A A_M u_A(t) \cos(2\pi \Delta f t)$, represents the beat jamming component. This component effectively generates an interference signal with a center frequency of Δf and a bandwidth identical to that of the legitimate signal $u_A(t)$.

High-speed communication systems are particularly vulnerable because their wide signal bandwidth increases the likelihood that the beat jamming component overlaps with the original signal spectrum. The FH scheme counteracts this by dynamically shifting Alice's carrier frequency f_A, which results in a variation of Δf. By implementing a sufficiently wide frequency hop, the system ensures that Δf is large enough to shift the entire beat jamming spectrum outside of Bob's receiver bandwidth. Consequently, the interference can be effectively filtered out, allowing the original signal to be recovered cleanly.

Therefore, by rapidly tuning the lasing frequency of one of the lasers, THz carrier frequency hopping can be achieved. The tuning range of light is wide and flexible. This allows the theoretical FH range to span hundreds of GHz or even cross dual-band. The core bottleneck of photonics-based FH technology is the laser's wavelength tuning speed, known as the transition time. Communication must be paused during this frequency switching, but a long transition time compresses the dwell time available for data transmission, thereby severely reducing communication efficiency. To maintain constant communication efficiency, a longer transition time forces the dwell time to also become longer, leading to a reduction in the FH rate and the FH system then remaining on a single carrier frequency for too long. If eavesdropping or jamming occurs during this period, a large amount of information will be continuously leaked or jammed. Furthermore, the number of FH carriers and the FH interval are both important metrics. Increasing the number of FH carriers can enhance the randomness and complexity of the FH system. A wide FH interval allows for maximum separation from an eavesdropping band. In non-coherent communication, this also helps to completely escape the increasingly wide beat jamming range.

Nallappan et al. pioneered the use of wavelength tunable distributed feedback lasers (DFB-LD) to implement THz FH with OOK modulation for jamming avoidence, as shown in Figure 3A [36].

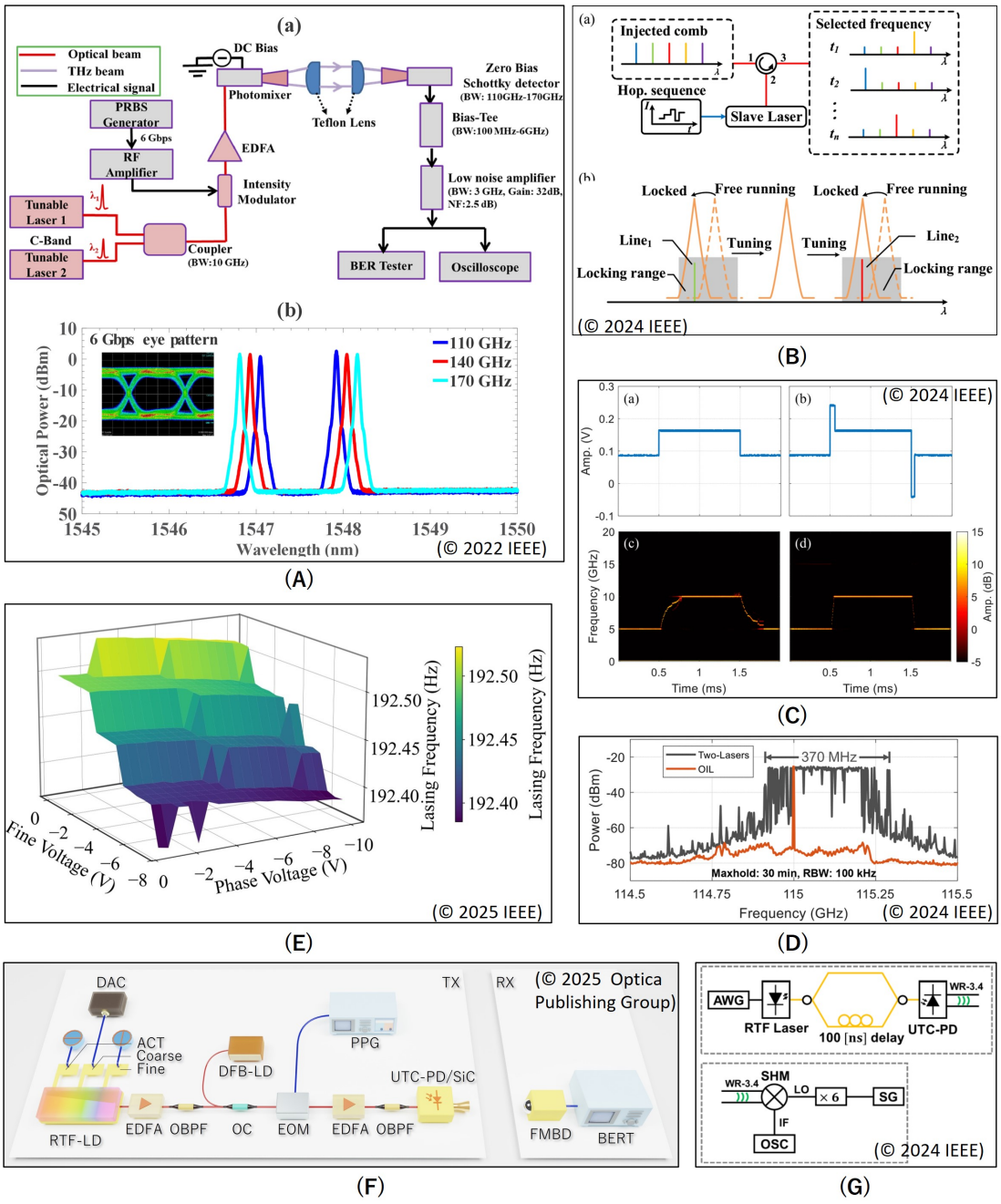


Figure 3. (**A-a**) FH system setup based on two DFB-LD [36]. (**A-b**) The modulated optical spectra of the two tunable DFB-LDs for THz generation with optical eye pattern of 6 Gbps communication. (**B**) FH enabled by OIL [38]. (**C-a**) Current control signal without turbo pulse. (**C-b**) Time-frequency diagram of FH signal without turbo pulse. (**C-c**) Current control signal with turbo pulse. (**C-d**) Time-frequency diagram of FH signal with turbo pulse [38]. (**D**) Improved frequency stability by OIL [38]. (**E**) Relationship among Fine voltage, Phase voltage, and lasing frequency of the RTF-LD [39]. (**F**) Experimental setup of [40]. (**G**) Experimental setup of [41]. PRBS: Pseudo-random binary sequence; EDFA: Erbium-doped fiber amplifier; BER: Bit error rate; OIL: Optical injection locking; RBW: Resolution bandwidth; DAC: Digital-to-analog converter; ACT: Active layer; RTF-LD: Reflection-type transversal filter laser; OBPF: optical bandpass filter; DFB-LD: distributed feedback laser; OC: Optical coupler; EOM: electro-optic modulator; PPG: Pulse pattern generator; UTC-PD/SiC: Uni-traveling-carrier photodiode based on SiC substrate; FMBD: Fermi-level managed barrier diode; BERT: BER tester; AWG: Arbitrary waveform generator; SHM: Subharmonic mixer; OSC: Oscilloscope; SG: Signal generator.

Limited by the ms-level tuning speed of DFB-LDs, which is based on the thermo-optic (TO) effect, this scheme first employs a form of chirp spread spectrum (CSS). The CSS system linearly sweeps the lasing frequency to tune the THz carrier frequency output by the UTC-PD. Lyu et al. pointed out that in widely studied integrated sensing and communication (ISAC) technology, a single-carrier ISAC that modulates signals onto the swept-frequency components used for frequency-modulated continuous-wave (FMCW) radar can also be considered a CSS system, offering enhanced security [42,43]. However, linearly swept signals have a predictable pattern, making them difficult to hide. Li et al. employed a tunable distributed feedback laser array (TLA) [44,45]. This scheme achieves wavelength switching by rapidly changing the injection current of individual DFB lasers within the TLA. The system successfully demonstrated 10-carrier FH with 10 GHz interval in the 300 GHz band, and applied OOK communication at each individual carrier frequencies. This approach offers higher integration and lower cost. However, its underlying principle still relies on the TO effect, limiting the hopping rate to only 100 hops/s. Yang et al. proposed a scheme based on optical injection locking (OIL) [38,46]. This scheme uses an optical frequency comb (OFC) as a master laser to provide a set of stable frequency references. A slave DFB laser is tuned by adjusting its current, causing it to lock onto a specific comb line from the OFC. FH is realized by adjusting the current to lock the slave laser to different comb lines, as shown in Figure 3B. Furthermore, Yang et al. applied a pre-emphasis current control signal named a "turbo pulse" to accelerate the thermal response, as shown in Figure 3C. This enabled a faster hopping rate of 1 khops/s with TO-effect-based DFB-LD. As shown in Figure 3D, OIL further improved frequency stability. This system successfully demonstrated 5-carrier FH with a 5 GHz interval in the 100 GHz band, and first applied off-line quadrature phase shift keying (QPSK) communication in the THz FH system.

To pursue a faster hopping rate, Ye et al. adopted a high-speed electro-optic (EO) effect wavelength tunable laser: the reflection-type transversal filter laser (RTF-LD). The RTF-LD utilizes the EO effect rather than the TO effect to change the refractive index, achieving an extremely fast response speed. The RTF-LD has multiple tuning electrodes with different step lengths. The relationship among the Fine electrode, the Phase electrode, and the lasing frequency is shown in Figure 3E. The Phase electrode alone can achieve multiple FH carriers, but the interval is small [47]. The Fine electrode alone can achieve FH with an interval as high as 40 GHz [40,48], whose system configuration is shown in Figure 3F. Although the number of FH carriers implemented is currently small, the FH interval of up to 40 GHz exceeds the bandwidth of common THz receivers such as Schottky barrier diodes (SBD) or Fermi-level managed barrier diodes (FMBD). This shows great promise for anti-jamming in non-coherent communication. Benefiting from the EO effect, a record-breaking hopping rate of up to 75 Mhops/s was achieved, which is possible against follow-on jammer [49]. Furthermore, a scheme using the Fine electrode for FH while simultaneously using the Phase electrode for frequency shift keying (FSK) modulation not only achieves anti-eavesdropping FH but also saves the system's need for an external modulator [39,50]. Masutomi et al. proposed a novel architecture using only one RTF laser and a delayed self-multiplexer, as shown in Figure 3G [41,51]. By switching the laser between three lasing frequencies and using delayed interference, the system ensures that only two lightwave frequencies are photomixed during each hopping interval. These pairings are continuously rotated. This achieves a low-cost, low-energy THz FH system.

However, regardless of the hardware scheme, pausing communication during the transition time is inevitable and requires coordination from the link layer and the data layer. Consequently, current research has primarily focused on independent communication performance measurements at individual carrier frequencies or offline evaluations. Recently,

FH and real-time OOK communication by leveraging an ultra-high hopping rate was achieved [49], but achieving simultaneous frequency hopping with real-time high-order modulation remains challenging.

A performance comparison of the aforementioned THz FH systems is summarized in Table 1. Besides the aforementioned techniques, other technologies have achieved high-speed FH in the microwave and mmW bands. Examples include utilizing the period 1 and period 2 dynamic effects of semiconductor lasers [52,53] or using high-speed EO modulators [54,55]. Further increasing the FH range could also allow these technologies to be applied in the THz domain.

Table 1. Performance comparison of various THZ FH systems.

Reference	Year	Frequency (GHz)	FH Interval (GHz)	Number of FH Carrier	Hopping Rate (hops/s)	Communication
[36]	2022	110–170	–	–	–	Per-carrier OOK
[45]	2024	288–331	8	10	100	Per-carrier OOK
[46]	2024	115–140	5	5	1 k	Off-line OOK
[38]	2024	115–140	5	5	1 k	Off-line QPSK
[47]	2024	301.0–305.5	0.6	8	20 M	–
[41]	2024	286–321	35	2	5 M	–
[40]	2025	240–320	40	3	5 M	Per-carrier OOK
[39]	2025	230–310	40	3	5 M	Per-carrier FSK
[49]	2025	235–275	40	2	75 M	Real-time OOK

3.2. Environment-Adaptive Propagation

Environment-adaptive propagation also controls the carrier frequency. Unlike FH, which rapidly and randomly hops the carrier frequency during communication to achieve spectrum spreading, environment-adaptive propagation emphasizes selecting the most secure carrier frequency based on the environmental conditions. This technique leverages the unique molecular absorption of the THz channel, which is highly frequency-dependent and distance-dependent, creating strong attenuation peaks, particularly due to water vapor [56]. The water vapor absorption loss (WVAL) grows exponentially with distance and increases more rapidly than free-space path loss (FSPL), as shown in Figure 4a.

To mathematically quantify the security gain provided by environment-adaptive propagation, we analyze the total path loss in the THz band, which consists of the FSPL and the WVAL. Both components depend on the transmission distance d and the carrier frequency f. The FSPL is determined by the Friis transmission formula:

$$\mathrm{FSPL} = 20\left(\log d - \log f + \frac{1}{2}\log\frac{c^2}{A_r A_t}\right) \quad (\mathrm{dB}), \tag{6}$$

where A_r and A_t are the effective areas of the receiver and transmitter antennas, respectively, and c is the speed of light. The slope of FSPL with respect to the logarithm of distance is constant:

$$\frac{\partial \mathrm{FSPL(dB)}}{\partial(\log d)} = 20 \quad \mathrm{dB/decade}. \tag{7}$$

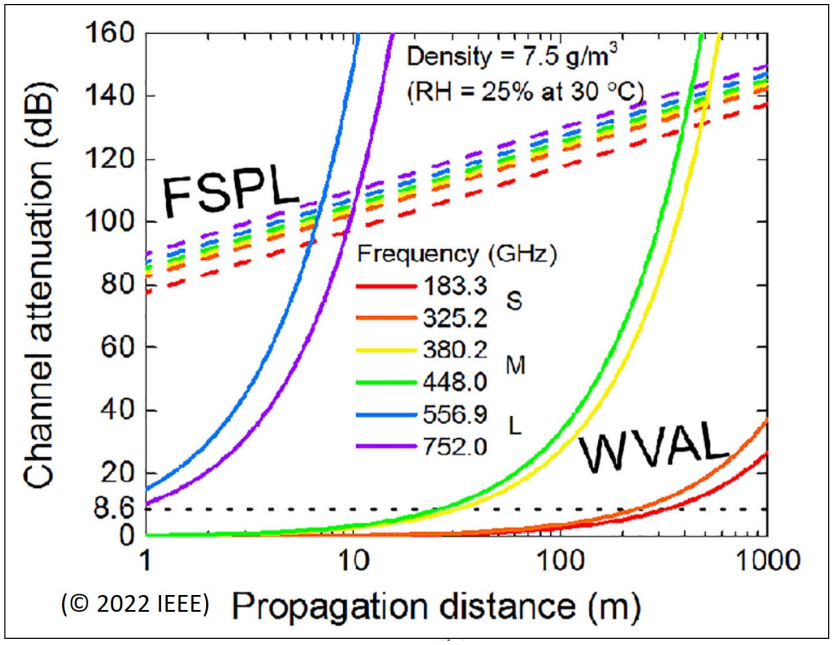
In contrast, the unique security feature of THz communications arises from the WVAL, which grows exponentially with distance according to Beer's law. In the logarithmic decibel scale, this linear relationship is expressed as

$$\mathrm{WVAL} = 4.3 G_c(f) \cdot \mathrm{RH} \cdot d \quad (\mathrm{dB}), \tag{8}$$

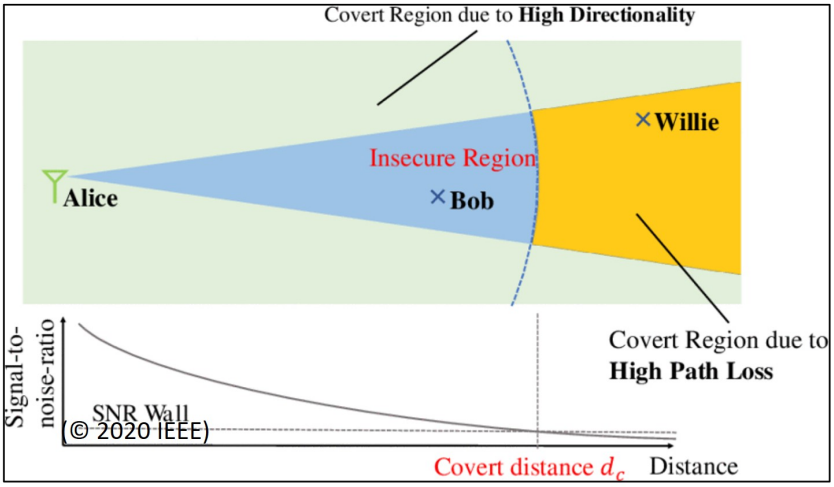
where RH represents the relative humidity, and $G_c(f)$ is the frequency-dependent molecular absorption coefficient, typically modeled by the van Vleck–Weisskopf lineshape function. By selecting a carrier frequency f that aligns with an absorption peak, the attenuation slope behaves differently from FSPL:

$$\frac{\partial \mathrm{WVAL(dB)}}{\partial(\log d)} = \frac{\mathrm{WVAL}}{0.43} \quad (\mathrm{dB/decade}). \tag{9}$$

Equation (9) indicates that unlike the constant slope of FSPL, the attenuation rate of WVAL increases proportionally with the total absorption loss. Consequently, at absorption peaks, the signal strength drops precipitously beyond a certain distance. This physical phenomenon allows Alice to define a precise "secure zone" where the signal is strong enough for Bob but attenuates below the detection threshold for a distant Eve.



(a)



(b)

Figure 4. (**a**) Channel attenuation versus propagation distance with selected frequencies corresponding to the peaks of water vapor absorption lines, in an atmosphere with water vapor density of 7.5 g/m^3 (i.e., relative humidity of 25%) and temperature of 30 °C [56]. (**b**) Illustration of SNR wall and eavesdropping distance [57]. RH: Absorption coefficient. Willie: Eavesdropper.

Alice can exploit this physical property and tune the carrier frequency to be on or near one of these absorption peaks. This action significantly attenuates the signal for a farther Eve while keeping the link viable for the closer Bob. This mechanism effectively restricts the signal's broadcast range. This strategy is formalized in techniques like distance-adaptive absorption peak modulation (DA-APM) or distance-adaptive absorption peak hopping (DA-APH) [57,58]. The primary goal is to minimize the eavesdropping distance, as shown in Figure 4b. The DA-APM framework involves an optimization process to select hopping frequencies that are at the molecular absorption peaks, which traditional communication systems typically avoid. The system then optimizes parameters such as power allocation and pulse-combining gain for these selected sub-bands to meet reliability, power, and covertness constraints. Gao et al. demonstrated through numerical results that this DA-APM approach can reduce the eavesdropping distance by approximately 60% compared to a random frequency selection method. The distance-dependent bandwidth variation is a fundamental challenge for THz links. Hall et al. experimentally demonstrated an adaptive THz physical layer using deep learning. They trained a convolutional neural network (CNN) for autonomous modulation and bandwidth classification (MBC). This adaptability enhances security by making transmission parameters flexible and less predictable for adversaries [59].

3.3. Noise Masking

This category of techniques leverages noise properties, either by injecting AN or by generating noise-like information signals, to mask the legitimate communication from eavesdroppers.

Artificial noise (AN) is a prominent PLS technique where a carefully designed noise signal is superimposed on the information signal. This noise is intended to be nullified at or have minimal impact on Bob while simultaneously acting as significant interference at Eve, thereby degrading the wiretap channel. Traditional transmitter-based AN (Tx-AN) often uses multi-antenna beaming to protect Bob. He et al. investigated the effectiveness of Tx-AN against a specific threat where Eve uses a scatterer placed inside the THz path to intercept signals, as shown in Figure 5a [60]. By analyzing the secrecy transmission probability (STP) and $\bar{c}_s$, they demonstrated that Tx-AN is an effective countermeasure and analyzed the optimal power allocation. However, Tx-AN becomes ineffective in THz communications when Eve herself is in the THz path, as the legitimate and eavesdropping channels become highly correlated. To address this, Gao et al. proposed a receiver-based AN (Rx-AN) scheme where Bob transmits the AN, as shown in Figure 5b [61]. While this avoids the channel correlation problem, it traditionally requires high-complexity self-interference cancellation (SIC) hardware, which is challenging and costly in the THz band. Gao et al. also proposed an SIC-free Rx-AN scheme that cleverly exploits the temporal broadening effect (TBE), a unique property of THz channels [62]. In this mechanism, THz pulses naturally broaden in the time domain as they propagate due to frequency-selective absorption, with the effect becoming more pronounced over longer distances. At Bob, the self-interference AN path is extremely short, causing negligible TBE and keeping the AN pulse sharp. Conversely, the AN path to Eve is much longer, causing the AN pulse to broaden significantly and interfere with the information signal. Bob can then use a specific detection period to receive the information pulse, temporally avoiding his own sharp AN pulse and eliminating self-interference without any SIC hardware. Gao et al. further extended this to a randomly distributed eavesdropper scenario, using a deep neural network (DNN) to solve the complex non-convex optimization problem of minimizing the secrecy outage probability (SOP) [62]. This DNN-powered approach optimizes parameters like carrier frequency, power, and frame time. AN techniques have also been adapted for

network-level and hardware-specific challenges. Tian et al. proposed a blockage feature-based AN (BF-AN) for indoor networks, where APs that have an NLoS link to the user are selected to transmit AN [63]. This effectively jams eavesdroppers without interfering with the user's primary LoS link. Furthermore, He et al. investigated the impact of non-ideal hardware, specifically imperfect analog-to-digital converter (ADC) sampling [64]. They identified that synchronization noise from timing errors and quantization noise from limited resolution create a trade-off. Under ADC power constraints, increasing the sampling rate reduces synchronization noise but increases quantization noise, but an optimal sampling rate exists to maximize security.

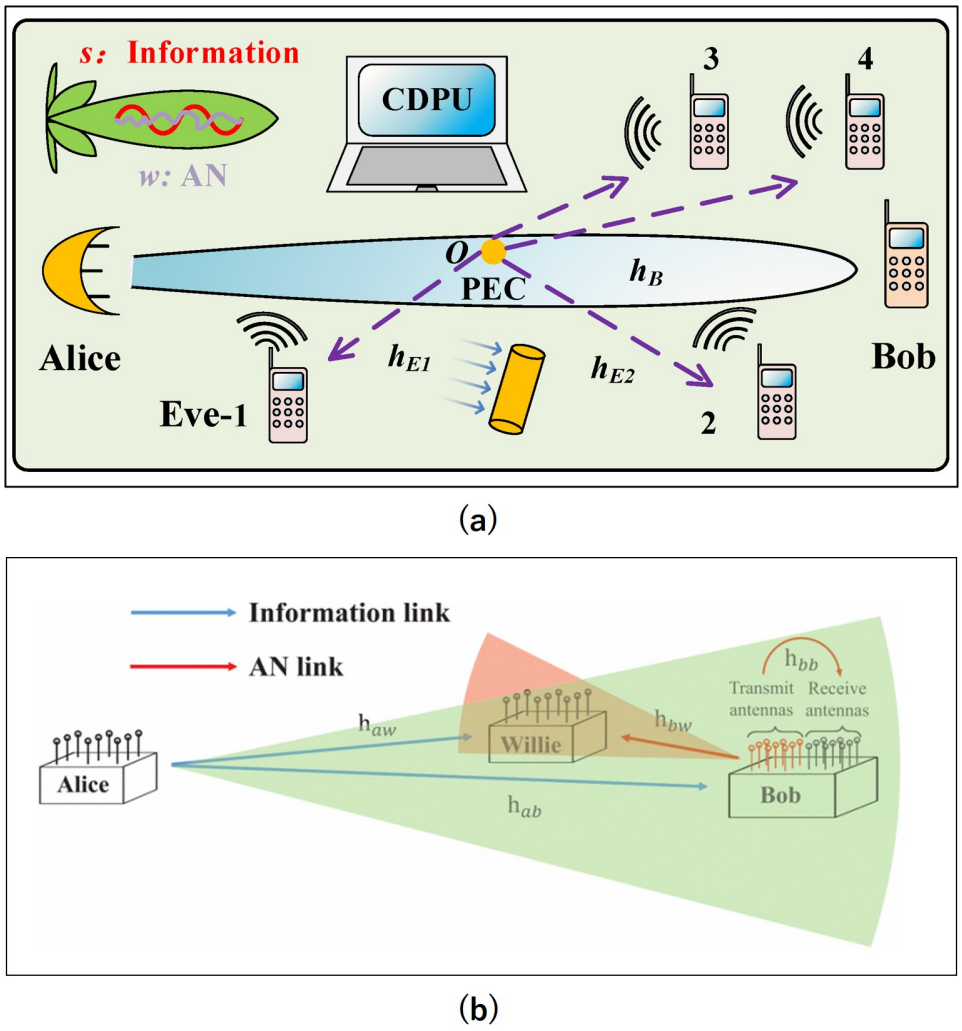


Figure 5. (**a**) System model: Alice transmits a highly directive THz information s to Bob with or without AN w. A PEC located at the edge of the beam can scatter the incident THz wave to Eves in all directions [60]. (**b**) Illustration of a wiretap channel with receiver-based AN [61]. h_B: channel between Alice and Bob; h_{Ei}: channel between Alice and the i-th Eve; CDPU: Central data processing unit; PEC: Perfect electric conductor.

Besides injecting artificial noise, another paradigm is to mask the data by making the information signal itself resemble noise, often referred to as random communication. Deng et al. utilize physical chaos generated from a nonlinear photonic cavity [65]. This analog chaos signal directly masks the low-amplitude plaintext data. The legitimate receiver then uses a pre-shared, trained NN to perform chaos synchronization, reconstruct the chaos, and recover the original message. Chen et al. propose a digital chaos scheme where secret keys, the initial values of a multi-scroll chaotic system, generate pseudo-random sequences [66].

In digital chaos-based security schemes, the core mechanism involves generating a PRBS from a continuous chaotic system to mask the information signal. Assuming a chaotic sequence $\{z\}$ is generated by a multi-scroll chaotic map, the binary sequence $\{z'\}$ required for bit-level XOR encryption can be derived as follows:

$$z'_i = \mathrm{mod}(\mathrm{Extract}(z_i, m), 2), \tag{10}$$

where the function $\mathrm{Extract}(z_i, m)$ extracts the m-th digit from the decimal part of the chaotic state value z_i, returning an integer ranging from 0 to 9. The modulo operation $\mathrm{mod}(a, b)$ returns the remainder of a divided by b. By performing this operation, the continuous chaotic values are quantized into a binary stream of 0 s and 1 s. To ensure randomness and sensitivity to initial conditions, while accounting for the finite computing precision of digital processors, a typical value for m is set to 15. This generated PRBS $\{z'_i\}$ is then XORed with the plaintext bits, effectively masking the data with noise-like characteristics that are computationally infeasible to predict without the exact initial secret keys.

In encryption, a bit-level XOR operation is performed, and then constellation masking is carried out by adding chaotic sequences to the I/Q values. Moreover, some schemes base their security on the principles of quantum physics. Ottaviani et al. explored the feasibility of THz quantum key distribution (QKD) [67]. This technique uses quantum mechanics to provide an unconditionally secure way for Alice and Bob to negotiate a shared secret key. Zhang et al. proposed a direct quantum noise secured communication scheme [68]. This scheme uses a shared key to drive a high-order diffusion algorithm, mapping QPSK to 65536-PSK. At such a high order, the distance between adjacent symbols becomes smaller than the system's inherent quantum noise. For Eve, who does not have the key, the signal is completely masked by quantum noise and cannot be deciphered. Bob, however, possesses the key and can perform the inverse-diffusion operation to successfully recover the data.

3.4. Comparative Analysis of Signal-Based Techniques

To provide a holistic view of the applicability of signal-based PLS techniques in practical 6G scenarios, we compare them in terms of security mechanism, hardware complexity, real-time feasibility, and robustness against mobility, as summarized in Table 2.

- Implementation complexity and real-time feasibility: FH imposes strict requirements on hardware agility. Achieving Gbit/s-level secure transmission requires tunable lasers with nanosecond-level switching speeds and precise synchronization between Alice and Bob. AN, particularly receiver-based schemes, faces high complexity due to the need for SIC hardware and high-precision ADCs to prevent the noise from overwhelming the legitimate signal. In contrast, environment-aware propagation is the most hardware-efficient, as it primarily relies on intelligent carrier frequency selection and power control algorithms without requiring additional active optical components.
- Mobility and robustnes: FH exhibits high robustness against mobility because the rapid switching of frequencies inherently provides frequency diversity, mitigating the fading effects caused by user movement. Environment-aware propagation techniques are moderately sensitive to mobility. Since absorption loss is distance-dependent, a moving user changes the secure transmission window, requiring adaptive modulation updates. AN is the most sensitive to mobility, especially in near-field scenarios, as the movement of the receiver can alter the channel correlation properties, potentially rendering the pre-calculated null-space noise ineffective or even harmful to the legitimate user.

Table 2. Comparison of signal-based PLS techniques in THz communications.

Technique	Primary Security Mechanism	Implementation Complexity	Real-Time Feasibility	Mobility Tolerance
FH	Rapidly changing carrier frequency to avoid jamming or eavesdropping.	**High**: Requires ultra-fast tunable lasers and strict synchronization.	**Medium**: OOK achieved but high-order modulation remains challenging.	**High**: Frequency diversity mitigates fading; less sensitive to pointing errors.
Environment-adaptive propagation	Utilizing molecular absorption to limit range.	**Medium**: Relies primarily on carrier frequency selection and power control.	**High**: Feasible with standard adaptive modulation schemes.	**Medium**: Distance changes require dynamic updates to modulation schemes.
Noise masking	Injecting noise to degrade Eve's SINR and Signal mimics noise characteristics.	**High**: complex SIC and synchronization of chaotic maps required.	**Medium**: Constraints on ADC precision and SIC latency limits speed.	**Low**: Highly sensitive to channel correlation changes caused by movement.

4. Spatial-Based PLS Techniques

4.1. Reconfigurable Intelligent Surfaces (RIS)

Compared with conventional RF systems, terahertz links offer inherently stronger spatial confidentiality and lower passive interception probability owing to their narrow beams and severe path loss. However, their susceptibility to blockage undermines link reliability and introduces new security vulnerabilities in reflection paths and beam-control signaling, making physical-layer protection both more crucial and more complex. To mitigate these risks, reconfigurable intelligent surfaces (RIS) have been proposed [69–71]. RIS technology programmably manipulates the propagation environment. This capability shifts part of the security function from encryption-based post-processing directly to the physical layer by enabling energy focusing, leakage suppression, controlled channel decorrelation, and reflective path reconfiguration.

A joint optimization framework under discrete RIS phase constraints was developed to enhance physical-layer security in THz multiple-input single-output (MISO) systems [72], as shown in Figure 6a. The secrecy rate is maximized by alternately optimizing the base-station precoder and the RIS reflection coefficients: the precoder is obtained via the Rayleigh–Ritz generalized eigenvector method, while the discrete RIS phases are directly selected from a finite set using a cross-entropy (CE) search strategy. This discrete-domain optimization avoids the conventional "continuous design followed by quantization" pipeline, thereby improving implementation feasibility without sacrificing security performance. Simulation results further demonstrate that the secrecy rate monotonically increases with the number of RIS elements, as shown in Figure 6b, and that the proposed discrete-phase design can approach the performance of continuous-phase schemes despite limited phase resolution. Complementing the discrete-phase perspective above, a continuous-phase dual-path framework has also been investigated [73]. One branch is a low-complexity sequential design (SD) grounded in LoS matching, while the other is a higher-performance joint design (JD) that integrates the Dinkelbach transformation with an alternating direction method of multiplier (ADMM)-based solver. Methodologically, SD emphasizes implementability via closed-form updates, whereas JD provides interpretable iterative updates with convergence considerations. Empirically, under generalized channel models that span both mmWave and THz regimes, both designs verify the benefit of RIS assistance for spatial secrecy while

operating entirely in the continuous phase domain without quantization constraints. Together, these two studies show that RIS can significantly enhance physical-layer security in THz MISO systems. Even under limited phase resolution, near-optimal secrecy-rate performance can still be achieved.

Recent work has extended this line of research to more general MIMO architectures, as shown in Figure 6c. In particular, RIS has been integrated with MIMO-nonorthogonal multiple access (NOMA) and hybrid precoding structures to support spatial multiplexing and secure multi-cluster transmission [74]. Users are first grouped based on channel correlation, and cluster-head users are selected. Discrete-phase analog precoding and zero-forcing digital precoding are then jointly designed to suppress both intra- and inter-cluster interference. Under total power and minimum-rate constraints, an alternating-optimization framework iteratively updates power allocation and RIS phase shifts to maximize the sum secrecy rate (SSR). Simulation results verify that passive RIS beamforming effectively suppresses eavesdropping, and further reveal a performance–efficiency trade-off: the fully connected hybrid precoder achieves higher SSR, while the sub-connected structure offers superior secrecy energy efficiency, as illustrated in Figure 6d. Compared with earlier single-user MISO designs, this work advances toward system-level secure THz transmission, supporting multi-cluster operation and more practical architectural constraints.

In addition to model-driven RIS optimization for secrecy enhancement, several complementary directions have emerged that broaden the design space toward practical and intelligent secure THz systems. A first line of work leverages channel randomization and opportunistic user scheduling to secure THz links without requiring real-time RIS control, where pre-generated RIS reflection patterns are reused across uplink and downlink to induce channel decorrelation and hinder interception while maintaining transmission reliability [75]. Unlike iterative beamforming-centric designs, this strategy emphasizes low-overhead system-level robustness, making RIS-enabled security more feasible for dynamic environments. A second direction introduces learning-driven RIS control, where deep neural architectures learn near-optimal reflection and beamforming policies under multi-user THz settings, achieving secrecy-energy efficiency close to genie-aided upper bounds without relying on convex optimization [76]. This paradigm shift toward intelligent RIS adaptation highlights the role of AI in future secure 6G deployments. Moreover, research on artificial-noise-assisted THz transmission demonstrates that purposeful jamming and interference injection can further suppress eavesdropping in highly directional THz channels, providing an orthogonal protection mechanism that complements RIS-based wavefront engineering [77]. Collectively, these studies move beyond purely deterministic optimization and point toward hybrid secure architectures that combine programmable propagation, learning-enabled control, and interference-domain defense to address realistic deployment constraints and high-mobility threats in next-generation THz systems.

Beyond point-to-point terrestrial settings, the propagation characteristics and channel constraints in different THz deployment scenarios fundamentally shape RIS design and optimization. For aerial networks, Kim et al. proposed a secure RIS-assisted UAV communication framework that integrates deep learning to adaptively configure RIS reflection phases and transmit beamforming [78]. This approach significantly enhances secrecy rate and energy efficiency in highly dynamic, NLoS UAV–ground links, demonstrating the security potential of RIS in airborne environments. Similarly, targeting high-mobility ground scenarios, Zhu et al. surveyed RIS applications in THz/mmWave vehicular communications, highlighting how intelligent reflecting and diffraction routing can mitigate severe blockage and rapid fading caused by vehicle mobility, thereby improving link robustness and anti-eavesdropping capability in V2X systems [79]. In contrast, Yuan et al. investigated RIS-aided THz secure transmission in non-terrestrial networks (NTNs), establishing

stochastic channel models for satellite, high-altitude platform (HAP), and UAV layers, and deriving closed-form expressions for the ergodic secrecy rate to illuminate the impact of atmospheric turbulence and phase uncertainty on secure performance [80].

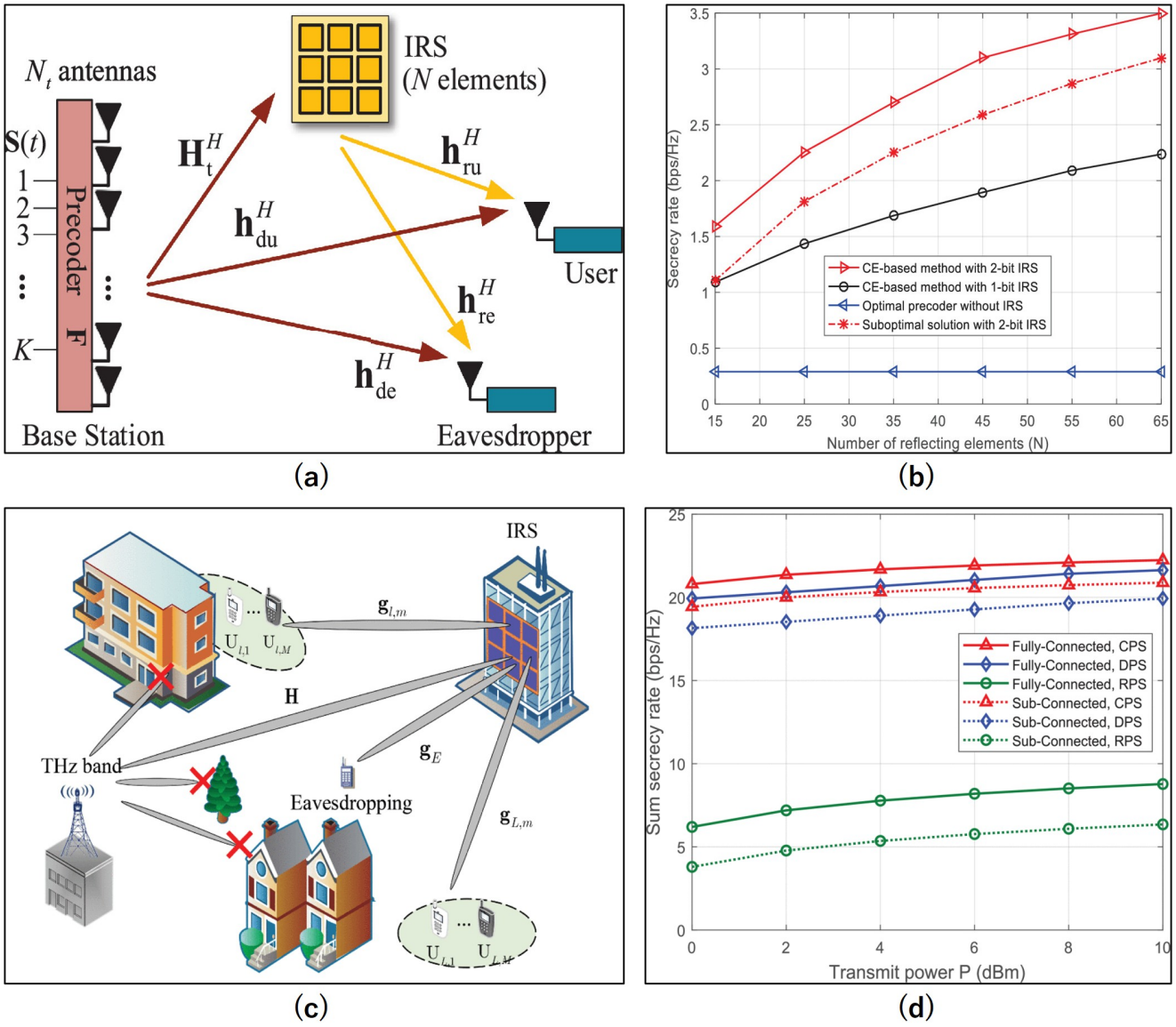


Figure 6. (**a**) RIS-assisted THz MISO wiretap model with a base station (with N_t antennas), an N-element RIS, a user, and an eavesdropper [72]. (**b**) Secrecy rate versus RIS size N under discrete phase control [72]. (**c**) System model of an IRS-assisted THz MIMO–NOMA secure network with a hybrid-precoding base station, a RIS, clustered users, and an eavesdropper [74]. (**d**) Sum secrecy rate comparison for fully connected and sub-connected hybrid precoders in an RIS-assisted THz MIMO–NOMA system [74]. CE: Cross-entropy; CPS: Continuous phase shift; DPS: Discrete phase shift; RPS: Random phase shift.

4.2. Secure Beamforming

Beamforming has become a cornerstone of secure wireless system design, and its significance is even more pronounced at THz frequencies. At conventional microwave and millimeter-wave (mmWave) bands, transmitters rely on beamforming techniques to sharpen spatial directionality, confine radiated energy to a limited region, and manipulate the spatial distribution of interference. These functions jointly limit the exposure of useful

signals and reduce the effectiveness of both passive interception and intentional disruption at the physical layer [81–83]. Beyond the physical layer, the inherent spatial filtering capability provided by beamforming also contributes to security at higher layers by narrowing the potential attack surface, reinforcing the robustness of control channels, and enabling advanced mechanisms such as spatial-feature-based key generation and direction-aware secure routing [84–86]. On this basis, beamforming serves as a direct and versatile enabler of enhanced physical-layer confidentiality. One fundamental approach is spatial precoding, in which transmission weights are optimized so that energy is concentrated toward an intended receiver, while undesired directions experience sidelobe suppression or deep nulls. This configuration effectively widens the signal-to-interference-plus-noise ratio (SINR) disparity between the legitimate link and any potential eavesdropping paths in the angular domain [87,88]. In addition, more sophisticated designs based on directional modulation and constellation-aware beamforming manipulate the phase and amplitude distribution across antenna elements. As a result, the correct signal constellation appears only along specific spatial (and sometimes frequency-dependent) directions, whereas receivers positioned elsewhere observe severely distorted symbol patterns. This distortion prevents reliable demodulation by unintended listeners, even in scenarios where the received power is not significantly attenuated [89–91]. In networked or cooperative configurations, security can be further reinforced through coordinated beamforming among multiple nodes. Distributed relays or cooperating base stations can synchronize their transmissions to coherently boost the desired signal toward the legitimate user while simultaneously suppressing radiation toward suspicious areas. Alternatively, they may emit intentional jamming signals in a coordinated manner, reshaping the electromagnetic environment to favor secure communication at the network scale [92–94].

At THz frequencies, the contribution of beamforming to physical-layer security extends beyond what is typically observed in lower-frequency bands. Its influence is shaped not only by enhanced spatial concentration, but also by the distinctive propagation characteristics of THz waves and the emerging architectures of THz hardware. Because THz signals experience pronounced free-space attenuation and molecular absorption, communication links are generally dominated by highly directive line-of-sight components. As a result, useful signal energy is confined to an extremely narrow angular region, substantially restricting the spatial positions from which an eavesdropper can intercept the transmission. This naturally occurring “spatial corridor” effect provides an inherent security advantage for THz systems, as illustrated in Figure 7A [95–98]. From a system-design perspective, many theoretical studies envision future THz networks employing ultra-dense antenna arrays capable of fine-grained sidelobe manipulation and multi-beam generation. Such configurations would offer abundant spatial degrees of freedom, enabling direction-aware modulation techniques and secure multi-user beam allocation strategies [99]. Although current THz hardware remains limited in terms of array dimensions and integration density, a number of experimental demonstrations have already verified the feasibility of spatially constrained “decodable regions” using dual-beam architectures, as shown in Figure 7B. In these testbeds, two THz beams are superimposed in space and processed through heterodyne mixing or analog logic operations, such as AND or XOR.

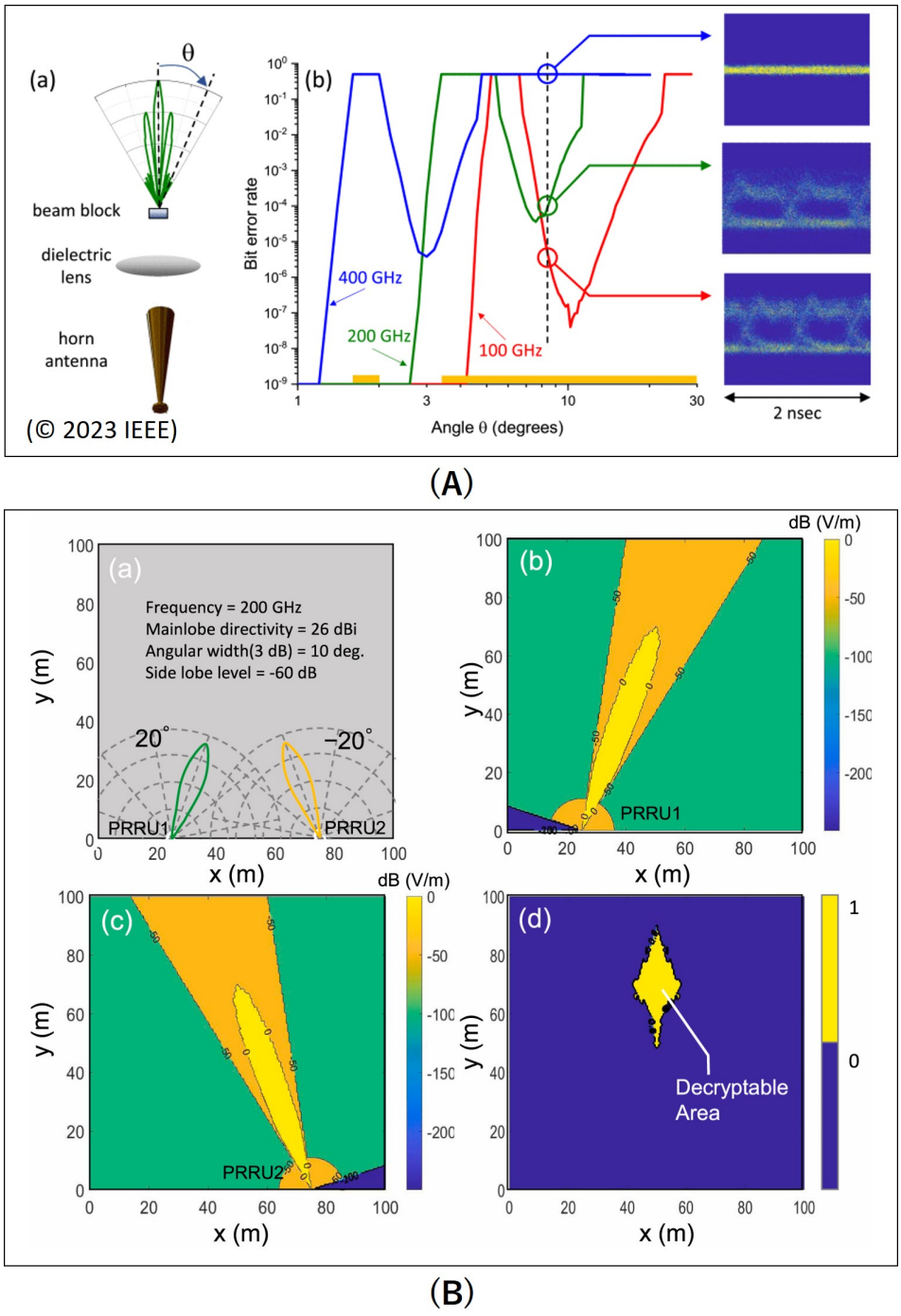


Figure 7. (**A-a**) An illustration of the experimental setup schematic. A horn antenna and 4-mm beam block generate frequency-dependent radiation patterns [95,96]. (**A-b**) BER and Eye vs. angle for 100, 200, and 400 GHz signals and blind regions are highlighted by orange bars [95,96]. (**B-a**) Illustration of 200 GHz radiation patterns of PRRU1 and PRRU2 [100]. (**B-b**) The distribution of E-field strength by PRRU1 [100]. (**B-c**) The distribution of E-field strength by PRRU2 [100]. (**B-d**) The distribution of E-field strength by PRRU1 [100]. PRRU: Photonic remote radio unit; THz-ED: THz envelope detector.

To mathematically explain the dual-beam spatial mixing, we consider a scenario where Alice transmits two separate signal streams, $S_1(t)$ and $S_2(t)$, via two spatially separated transmitters. These signals are designed such that the original message $M(t)$ can only be

recovered through a logical operation on both signals. The total received electromagnetic field $E_{Rx}(t)$ at a spatial location $\mathbf{r}$ is the superposition of the two beams:

$$E_{Rx}(t, \mathbf{r}) = h_1(\mathbf{r})E_1(t) + h_2(\mathbf{r})E_2(t). \tag{11}$$

where $h_k(\mathbf{r})$ represents the channel response from the k-th transmitter to the location $\mathbf{r}$, and $E_k(t)$ is the transmitted THz field. The security relies on the fact that an eavesdropper outside the beam overlap region receives only one of the components, making decryption impossible.

For OOK, the system typically implements a logical AND operation. The receiver employs an envelope detector with a power threshold γ_{th}. The demodulated bit $y[n]$ is given by:

$$y_{AND}[n] = \begin{cases} 1, & \text{if } |E_1|^2 + |E_2|^2 > \gamma_{th} \\ 0, & \text{otherwise.} \end{cases} \tag{12}$$

Here, the threshold γ_{th} is set such that the power of a single beam is insufficient to trigger a '1'. Thus, $y_{AND} = x_1 \wedge x_2$, ensuring that data is recoverable only where both beams coexist.

For FSK, the system achieves a logical XOR operation, which provides stronger cryptographic security. Assuming the two beams carry frequencies $f_A(t)$ and $f_B(t)$ corresponding to data bits d_A and d_B, the receiver detects the combined signal. In a photonic-assisted system, these THz waves are generated by photomixing optical signals. The demodulated output y_{XOR} depends on the instantaneous frequency combination:

$$y_{XOR}[n] = d_A[n] \oplus d_B[n]. \tag{13}$$

Physically, this is realized by mapping the four possible frequency pairs (f_{A0}, f_{B0}), (f_{A0}, f_{B1}), (f_{A1}, f_{B0}), (f_{A1}, f_{B1}) to specific output symbols. Since $d_A \oplus d_B$ is required to recover the message, an eavesdropper intercepting only Beam A (containing d_A) or Beam B (containing d_B) retrieves only random data, ensuring unconditional security at the physical layer.

Under this configuration, correct demodulation occurs exclusively within the spatial overlap zone of the two beams, while signals received outside this region remain unintelligible. Importantly, these experimentally observed decryption zones are significantly smaller than the coverage areas encountered in conventional wireless systems, as shown in Figure 7B [100–105]. These findings confirm that even with modest array sizes and limited steering capability, THz transmissions can already be exploited to form precisely defined, spatially selective decryption windows in practical environments. This experimental evidence aligns with broader system-level predictions that the highly directional nature of THz beams is fundamentally advantageous for spatial secrecy. At present, beam control within prototype THz platforms is predominantly realized through optics-assisted solutions or compact antenna arrays, whereas more complex hybrid and analog beamforming schemes remain largely confined to theoretical models that describe scalable future architectures. In wideband scenarios, both modeling and experimental results reveal frequency-dependent phenomena, including beam squint and angular dispersion [106]. While these effects are often regarded as imperfections, they may in fact be leveraged from a security standpoint, since the increased unpredictability of signal propagation outside the intended direction can further hinder unauthorized demodulation [107]. Furthermore, the strong interdependence between spatial and frequency domains in THz beam training and channel acquisition has motivated the development of randomized beam-scanning strategies, protected pilot designs, and structured codebooks, all aimed at minimizing

spatial information leakage during the alignment process. While these concepts have yet to be comprehensively validated in hardware implementations, they offer promising avenues for enhancing the security of THz communication systems [108,109]. In summary, both experimental demonstrations and theoretical investigations consistently point to the same conclusion: the extreme directivity of THz radiation, combined with multi-beam interaction mechanisms, naturally supports the creation of spatially confined secure zones, strengthens direction-dependent confidentiality, and suppresses unintended reception. Fully exploiting these intrinsic advantages, however, will depend on continued advancements in antenna integration, system stability, and broadband beam management.

4.3. Wavefront Hopping

With the development of RIS and antenna array technologies, the ability to control the THz wavefront is continuously improving. In the near field, transmitter antenna arrays are no longer limited to generating simple plane waves. Instead, they can construct various complex wavefronts. These include non-diffracting beams such as Bessel beams and self-accelerating curved beams such as Airy beams.

Inspired by the FH technology introduced in Section 3.1, Petrov et al. proposed the wavefront hopping concept, that THz waves can be dynamically switched between different wavefronts [110]. From a PLS perspective, wavefront hopping provides a powerful security mechanism based on spatial diversification. As detailed by Petrov et al., a secure message can be split into K distinct parts. The transmitter then sequentially hops through K different spatial wavefronts, sending one message part over each wavefront. For example, Part 1 may be sent on a narrow, non-diffracting Bessel beam, Part 2 on an Airy beam curving to the left, and Part 3 on an Airy beam curving to the right, as shown in Figure 8a. The security of this scheme relies on the fact that an attacker must successfully capture all K message parts to reconstruct the full encryption key or message [111]. Because different wavefronts possess unique spatial energy distributions, an attacker at a single location is unlikely to be in the high-power region for all K wavefronts. This forces the attacker to either deploy multiple cooperating units or accept a failed interception. Guerboukha et al. experimentally demonstrated the feasibility of wavefront hopping [112]. They showed that a system can hop from a standard straight beam, such as a Bessel beam, to a curved Airy beam. This allows the communication link to circumvent an obstacle in the middle of the path. A fundamental challenge for wavefront hopping is determining which wavefront to hop to. The set of possible beam trajectories is infinite. Modeling the optimal curved beam around a blocker in the near field is computationally intractable for real-time applications. To solve this, Chen et al. proposed a physics-informed machine learning (ML) framework. This approach uses a neural network, trained on electromagnetic simulations, to instantly predict the optimal Airy beam parameters, such as curvature and focal length, based on the geometry of the blocker and receiver, as shown in Figure 8b [113]. Experimental results confirmed that this AI learned Airy beam could successfully circumvent blockages. It achieved orders of magnitude better BER performance than conventional beam steering or beam focusing techniques. In summary, wavefront hopping utilizes unique near-field THz beams and leverages AI-based optimization techniques. It provides an advanced method to simultaneously enhance link stability against both jamming and eavesdropping.

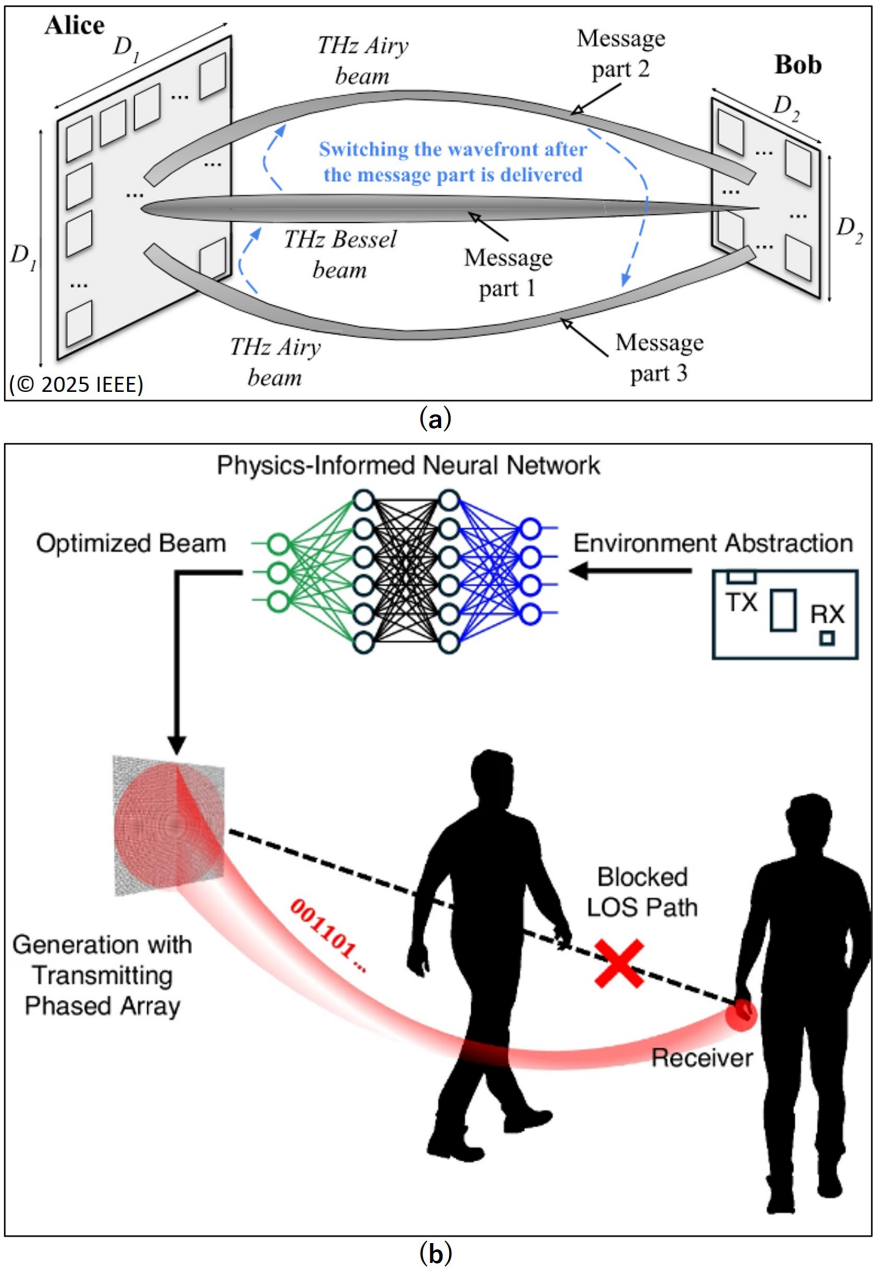


Figure 8. (**a**) Multi-beam schemes with two Airy beams and a Bessel beam [111]. (**b**) Illustration of the physics-informed learning framework for optimal Airy beams [113].

4.4. Comparative Analysis of Spatial-Based Techniques

Spatial-based techniques leverage the unique propagation characteristics of THz waves. Their practical deployment faces distinct trade-offs between hardware cost and alignment stability, as compared in Table 3.

- Implementation complexity: RIS offer a cost-effective solution with passive elements, but the "implementation complexity" shifts to the channel estimation phase, which creates significant signaling overhead. Secure beamforming is the most mature technology, balancing complexity and performance through standard phased arrays or lens antennas. Wavefront hopping offers high theoretical security by utilizing multi-dimensional beam structures (e.g., Airy/Bessel beams). However, it incurs high complexity in holographic beamforming generation and requires computationally intensive optimization for trajectory planning, while being restricted to near-field applications.

- Mobility Challenges: All spatial techniques are inherently sensitive to alignment errors. RIS and secure beamforming are particularly vulnerable to user mobility. A slight positional shift can move the user out of the narrow high-gain beam or the "quiet zone", leading to outages or leakage. To address this, beam-tracking is required [106,114]. Wavefront hopping, particularly with self-bending Airy beams, offers a unique advantage in bypassing obstacles, providing better robustness in dynamic, obstacle-rich environments compared to rigid line-of-sight beamforming.

Table 3. Comparison of spatial-based PLS techniques in THz communications.

Technique	Primary Security Mechanism	Implementation Complexity	Real-Time Feasibility	Mobility Tolerance
RIS	Programmable reflection and multipath.	**High**: Passive hardware, but high overhead for channel estimation.	**Medium**: Latency in channel estimation limits fast adaptation.	**Low**: Requires continuous beam tracking.
Secure beamforming	Spatial energy concentration and sidelobe suppression.	**Low**: Standard phased antenna arrays or lens.	**High**: Mature technology.	**Low**: Requires continuous beam tracking.
Wavefront hopping	Switching between varying spatial modes.	**High**: Requires complex holographic beamforming and optimization.	**Low**: Computationally intensive for trajectory planning.	**Medium**: Self-bending beams can bypass obstacles, offering robustness in NLoS.

5. Conclusions

THz communication is a cornerstone technology for the 6G vision, offering unprecedented bandwidth resources. However, its ultra-high data rate implies that the consequences of information leakage are exceptionally severe. This review has comprehensively surveyed PLS techniques for THz communications above 100 GHz, systematically classifying them into signal-based and spatial-based technologies.

In the signal domain, we analyzed three primary approaches. First, FH was highlighted for its evolution toward nanosecond-level switching speeds using electro-optic effects, addressing the challenge of hopping rates. Second, environment-adaptive propagation was discussed, which intelligently exploits molecular absorption peaks to physically restrict the broadcast range and achieve covertness. Third, noise masking techniques were reviewed, emphasizing recent AN schemes, emerging chaos-based data masking and quantum-noise secured schemes.

In the spatial domain, we summarized the role of RIS in actively reconstructing channel environments to suppress eavesdropping. We also examined secure beamforming, which leverages the high directivity of THz waves to create "spatial corridors" and geometrically confined decryption zones via dual-beam mixing. Additionally, wavefront hopping was highlighted as a method to enforce spatial signal diversity using structured beams like Airy beams, often aided by physics-informed machine learning for trajectory optimization.

Moving forward, bridging the gap between theoretical PLS models and practical deployment remains a priority. Future research will likely focus on developing hybrid security architectures that combine signal and spatial techniques, as well as leveraging AI to cope with the hardware constraints and dynamic nature of real-world 6G networks.

In conclusion, THz PLS is a dynamic and critical research frontier. New technologies are continuously emerging. Future research will increasingly focus on leveraging AI and

quantum technology for system optimization and achieving unpredictable physical layers. Furthermore, developing hybrid security architectures that merge multiple spatial and signal domain techniques will be key, such as combining RIS with AN or combining wavefront hopping with FH. We hope this review will attract more researchers to join the THz PLS research family and promote secure and reliable THz communication to every household.

Author Contributions: Conceptualization, S.Y. and M.C.; investigation, S.Y. and M.C.; resources, S.Y.; writing—original draft preparation, S.Y. and M.C.; writing—review and editing, Y.M. and K.K.; visualization, S.Y.; supervision, Y.M. and K.K.; project administration, M.C., Y.M. and K.K.; funding acquisition, Y.M. and K.K. All authors have read and agreed to the published version of the manuscript.

Funding: This work was supported in part by the MIC/FORWARD JPMI241010003, the National Institute of Information and Communications Technology JPJ012368C02801, JPJ012368C00901 and JSPS KAKENHI Grant Number: JP24H00319, JP24K17324, 25K22089.

Data Availability Statement: The data presented in this study are available on request from the corresponding author.

Conflicts of Interest: The authors declare no conflicts of interest.

References

1. Jiang, W.; Zhou, Q.; He, J.; Habibi, M.A.; Melnyk, S.; El-Absi, M.; Han, B.; Di Renzo, M.; Schotten, H.D.; Luo, F.L.; et al. Terahertz communications and sensing for 6G and beyond: A comprehensive review. *IEEE Commun. Surv. Tutorials* **2024**, *26*, 2326–2381. [CrossRef]
2. Ducournau, G.; Nagatsuma, T. Wireless communications in the THz range. In *Fundamentals of Terahertz Devices and Applications*; John Wiley & Sons, Inc.: Hoboken, NJ, USA, 2021; pp. 479–510.
3. Dat, P.T.; Akahane, K. Photonic Technology for Millimeter-Wave and Terahertz-Wave Communications in IMT-2030 and Beyond. *IEEE Commun. Stand. Mag.* 2025, *early access*. [CrossRef]
4. Lee, S.; Hara, S.; Yoshida, T.; Amakawa, S.; Dong, R.; Kasamatsu, A.; Sato, J.; Fujishima, M. An 80-Gb/s 300-GHz-band single-chip CMOS transceiver. *IEEE J. Solid-State Circuits* **2019**, *54*, 3577–3588. [CrossRef]
5. Ding, J.; Yu, J.; Li, W.; Wang, K.; Zhou, W.; Zhang, J.; Zhu, M.; Xie, T.; Yu, J.; Zhao, F. High-speed and long-distance photonics-aided terahertz wireless communication. *J. Light. Technol.* **2023**, *41*, 3417–3423. [CrossRef]
6. Zhang, J.; Zhu, M.; Hua, B.; Lei, M.; Cai, Y.; Zou, Y.; Tong, W.; Ding, J.; Tian, L.; Ma, L.; et al. Real-time demonstration of 100 GbE THz-wireless and fiber seamless integration networks. *J. Light. Technol.* **2022**, *41*, 1129–1138. [CrossRef]
7. Dat, P.T.; Kanno, A.; Yamamoto, N.; Kawanishi, T. Seamless Convergence of Fiber and Wireless Systems for 5G and Beyond Networks. *J. Light. Technol.* **2019**, *37*, 592–605. [CrossRef]
8. Nagatsuma, T.; Gao, W.; Kawamoto, Y.; Ohara, T.; Ito, H.; Ishibashi, T. InP-based Integrated Circuits on SiC/Si Substrates for Terahertz Communications. *J. Light. Technol.* **2025**, *43*, 9765–9774. [CrossRef]
9. Liu, C.; Li, Z.; Yamazaki, Y.; Herdian, H.; Wang, C.; Tian, A.; Sakamaki, J.; Nie, H.; Fu, X.; Kato, S.; et al. A 640-Gb/s 4 × 4-MIMO D-Band CMOS Transceiver Chipset. *IEEE J. Solid-State Circuits* **2024**, *60*, 1132–1149. [CrossRef]
10. Che, M.; Kondo, K.; Kato, K. Generating and enhancing THz pulses via an antenna-coupled unitraveling-carrier photodiode array. *IEEE Trans. Terahertz Sci. Technol.* **2023**, *13*, 280–285. [CrossRef]
11. Ichikawa, D.; Gao, W.; Ngo, N.H.; Ohara, T.; Tanaka, M.; Murakami, S.; Yamada, Y.; Yamane, H.; Nishida, Y.; Fujita, M.; et al. Terahertz On-Chip Communications With Hybrid Electronic-Photonic Interconnects. *IEEE Trans. Terahertz Sci. Technol.* **2025**, *15*, 751–762. [CrossRef]
12. Qian, C.; Che, M.; Kamiura, Y.; Doi, R.; Ishibashi, T.; Mikami, Y.; Kato, K. 3-mW-output 300-GHz ultra-compact photonic THz-wave generator. In Proceedings of the 2024 IEEE Opto-Electronics and Communications Conference (OECC), Melbourne, Australia, 30 June–4 July 2024; pp. 1–3.
13. John, L.; Tessmann, A.; Leuther, A.; Neininger, P.; Merkle, T.; Zwick, T. Broadband 300-GHz power amplifier MMICs in InGaAs mHEMT technology. *IEEE Trans. Terahertz Sci. Technol.* **2020**, *10*, 309–320. [CrossRef]
14. Che, M.; Kanaya, H.; Kato, K. Optically controlled THz power tuning based on interference at transmission line. *Opt. Express* **2021**, *29*, 20034–20044. [CrossRef]

15. Li, L.; Long, T.; Yang, X.; Zhang, Z.; Wang, L.; Wang, J.; Wang, M.; Lu, J.; Yu, J.; Chen, B. Modified uni-travelling-carrier photodiodes with 206 GHz bandwidth and 0.81 AW^{-1} external responsivity. *Nat. Photonics* **2025**, *19*, 1301–1308. [CrossRef]
16. Malevich, Y.; Ergoktas, M.S.; Bakan, G.; Steiner, P.; Kocabas, C. Very-large-scale reconfigurable intelligent surfaces for dynamic control of terahertz and millimeter waves. *Nat. Commun.* **2025**, *16*, 2907. [CrossRef]
17. Abdo, I.; Jyo, T.; Pander, A.; Wakita, H.; Shiratori, Y.; Muto, M.; Hamada, H.; Nagatani, M.; da Gomez, C.; Wang, C.; et al. 300-ghz-band four-element cmos-inp hybrid phased-array transmitter with 36circ steering range. *IEEE Microw. Wirel. Technol. Lett.* **2023**, *33*, 887–890. [CrossRef]
18. Long, J.; Yu, J.; Wang, C.; Zhang, L.; Sang, B.; Wu, Y.; Yang, X.; Wei, Y.; Wang, K.; Zhou, W.; et al. 510-Gbps 322-GHz Photonics-Aided Terahertz Wireless Transmission System With MIMO Embedded Adaptive Phase Recovery Equalizer. *IEEE Trans. Microw. Theory Tech.* **2024**, *73*, 3597–3607. [CrossRef]
19. Wang, M.; Yu, J.; Zhao, X.; Bian, C.; Zhou, W.; Wang, K. K-means non-uniform-quantization digital–analog radio-over-fiber scheme for THz-band photonics-aided wireless fronthaul. *Opt. Lett.* **2024**, *49*, 2801–2804. [CrossRef] [PubMed]
20. Yu, J.; Wang, Y.; Ding, J.; Zhang, J.; Li, W.; Wang, F.; Wang, C.; Wang, K.; Tan, Y.; Zhu, M.; et al. Broadband photon-assisted terahertz communication and sensing. *J. Light. Technol.* **2023**, *41*, 3332–3349. [CrossRef]
21. Wei, Y.; Yu, J.; Zhao, X.; Yang, X.; Wang, M.; Li, W.; Tian, P.; Han, Y.; Zhang, Q.; Tan, J.; et al. Demonstration of a photonics-aided 4600-m wireless transmission system in the sub-THz band. *J. Light. Technol.* **2024**, *42*, 8564–8576. [CrossRef]
22. Li, W.; Yu, J.; Zhu, B.; Wang, F.; Ding, J.; Zhang, J.; Zhu, M.; Zhao, F.; Xie, T.; Wang, K.; et al. Photonic terahertz wireless communication: Towards the goal of high-speed kilometer-level transmission. *J. Light. Technol.* **2023**, *42*, 1159–1172. [CrossRef]
23. Kamiura, Y.; Doi, R.; Ssali, H.; Che, M.; Mikami, Y.; Kato, K. 300-GHz Beam-Steering Wireless Communication Enabled by 4-Array InGaAs UTC-PD on SiC Substrate and Optical Phased Array. *J. Light. Technol.* **2025**, *43*, 6050–6057. [CrossRef]
24. Webber, J.; Oshiro, A.; Iwamatsu, S.; Nishida, Y.; Fujita, M.; Nagatsuma, T. 48-Gbit/s 8K video-transmission using resonant tunnelling diodes in 300-GHz band. *Electron. Lett.* **2021**, *57*, 668–669. [CrossRef]
25. Liu, K.; Feng, Y.; Han, C.; Chang, B.; Chen, Z.; Xu, Z.; Li, L.; Zhang, B.; Wang, Y.; Xu, Q. High-speed 0.22 THz communication system with 84 Gbps for real-time uncompressed 8K video transmission of live events. *Nat. Commun.* **2024**, *15*, 8037. [CrossRef]
26. *IEEE Std 802.15.3-2023*; IEEE Standard for Wireless Multimedia Networks. Institute of Electrical and Electronics Engineers (IEEE): Piscataway, NJ, USA, 2024; pp. 1–684.
27. Petrov, V.; Kurner, T.; Hosako, I. IEEE 802.15. 3d: First standardization efforts for sub-terahertz band communications toward 6G. *IEEE Commun. Mag.* **2020**, *58*, 28–33. [CrossRef]
28. Ma, J.; Shrestha, R.; Adelberg, J.; Yeh, C.Y.; Hossain, Z.; Knightly, E.; Jornet, J.M.; Mittleman, D.M. Security and eavesdropping in terahertz wireless links. *Nature* **2018**, *563*, 89–93. [CrossRef] [PubMed]
29. Doeker, T.; Herold, C.; Eckhardt, J.M.; Kürner, T. Eavesdropping measurements for applications in office environments at low THz frequencies. *IEEE Trans. Microw. Theory Tech.* **2023**, *71*, 2748–2757. [CrossRef]
30. Taleb, F.; Hernandez-Cardoso, G.G.; Castro-Camus, E.; Koch, M. Transmission, reflection, and scattering characterization of building materials for indoor THz communications. *IEEE Trans. Terahertz Sci. Technol.* **2023**, *13*, 421–430. [CrossRef]
31. Li, P.; Wang, J.; Zhao, L.; Gao, X.; Song, F.; Sun, H.; Ma, J. Scattering and eavesdropping in terahertz wireless link by wavy surfaces. *IEEE Trans. Antennas Propag.* **2023**, *71*, 3590–3597. [CrossRef]
32. Li, P.; Liu, W.; Zhao, J.; Cui, J.; Ge, Y.; Niu, Q.; Yang, Y.; Meng, X.; Sun, H.; Ma, J. Eavesdropping risk in terahertz channels by coverings on wavy surfaces. *Opt. Express* **2025**, *33*, 48451–48465. [CrossRef] [PubMed]
33. Li, P.; Liu, W.; Li, D.; Zhang, M.; Wang, X.; Sun, H.; Ma, J. Eavesdropping risk evaluation for non-line-of-sight terahertz channels by a metallic wavy surface in rain. *J. Opt. Soc. Am. B* **2024**, *41*, 1995–2002. [CrossRef]
34. Shrestha, R.; Guerboukha, H.; Fang, Z.; Knightly, E.; Mittleman, D.M. Jamming a terahertz wireless link. *Nat. Commun.* **2022**, *13*, 3045. [CrossRef]
35. Priyadarshani, R.; Ata, Y.; Alouini, M.S. Jamming intrusions in extreme bandwidth communication: A comprehensive overview. *IEEE Open J. Commun. Soc.* **2025**, *6*, 7125–7149. [CrossRef]
36. Nallappan, K.; Skorobogatiy, M. Photonics based frequency hopping spread spectrum system for secure terahertz communications. *Opt. Express* **2022**, *30*, 27028–27047. [CrossRef] [PubMed]
37. Li, Z.; Guan, L.; Li, C.; Radwan, A. A secure intelligent spectrum control strategy for future THz mobile heterogeneous networks. *IEEE Commun. Mag.* **2018**, *56*, 116–123. [CrossRef]
38. Yang, Z.; Yang, F.; Wen, Z.; Wang, H.; Liu, Y.; Jiang, H.; Chen, F.; Liu, Y.; Li, M.; Zhang, J. Ultra-wideband photonic frequency-hopping waveform generator enabled by optical injection locking for secure terahertz wireless communications. *J. Light. Technol.* **2024**, *42*, 6788–6797. [CrossRef]
39. Ye, S.; Kaide, R.; Kamiura, Y.; Masutomi, N.; Li, B.; Wang, Y.; Che, M.; Mikami, Y.; Ueda, Y.; Kato, K. Photonic Frequency Hopping and De-Hopping System by Ultra-Fast Wavelength Tunable Laser for Secure Terahertz Wireless Communication. *J. Light. Technol.* **2025**, *43*, 9901–9911. [CrossRef]

40. Ye, S.; Masutomi, N.; Li, B.; Kamiura, Y.; Kaide, R.; Doi, R.; Wang, Y.; Che, M.; Mikami, Y.; Ueda, Y.; et al. Ultra-fast photonic frequency hopping driven by reflection-type transversal filter laser for anti-jamming terahertz communications. *Opt. Lett.* **2025**, *50*, 3070–3073. [CrossRef]
41. Masutomi, N.; Ye, S.; Li, B.; Kaide, R.; Che, M.; Mikami, Y.; Ueda, Y.; Kato, K. Cost-Effective and Energy-Efficient Photonics-Based Frequency Hopping by Single Wavelength-Tunable Laser for Secure THz Communication. *Photonics* **2025**, *12*, 76. [CrossRef]
42. Han, C.; Wu, Y.; Chen, Z.; Chen, Y.; Wang, G. THz ISAC: A physical-layer perspective of terahertz integrated sensing and communication. *IEEE Commun. Mag.* **2024**, *62*, 102–108. [CrossRef]
43. Lyu, Z.; Zhang, L.; Deng, Q.; Fang, X.; Bai, L.; Ozolins, O.; Zhang, H.; Liu, G.; Pang, X.; Yu, X. Photonic Chirp Spread Spectrum THz-ISAC: Constraints and Design Considerations. *IEEE Trans. Microw. Theory Tech.* **2025**. [CrossRef]
44. Li, B.; Ye, S.; Che, M.; Tang, H.; Kato, K. Demonstration of Frequency Hopping in 300-GHz Band by Photomixing using Tunable DFB Laser Array. In Proceedings of the 2023 28th Microoptics Conference (MOC), Miyazaki, Japan, 24–27 September 2023; pp. 1–2.
45. Li, B.; Ye, S.; Che, M.; Tang, H.; Masutomi, N.; Mikami, Y.; Kato, K. Demonstration of THz frequency hopping in the 300 GHz band based on UTC-PD and tunable DFB laser array. *Jpn. J. Appl. Phys.* **2024**, *63*, 04SP86. [CrossRef]
46. Yang, Z.; Yang, F.; Zhang, J. Photonic-assisted THz Wideband Frequency Hopping and Secure Communication Based on Optical Injection Locking. In Proceedings of the CLEO: Science and Innovations, Charlotte, NC, USA, 5–10 May 2024; p. JTu2A–68.
47. Ye, S.; Masutomi, N.; Li, B.; Matsumoto, R.; Kaide, R.; Tang, H.; Kamiura, Y.; Che, M.; Mikami, Y.; Ueda, Y.; et al. Photonic Frequency Hopping Driven by High-Speed Wavelength Tunable Laser for Secure Terahertz-wave Communication. In Proceedings of the Optical Fiber Communication Conference, San Diego, CA, USA, 24–28 March 2024; p. W4A–3.
48. Ye, S.; Kamiura, Y.; Li, B.; Kaide, R.; Wang, Y.; Che, M.; Mikami, Y.; Ueda, Y.; Kato, K. Self-coherent Photonic Terahertz Link at 300-GHz-band Against Modulated Jamming. *Opt. Lett.* 2025, *in press*. [CrossRef]
49. Ye, S.; Kaide, R.; Kamiura, Y.; Li, B.; Wang, Y.; Che, M.; Mikami, Y.; Ueda, Y.; Kato, K. Highly Secure Photonics-Based Terahertz Frequency Hopping System for Jamming Avoidance With Ultra-Fast Hopping-Rate. *J. Light. Technol.* **2025**, 1–9. [CrossRef]
50. Ye, S.; Matsutomi, N.; Matsumoto, R.; Kaide, R.; Li, B.; Che, M.; Mikami, Y.; Ueda, Y.; Kato, K. Eavesdropping Avoid Terahertz-Wave Frequency Hopping Spread Spectrum FSK System Driven by Ultra-Fast Wavelength Tunable Laser. In Proceedings of the 2024 International Topical Meeting on Microwave Photonics (MWP), Pisa, Italy, 7–20 September 2024; pp. 1–4.
51. Masutomi, N.; Ye, S.; Li, B.; Kaide, R.; Che, M.; Mikami, Y.; Ueda, Y.; Kato, K. 300-GHz-band Frequency Hopping with a Single Tunable Laser Diode for Secure THz Communication. In Proceedings of the 50th European Conference on Optical Communication (ECOC 2024), Frankfurt, Germany, 22–26 September 2024; pp. 1204–1207.
52. Lin, H.W.W.; Sung, C.A.; Hung, Y.H. Microwave frequency switching delays in phase-locked period-one dynamics of semiconductor lasers. *Opt. Lett.* **2024**, *49*, 258–261. [CrossRef] [PubMed]
53. Yu, X.; Zhang, F.; Yan, X.; Wu, G.; Han, X.; Pan, S.; Wang, K. Microwave Generation by P2 Dynamics of Optically Injected Semiconductor Laser. *J. Light. Technol.* **2025**, *43*, 4895–4902. [CrossRef]
54. Liu, Y.; Yang, F.; Yang, Z.; Wen, Z.; Jiang, H.; Chen, F.; Liu, Y.; Li, M.; Zhang, J. Ultra-wideband and Multi-octave Tunable Millimeter Wave Generation based on Photonic Multiplication and Delay-matched Heterodyne. *J. Light. Technol.* **2024**, *42*, 8109–8116. [CrossRef]
55. Liu, X.; Lu, Q.; Cheng, T.; Li, R.; Cheng, M.; Liu, D.; Deng, L. Ultra-Short Period, Wideband, and Uninterrupted Microwave Photonic Frequency-Hopping Communication. In Proceedings of the 2025 Optical Fiber Communications Conference and Exhibition (OFC), San Francisco, CA, USA, 30 March–3 April 2025; p. Th2A.25.
56. Fang, Z.; Guerboukha, H.; Shrestha, R.; Hornbuckle, M.; Amarasinghe, Y.; Mittleman, D.M. Secure communication channels using atmosphere-limited line-of-sight terahertz links. *IEEE Trans. Terahertz Sci. Technol.* **2022**, *12*, 363–369. [CrossRef]
57. Gao, W.; Chen, Y.; Han, C.; Chen, Z. Distance-adaptive absorption peak modulation (DA-APM) for terahertz covert communications. *IEEE Trans. Wirel. Commun.* **2020**, *20*, 2064–2077. [CrossRef]
58. Gao, W.; Chen, Y.; Han, C.; Chen, Z. Distance-adaptive absorption-peak hopping (DA-APH) modulation for terahertz covert communications. In Proceedings of the 2019 IEEE Global Communications Conference (GLOBECOM), Waikoloa, HI, USA, 9–13 December 2019; pp. 1–6.
59. Hall, J.; Jornet, J.M.; Thawdar, N.; Melodia, T.; Restuccia, F. Deep learning at the physical layer for adaptive terahertz communications. *IEEE Trans. Terahertz Sci. Technol.* **2023**, *13*, 102–112. [CrossRef]
60. He, Y.; Zhang, L.; Liu, S.; Zhang, H.; Yu, X. Secure transmission of terahertz signals with multiple eavesdroppers. *Micromachines* **2022**, *13*, 1300. [CrossRef] [PubMed]
61. Gao, W.; Han, C.; Chen, Z. Receiver artificial noise aided terahertz secure communications with eavesdropper in close proximity. In Proceedings of the GLOBECOM 2020—2020 IEEE Global Communications Conference, Taipei, Taiwan, 7–11 December 2020; pp. 1–6.
62. Gao, W.; Han, C.; Chen, Z. DNN-powered SIC-free receiver artificial noise aided terahertz secure communications with randomly distributed eavesdroppers. *IEEE Trans. Wirel. Commun.* **2021**, *21*, 563–576. [CrossRef]

63. Tian, S.; Ju, Y.; Liu, L.; Pei, Q.; Zhang, N.; Wu, C.; Mumtaz, S. Secure terahertz indoor communications using blockage feature-based artificial noise in 6G. In Proceedings of the GLOBECOM 2023—2023 IEEE Global Communications Conference, Kuala Lumpur, Malaysia, 4–8 December 2023; pp. 7261–7266.
64. He, Y.; Zhang, L.; Yang, H.; Zhang, H.; Yu, X. Impacts of sampling on the artificial noise-assisted terahertz secure communication systems. *Phys. Commun.* **2024**, *67*, 102507. [CrossRef]
65. Deng, Q.; Zhang, L.; Lyu, Z.; Pang, X.; Ozolins, O.; Yu, X. Private communication with photonic terahertz chaos. *Adv. Photonics* **2024**, *6*, 066004. [CrossRef]
66. Chen, Q.; Peng, C.; Zhao, L.; You, W.; Wen, H.; Li, J. Physical layer encryption based on digital chaos in THz wireless communication. *Opt. Fiber Technol.* **2025**, *90*, 104118. [CrossRef]
67. Ottaviani, C.; Woolley, M.J.; Erementchouk, M.; Federici, J.F.; Mazumder, P.; Pirandola, S.; Weedbrook, C. Terahertz quantum cryptography. *IEEE J. Sel. Areas Commun.* **2020**, *38*, 483–495. [CrossRef]
68. Zhang, L.; Deng, Q.; Zhang, H.; Yang, Z.; Pang, X.; Bobrovs, V.; Popov, S.; Wu, Y.; Yu, X.; Ozolins, O.; et al. Quantum noise secured terahertz communications. *IEEE J. Sel. Top. Quantum Electron.* **2022**, *29*, 8400110. [CrossRef]
69. Xu, J.; Yuen, C.; Huang, C.; Ul Hassan, N.; Alexandropoulos, G.C.; Di Renzo, M.; Debbah, M. Reconfiguring wireless environments via intelligent surfaces for 6G: Reflection, modulation, and security. *Sci. China Inf. Sci.* **2023**, *66*, 130304. [CrossRef]
70. You, X.; Fumeaux, C.; Withayachumnankul, W. Tutorial on broadband transmissive metasurfaces for wavefront and polarization control of terahertz waves. *J. Appl. Phys.* **2022**, *131*, 061101. [CrossRef]
71. You, X.; Fumeaux, C.; Withayachumnankul, W. Circuit-based design and optimization for broadband terahertz metasurfaces. In Proceedings of the 2021 46th International Conference on Infrared, Millimeter and Terahertz Waves (IRMMW-THz), Chengdu, China, 29 August–3 September 2021; pp. 1–2.
72. Chen, W.; Chen, Z.; Ma, X.; Chi, Y.; Li, Z. Secrecy rate optimization for intelligent reflecting surface aided multi-input-single-output terahertz communication. *Microw. Opt. Technol. Lett.* **2020**, *62*, 2760–2765. [CrossRef]
73. Ning, B.; Chen, Z.; Chen, W.; Li, L. Improving security of THz communication with intelligent reflecting surface. In Proceedings of the 2019 IEEE Globecom Workshops (GC Wkshps), Waikoloa, HI, USA, 9–13 December 2019; pp. 1–6.
74. Xu, J.; Zhu, Z.; Chu, Z.; Niu, H.; Xiao, P.; Lee, I. Sum secrecy rate maximization for IRS-aided multi-cluster MIMO-NOMA terahertz systems. *IEEE Trans. Inf. Forensics Secur.* **2023**, *18*, 4463–4474. [CrossRef]
75. Youn, J.; Son, W.; Jung, B.C. Physical-layer security improvement with reconfigurable intelligent surfaces for 6G wireless communication systems. *Sensors* **2021**, *21*, 1439. [CrossRef] [PubMed]
76. Kiran, A.; Sonker, A.; Jadhav, S.; Jadhav, M.M.; Naga Ramesh, J.V.; Muniyandy, E. Secure communications with THz reconfigurable intelligent surfaces and deep learning in 6G systems. *Wirel. Pers. Commun.* **2024**, 1–17. [CrossRef]
77. Qiao, J.; Zhang, C.; Dong, A.; Bian, J.; Alouini, M.S. Securing intelligent reflecting surface assisted terahertz systems. *IEEE Trans. Veh. Technol.* **2022**, *71*, 8519–8533. [CrossRef]
78. Kim, D.; Jeong, S.; Kang, J. Energy-efficient secure offloading system designed via UAV-mounted intelligent reflecting surface for resilience enhancement. *IEEE Internet Things J.* **2023**, *11*, 3768–3778. [CrossRef]
79. Zhu, Y.; Mao, B.; Kato, N. Intelligent reflecting surface in 6G vehicular communications: A survey. *IEEE Open J. Veh. Technol.* **2022**, *3*, 266–277. [CrossRef]
80. Yuan, J.; Chen, G.; Wen, M.; Tafazolli, R.; Panayirci, E. Secure transmission for THz-empowered RIS-assisted non-terrestrial networks. *IEEE Trans. Veh. Technol.* **2022**, *72*, 5989–6000. [CrossRef]
81. Wu, Y.; Khisti, A.; Xiao, C.; Caire, G.; Wong, K.K.; Gao, X. A survey of physical layer security techniques for 5G wireless networks and challenges ahead. *IEEE J. Sel. Areas Commun.* **2018**, *36*, 679–695. [CrossRef]
82. Niu, H.; Xiao, Y.; Lei, X.; Chen, J.; Xiao, Z.; Li, M.; Yuen, C. A survey on artificial noise for physical layer security: Opportunities, technologies, guidelines, advances, and trends. *IEEE Commun. Surv. Tutor.* **2025**. [CrossRef]
83. Fu, H.; Zhang, X.; Peng, L. Performance Analysis of Artificial Noise-Assisted Location-Based Beamforming in Rician Wiretap Channels. *Entropy* **2023**, *25*, 1626. [CrossRef]
84. Shehadeh, Y.E.H.; Hogrefe, D. A survey on secret key generation mechanisms on the physical layer in wireless networks. *Secur. Commun. Netw.* **2015**, *8*, 332–341. [CrossRef]
85. Xia, E.; Hu, B.J.; Shen, Q. A survey of physical layer secret key generation enhanced by intelligent reflecting surface. *Electronics* **2024**, *13*, 258. [CrossRef]
86. Xiao, Q.; Zhao, J.; Feng, S.; Li, G.; Hu, A. Securing NextG networks with physical-layer key generation: A survey. *Secur. Saf.* **2024**, *3*, 2023021.
87. Li, J.; Ye, N.; Ma, S.; Bu, X.; An, J. Multi-user hybrid beamforming design for physical layer secured mmWave LOS communications. *Electronics* **2021**, *10*, 2635.
88. Sanenga, A.; Mapunda, G.A.; Jacob, T.M.L.; Marata, L.; Basutli, B.; Chuma, J.M. An overview of key technologies in physical layer security. *Entropy* **2020**, *22*, 1261. [CrossRef] [PubMed]

89. Ansari, O.; Amin, M. Directional modulation techniques for secure wireless communication: A comprehensive survey. *EURASIP J. Wirel. Commun. Netw.* **2022**, *2022*, 93. [CrossRef]
90. Chen, J.; Xiao, Y.; Lei, X.; Ding, Y.; Niu, H.; Liu, K.; Zhong, Y.; Yang, S.; Fusco, V.; Xiang, W. A Survey on Directional Modulation: Opportunities, Challenges, Recent Advances, Implementations, and Future Trends. *IEEE Internet Things J.* **2025**, *12*, 32581–32615. [CrossRef]
91. Qiu, B.; Cheng, W.; Zhang, W. Decomposed and distributed directional modulation for secure wireless communication. *IEEE Trans. Wirel. Commun.* **2023**, *23*, 5219–5231. [CrossRef]
92. Liu, Z.; Shang, Y.; Zhang, R.; Xiang, H. Relay selection based on coalitional game for secure wireless networks. *IET Commun.* **2014**, *8*, 1355–1363. [CrossRef]
93. Jameel, F.; Wyne, S.; Kaddoum, G.; Duong, T.Q. A comprehensive survey on cooperative relaying and jamming strategies for physical layer security. *IEEE Commun. Surv. Tutor.* **2018**, *21*, 2734–2771. [CrossRef]
94. Atallah, M.; Kaddoum, G.; Kong, L. A survey on cooperative jamming applied to physical layer security. In Proceedings of the 2015 IEEE International Conference on Ubiquitous Wireless Broadband (ICUWB), Montreal, QC, Canada, 4–7 October 2015; pp. 1–5.
95. Cohen, A.; D'Oliveira, R.G.; Yeh, C.Y.; Guerboukha, H.; Shrestha, R.; Fang, Z.; Knightly, E.; Médard, M.; Mittleman, D.M. Absolute security in high-frequency wireless links. In Proceedings of the 2022 IEEE Conference on Communications and Network Security (CNS), Austin, TX, USA, 3–5 October 2022; pp. 46–54.
96. Cohen, A.; D'Oliveira, R.G.; Yeh, C.Y.; Guerboukha, H.; Shrestha, R.; Fang, Z.; Knightly, E.W.; Médard, M.; Mittleman, D.M. Absolute security in terahertz wireless links. *IEEE J. Sel. Top. Signal Process.* **2023**, *17*, 819–833. [CrossRef]
97. Akyildiz, I.F.; Jornet, J.M.; Han, C. Terahertz band: Next frontier for wireless communications. *Phys. Commun.* **2014**, *12*, 16–32. [CrossRef]
98. Han, C.; Akyildiz, I.F. Distance-aware multi-carrier (DAMC) modulation in terahertz band communication. In Proceedings of the 2014 IEEE International Conference on Communications (ICC), Sydney, NSW, Australia, 10–14 June 2014; pp. 5461–5467.
99. Han, C.; Bicen, A.O.; Akyildiz, I.F. Multi-wideband waveform design for distance-adaptive wireless communications in the terahertz band. *IEEE Trans. Signal Process.* **2015**, *64*, 910–922. [CrossRef]
100. Che, M.; Chen, H.; Ueda, Y.; Kato, K. Secured THz communication in photonic microcell networks based on spatial wave mixing of steered beams. *Opt. Switch. Netw.* **2024**, *54*, 100773. [CrossRef]
101. Yamauchi, K.; Kawai, Y.; Che, M.; Ito, H.; Ishibashi, T.; Kato, K. Terahertz heterodyne AND operation for physically encrypted wireless communication. In Proceedings of the 2020 European Conference on Optical Communications (ECOC), Brussels, Belgium, 6–10 December 2020; pp. 1–4.
102. Yamauchi, K.; Kato, K. Optical heterodyne AND operation as emulation of physical layer security at wireless communication. *IEICE Electron. Express* **2021**, *18*, 20210008. [CrossRef]
103. Kato, K. Photonics-assisted terahertz-wave beam steering and its application in secured wireless communication. *Photonics* **2021**, *9*, 9. [CrossRef]
104. Chen, H.; Che, M.; Seiki, N.; Shiramizu, T.; Yano, T.; Mikami, Y.; Ueda, Y.; Kato, K. Physically Encrypted Wireless Transmission Based on XOR between Two Data in Terahertz Beams. *Electronics* **2023**, *12*, 2629. [CrossRef]
105. Kamiura, Y.; Iwamoto, S.; Mikami, Y.; Kato, K. Physical-Layer Encryption for Terahertz Wireless Communication via Logical AND Operation of Dual Beams. *Electronics* **2025**, *14*, 3762. [CrossRef]
106. Li, B.; Che, M.; Ye, S.; Yang, D.; Tang, H.; Mikami, Y.; Kato, K. Photonic-Assisted Frequency-Independent Beam Steering for Wideband Terahertz Wireless Applications. *J. Light. Technol.* **2025**, *43*, 9950–9958. [CrossRef]
107. Méndez-Rial, R.; Rusu, C.; González-Prelcic, N.; Alkhateeb, A.; Heath, R.W. Hybrid MIMO architectures for millimeter wave communications: Phase shifters or switches? *IEEE Access* **2016**, *4*, 247–267. [CrossRef]
108. Attaoui, W.; Bouraqia, K.; Sabir, E. Initial access & beam alignment for mmWave and terahertz communications. *IEEE Access* **2022**, *10*, 35363–35397. [CrossRef]
109. Madhekwana, S.; Usman, M.A.; Ayyub, A.; Politis, C. Beam alignment for mmWave and THz: Systematic review: S. Madhekwana et al. *Telecommun. Syst.* **2025**, *88*, 87. [CrossRef]
110. Petrov, V.; Guerboukha, H.; Mittleman, D.M.; Singh, A. Wavefront hopping: An enabler for reliable and secure near field terahertz communications in 6G and beyond. *IEEE Wirel. Commun.* **2024**, *31*, 48–55. [CrossRef]
111. Petrov, V.; Guerboukha, H.; Singh, A.; Jornet, J.M. Wavefront hopping for physical layer security in 6G and beyond near-field THz communications. *IEEE Trans. Commun.* **2025**, *73*, 2996–3012. [CrossRef]
112. Guerboukha, H.; Zhao, B.; Fang, Z.; Knightly, E.; Mittleman, D.M. Curving THz wireless data links around obstacles. *Commun. Eng.* **2024**, *3*, 58. [CrossRef]

113. Chen, H.; Kludze, A.; Ghasempour, Y. A physics-informed Airy beam learning framework for blockage avoidance in sub-terahertz wireless networks. *Nat. Commun.* **2025**, *16*, 7387. [CrossRef] [PubMed]
114. Li, B.; Che, M.; Ye, S.; Mikami, Y.; Kato, K. Demonstration of Optoelectronic THz Beam Tracking Using Real-time Phase Optimization. *IEEE Photonics Technol. Lett.* **2025**, *37*, 1109–1112. [CrossRef]

Disclaimer/Publisher's Note: The statements, opinions and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of MDPI and/or the editor(s). MDPI and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions or products referred to in the content.