Security and Angle-Frequency Coupling in Terahertz WLANs

Chia-Yi Yeh, *Member, IEEE*, Yasaman Ghasempour, *Member, IEEE*, Yasith Amarasinghe, *Member, IEEE*, Daniel M. Mittleman, *Fellow, IEEE*, and Edward W. Knightly, *Fellow, IEEE*

***Abstract*— This paper presents the first security study of THz networks employing antennas with the angle-frequency coupling property. Using Leaky Wave Antennas (LWAs) as a representative, we explore the unique security properties due to the frequency-dependent radiation. We show via both analytical models and over-the-air experiments that LWA links exhibit non-uniform secrecy capacity across sub-channels, yielding advantages to an eavesdropper at edge frequencies. Yet, because different frequencies emit towards different angles, the eavesdropper is thwarted from easily intercepting an entire wideband transmission. The experiments diverge from the analytical model in that the model underpredicts the eavesdropper's advantage at angles smaller than the target user and subsequent asymmetric performance across angles. Nonetheless, both the model and measurements show that increasingly wide bandwidth and correspondingly wide beams have only a modest marginal security penalty. Further, we find the LWA link secrecy not only depends on the target user angle (due to nonlinearity of LWA's frequency-angle coupling), but also the beamwidth of the frequency components that constitute the collective LWA transmission.**

***Index Terms*— Terahertz, leaky wave antenna, physical layer security, angular dispersion.**

I. Introduction

THE use of frequencies above 100 GHz for wireless links is rapidly emerging as one of the accepted paradigms for future (beyond 5G) wireless systems [2], [3], [4], [5]. For the first time, in March 2019, the US Federal Communications Commission (FCC) adopted rules to encourage development of technologies above 95 GHz [6]. Subsequently, in November 2019, the World Radiocommunication Conference adopted a resolution to encourage sharing between active and passive radio services at frequencies up to 450 GHz [7]. These high-frequency communications systems, which we refer to as terahertz (THz) links, offer numerous advantages, such as plentiful bandwidth [8] for ultra-high-speed data transmission [9], [10], [11]. Another commonly cited advantage is the enhanced resilience against malicious attacks, as these highly directional links are presumably more secure against eavesdropping and jamming. In the modern era of wireless interconnected devices, the issue of security is a forefront concern.

With a large bandwidth available in the THz regime, directional transmission can exhibit angular dispersion, i.e., frequency-dependent radiation direction. Prior works have proposed to use angular dispersion to improve wireless network performance and for direction estimation in lower bands [12], [13], [14], [15], [16]. Recently, angular dispersion attracts interest in millimeter wave (mmWave) and THz networks, as it manifests in many antenna structures envisioned for these high frequencies [17], [18], [19], [20], including beam squint in phased arrays [21] and the Leaky Wave Antennas (LWAs) [22]. People envision angular dispersion to enable THz networks, with ideas to exploit the frequency-dependent radiation for beam steering [23], [24], [25], [26], [27], [28], [29], [30], path discovery [31], [32], [33], [34], [35], [36], [37], backscatter [38], and enlarge coverage [39]. While angular dispersion can be mitigated by precoding, beamforming codebook design [40], [41], [42], [43], [44] or device architectures such as lens [45] or true time delay [46], [47], [48], angular dispersion will likely exhibit in many future THz transmissions.

While we envision frequency-dependent radiation in many future THz networks, its implication for security has yet to be studied. Unlike conventional directional links, frequency-dependent radiation suggests that the transmission signal footprint widens with increasing bandwidth, which can give an advantage to an eavesdropper.

In this paper, we perform the first security study of the angle-frequency coupled THz networks. To this end, we establish THz links using parallel-plate LWAs from the transmitter Alice to the receiver Bob, in the presence of an eavesdropper Eve. Because the LWA link is frequency-dependent, we channelizes the link in the frequency domain and define a security metric termed subchannel secrecy capacity, so that we can understand security not only in aggregate, but also in its individual frequency components. Using model-driven

Manuscript received 25 February 2022; revised 19 December 2022 and 27 May 2023; accepted 25 September 2023; approved by IEEE/ACM TRANSACTIONS ON NETWORKING Editor K. Chowdhury. This work was supported in part by Cisco; in part by Intel; in part by NSF under Grant CNS-1923782, Grant CNS-1827940, Grant CNS-1824529, Grant CNS-1801857, Grant CNS-1801865, Grant CNS-1518916, and Grant CNS-2148132; and in part by the DOD: Army Research Laboratory under Grant W911NF-1920269. The work of Yasaman Ghasempour was supported in part by NSF under Grant CNS-2145240 and in part by the U.S. Air Force Office of Scientific Research under Grant FA9550-22-1-0382. A preliminary version of this paper was presented at ACM WiSec 2020 [DOI: 10.1145/3395351.3399365]. *(Corresponding author: Chia-Yi Yeh.)*

Chia-Yi Yeh is with the EECS, MIT, Cambridge, MA 02139 USA, and also with the School of Engineering, Brown University, Providence, RI 02912 USA (e-mail: cyyeh@mit.edu).

Yasaman Ghasempour is with the Department of Electrical and Computer Engineering, Princeton University, Princeton, NJ 08544 USA.

Yasith Amarasinghe was with the School of Engineering, Brown University, Providence, RI 02912 USA. He is now with the Department of Electronics and Photonics, Aarhus University, 8200 Aarhus, Denmark.

Daniel M. Mittleman is with the School of Engineering, Brown University, Providence, RI 02912 USA.

Edward W. Knightly is with the Department of Electrical and Computer Engineering, Rice University, Houston, TX 77005 USA.

This article has supplementary downloadable material available at https://doi.org/10.1109/TNET.2023.3321641, provided by the authors.

Digital Object Identifier 10.1109/TNET.2023.3321641

analysis and over-the-air measurements, we demonstrate THz angularly dispersive links' unique security properties in spatial and frequency domain, showing that while angular dispersion negatively impacts link secrecy, the security penalty is surprisingly modest.

First, we show that the subchannel secrecy capacity is nonuniform across the transmission band and is eavesdropping-angle-dependent for angle-frequency coupled links. Indeed, since different frequency components emit toward slightly different directions, Eve intercepts a different signal-to-noise ratio (SNR) profile when she is at different angular locations. For Eve at an angle larger than Bob's angle, she intercepts low frequencies better than high frequencies and vice versa, resulting in eavesdropping-angle-dependent and non-uniform secrecy across frequency channels.

Next, we find a larger bandwidth necessarily yields a wider signal footprint for LWA links, yet, surprisingly, the widening signal footprint results in an unexpectedly small security penalty. Indeed, because a wider bandwidth (wider range of frequencies) corresponds to a wider beamwidth (wider range of angles), the situation may appear dire, that LWA links will either be secure but slow or vice versa. Fortunately, we find that since high and low frequencies are maximized on opposite sides of Bob, Eve cannot simultaneously be on both sides and intercept the entire bandwidth. Thus, while a wider signal footprint (due to larger bandwidth) still results in a less secure LWA link, is not as severe as one would expect based on the signal footprint.

As an extension to our conference version [1], we further examine the secrecy of general LWA links by two fundamental characteristics, namely, *(i)* how fast the radiation direction shifts with frequency, which we term angular dispersion level, and *(ii)* how directional the beam is for each frequency channel, which we characterize by single-tone half power beamwidth (HPBW).

We show that a higher angular dispersion level, that is, a faster shift in radiation direction with frequency, results in a less secure link, despite using the same transmission bandwidth. Since the angle-frequency coupling is nonlinear for LWA, to examine links with varying angular dispersion levels, we study LWA links toward Bob at different angles. Due to the nonlinear angle-frequency coupling, the same bandwidth creates a wider angular span for Bob at a smaller angle, and thus a less secure link given the same transmission bandwidth. Yet, interestingly, regardless of the angular dispersion level, we find that the link shows a comparable eavesdropping resilience as long as the link has a similar angular span.

We next demonstrate that a wider single-tone HPBW results in a less secure link, even when the collective radiation results in the same scanning range. Indeed, unlike other conventional directional links, LWA links are composed of frequencies with distinct radiation patterns so the security of angularly dispersive links requires consideration of the frequency components that constitute the transmission. Thus, the collective beamwidth alone cannot adequately characterize the security of a THz network with angular dispersion.

Last, we perform an extensive set of over-the-air experiments using a THz source, a custom LWA antenna, and a wideband receiver to experimentally study the security for THz networks with angular dispersion. We find that while the LWA model accurately predicts the peak radiation angle for each frequency, it underestimates the radiation at angles less than the peak. Thus, the measured response of the LWA link is even more asymmetric than predicted. The effect is that the model underestimates subchannel secrecy capacity when Eve is at a larger angle than Bob, but overestimates it when she is at a smaller angle. Indeed, when Eve is at a smaller angle than Bob, she is a more devastating threat for the measured LWA link. Despite the difference between the measured pattern and the model, the security properties we find using the model are also observed in the experiments, including the bandwidth and beamwidth coupling, the surprisingly small security penalty compared to the beamwidth increment when the bandwidth increases, and varying eavesdropping resilience towards Bob at different angles.

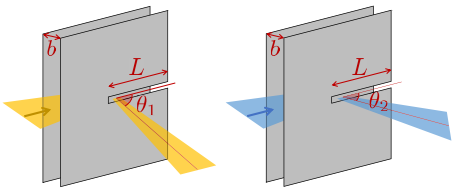

Fig. 1. Terahertz leaky wave antenna beam steering leveraging frequency-angle coupling.

II. Foundations for LWA Security

To study the security for THz links with frequency-varying radiation, we employ a parallel-plate LWA with angle-frequency coupling for THz networks. As shown in Fig. 1, the parallel-plate LWA consists of two parallel plates with an opening slot on one of the plates. Employing the LWA, a transmitter can steer between two different angles θ_1 and θ_2 by changing the input frequency (depicted by color). In the following, we review the parallel-plate LWA radiation model, describe the LWA-enabled THz network, and define the eavesdropper scenario and security metric.

A. LWA Radiation Characterization

The radiation pattern of a parallel-plate LWA has been characterized using a simplified model, where the LWA is abstracted as a uniform finite aperture of length L with an emission distribution at the aperture described by an attenuation constant α and a phase constant β, where the former describes how fast the traveling wave decays due to leakage and the later describes the phase variation of traveling wave. For a parallel-plate waveguide, the dominant transverse electric (TE) mode is TE_1 mode [49] and supports frequency f larger than the cutoff frequency $f_{co} = c/2b$, with c being the speed of light. The phase constant β of the TE_1 mode relates to the plate separation b (through the expression of the cutoff frequency f_{co}) by

$$\beta(f) = k_0\sqrt{1-\left(\frac{f_{co}}{f}\right)^2}, \tag{1}$$

where $k_0 = \frac{2\pi f}{c}$ is the free-space wavenumber. As for the attenuation constant α, it can be engineered [50] but the designed parameters have not been formally characterized. In this work, we model the attenuation constant being consistent across all frequencies based on our empirical observations. With the abstracted model, the E-field of the LWA for frequency f towards angle θ (defined with respect to the

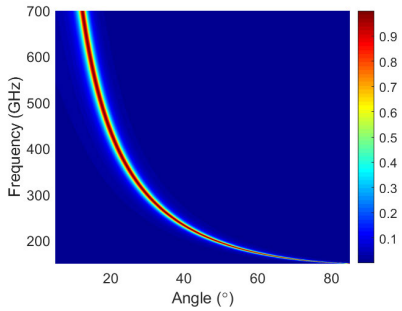

Fig. 2. Normalized LWA radiation pattern according to Equation (2). Plate separation $b = 1$ mm, slot length $L = 3$ cm, and $\alpha = 50$ rad/m.

waveguide propagation direction as illustrated in Fig. 1) is [22], [51]

$$G(f,\theta) = L\sin c\left(\left[\beta(f) - j\alpha - k_0\cos\theta\right]\frac{L}{2}\right), \quad (2)$$

While Equation (2) consists of multiple nonlinear components that prevent us from easily visualizing the radiation pattern, we can first understand the behavior of $G(f,\theta)$ for a fixed frequency component. For a certain frequency f, the radiation pattern $G(f,\theta)$ indicates a sinc-like radiation pattern across angles. Note that the radiation pattern is not exactly $\sin c$ because of the $\cos\theta$ term. The beamwidth of the sinc-like radiation pattern depends on the attenuation constant α [51], where the general form can be found in [52]. Namely, a larger α implies a wider angular spread while a smaller α results in a narrower beam. Now that we know the radiation is sinc-like with the beamwidth determined by α, the last component is to determine the maximum radiation angle. Recall that the complex $\sin c$ function maximizes when

$$\Re(\beta(f) - j\alpha - k_0\cos\theta)\frac{L}{2} = 0. \quad (3)$$

Therefore, the maximum radiation happens at the angle

$$\theta_{max}(f) = \sin^{-1}\left(\frac{c}{2bf}\right). \quad (4)$$

Equation (4) describes the peak angle of a certain frequency. That is, when a higher frequency component is coupled into the LWA, the radiation emits towards a smaller angle. In contrast, if a lower frequency component is coupled into the LWA, it emits at a larger angle.

From the above analysis, we see that the LWA radiation can be described in two parts: first, a nonlinear frequency-angle coupling relationship described by Equation (4) and second, the angular spread of each single-tone frequency component determined by α.

Fig. 2 shows an example LWA radiation pattern normalized per frequency for a LWA with a plate separation of $b = 1$ mm, slot length $L = 3$ cm, $\alpha = 50$ rad/m, and cutoff frequency $f_{co} = 150$ GHz. Observe the nonlinear frequency-angle coupling relationship described by Equation (4): lower frequencies emit towards larger angles whereas higher frequencies emit towards smaller angles. The frequency range spans from 150 GHz to 700 GHz for a receiver located from $10°$ to $80°$. Also, with a relatively small α, the beamwidth is quite narrow. Note that the attenuation constant relates to the radiation efficiency η by $\eta = 1 - e^{-2\alpha L}$, and thus $\alpha = 50$ rad/m yields a radiation efficiency $\eta = 95\%$.

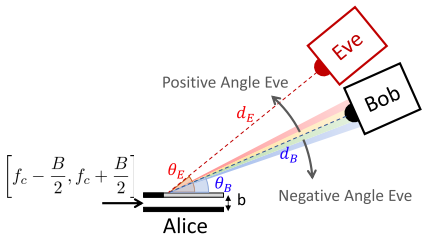

Fig. 3. Leaky wave antenna transmission under passive eavesdropping.

While different devices can have different frequency-angle coupling relationships, for instance, an S-shape frequency-angle relationship demonstrated in [35], angularly dispersive links are fundamentally characterized by two factors: the rate at which the radiation direction varies with frequency, and the beamwidth of each frequency. By exploring both factors in Sec. III-C, our results can be applied to general angularly dispersive links.

B. Steering From Alice to Bob

We model a THz local area network in which a transmitter (Alice) uses a LWA to transmit to a static receiver (Bob) located at an angle θ_B and a distance d_B, as illustrated in Fig. 3. Without loss of generality, the receiver is modeled as an isotropic antenna. For the THz local area network, we envision the transmission distance to be a few meters to tens of meters [53]. Assume Alice has acquired Bob's angular location θ_B via a path discovery phase [32]. To reach Bob, Alice selects f_c, the center frequency for the transmission, as the frequency that emits towards Bob's angle according to the known frequency-angle relationship, $\theta_{max}(f_c) = \theta_B$. When Alice employs a transmission bandwidth B, the frequency band chosen for the transmission is $[f_c - \frac{B}{2}, f_c + \frac{B}{2}]$. The frequency band is further divided into K subchannels, each with a bandwidth of $\frac{B}{K}$.

To model the resulting signal strength in space, we assume the subchannel bandwidth B/K is narrow enough and the strength S in the k-th frequency channel can be approximated at f_k, the center frequency of channel k. Assume Alice employs a uniform transmit power P for each frequency channel $k \in \{1,\cdots,K\}$, in the line-of-sight (LoS) scenario, the received signal strength S at location at location (d,θ) in the k-th frequency can then be represented as

$$S_{(d,\theta)}(f_k) = P\cdot\gamma(d,f_k)\cdot|G(f_k,\theta)|^2, \quad (5)$$

where $\gamma(d,f)$ is the channel gain from the transmitter to the receiver, which is assume to follow the free-space pathloss, $\gamma(d,f) = (4\pi df/c)^2$. Thus, for Bob at angle θ_B and distance d_B, the SNR is

$$\text{SNR}_k^{Bob} = \frac{P\cdot\gamma(d_B,f_k)\cdot|G(f_k,\theta_B)|^2}{\sigma_B^2}, \quad (6)$$

where σ_B^2 is the noise power at Bob, which is assumed to be flat across the whole transmission band.

C. Threat Model

As Alice transmits to Bob with the selected frequency band, an eavesdropper (Eve) tries to intercept the signals from Alice

to Bob. For a single Eve located at an angle θ_E and a distance d_E, her subchannel SNR can be expressed as

$$\text{SNR}_k^{Eve} = \frac{P \cdot \gamma(d_E, f_k) \cdot |G(f_k, \theta_E)|^2}{\sigma_E^2}, \tag{7}$$

where σ_E^2 is the noise power at Eve, which is assumed to be flat across the whole transmission band and is independent of Bob's noise.

We observe that Eve's subchannel SNR differs from Bob's subchannel SNR due to pathloss, noise power, and antenna gain. The effect of pathloss and noise power is clear. Namely, Eve has an advantage for eavesdropping when the channel gain is higher (smaller pathloss) or the noise power is lower, and thus resulting in a higher SNR. Therefore, without loss of generality, we assume Eve have no advantage on pathloss and noise power compared to Bob. That is, Bob and Eve have the same noise power across the transmission band $\sigma_B^2 = \sigma_E^2$, and experience the same pathloss $\gamma(d_B, f_k) = \gamma(d_E, f_k)$ by locating at the same distance from Alice. $d_B = d_E$.

In contrast, the effect of the LWA radiation is rather complicated, as it varies with different subchannels. With angular dispersion, both Bob and Eve are expected to receive nonuniform signal strength across the frequency channels, and thus the secrecy level is expected to vary within the transmission band. This novel frequency-varying physical layer secrecy behavior is a key focus of this study.

D. Security Metric

Despite the broadcast nature of wireless channels, secrect transmission is possible considering different channel conditions at Bob and Eve [54], [55], [56]. Specifically, when Eve has a worse channel condition than Bob, a positive rate of secrecy can be achieved between Alice and Bob. That is, when Eve's observation through her channel contains less information compared to Bob, the information gap between Bob and Eve enables the secret transmission between Alice and Bob. The highest achievable secrecy rate is defined as secrecy capacity.

For frequency-varying channels as seen in the LWA link, the total secrecy capacity is the integral across the transmission band. As an approximation, we calculate subchannel secrecy capacity assuming the channel is frequency-flat within the subchannel and consider the total secrecy capacity to be the summation of subchannel secrecy capacity across independent subchannels [57]. Specifically, subchannel secrecy capacity for subchannel k is defined as [56]

$$C_S^k = \frac{B}{K}\left[\log_2\left(1+\text{SNR}_k^{Bob}\right) - \log_2\left(1+\text{SNR}_k^{Eve}\right)\right]^+, \tag{8}$$

where $[x]^+ = \max\{0, x\}$. And the total secrecy capacity of the LWA is $C_S = \sum_{k=1}^{K} C_S^k$. Thus, Alice can be viewed as dividing her data to Bob over different channels, each of which must be considered separately in order to characterize the aggregate effect.

III. LWA Link Security Properties

In this section, we study the security properties of LWA links and their differences from conventional directional links via the physics-based model described in Sec. II. While the findings here are based on the LWA radiation model, they can be generalized to other antennas with angular dispersion.

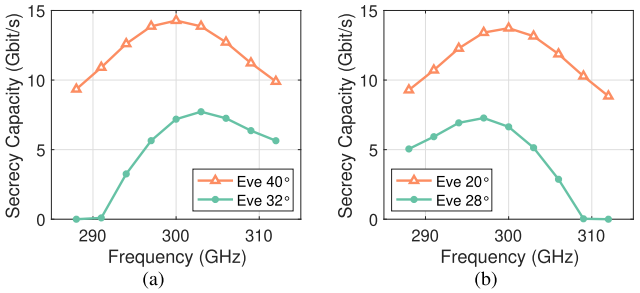

Fig. 4. Non-uniform subchannel secrecy capacity of a LWA link for Bob at 30° with a transmission bandwidth of 27GHz, for (a) positive angle Eve and (b) negative angle Eve.

A. Geometry Dependent Non-Uniform Secrecy

Because of the LWA's coupling between frequency and space, the non-uniform secrecy across the frequency domain depends directly on Bob and Eve's geometry in the spatial domain. To illustrate this phenomena, we present a specific example of how Bob and Eve's location determines the secrecy level across the transmissions band. Moreover, we show how edge frequencies, although being vulnerable for a wider Eve locations, prevent Eve from receiving information across the whole transmission band.

1) Subchannel Secrecy: From Sec. II, we know that lower frequencies emit towards larger angles and higher frequencies towards smaller angles. The varying radiation pattern for different frequencies leads to varying SNR at Bob and Eve across frequency, resulting in a non-uniform secrecy level across the transmission band. To explore the underlying mechanisms that control this change, we numerically compute the subchannel secrecy capacity for Eve located at an angle larger than Bob's angle, which we call positive angle Eve in the following. In this scenario, Bob locates at 30° and Eve locates at 32° or 40°, representing an angularly close and far Eve respectively. While we only examine Eve at angular locations within a few degrees from Bob, all the key performance metrics vary only in a limited angular range since the link is directional.

For the model-driven analysis, we employ parameters corresponding to our experimental setup in Sec. IV. The LWA has a plate separation $b = 1$ mm, slot length $L = 3$ cm, and $\alpha = 50$ rad/m, which is the same as the example we show in Fig. 2. According to the LWA parameters and Bob's location, the center frequency f_c of the transmission is 300 GHz. We use a transmission bandwidth of 27 GHz which is further divided into 9 subchannels, each 3 GHz wide, which also corresponds to the frequency resolution of the time-domain system we employ in the experiment. The transmission lies within a low atmospheric absorption window from 250 to 325 GHz, which is defined by the approved 802.15.3d standard [58]. The transmit power P of each subchannel is set to the value so that the SNR of the center frequency received at Bob is 15 dB. The subchannel SNR and secrecy capacity can then be calculated as described in Sec. II.

Fig. 4a shows the subchannel secrecy capacity across the 27 GHz transmission band. Note first that, as also occurs without LWAs, subchannel secrecy capacity is higher when Eve is at a greater angular distance from Bob. Indeed, the theoretical LWA radiation pattern in Equation (2) has a main lobe and side lobes following a complex sinc function. For the LWA parameters chosen in this example, the side lobes are barely visible because of the large magnitude difference

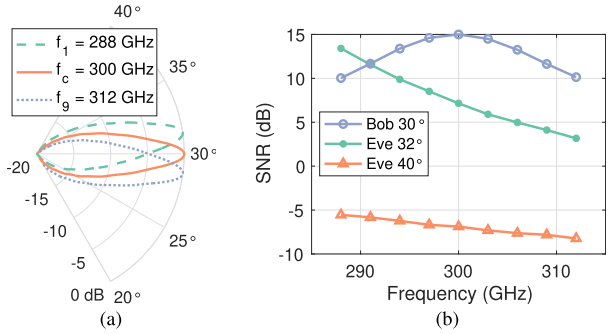

Fig. 5. (a) Radiation pattern. (b) Bob and Eve subchannel SNR. Bob locates at 30° and the bandwidth for the transmission is 27GHz.

between the main lobe and the side lobes. As a result, the farther Eve is relative to Bob, the weaker the signals Eve receives, resulting higher secrecy capacity across subchannels.

Next, we observe that the non-uniformity of subchannel secrecy capacity manifests as a concave function of frequency until reaching zero secrecy capacity. For Eve farther away angularly at 40°, the subchannel secrecy capacity peaks at the center frequency and drops nearly symmetrically towards the edge frequencies.

Lastly, we observe that, quite strikingly, when Eve is closer to Bob at 32°, subchannel secrecy capacity peaks at a frequency larger than the center frequency. Thus, despite having transmitted data equally above and below the center frequency, the curve does not peak at the center frequency. Moreover, the secrecy capacity drops faster towards the lower frequencies than towards to higher frequencies and drops to zero for the lowest two subchannels in this setup.

To explore the reason behind the peak shift and the aforementioned concavity and asymmetry, we next visualize the LWA transmissions in the spatial domain, and examine Bob and Eve's SNRs that result in the secrecy capacity. Fig. 5a illustrates the radiation patterns of the center (f_c), lowest (f_1), and highest (f_9) frequency channels of the 27 GHz transmission. From Fig. 5a, we clearly observe that the center frequency emits directly towards Bob at 30°, while higher and lower frequencies emit towards angles slightly smaller or larger from Bob, as dictated by the frequency-angle coupling in Equation (4). Based on the frequency-dependent radiation pattern, Bob and Eve's SNRs are shown in Fig. 5b.

From Fig. 5b, Bob indeed receives the highest SNR at the center frequency as the center frequency is chosen so that the radiation pattern maximizes at Bob's location, 30°. Since frequencies higher or lower than the center frequency have radiation patterns maximized slightly off Bob's angle, Bob receives a degraded SNR except for the center frequency.

In comparison, Eve's SNR decreases with frequency, for both Eve locations, with higher SNR when she is angularly closer to Bob. Moreover, while it is always beneficial for Eve to be angularly closer to Bob, her SNR decays more rapidly when she is closer. This is due to the relatively narrow radiation pattern as shown in Fig. 5a. In fact, the single-tone HPBW in this example is approximately 1.9°. For Eve located 10° away from Bob, she can barely receive the signals. In contrast, for Eve located only +2° away from Bob, she can receive higher SNR, especially for the frequencies having a radiation pattern towards a larger angle, that is, lower frequencies.

Understanding Bob and Eve's SNR, we can revisit the subchannel secrecy capacity trend in Fig. 4a. When Eve is at a positive angle with respect to Bob, she intercepts lower frequencies better. However, when Eve is angularly separated from Bob, the SNR across the transmission band is low and the secrecy capacity is mainly determined by Bob's SNR. Thus, secrecy capacity is highest at the center frequency and lower on the edges when Eve is far from Bob. In contrast, when Eve is closer to Bob, Eve's advantage on lower frequencies becomes more evident yielding two effects: *(i)* the peak secrecy level is no longer at the center frequency but has now moved higher and *(ii)* at lower frequencies, Eve's high SNR sharply reduces secrecy capacity. At higher frequencies, Eve has moderately diminishing reductions in SNR. Yet, Bob's SNR also suffers from the off-target radiation at higher frequency channels, yielding a nearly flat but modestly decreasing secrecy capacity.

While Fig. 4a examines positive angle Eve, Fig. 4b demonstrates the subchannel secrecy capacity when Eve is on the negative angle side of Bob. From Fig. 4b, we observe an opposite trend compared to Fig. 4a, showing a negative angle Eve having an advantage for the higher frequency channels when she is at a smaller angle compared to Bob.

While Eve is at the same distance as Bob in the above evaluation, we note that the non-uniform secrecy as observe in Fig. 4 remains even for a different eavesdropping distance. When varying the eavesdropping distance, a relatively frequency-flat pathloss is introduced to Eve's received signal, so that Eve's SNR is shifted by a constant across the frequency channels. For example, if Eve is at a closer distance to Alice than Bob, Eve's SNR will be shifted upward in Fig. 5b. With a similar concave SNR at Bob and the decreasing SNR at Eve, subchannel secrecy capacity across frequency channels is expected to be non-uniform even for different eavesdropping distances, just as shown in Fig. 4.

In summary, when Eve is more angularly separated from Bob, the subchannel secrecy level is mostly limited by Bob's SNR, which is highest for the center frequency and lower towards the edge frequencies. However, as Eve approaches Bob, the secrecy level suffers from frequency-biased SNR loss and Eve impairs the secrecy level of the lower frequencies more.

2) Vulnerable but Complementary Edge Frequencies: In the previous subsection, we observe the non-uniform secrecy level across the transmission band for a LWA link, indicating that some frequency components, more likely the edge frequencies, have lower secrecy level due to both Bob's SNR limitation and Eve's frequency-biased eavesdropping. Here, we show that in addition to suffering from reduced secrecy capacity, the edge frequencies are also more vulnerable in the spatial domain.

To this end, we define an "insecure zone" for each subchannnel. Specifically, an insecure zone is an angular region in the spatial domain such that when Eve locates within the insecure zone, the secrecy level of that subchannel is below a certain threshold. In other words, the subchannel is less secure than a certain criterion when Eve falls within this angular region. Since the edge frequencies suffer from lower subchannel secrecy capacity due to Bob's SNR limitation, we define the insecure zone based on a per-channel normalization. Without the per-channel normalization, the resulting insecure zone would penalize edge frequencies.

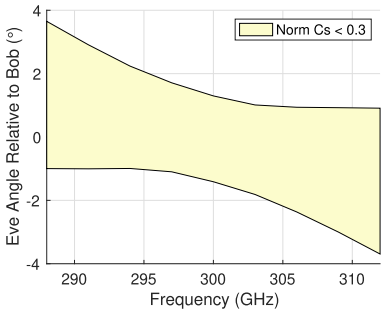

Fig. 6. Insecure zone of each subchannel with a threshold of 0.3 illustrates vulnerable but complementary edge frequencies. Bob locates at 30° and the bandwidth for the transmission is 27GHz.

In particular, we define insecure zone based on the normalized subchannel secrecy capacity, which is subchannel secrecy capacity normalized to the subchannel Shannon capacity:

$$C^k_{S,\text{norm}} = \frac{C^k_S}{\frac{B}{K}\log_2\left(1+\text{SNR}^{Bob}_k\right)}.$$

Thus, normalized subchannel secrecy capacity ranges from 0 to 1. When Eve does not exist, the subchannel secrecy capacity equals to the subchannel Shannon capacity, making the normalized subchannel secrecy capacity to be 1. In contrast, when Eve receives the same or even higher SNR than Bob for a certain subchannel, the normalized secrecy capacity is 0. The normalized secrecy capacity not only provides a fair comparison for different channels, but it also has a physical meaning and represents the percentage of communication capacity that can be for secure transmission between Alice and Bob.

Following the previous setup, we continue to study the case when Bob is at 30° for a transmission bandwidth of 27 GHz, using the same LWA parameters as before. Eve locates within 10° around Bob, both on the positive side and negative side. The normalized channel secrecy capacity is computed for all eavesdropping angles so that the insecure zone can be determined accordingly.

Fig. 6 shows the insecure zone of different subchannels for Bob at 30° based on a threshold of 0.3. First, we observe that no frequency achieves a normalized secrecy capacity more than 0.3 when Eve is sufficiently close to Bob (within about 1°). However, edge frequencies have a normalized secrecy capacity below 0.3 for a wider range of eavesdropping angles than the center frequency. Specifically, lower frequency components remain insecure for a larger angle range for Eve located at a greater angle than Bob, whereas higher frequency components are vulnerable under a wider range of locations when Eve has a lower angle than Bob.

From Fig. 6, we observe that the edge frequencies are relatively more vulnerable in the spatial domain compared to the center frequency for a LWA link, which is a characteristic not present in conventional directional links. As an example, if the link has no angular dispersion so that all frequency channels exhibit the same radiation pattern as the center frequency at 300 GHz, the insecure zone of all frequency channels should have been within 1° from Bob. In contrast, the radiation pattern of a LWA varies with frequency. Consequently, the lower frequency with a radiation pattern that peaks at a angle slightly larger than Bob's location are more vulnerable to a positive angle Eve. Similarly, high frequency component whose radiation maximizes at a smaller angle than Bob's are more exposed to a negative angle Eve.

Fortunately, although edge frequencies are more vulnerable in the spatial domain for a LWA link, their insecure zones fall in different regions. As a result, although a single Eve can intercept either the lower edge or the higher edge of the transmission band more easily, it is still hard for Eve to get both at the same time. That is, when the secrecy level of one edge gets low, the secrecy level of the other edge remains high, complementing each other. While Fig. 6 illustrates the insecure zone for a same-distance Eve, the trend remains also for Eve at a closer or further distance from Alice.

While leveraging the unique security property to achieve a more secure link is not the focus of the paper, we point out that the complementary property of edge frequencies has great potential in preserving link secrecy despite the vulnerability at edge frequencies. In the most simplified form to illustrate, we can assume that half of the subchannels are exposed to a single Eve at a fixed location, whereas the other half of the subchannels remain secure, for all Eve locations. In this case, even without knowing Eve's location, Alice can distribute two shares of information into the two sets of subchannels so that only when both shares are received can the receiver decode the information [59]. Eve, being able to receive only half of the subchannels and thus only one share, fails to decode any information from Alice to Bob, even if she intercepts half of the subchannels. For the extension to the simplified discussion above, please see our follow-up work on secure angularly dispersive links with coding [60].

In summary, we find that edge frequencies of a LWA transmission are more vulnerable in the spatial domain compared to the center frequency. Nonetheless, we also find that the secrecy level of the two edges complement each other, preventing Eve from intercepting the entire transmission band. These properties are unique to a link exhibiting an angle-frequency coupling and has a great potential in realizing a secure transmission.

B. Bandwidth and Beamwidth Coupling

1) LWA Beamwidth Increases With Bandwidth: For traditional directional transmissions, beamwidth is determined by the size of the antenna array, or physical shape of the antenna (e.g. horn antennas), and therefore the beamwidth is fixed regardless of the bandwidth chosen, up to some cutoffs. However, since LWA links are based on the frequency-angle coupling property, the larger the bandwidth, the wider the angular span of the selected frequencies, resulting a wider beam. In the following, we use collective radiation pattern and single-tone radiation pattern to distinguish between the overall link spanning the transmit bandwidth B and the individual frequencies that constitute the beam. If not specified, we refer to the collective beam.

To quantitatively examine the signal footprint expansion with transmission bandwidth, we define the collective radiation $G_{sum}(f_c, B)$ for band centered at f_c with bandwidth B is obtained by summing the radiation across the frequency band:

$$G_{sum}(f_c, B) = \int_{f_c-\frac{B}{2}}^{f_c+\frac{B}{2}} G(f,\theta)\, df \tag{9}$$

Fig. 7 illustrates the normalized single-tone radiation pattern G and the normalized collective radiation pattern G_{sum} for

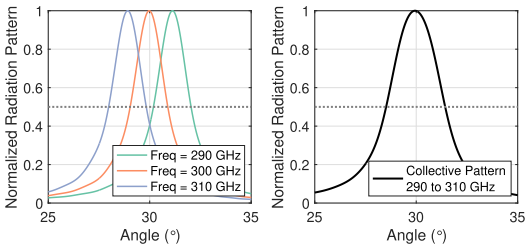

Fig. 7. Single-tone (left) and collective radiation patterns (right) for transmission from 290 GHz to 310 GHz.

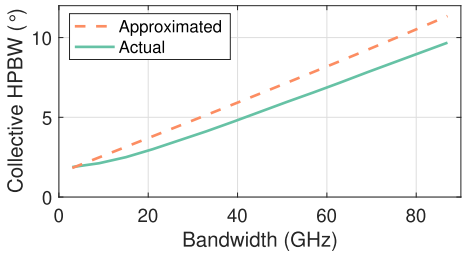

Fig. 8. The collective HPBW of LWA link when the bandwidth increases from 3 GHz to 87 GHz, for Bob at 30° with center frequency $f_c = 300$ GHz.

the transmission from 290 GHz to 310 GHz. From Fig. 7, we observe that the collective transmission with a bandwidth becomes wider in space. From the single-tone and collective radiation pattern G and G_{sum}, we then obtain their HPBWs that quantify the signal footprint.

While the beamwidth obtained based on the collective radiation pattern is exact, the scaling is less intuitive. Thus, in addition to the actual beamwidth obtained from the radiation pattern G_{sum}, we approximate the collective beamwidth by the angular span of the transmission, from channel 1 emitting towards $\theta_{max}(f_1)$ to channel K emitting towards $\theta_{max}(f_K)$, with a single-tone HPBW $\Delta\theta_{sgl}$:

$$\Delta\theta_{sum} \approx \left|\theta_{max}(f_1) - \theta_{max}(f_K)\right| + \Delta\theta_{sgl}, \qquad (10)$$

where the model-based single-tone HPBW is $\Delta\theta_{sgl} = 2\alpha b/\pi$ [51], [61].

To examine the bandwidth and beamwidth coupling, we apply the same setup as before with the exception that rather than fixing the bandwidth to 27 GHz, we consider bandwidths from 3 GHz to 87 GHz. Fig. 8 illustrates the actual and approximated HPBW of the all-tone radiation pattern as the bandwidth increases for Bob at 30°. We observe that both the actual beamwidth and the approximated beamwidth increase nearly linearly with bandwidth. Indeed, due to the widening angular span as the total bandwidth of the selected frequencies increases, the collective HPBW also increases.

However, from Fig. 8, we further observe that the actual collective HPBW is smaller than the beamwidth approximated by the angular span of the transmission. This result shows that the actual beamwidth and the angular span are highly correlated, but not the same. Indeed, the approximated beamwidth by angular span covers a wider angular range due to the more relaxed constraint: only one frequency channel is required to be received within 3dB. In contrast, the actual HPBW is based on the sum of radiations across all frequencies, and thus the beamwidth characterizes the angular region where the collective radiation across the transmission band is large enough, not in just one frequency channel.

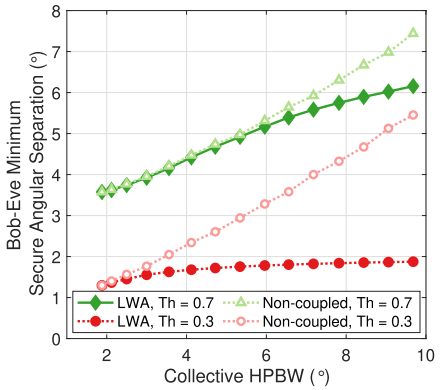

Fig. 9. Minimum angular separation between Bob and a positive-angle Eve required to achieve a certain normalized secrecy capacity as the transmission beamwidth increases due to increasing bandwidth, for two thresholds $[0.3, 0.7]$. The non-coupled baseline is a hypothetical link with the same collective radiation pattern that widens with bandwidth as the LWA link but has no frequency-angle coupling.

Despite the difference between the actual and approximated collective beamwidth, Fig. 8 clearly demonstrates a coupling between bandwidth and beamwidth, which suggests an unfortunate choice between large bandwidth (higher data rate) and a narrow beam (better security resilience). While a wider beam lessens security resilience for a conventional directional link, we will show that it is more complicated for a LWA link.

2) Large Bandwidth Comes With Little Security Sacrifice: As described above, larger bandwidth implies a wider beam for a LWA link. Typically one would expect a less directional transmission to be less secure. While this statement is still true for a LWA link, we will show that the security degradation is substantially less than a conventional link without the frequency-angle coupling property.

To compare the secrecy level under different bandwidth, a metric that does not scale with the bandwidth is needed. Thus, we define "normalized secrecy capacity" as the total secrecy capacity divided by Bob's total Shannon capacity

$$C_{S,\text{norm}} = \frac{C_S}{\sum_{k=1}^{K} \frac{B}{K} \log_2\left(1 + \text{SNR}_k^{Bob}\right)}$$

which is between 0 and 1 and represents the percentage of information that is secure.

We further introduce a concept of "security separation" based on the normalized secrecy capacity. For a directional transmission, the normalized secrecy capacity is lower when Eve is angularly closer to Bob. To achieve a certain secrecy target, Eve has to locate angularly separately enough from Bob. That is, a "security separation" is required to achieve a certain secrecy level. A small security separation is desired for directional transmission, because it means that the link fails to provide the targeted secrecy level only when Eve locates in a small angular region. Typically, to maintain a certain secrecy level, the security separation between Bob and Eve is expected to be larger when a wider beam is used. Also, when considering a certain directional transmission, the security separation between Bob and Eve is expected to be larger when a higher secrecy level is required.

Fig. 9 demonstrates the security separation required to achieve certain secrecy levels as the beam widens when Eve locates at an angle larger than Bob's angle. Recall that beamwidth is determined by bandwidth for the LWA link and

they have a nearly proportional relationship as shown in Fig. 8. Thus, the x-axis in Fig. 9 also represents increasing bandwidth. In addition to the LWA link represented by solid lines, the dashed lines marked as "non-coupled" are also shown for comparison, representing a hypothetical link that has the same widening collective radiation pattern as the LWA link but no frequency-angle coupling property, i.e., radiation pattern remains the same for all frequency channels.

Fig. 9 shows the required security separation for two normalized secrecy capacity thresholds: 0.3 and 0.7. These two thresholds are chosen to show the two extreme cases: low and high normalized secrecy capacity. The general trends confirm that the security separation between Bob and Eve needs to be larger when the required secrecy level is higher, and the security separation is smaller when the beam is narrower, suggesting that the narrower beam is more secure. However, the striking behavior is that security separation scales differently according to the targeted secrecy levels. When only 30% of the communication capacity is used for secure transmission, the required angular separation between Bob and Eve barely increases as the beam widens. In contrast, when a larger portion of the communication capacity is used for secure transmission, the security separation between Bob and Eve increases more as the beamwidth grows.

The almost flat angular separation curve under the lower secrecy requirement seems too good to be true, because it suggests that a fixed-location Eve at about 2° larger than Bob's angle barely benefits from a wider LWA beam. In comparison, the dashed line, which represents a link having the same radiation pattern as the LWA link but without the frequency-angle coupling property, illustrates a more typical security separation trend: the security separation between Bob and Eve increases proportionally to the collective HPBW to maintain the goal of using 30% of the communication capacity for secure transmission. In contrast, the LWA security separation curve, shown in red, is almost flat given the same secrecy level target.

This counter-intuitive behavior comes from the diverging single-tone radiation pattern as the bandwidth increases. The newly added frequencies, one above the center frequency and the other below the center frequency, both radiate outward from Bob's angle, with the higher frequency towards the smaller angle and the lower frequency towards the larger angle. When Eve is not extremely close to Bob angularly, only one of the newly added edge frequencies is more accessible, while the other edge frequency falls out of reach.

For example, a positive Eve will intercept the lower frequency edge much better than the higher frequency if Alice and Bob increase their transmission bandwidth. That is, when expanding the bandwidth, Alice and Bob can expect a portion (less than 50%) of the newly added capacity being secure against eavesdropping as long as Eve is not very close to Bob. As a result, the minimum secure angular separation does not substantially increase if the required secrecy threshold is low.

However, when a larger portion of the communication capacity is employed for secure transmission, Alice and Bob need all frequencies, not just part of them to be resilient against eavesdropping. Therefore, the minimum security separation between Bob and Eve need to be wider with increasing bandwidth so that both of the newly added edge frequencies are protected. Thus, we observe that in Fig. 9 security separation scales much faster when the threshold is 0.7 compared to a threshold of 0.3. Indeed, we observe that the scaling between the LWA and the traditional non-coupled system converges for a threshold of 0.7. Yet, we point out the angular dispersion still benefits the LWA link compared to a non-coupled link, as shown by the divergence of the solid dark green curve and the dotted light green curve in the larger bandwidth regime.

We note that non-coupled baseline link widens with increasing bandwidth, and thus does not represent the typical bandwidth increase in conventional directional links. For a non-widening link, the minimum angular separation between Bob and Eve remains the same and does not increase with bandwidth. Thus, despite the surprisingly small increase in minimum secure angular separation for the LWA link, a conventional link that does not widen with bandwidth is still more secure.

In summary, it is true that the LWA link is more secure when the beam is narrower. However, link secrecy drops unexpectedly slowly when the beam is wider, especially when only a smaller portion of the communication capacity is used for secure transmission. Based on these observations, Alice can almost choose whatever bandwidth she wants without concern about the security penalty when employing only a smaller portion of the communication capacity for secure transmission. However, if a higher rate of secure transmission is needed, Alice still has to limit the transmission bandwidth in exchange for extra link secrecy.

C. Security of General LWA Links

In Sec. III-A and Sec. III-B, we examine a specific LWA link for Bob at 30° with fixed LWA parameters. In this subsection, we further study the security of general angularly dispersive links. Since angularly dispersive links are characterized by two main factors, namely, *(i)* how fast the radiation direction shifts with frequency, and *(ii)* how directional the beam is for each frequency channel, we systematically study these two factors in this section.

1) Different Angular Dispersion Levels: First, we examine how angular dispersion level impacts LWA link secrecy. Here, angular dispersion level characterizes how fast the radiation direction changes with frequency, where a higher angular dispersion level indicates a wider angular scanning range for the same bandwidth. Since the frequency-angle coupling is non-linear as shown in Equation (4), for different Bob locations, the same bandwidth results in different angular spans. Thus, by examining LWA links toward different Bob angular locations, we study how angular dispersion level impacts LWA link secrecy.

To formally characterize the angular dispersion level for LWA links toward Bob at different angular locations, we derive the change in radiation direction with frequency, $\frac{d\theta_{max}(f)}{df}$, from Equation (4):

$$\frac{d\theta_{max}(f)}{df} = \frac{-c}{2bf^2\sqrt{1-\frac{c^2}{4b^2f^2}}}. \tag{11}$$

From Equation (11), the negative sign represents the reverse relationship between frequency and the maximum radiation angle: higher frequency corresponds to smaller emitting angle. Equation (11) also shows that higher frequency makes a larger denominator, indicating that radiation direction changes less rapidly with frequency in a higher frequency regime. As a

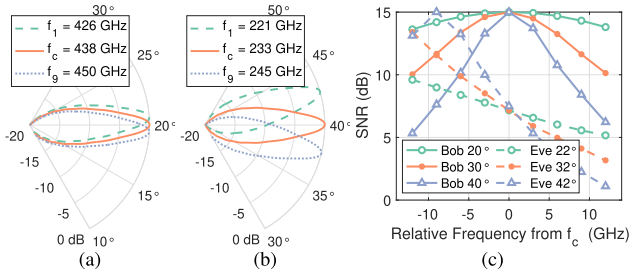

Fig. 10. (a)(b) Single-tone radiation pattern of center and edge frequencies for Bob at 20° and 40°. (c) Bob and Eve subchannel SNR for a transmission bandwidth of 27 GHz, for Bob at different angular locations and Eve at 2° positive to Bob.

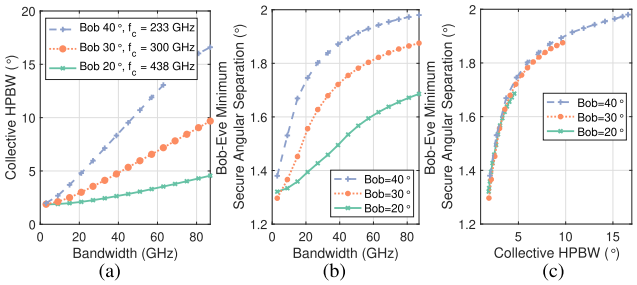

Fig. 11. (a) Collective HPBW and (b)(c) minimum angular separation between Bob and positive-angle Eve to achieve a normalized secrecy capacity of 0.3, for Bob at different angular locations.

result, when Bob locates at a smaller angle (corresponding to higher frequencies), the subchannel radiation directions within the selected bandwidth concentrate closer together, yielding a smaller angular dispersion level.

In the following, we examine LWA links toward Bob at 20°, 30°, and 40°, with Bob at a smaller angle experiencing a less angularly dispersive link. While Bob can locate outside 20° to 40°, the choice of these three angular locations allows us to examine the trend across angular locations. Here, we apply the same setup and LWA parameters as in Sec. III-B. For the three Bob locations, we consider the same set of bandwidths from 3 GHz to 87 GHz.

To demonstrate the varying angular dispersion level at different angular locations, Fig. 10a and Fig. 10b illustrate the single-tone radiation pattern of the center (f_c), lowest (f_1), and highest (f_9) frequency channels of a 27 GHz transmission, for Bob at 20° and 40°, respectively. We observe that the angular span of the transmission toward Bob at 40° is noticeably wider than the transmission towards Bob at 20°, despite the same transmission bandwidth. This result matches Equation (11) which indicates that the radiation direction shifts slower in the higher frequencies.

Next, we examine how angular dispersion level impacts Bob and Eve's received signal strength in each frequency channel. Fig. 10c compares the subchannel SNR for transmissions toward three Bob angular locations, 20°, 30°, and 40°, all with a total bandwidth of 27 GHz. The solid lines show Bob's SNR in each frequency channel, whereas the dashed lines show Eve's subchannel SNR when she is at 2° positive to Bob. We observe that, for the more angularly dispersive link (Bob at 40°), Bob's subchannel SNR decreases more significantly from the center frequency to edge frequencies. At the same time, the more angularly dispersive link allows the positive angle Eve to intercept the lower frequency channels with higher SNR. The decrease in Bob's subchannel SNR and the increase in Eve's subchannel SNR together suggest a less secure link when the link is more angularly dispersive.

Since the angular footprint of the transmission correlates to link secrecy, we next examine the collective HPBW of LWA links for different Bob locations. Fig. 11a demonstrates the link collective HPBW at different Bob locations as the bandwidth increases. We observe that, for Bob at different angles, the collective beamwidth of the LWA link increases at different rates with increasing bandwidth. When the bandwidth is 3 GHz, the collective HPBW at different Bob locations is similar (∼2°). As the bandwidth increases to 87 GHz, the collective HPBW increases for all Bob locations. However, the beamwidth increases much slower for Bob at 20° than Bob at 40°. When the bandwidth is 87 GHz, the collective HPBW is only 4.5° for Bob at 20°, whereas for Bob at 40°, the collective HPBW reaches 16.5°. Indeed, since LWA has a nonlinear frequency-angle coupling relationship described by Equation (4), the same selected bandwidth results in different collective radiation patterns considering different Bob locations.

With the beamwidth shown in Fig. 11a, we next examine the corresponding secrecy level of the LWA links. Similar to Sec. III-B, we employ the security separation metric to compare the eavesdropping resilience at different Bob locations. Namely, a larger minimum Bob-Eve angular separation indicates the normalized secrecy capacity is below the targeted threshold for a larger range of angle, and thus is less secure. We learn in Sec. III-B that the transmission bandwidth and the collective LWA beamwidth are positively correlated to the minimum Bob-Eve secure angular separation. Yet, we yet to know whether transmissions toward Bob at different angles yield a different behavior.

Fig. 11b and Fig. 11c show the minimum secure separation between Bob and Eve under a threat of a positive-angle Eve when the target normalized secrecy capacity is 0.3, as a function of total transmission bandwidth and collective HPBW, respectively. As before, we observe that the required angular separation between Bob and Eve increases with transmission bandwidth and HPBW, with the required Bob-Eve angular separation increment being only a fraction of the beamwidth increment, indicating relatively consistent link secrecy despite a significantly wider beam.

Next, when comparing the three curves representing three Bob angular locations, we observe that they cover different ranges of collective HPBW and different ranges of Bob-Eve angular separation. For the largest bandwidth of 87 GHz in the evaluation, Bob at 40° requires a Bob-Eve angular separation of almost 2° to achieve the targeted secrecy, while the same bandwidth transmission towards Bob at 20° only requires less than 1.7°. Indeed, from Fig. 11a, we know that the same bandwidth yields a wider collective HPBW for Bob at a larger angle due to LWA's nonlinear angle-frequency coupling. Fig. 11b and Fig. 11c further show that the larger collective HPBW for a larger-angle Bob results in a less secure link, indicated by a larger Bob-Eve angular separation requirement. This observation indicates that, despite employing the same LWA, the link secrecy varies when transmitting towards Bob at different angular locations, with a larger angle being less secure.

Yet, perhaps surprisingly, we observe that the same collective HPBW, despite for Bob at different angles, results in

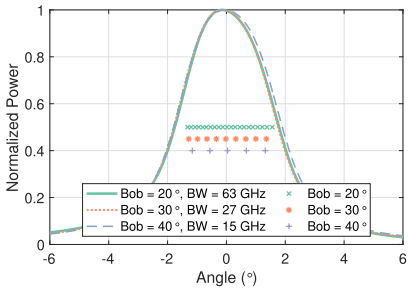

Fig. 12. LWA link collective radiation pattern and subchannel peaks for different Bob locations.

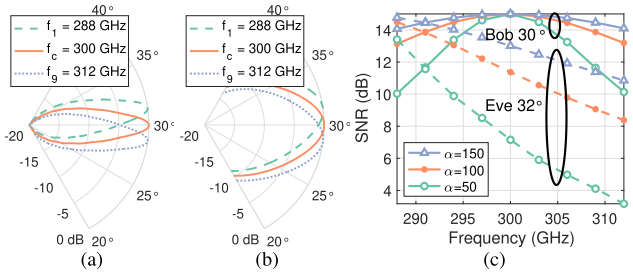

Fig. 13. (a)(b) Single-tone radiation pattern of center and edge frequencies for $\alpha = 50$ and $\alpha = 150$ rad/m. (c) Bob and Eve subchannel SNR for a transmission bandwidth of 27 GHz, for Bob at 30° and Eve at 32°.

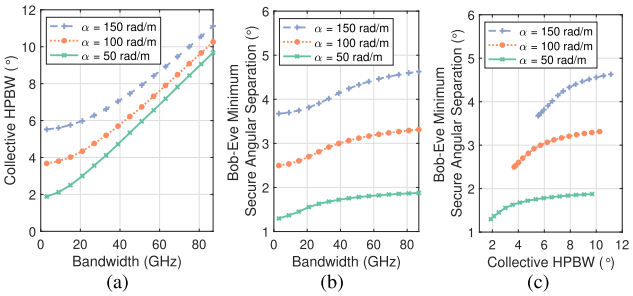

Fig. 14. (a) Collective HPBW and (b)(c) minimum angular separation between Bob and positive-angle Eve to achieve a normalized secrecy capacity of 0.3, for varying attenuation constant (α).

almost the same angular separation requirements to achieve the target secrecy, as shown by the almost overlapping curves in Fig. 11c. We emphasize that, even for the same beamwidth, the frequency components that constitute the collective transmission are different at different Bob angles. Thus, the collective HPBW being able to characterize the LWA link secrecy across different Bob angular locations is not evident.

To understand why LWA links for different Bob angles have a unified security behavior as shown in Fig. 11c, Fig. 12 shows the collective radiation pattern of the three LWA links with a similar collective HPBW of $\sim 3.6°$ for Bob at 20°, 30°, and 40°. To achieve the same collective beamwidth, different bandwidth values are used for different Bob angles. The radiation pattern is offset so that the target angle is aligned at 0°. Fig. 12 also shows the subchannel radiation peaks that constitute the link. Notice that the subchannel peaks are marked with arbitrary magnitude since the purpose is only to align them angularly side by side for comparison.

From Fig. 12, we observe that the collective beam patterns of the three similar-HPBW links are almost identical, despite the fact that the three collective patterns consist of different frequency components. Indeed, the subchannel peaks lie closer together for Bob at a smaller angle, matching Equation (11) that indicates the radiation direction varies slower with frequency for higher frequency (i.e., smaller Bob angle) regime. This denser subchannel beam distribution in the spatial domain allows the peaks of edge frequencies to spread wider in the angular domain and still results in the same radiation pattern for Bob at a smaller angle. Despite the difference in frequency components, the almost identical collective beamwidth explains the unified security behavior across different Bob angles.

From the above discussion, we find that the same LWA results in varying eavesdropping resilience when transmitting toward Bob at different angles due to different angular dispersion levels. Yet, we also see that LWA links towards Bob at different angles have a unified security behavior that can be characterized by the collective beamwidth, despite differences in subchannel radiation composition. While eavesdropping resilience can be characterized by collective HPBW for links formed with the same LWA with a consistent single-tone beamwidth across frequency, we next show that links formed by different LWAs with varying single-tone beamwidth can have very different eavesdropping resilience despite having the same collective signal footprint.

2) Different Single-Tone Beamwidths: In this subsection, we study the second factor that characterizes angularly dispersive links, namely, the directivity of each frequency channel. As modeled by Equation (2), the LWA radiation of each frequency component is a sinc-like pattern with the beamwidth depending on the attenuation constant α [51], [52], more specifically, $\Delta\theta_{sgl} = 2\alpha b/\pi$ as discussed in Sec. III-B. To explore how single-tone directivity impacts angularly dispersive link secrecy, we examine LWA links with varying LWA attenuation constant α.

To this end, we employ the same setup as in Sec. III-B for 3 α values: 50, 100, and 150 rad/m. Specifically, Bob is at 30° and the transmission bandwidth varies from 3 GHz to 87 GHz. In practice, the attenuation constant α can depend on multiple factors such as the LWA material and the width of the slot opening, and can vary for different LWA [62].

To demonstrate the varying single-tone beamwidth due to different attenuation constant α, Fig. 13a and Fig. 13b illustrate the single-tone radiation pattern of the center (f_c), lowest (f_1), and highest (f_9) frequency channels of a 27 GHz transmission, for attenuation constant $\alpha = 50$ and $\alpha = 150$ rad/m, respectively. We observe that for a larger attenuation constant α, the single-tone radiation is wider. Yet, varying α only changes the single-tone beamwidth but not the maximum angle it points to.

Next, we examine how the single-tone beamwidth impacts Bob and Eve's received signal strength in each frequency channel. Fig. 13c compares the subchannel SNR for transmissions using LWAs with different attenuation constants $\alpha = 50$, 100, and 150 rad/m toward Bob at 30°, all with a total bandwidth of 27 GHz. The solid lines show Bob's SNR in each frequency channel, whereas the dashed lines show Eve's subchannel SNR when she is at 2° positive to Bob. We observe that, when the single-tone beamwidth is wider ($\alpha = a50$ rad/m), both Bob's and Eve's subchannel SNR increases. Also, the SNR gap between Bob and Eve becomes smaller with a larger α, suggesting a less secure link when the single-tone beamwidth is wider.

Since the angular footprint of the transmission correlates to link secrecy, we next examine the collective HPBW of LWA links for different α values. Fig. 14a demonstrates the

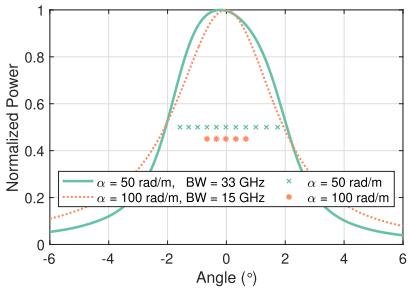

Fig. 15. LWA link collective radiation pattern and subchannel peaks for different attenuation constant α values.

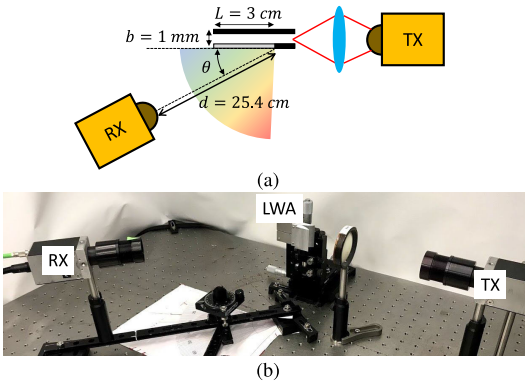

Fig. 16. (a) Experiment diagram. (b) Experiment setup.

link collective HPBW for LWAs with different α values. We observe that the collective HPBW scales with bandwidth, and a larger α (wider single-tone beamwidth) leads to a wider collective HPBW, as we expect.

We next quantify the link eavesdropping resilience by the required minimum security separation between Bob and Eve as in Sec. III-B. Fig. 14b and Fig. 14c demonstrate the minimum security angular separation between Bob and Eve required to achieve a target normalized secrecy capacity of 0.3 under a threat of a positive-angle Eve, as a function of bandwidth or collective HPBW, respectively.

From Fig. 14b, we observe that a larger transmission bandwidth results in a larger minimum secure angular separation, as we expect. In addition, we find that for LWA link with a larger α value, a wider angular separation is needed. We note that the maximum radiation direction for each frequency channel remains the same regardless of the α values, and thus the difference in minimum angular separation shown here is due to wider single-tone radiation.

We next examine whether the collective HPBW can characterize LWA link secrecy, as we observe in the previous subsection for different angular dispersion levels. From Fig. 14c, we find that the same collective HPBW can result in very different secrecy levels, unlike Fig. 11c. The required security separation increases by $\sim 1^\circ$ when α increases from 50 to 100 rad/m as well as from 100 to 150 rad/m, despite the same collective HPBW. This result clearly shows that the HPBW of the collective radiation pattern solely cannot characterize the eavesdropping resilience of an angularly dispersive link, especially when the single-tone directivity varies.

To understand why larger α results in a less secure link despite the same collective HPBW, we examine the collective radiation pattern and the subchannels that constitute the link for two α values. Specifically, we consider two links with collective HPBW $\sim 4^\circ$ via LWA with $\alpha = 50$ and 100 rad/m respectively. Also, different bandwidth are used to achieve the specific collective HPBW.

Fig. 15 shows the radiation pattern of the two links with a similar collective HPBW of $\sim 4^\circ$ and the subchannel radiation peaks that constitute the links. As before, the target angle (30° in this case) is offset to 0°. Also, the subchannel peaks are marked with arbitrary magnitude with the goal of aligning them angularly for comparison.

In Fig. 15, we observe that the two radiation patterns are quite different despite having a similar collective HPBW. Specifically, for the LWA link with a smaller α, the radiation pattern has a sharper drop at the edge of the main lobe. In contrast, the LWA link with a larger α shows a longer tail. Indeed, the longer tail in the larger α case is a result of wider single-tone radiation patterns. As each single-tone radiation pattern is wider, Eve can receive better signals at the same angular separation from Bob, resulting a less eavesdropping resilient link. Although the subchannel peaks spread wider in the angular domain for the smaller α LWA, the benefit of a narrower single-tone radiation pattern dominates and yields a more eavesdropping resilient link given the same collective HPBW.

From the above discussions on both varying Bob locations and varying single-tone beamwidths, we conclude that the collective HPBW is correlated to LWA link secrecy. While collective HPBW successfully characterizes LWA link secrecy for a single LWA transmitting towards different user angles, however, it cannot serve as a general indicator for eavesdropping resilience across different LWAs with different α values. Instead, LWA link secrecy requires consideration of the frequency components that constitute the transmission.

IV. Experimental Evaluation

In this section, we experimentally study the security of LWA links using over-the-air measurements and compare its properties with the above results based on models in Sec. III.

A. Experimental Setup

We measure the radiation pattern of a custom LWA device for experimental validation. The LWA consists of two 4×4 cm^2 metal plates with thickness of 1 mm. The two metal plates are connected by spacers at the 4 corners, making the plate separation $b = 0.95$ mm. We create a slot on one of the plate, with the slot length $L = 3$ cm and a slot width of 1 mm.

To measure the radiation pattern of the LWA, we use T-Ray 4000 TD-THz System [63] for generating and receiving THz signals. This system enables THz wideband measurements by generating a THz-range wideband source at the transmitter and logging time-domain samples at the receiver. The generated spectrum from the transmitter spans the range from below 150GHz to above 1.5 THz. On the receiver side, with the sampling rate of 12.8 THz (1 sample every 78 femtoseconds) and 4096 time-domain samples, we can observe frequencies with a resolution of 3.13 GHz.

Fig. 16a illustrates the experiment diagram and Fig. 16b demonstrates the experiment setup. During the measurement, the transmitter couples the THz pulse into the LWA. An additional lens is used to maximize the coupling from the

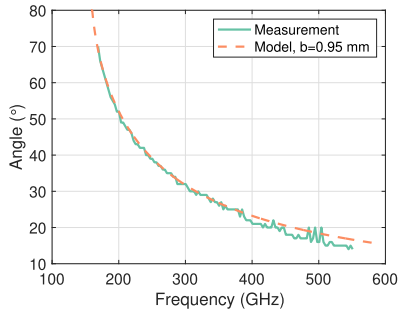

Fig. 17. Maximum radiation angle of each frequency.

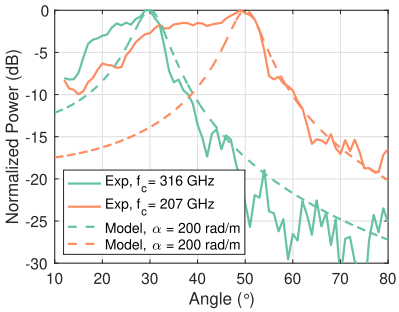

Fig. 18. Measured single-tone radiation pattern, matched with model prediction when $\alpha = 200$ rad/m.

THz source to the LWA. Different frequency components then emit from the LWA slot towards different angles. The receiver is placed facing the LWA slot at a distance $d = 25.4$ cm from the LWA. Both the transmitter and receiver are vertically polarized. The receiver has a lens with a diameter of 4 cm. At a distance of 25.4 cm, the lens has an aperture of $4.5°$. We place the receiver at $12° < \theta < 80°$ with $1°$ resolution in the measurement. To obtain precise receiver angle measurement, we place the receiver on a rail with one end centered at the LWA location, and measure the angle between the rail and a reference axis. While the transmission distance is relatively short in the experiments, we point out that it is due to the limitation of the low-power transmitter. With higher power transmitters, the transmission distance can be increased.

Once the time-domain samples at $12° < \theta < 80°$ are collected, the frequency spectrum of the received signals is obtained via discrete Fourier transform. As a result, we obtain a LWA dataset containing the frequency spectrum of all measured angles. Although the THz wideband signal is not flat across frequencies, by normalizing the received power per frequency, we obtain the radiation pattern per frequency.

B. The Alice-Bob LWA Link

Equation (4) characterizes the angle of maximum radiation as a function of the input frequency and is a key property of the LWA's angle-frequency coupling. Thus, we first examine how well the model predicts the measured values using the aforementioned experimental setup and present the results in Fig. 17. The results indicate an excellent match between frequencies of 169 and 388 GHz, with a slight deviation at the highest frequencies.

Next, we compare the measured radiation pattern against the model prediction. For the comparison, we select two frequency tones, 316 GHz and 207 GHz, which have maximum radiation toward $30°$ and $50°$ in the experiment. The model parameters are computed from the LWA's geometry with the exception of the attenuation constant α, since the attenuation constant is modeled with respect to parallel-plate LWA geometry and material in the literature. Hence, we fit the best empirical value of $\alpha = 200$ rad/m. Fig. 18 shows the measurement results along with the values predicted by Equation (2).

Beginning with the higher frequency of 316 GHz, we observe that the model succeeds in predicting peak reception at $30°$ and a generally decreasing trend above and below that angle. However, at lower angles, the model underestimates the received power. Likewise, for 207 GHz the model also correctly predicts peak radiation at $50°$ but the discrepancies at lower frequencies are even more pronounced, with the model severely under estimating antenna gain by over 10 dB at some angles. Thus, the measured beam exhibits strong asymmetry not predicted by the model. In contrast, at higher frequencies greater than the peaks, the measured power generally decreases with angle, albeit with non-monotonic and irregular deviations both above and below the model's predicted values. These irregularities reflect the imperfection of practical beams, and the larger fluctuations in the low power regime also reflect a greater impact of noise when the signal strength is low.

To understand the strong asymmetry exhibited in the measurements, we point out that the radiation model in Equation 2 assumes uniform electric field distributions across the slot width. Recent study [50] has shown that the assumption becomes invalid when the wavelength is comparable or smaller than the slot width, as in the THz regime, and resulting in a broad angle emission towards the smaller angles, matching the measured pattern shown in Fig. 18. With the irregularities and asymmetry in the measured radiation pattern, we next examine the resulting secrecy performance.

C. Empirical Security

Using the LWA over-the-air measurement, we experimentally evaluate the security of the Alice-Bob link by comparing Bob's receptions to Eve's and using the same security metrics as previously. In all cases, we compare to the model predictions as a baseline. As the above measurements indicate that the model does not capture the extent beam asymmetry and non-monotonic irregularities in beam pattern, this study will characterize how such modeling errors impact security properties.

1) Asymmetry: Since beam asymmetry is the main source of modeling error, we begin with that case. In particular, we first measure subchannel secrecy to examine eavesdropping asymmetry created by the asymmetric measured beam pattern. We examine the scenario where Bob is at $30°$, and Eve is either at a positive angle or negative angle from Bob. Analogous to the process in the model-driven analysis, we obtain the subchannel secrecy capacity of the LWA link from the measured radiation pattern. Since the frequency resolution of the LWA dataset is 3.13 GHz, each frequency in the LWA dataset represent the center frequency of a subchannel with bandwidth of 3.13 GHz. A bandwidth of 28 GHz, that is, 9 subchannels, is used in the transmission.

Fig. 19 depicts the experimental subchannel secrecy capacity across the 28 GHz for Bob at $30°$ and Eve locates on $+2°$ and $-2°$ relative to Bob. For comparison, the dotted lines shows the model predicted subchannel secrecy capacity based on the best matching $\alpha = 200$ rad/m.

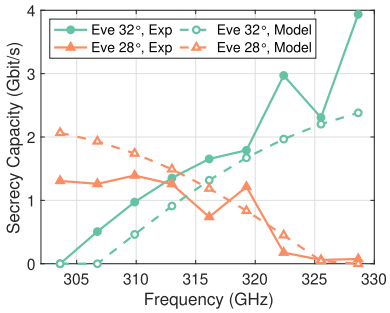

Fig. 19. Experimental subchannel secrecy capacity when Bob is at 30° and Eve is at 28° or 32°, with a total bandwidth of 28.2 GHz.

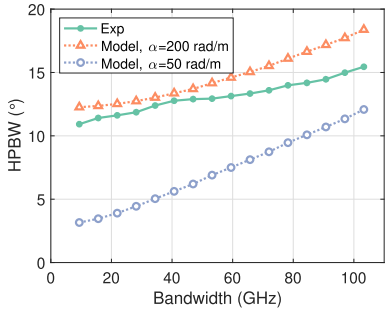

Fig. 20. Experimental all-tone HPBW as bandwidth increases compared to the model.

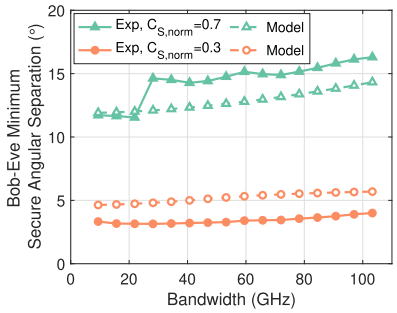

Fig. 21. The experimental minimum Bob-Eve angular separation required to achieve a targeted normalized secrecy capacity of 0.3 or 0.7.

First, observe that the experimental subchannel secrecy capacity follows the trend of the model predicted value. Despite the fluctuation likely due to noise and experimental error, subchannel secrecy capacity largely increases with frequency when Eve locates at an angle larger than Bob's angle, and largely decreases when Eve locates at a smaller angle compared to Bob.

However, we also observe that the experimental subchannel secrecy level is underestimated by the model when Eve is at 32°, but overestimated when Eve is at 28°. This eavesdropping asymmetry comes from the asymmetric beam. As we see in Fig. 18, the beam pattern decays more rapidly towards larger angles but decays much more slowly towards the smaller angles. This suggests that an eavesdropper located on a smaller angle than Bob's angle receives a higher SNR compared to a equal angularly separated Eve that locates on the larger angle side from Bob. As a result, the link secrecy level is lower in the presence of a negative angle Eve, implying that a negative angle Eve is a more devastating threat for the measured LWA link.

2) Bandwidth and Beamwidth Coupling: Since each frequency has a different radiation pattern, the collective beam pattern changes with the bandwidth of the transmission. Here, we study the experimental relationship between beamwidth and bandwidth using the same measurement setup and compare the results with the model. Two collective HPBW based on the model are shown in Fig. 20, one with $\alpha = 50$ rad/m studied in Sec. III-B, and the other is the best matching $\alpha = 200$ rad/m.

First, focusing on the model's prediction, observe that α impacts beamwidth scaling, as also observed earlier in Fig. 14a. Specifically, when α is larger, the collective beamwidth is larger and the beamwidth increases with bandwidth with more concavity. Since the collective beam pattern depends on each single-tone radiation pattern, when the single-tone radiation pattern is more directional (corresponding to a smaller α), so is the collective beam pattern. As to the more concave beamwidth growth when α is large, it represents a less drastic beam pattern change when the single-tone radiation pattern is wider, especially when the bandwidth is smaller.

However, the experimental results differ in two key ways. First, the experimental relationship does not exhibit the model's suggested concavity when the single-tone radiation is wider, but rather it is nearly linear with some irregularity at approximately 40 GHz of bandwidth. Second, the measurements have consistently smaller collective HPBW than predicted by the model based on the best matching $\alpha = 200$ rad/m. Nonetheless, the general trend of increasing beamwidth with bandwidth remains. Thus, we next experimentally study the bandwidth-beamwidth relationship on security.

3) Bandwidth, Beamwidth, and Security: Because beamwidth increases with bandwidth, it also impacts security. While we expect that wider beam transmissions are less secure, we found with the model that this is only marginally the case when the target secrecy level is 0.3 (cf. Sec. III-B). Here, we experimentally study the minimum Bob-Eve angular separation required to achieve targeted security thresholds: normalized secrecy capacity of 0.3 or 0.7, considering a positive angle Eve as in Sec. III-B. The results are shown in Fig. 21 along with the model predictions.

First, observe that with a lower security threshold of 0.3, the experiments also indicate a nearly-flat behavior. Thus, the unexpected behavior revealed by the model remains in the experimental system: as beamwidth widens due to increased bandwidth, the minimum secure angular separation remains nearly unchanged. Hence, if the security requirement is relatively low at 0.3, Alice and Bob can use wide bandwidth, desirable for increasing data rate, with minimal cost in vulnerability to Eve.

Next, for a higher security threshold of 0.7, the experiments follows the general trend of angular increase by the model prediction, despite local fluctuations and a sudden increase when the bandwidth expands from 21.9 GHz to 28.2 GHz. Regarding the local fluctuations, it is mainly due to the irregularities in the measured LWA beam. As for the sudden increase when the bandwidth expands from 21.9 GHz to 28.2 GHz, it is a result of a strong side lobe in one of the newly added frequency channels.

To support our analysis, Fig. 22 shows the radiation pattern of the edge frequency channels when the bandwidth increases from 21.9 GHz to 28.2 GHz, with Fig. 22a showing the lower edge frequency and Fig. 22b showing the higher edge frequency. Since the results in Fig. 21 are based on the threat of a positive angle Eve, Fig. 22 shows only the angles larger

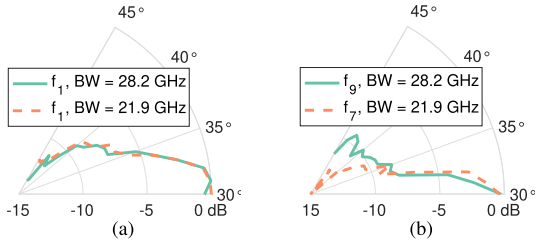

Fig. 22. Measured single-tone radiation patterns of the edge frequency channels for Bob at 30° for the (a) lower and (b) higher edge frequency channels, when the total bandwidth B increases from 21.9 GHz (total $K = 7$ frequency channels, green solid curves) to 28.2 GHz (total $K = 9$ frequency channels, orange dashed curves).

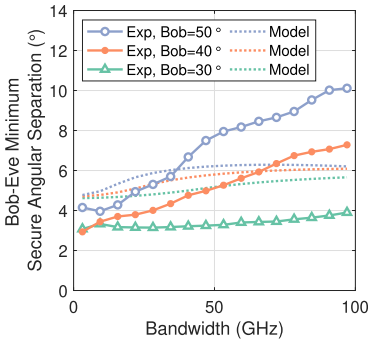

Fig. 23. The experimental minimum Bob-Eve separation required to achieve a normalized secrecy capacity of 0.3, for Bob and 30°, 40°, and 50°.

than $\theta_B = 30°$. When the transmission has a bandwidth of 21.9 GHz bandwidth (orange dashed curves), we observe that the two edge frequencies do not exhibit strong side lobes towards angles larger than Bob's angle at 30°. However, when the bandwidth increases to 28.2 GHz (green solid curves), we observe that one of the edge frequency channels, the higher one (f_9), exhibits strong side lobes all the way to 45°. Due to the leakage towards the angles larger than Bob's angle, Eve can obtain better signals for a larger angular span, and thus cause a sudden increase in Bob-Eve angular separation requirement in Fig. 21. We note that when the target normalized secrecy is lower, the side lobe does not have a strong impact. In comparison, when the target secrecy level is higher, the link secrecy is more sensitive to irregularities in practical beams.

Finally, in Fig. 21, we observe that the experimental minimum security separation is smaller than the model prediction for the lower security requirement of 0.3, but larger than the model prediction when the security requirement is higher at 0.7. Recall that the measured radiation pattern is asymmetric that the beam pattern on the smaller angle side of the peak is underestimated. When Eve locates relatively close to Bob on the larger angle side, the model underestimates the secrecy capacity and therefore predicts a larger minimum security separation. In contrast, the model predicts that the radiation pattern dies off almost monotonically and does not predict the possible side lobes in an actual LWA link. As a result, the model predicts a relatively optimistic minimum security separation, not incorporating the potential side lobes that would otherwise make the minimum security separation wider.

4) Security and Bob's Angle: In Sec. III-C, we learn that LWA transmissions towards Bob at different angular locations have different security levels since the same bandwidth yield different beamwidths, due to the nonlinear frequency-angle coupling. Here, we experimentally compare the LWA link secrecy for Bob at different angular locations. As before, we characterize the link secrecy by the minimum Bob-Eve angular separation required to achieve a normalized secrecy capacity of 0.3. A smaller Bob-Eve angular separation represents a more secure link.

Fig. 23 demonstrates the minimum Bob-Eve angular separation for LWA transmissions towards Bob at 30°, 40°, and 50°, for a normalized secrecy capacity of 0.3. As we expect, Fig. 23 shows that the minimum angular separation increases with a larger bandwidth for Bob at all three angular locations, due to an expanding signal footprint.

Next, when comparing the three angular locations, we find that Bob at a larger angle suffers from a less secure link, as indicated by a larger Bob-Eve angular separation requirement. Indeed, as we discuss in Sec. III-C, the radiation direction varies faster in lower frequencies due to LWA's nonlinear frequency-angle relationship. Thus, when employing the same bandwidth, the lower frequencies emitting towards Bob at a larger angle yield a larger signal footprint, requiring Eve to be more angularly separated from Bob to achieve the targeted normalized secrecy capacity. Thus, Fig. 23 shows that a higher angular dispersion degrades the link secrecy.

However, we observe a significant difference between the experimental results and the model-driven results based on an attenuation constant $\alpha = 200$ rad/m. More specifically, the model predicts a much slower increase in Bob-Eve angular separation with increasing bandwidth compared to the experimental results. The root cause of this difference can be traced back to the stronger beam asymmetry in lower frequency channels as we observe from Fig. 18. Due to beam asymmetry, Bob continues to receive high SNR in lower frequency channels even when the maximum radiation direction steers away from Bob, resulting in a higher total channel capacity. Since Bob's channel capacity becomes higher than the model prediction, achieving the targeted normalized secrecy capacity of 0.3 becomes harder, and thus requires a larger Bob-Eve angular separation in experiments.

V. Related Work on Directional Link Security

Prior works have studied the security improvement with directional beams in high-frequency bands, including millimeter wave [64], [65], [66], [67], THz [68], [69], [70], [71], [72], and visible light communication [73], [74]. It has been demonstrated in both theory [66] and in experiments [69] that a more directional link is more resilient to eavesdropping, yet, a capable Eve can still launch a successful attack by carefully placing an object [65], [69] or even a metasurface [75] to scatter the signal to her location. Prior works also proposed to secure the transmission by jointly exploiting multiple directional beams, either from multipath [70] or intelligent reflecting surface [76], [77], [78]. Further, the idea of creating range-dependent directional radiation for security was also investigated based on frequency diverse array [79], [80]. While these prior works investigate directional links with different spatial characteristics, the security of a link with frequency-dependent radiation patterns has not been studied. Our conference paper [1] and this extended article are the first to explore the security properties of a THz link exhibiting angle-frequency coupling and demonstrate a previously unidentified interplay between security and bandwidth.

Our follow-up research further investigates secure coding for directional links with angular dispersion and demonstrates a significant security degradation when the coding does not consider angular dispersion [60].

VI. Conclusion and Future Work

This paper presents, for the first time, a security study of a THz link with frequency-dependent radiation direction. Using LWA as a representative, we perform an analytic and experimental investigation to show how the unique angle-frequency coupling impacts security. For angularly dispersive links, we find that the secrecy level varies across the transmission band, with edge frequencies being more vulnerable. Also, we find that angle-frequency coupled links challenge our typical expectations on a directional link, such as a surprising coupling between the transmission bandwidth and the collective beamwidth, and an unexpectedly small security penalty compared to the signal footprint increment. In addition, we explore two fundamental factors that characterize angularly dispersive links: angular dispersion level and single-tone beamwidth, and show that a higher angular dispersion level and wider single-tone radiation result in a less secure link.

As the first security study on angularly dispersive links, we examine static links under the threat of a single Eve. Important issues regarding mobility, multiple colluding eavesdroppers, and generalization to 3D are left for future work.

Acknowledgment

This extended version demonstrates general LWA link secrecy for different target user angular locations and different LWA parameters numerically and experimentally (Sec. III-C and Sec. IV-C.4), updates existing figures and discussions, adds supporting figures (Fig. 5a, 7, and 22), and updates related works.

References

[1] C.-Y. Yeh, Y. Ghasempour, Y. Amarasinghe, D. M. Mittleman, and E. W. Knightly, "Security in terahertz WLANs with leaky wave antennas," in *Proc. 13th ACM Conf. Secur. Privacy Wireless Mobile Netw.*, Jul. 2020, pp. 317–327.

[2] T. Kleine-Ostmann and T. Nagatsuma, "A review on terahertz communications research," *J. Infr., Millim., Terahertz Waves*, vol. 32, no. 2, pp. 143–171, Feb. 2011.

[3] T. Nagatsuma et al., "Terahertz wireless communications based on photonics technologies," *Opt. Exp.*, vol. 21, no. 20, pp. 23736–23747, 2013.

[4] D. M. Mittleman, "Perspective: Terahertz science and technology," *J. Appl. Phys.*, vol. 122, no. 23, Dec. 2017, Art. no. 230901.

[5] I. F. Akyildiz, J. M. Jornet, and C. Han, "Terahertz band: Next frontier for wireless communications," *Phys. Commun.*, vol. 12, pp. 16–32, Sep. 2014.

[6] UFC Commission. (2019). *FCC Opens Spectrum Horizons for New Services & Technologies*. [Online]. Available: https://www.fcc.gov/document/fcc-opens-spectrum-horizons-new-services-technologies

[7] World Radiocommunication Conference. (2019). *Resolution 731: Consideration of Sharing and Adjacent-Band Compatibility Between Passive and Active Services Above 71 GHz*. [Online]. Available: https://www.itu.int/en/ITU-R/conferences/wrc/2019/Documents/PFA-WRC19-E.pdf

[8] S. Mumtaz, J. M. Jornet, J. Aulin, W. H. Gerstacker, X. Dong, and B. Ai, "Terahertz communication for vehicular networks," *IEEE Trans. Veh. Technol.*, vol. 66, no. 7, pp. 5617–5625, Jul. 2017.

[9] A. Moldovan, P. Karunakaran, I. F. Akyildiz, and W. H. Gerstacker, "Coverage and achievable rate analysis for indoor terahertz wireless networks," in *Proc. IEEE Int. Conf. Commun. (ICC)*, May 2017, pp. 1–7.

[10] S. Koenig et al., "Wireless sub-THz communication system with high data rate," *Nature Photon.*, vol. 7, no. 12, pp. 977–981, Dec. 2013.

[11] J. M. Jornet and I. F. Akyildiz, "Channel modeling and capacity analysis for electromagnetic wireless nanonetworks in the terahertz band," *IEEE Trans. Wireless Commun.*, vol. 10, no. 10, pp. 3211–3221, Oct. 2011.

[12] S. Gupta, S. Abielmona, and C. Caloz, "Microwave analog real-time spectrum analyzer (RTSA) based on the spectral–spatial decomposition property of leaky-wave structures," *IEEE Trans. Microw. Theory Techn.*, vol. 57, no. 12, pp. 2989–2999, Dec. 2009.

[13] D. Piazza, M. D'Amico, and K. R. Dandekar, "Performance improvement of a wideband MIMO system by using two-port RLWA," *IEEE Antennas Wireless Propag. Lett.*, vol. 8, pp. 830–834, 2009.

[14] M. Poveda-García, A. Gömez-Alcaraz, D. Cañete-Rebenaque, A. S. Martinez-Sala, and J. L. Gómez-Tornero, "RSSI-based direction-of-departure estimation in Bluetooth low energy using an array of frequency-steered leaky-wave antennas," *IEEE Access*, vol. 8, pp. 9380–9394, 2020.

[15] A. Gil-Martínez, M. Poveda-García, J. A. López-Pastor, J. C. Sánchez-Aarnoutse, and J. L. Gómez-Tornero, "Wi-Fi direction finding with frequency-scanned antenna and channel-hopping scheme," *IEEE Sensors J.*, vol. 22, no. 6, pp. 5210–5222, Mar. 2022.

[16] J. L. Gómez-Tornero, "Smart leaky-wave antennas for iridescent IoT wireless networks," in *Antenna and Array Technologies for Future Wireless Ecosystems*. Wiley, 2022, pp. 119–181.

[17] S.-W. Qu, H. Yi, B. J. Chen, K. B. Ng, and C. H. Chan, "Terahertz reflecting and transmitting metasurfaces," *Proc. IEEE*, vol. 105, no. 6, pp. 1166–1184, Jun. 2017.

[18] D. Headland, Y. Monnai, D. Abbott, C. Fumeaux, and W. Withayachumnankul, "Tutorial: Terahertz beamforming, from concepts to realizations," *APL Photon.*, vol. 3, no. 5, May 2018, Art. no. 051101.

[19] S.-W. Qu, L. Xiao, H. Yi, B.-J. Chen, C. H. Chan, and E. Y. Pun, "Frequency-controlled 2-D focus-scanning terahertz reflectarrays," *IEEE Trans. Antennas Propag.*, vol. 67, no. 3, pp. 1573–1581, Mar. 2019.

[20] J. Tan and L. Dai, "Delay-phase precoding for THz massive MIMO with beam split," in *Proc. IEEE Global Commun. Conf. (GLOBECOM)*, Dec. 2019, pp. 1–6.

[21] R. J. Mailloux, *Phased Array Antenna Handbook*, 3rd ed. Norwood, MA, USA: Artech House, 2017.

[22] A. Sutinjo, M. Okoniewski, and R. Johnston, "Radiation from fast and slow traveling waves," *IEEE Antennas Propag. Mag.*, vol. 50, no. 4, pp. 175–181, Aug. 2008.

[23] N. J. Karl, R. W. McKinney, Y. Monnai, R. Mendis, and D. M. Mittleman, "Frequency-division multiplexing in the terahertz range using a leaky-wave antenna," *Nature Photon.*, vol. 9, no. 11, pp. 717–720, Nov. 2015.

[24] K. Murano et al., "Low-profile terahertz radar based on broadband leaky-wave beam steering," *IEEE Trans. Terahertz Sci. Technol.*, vol. 7, no. 1, pp. 60–69, Jan. 2017.

[25] J. Ma, N. J. Karl, S. Bretin, G. Ducournau, and D. M. Mittleman, "Frequency-division multiplexer and demultiplexer for terahertz wireless links," *Nature Commun.*, vol. 8, no. 1, pp. 1–8, Sep. 2017.

[26] M. Steeg and A. Stöhr, "High data rate 6 Gbit/s steerable multi-beam 60 GHz antennas for 5G hot-spot use cases," in *Proc. IEEE Photon. Soc. Summer Topical Meeting Ser. (SUM)*, Jul. 2017, pp. 141–142.

[27] B. Zhai, Y. Zhu, A. Tang, and X. Wang, "THzPrism: Frequency-based beam spreading for terahertz communication systems," *IEEE Wireless Commun. Lett.*, vol. 9, no. 6, pp. 897–900, Jun. 2020.

[28] Y. Ghasempour, Y. Amarasinghe, C.-Y. Yeh, E. Knightly, and D. M. Mittleman, "Line-of-sight and non-line-of-sight links for dispersive terahertz wireless networks," *APL Photon.*, vol. 6, no. 4, Apr. 2021, Art. no. 041304.

[29] Z. Lin, L. Wang, B. Tan, and X. Li, "Spatial-spectral terahertz networks," *IEEE Trans. Wireless Commun.*, vol. 21, no. 6, pp. 3881–3892, Jun. 2022.

[30] K. P. Dasala and E. W. Knightly, "Multi-user terahertz WLANs with angularly dispersive links," in *Proc. 23rd Int. Symp. Theory, Algorithmic Found., Protocol Design Mobile Netw. Mobile Comput.*, Oct. 2022, pp. 121–130.

[31] B. Husain, M. Steeg, and A. Stöhr, "Estimating direction-of-arrival in a 5G hot-spot scenario using a 60 GHz leaky-wave antenna," in *Proc. IEEE Int. Conf. Microw., Antennas, Commun. Electron. Syst. (COMCAS)*, Nov. 2017, pp. 1–4.

[32] Y. Ghasempour, C.-Y. Yeh, R. Shrestha, D. Mittleman, and E. Knightly, "Single shot single antenna path discovery in THz networks," in *Proc. 26th Annu. Int. Conf. Mobile Comput. Netw.*, Apr. 2020, pp. 1–13.

[33] Y. Ghasempour, R. Shrestha, A. Charous, E. Knightly, and D. M. Mittleman, "Single-shot link discovery for terahertz wireless networks," *Nature Commun.*, vol. 11, no. 1, pp. 1–6, Apr. 2020.

[34] Y. Ghasempour, C.-Y. Yeh, R. Shrestha, Y. Amarasinghe, D. Mittleman, and E. W. Knightly, "LeakyTrack: Non-coherent single-antenna nodal and environmental mobility tracking with a leaky-wave antenna," in *Proc. 18th Conf. Embedded Networked Sensor Syst.*, Nov. 2020, pp. 56–68.

[35] H. Saeidi, S. Venkatesh, X. Lu, and K. Sengupta, "THz prism: One-shot simultaneous localization of multiple wireless nodes with leaky-wave THz antennas and transceivers in CMOS," *IEEE J. Solid-State Circuits*, vol. 56, no. 12, pp. 3840–3854, Dec. 2021.

[36] J. Tan and L. Dai, "Wideband beam tracking in THz massive MIMO systems," *IEEE J. Sel. Areas Commun.*, vol. 39, no. 6, pp. 1693–1710, Jun. 2021.

[37] A. Kludze, R. Shrestha, C. Miftah, E. Knightly, D. Mittleman, and Y. Ghasempour, "Quasi-optical 3D localization using asymmetric signatures above 100 GHz," in *Proc. 28th Annu. Int. Conf. Mobile Comput. Netw.*, Oct. 2022, pp. 120–132.

[38] A. Kludze and Y. Ghasempour, "LeakyScatter: A frequency-agile directional backscatter network above 100 GHz," in *Proc. 20th USENIX Symp. Networked Syst. Design Implement.*, Boston, MA, USA, Apr. 2023, pp. 375–388.

[39] B. Zhai, A. Tang, C. Peng, and X. Wang, "SS-OFDMA: Spatial-spread orthogonal frequency division multiple access for terahertz networks," *IEEE J. Sel. Areas Commun.*, vol. 39, no. 6, pp. 1678–1692, Jun. 2021.

[40] M. Cai, J. N. Laneman, and B. Hochwald, "Beamforming codebook compensation for beam squint with channel capacity constraint," in *Proc. IEEE Int. Symp. Inf. Theory (ISIT)*, Jun. 2017, pp. 76–80.

[41] X. Liu and D. Qiao, "Space-time block coding-based beamforming for beam squint compensation," *IEEE Wireless Commun. Lett.*, vol. 8, no. 1, pp. 241–244, Feb. 2019.

[42] R. Zhang, W. Hao, G. Sun, and S. Yang, "Hybrid precoding design for wideband THz massive MIMO-OFDM systems with beam squint," *IEEE Syst. J.*, vol. 15, no. 3, pp. 3925–3928, Sep. 2021.

[43] N. J. Myers and R. W. Heath, "InFocus: A spatial coding technique to mitigate misfocus in near-field LoS beamforming," *IEEE Trans. Wireless Commun.*, vol. 21, no. 4, pp. 2193–2209, Apr. 2022.

[44] H. Yu, P. Guan, Y. Wang, and Y. Zhao, "Performance analysis and codebook design for mmWave beamforming system with beam squint," *IEEE Wireless Commun. Lett.*, vol. 10, no. 9, pp. 2013–2016, Sep. 2021.

[45] L. Wang, J. L. Gómez-Tornero, and O. Quevedo-Teruel, "Substrate integrated waveguide leaky-wave antenna with wide bandwidth via prism coupling," *IEEE Trans. Microw. Theory Techn.*, vol. 66, no. 6, pp. 3110–3118, Jun. 2018.

[46] Q. Ma, D. M. W. Leenaerts, and P. G. M. Baltus, "Silicon-based true-time-delay phased-array front-ends at Ka-band," *IEEE Trans. Microw. Theory Techn.*, vol. 63, no. 9, pp. 2942–2952, Sep. 2015.

[47] D. I. Lialios, N. Ntetsikas, K. D. Paschaloudis, C. L. Zekios, S. V. Georgakopoulos, and G. A. Kyriacou, "Design of true time delay millimeter wave beamformers for 5G multibeam phased arrays," *Electronics*, vol. 9, no. 8, p. 1331, Aug. 2020.

[48] C.-C. Lin et al., "Wideband beamforming with rainbow beam training using reconfigurable true-time-delay arrays for millimeter-wave wireless," 2021, *arXiv:2111.15191*.

[49] R. Mendis and D. M. Mittleman, "An investigation of the lowest-order transverse-electric (TE_1) mode of the parallel-plate waveguide for THz pulse propagation," *J. Opt. Soc. Amer. B, Opt. Phys.*, vol. 26, no. 9, pp. 6–13, 2009.

[50] H. Guerboukha et al., "Efficient leaky-wave antennas at terahertz frequencies generating highly directional beams," *Appl. Phys. Lett.*, vol. 117, no. 26, Dec. 2020, Art. no. 261103.

[51] F. Gross, *Frontiers in Antennas: Next Generation Design & Engineering*. New York, NY, USA: McGraw-Hill, 2010.

[52] W. Fuscaldo, D. R. Jackson, and A. Galli, "A general and accurate formula for the beamwidth of 1-D leaky-wave antennas," *IEEE Trans. Antennas Propag.*, vol. 65, no. 4, pp. 1670–1679, Apr. 2017.

[53] M. Koch, "Terahertz communications: A 2020 vision," in *Terahertz Frequency Detection and Identification of Materials and Objects*. Berlin, Germany: Springer, 2007, pp. 325–338.

[54] A. D. Wyner, "The wire-tap channel," *Bell Syst. Tech. J.*, vol. 54, no. 8, pp. 1355–1387, Oct. 1975.

[55] I. Csiszar and J. Korner, "Broadcast channels with confidential messages," *IEEE Trans. Inf. Theory*, vol. IT-24, no. 3, pp. 339–348, May 1978.

[56] S. Leung-Yan-Cheong and M. Hellman, "The Gaussian wire-tap channel," *IEEE Trans. Inf. Theory*, vol. IT-24, no. 4, pp. 451–456, Jul. 1978.

[57] Z. Li, R. Yates, and W. Trappe, "Secrecy capacity of independent parallel channels," in *Securing Wireless Communications at the Physical Layer*. Boston, MA, USA: Springer, 2010, pp. 1–18.

[58] V. Petrov, T. Kurner, and I. Hosako, "IEEE 802.15.3D: First standardization efforts for sub-terahertz band communications toward 6G," *IEEE Commun. Mag.*, vol. 58, no. 11, pp. 28–33, Nov. 2020.

[59] W. Trappe and L. C. Washington, *Introduction to Cryptography with Coding Theory*. London, U.K.: Pearson, 2006.

[60] C.-Y. Yeh, A. Cohen, R. G. L. D'Oliveira, M. Médard, D. M. Mittleman, and E. W. Knightly, "Angularly dispersive terahertz links with secure coding: From theoretical foundations to experiments," in *Proc. 15th ACM Conf. Secur. Privacy Wireless Mobile Netw.*, May 2022, pp. 268–273.

[61] D. R. Jackson and A. A. Oliner, *Leaky-Wave Antennas*. Hoboken, NJ, USA: Wiley, 2008, ch. 7, pp. 325–367.

[62] W. Fuscaldo, A. Galli, and D. R. Jackson, "Optimization of the radiating features of 1-D unidirectional leaky-wave antennas," *IEEE Trans. Antennas Propag.*, vol. 70, no. 1, pp. 111–125, Jan. 2022.

[63] I. Duling and D. Zimdars, "Revealing hidden defects," *Nature Photon.*, vol. 3, no. 11, pp. 630–632, Nov. 2009.

[64] L. Wang, M. Elkashlan, T. Q. Duong, and R. W. Heath, "Secure communication in cellular networks: The benefits of millimeter wave mobile broadband," in *Proc. IEEE 15th Int. Workshop Signal Process. Adv. Wireless Commun. (SPAWC)*, Jun. 2014, pp. 115–119.

[65] D. Steinmetzer, J. Chen, J. Classen, E. Knightly, and M. Hollick, "Eavesdropping with periscopes: Experimental security analysis of highly directional millimeter waves," in *Proc. IEEE Conf. Commun. Netw. Secur. (CNS)*, Sep. 2015, pp. 335–343.

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

[67] Y. Zhu, L. Wang, K.-K. Wong, and R. W. Heath, "Secure communications in millimeter wave ad hoc networks," *IEEE Trans. Wireless Commun.*, vol. 16, no. 5, pp. 3205–3217, May 2017.

[68] J. Federici and L. Moeller, "Review of terahertz and subterahertz wireless communications," *J. Appl. Phys.*, vol. 107, no. 11, Jun. 2010, Art. no. 111101.

[69] J. Ma et al., "Security and eavesdropping in terahertz wireless links," *Nature*, vol. 563, no. 7729, pp. 89–93, Nov. 2018.

[70] V. Petrov, D. Moltchanov, J. M. Jornet, and Y. Koucheryavy, "Exploiting multipath terahertz communications for physical layer security in beyond 5G networks," in *Proc. IEEE INFOCOM Conf. Comput. Commun. Workshops (INFOCOM WKSHPS)*, Apr. 2019, pp. 865–872.

[71] Z. Liu, J. Liu, Y. Zeng, and J. Ma, "Covert wireless communication in IoT network: From AWGN channel to THz band," *IEEE Internet Things J.*, vol. 7, no. 4, pp. 3378–3388, Apr. 2020.

[72] A. Cohen et al., "Absolute security in high-frequency wireless links," in *Proc. IEEE Conf. Commun. Netw. Secur. (CNS)*, Oct. 2022, pp. 46–54.

[73] J. Classen, J. Chen, D. Steinmetzer, M. Hollick, and E. Knightly, "The spy next door: Eavesdropping on high throughput visible light communications," in *Proc. 2nd Int. Workshop Visible Light Commun. Syst.*, Sep. 2015, pp. 1–14.

[74] G. J. Blinowski, "Practical aspects of physical and MAC layer security in visible light communication systems," *Int. J. Electron. Telecommun.*, vol. 62, no. 1, pp. 7–13, Mar. 2016.

[75] Z. Shaikhanov, F. Hassan, H. Guerboukha, D. Mittleman, and E. Knightly, "Metasurface-in-the-middle attack: From theory to experiment," in *Proc. 15th ACM Conf. Secur. Privacy Wireless Mobile Netw.*, May 2022, pp. 257–267.

[76] B. Ning, Z. Chen, W. Chen, and L. Li, "Improving security of THz communication with intelligent reflecting surface," in *Proc. IEEE Globecom Workshops (GC Wkshps)*, Dec. 2019, pp. 1–6.

[77] P. Wang, J. Fang, X. Yuan, Z. Chen, and H. Li, "Intelligent reflecting surface-assisted millimeter wave communications: Joint active and passive precoding design," *IEEE Trans. Veh. Technol.*, vol. 69, no. 12, pp. 14960–14973, Dec. 2020.

[78] J. Qiao, C. Zhang, A. Dong, J. Bian, and M.-S. Alouini, "Securing intelligent reflecting surface assisted terahertz systems," *IEEE Trans. Veh. Technol.*, vol. 71, no. 8, pp. 8519–8533, Aug. 2022.

[79] Y. Ding, J. Zhang, and V. Fusco, "Frequency diverse array OFDM transmitter for secure wireless communication," *Electron. Lett.*, vol. 51, no. 17, pp. 1374–1376, Aug. 2015.

[80] J. Lin, Q. Li, J. Yang, H. Shao, and W.-Q. Wang, "Physical-layer security for proximal legitimate user and eavesdropper: A frequency diverse array beamforming approach," *IEEE Trans. Inf. Forensics Security*, vol. 13, no. 3, pp. 671–684, Mar. 2018.