Security in Terahertz WLANs with Leaky Wave Antennas

Chia-Yi Yeh
Rice University
chia-yi.yeh@rice.edu

Yasaman Ghasempour
Rice University
ghasempour@rice.edu

Yasith Amarasinghe
Brown University
yasith_amarasinghe@brown.edu

Daniel M. Mittleman
Brown University
daniel_mittleman@brown.edu

Edward W. Knightly
Rice University
knightly@rice.edu

ABSTRACT

This paper presents the first security study of THz networks with Leaky Wave Antennas (LWAs). We employ a mix of analytical models and over-the-air experiments to explore the unique security properties of LWA links. We show via both models and experiments that the LWA's angle-frequency coupling leads to non-uniform secrecy capacity across sub-channels yielding advantages to an eavesdropper at edge frequencies. Yet, because different frequencies emit energy at 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.

CCS CONCEPTS

• **Security and privacy → Mobile and wireless security**.

KEYWORDS

Terahertz, Leaky Wave Antenna, Physical Layer Security

ACM Reference Format:
Chia-Yi Yeh, Yasaman Ghasempour, Yasith Amarasinghe, Daniel M. Mittleman, and Edward W. Knightly. 2020. Security in Terahertz WLANs with Leaky Wave Antennas. In *13th ACM Conference on Security and Privacy in Wireless and Mobile Networks (WiSec '20), July 8–10, 2020, Linz (Virtual Event), Austria.* ACM, New York, NY, USA, 11 pages. https://doi.org/10.1145/3395351.3399365

1 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 [1, 17, 24, 28]. For the first time, in March 2019, the US Federal Communications Commission (FCC) has adopted rules to encourage development of technologies above 95 GHz [4]. 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 [5]. These high-frequency communications systems, which we will refer to as terahertz (THz) links, offer numerous advantages, such as plentiful bandwidth [26] for ultra-high-speed data transmission [15, 18, 25]. Another commonly cited advantage is that of 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.

Leaky Wave Antennas (LWAs) provide a promising foundation for THz scale networking. While traditional phased arrays employed at millimeter wave encounter scaling limits impeding their realization at THz [9, 14], LWAs are dynamically steerable via a simple mechanism of frequency tuning. That is, a LWA's emission angle can be changed by controlling the carrier's center frequency [13, 16, 27].

In this paper, we perform the first security study of THz networks with LWA antennas. In particular, we make the following three contributions. First, we characterize the key elements of LWAs under a threat model in which an eavesdropper Eve attempts to intercept a directional THz transmission between Alice and Bob. We describe how the aforementioned angle-frequency coupling manifests via analytical models based on Maxwell's equations. In particular, because a LWA is a parallel plate waveguide with an emission slot, its behavior can be reasonably approximated using scalar diffraction theory. While the exact far-field radiation pattern is intractable, closed form approximations are available for the dominant transverse electric mode [12, 30]. Because this angle-frequency coupling that does not manifest in traditional systems such as phased arrays, we define a new security metric that we term subchannel secrecy capacity. Thus, we can understand security not only in aggregate, but also in its individual frequency-dependent components.

Second, we study the security properties of the THz link based on the physical model and the subchannel secrecy capacity metric. We first show that subchannel secrecy capacity is not symmetric around the transmission's center frequency. The key reason is that when Eve is at a different angle from Bob, she intercepts a different frequency profile due to the LWA's fundamental characteristics. For Eve at an angle larger than Bob's angle, she intercepts low frequencies better than high frequencies and vice versa. Consequently, her relatively high SNR in this regime sharply reduces secrecy capacity. We next explore the impact of bandwidth and beamwidth coupling in LWA links. Because wider bandwidth (using a wider range of frequencies) corresponds to a wider beamwidth (wider range of

WiSec '20, July 8–10, 2020, Linz (Virtual Event), Austria

ACM ISBN 978-1-4503-8006-5/20/07…$15.00
https://doi.org/10.1145/3395351.3399365

angles), the situation may appear dire, that LWA links will either be secure but slow or vice versa. Fortunately, we find that beamwidth and bandwidth widening has a unique effect: because high and low frequencies are maximized on opposite sides of Bob, Eve cannot simultaneously be on both sides, and hence she cannot simultaneously intercept the entire bandwidth. Thus, while narrow beams are still more secure than wider ones for LWA links, the scaling yields fundamental impediments for Eve.

Third, we perform an extensive set of over-the-air experiments using a THz source, LWA antenna, and a wideband receiver. We find that while the 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 (angles are measured with respect to the LWA's plates). Indeed, when Eve is at a smaller angle than Bob, she is a more devastating threat for the measured LWA link. Lastly, the experiments indicate that as bandwidth and beamwidth increase, there is little marginal penalty for security, i.e., the trend is increasing, but only very gradually.

Related Work. Prior work has studied the improvements and limits of security due to directional transmission in higher frequency bands, including studies in millimeter wave [29, 32–34, 36], THz [1, 8, 22], and visible light communication [2, 3]. However, such past studies consider a beam pattern that does not depend on frequency, resulting in an uniform secrecy level across the transmission band. In contrast, this work is the first to explore the security properties of a THz link consisting of frequency-dependent radiation pattern.

2 FOUNDATIONS FOR LWA SECURITY

2.1 Overview

Because LWAs emit different frequencies towards different angles, beam adaptation can be realised by tuning the transmit frequencies for LWA. This makes the LWA a good candidate for mobile THz networks, especially because conventional directional antenna techniques encounter challenges when scaling to the THz regime. For example, phased-array antennas encounter difficulties in designing a electronically controllable phase shifter above 100 GHz due to CMOS characteristics [9, 14]. Yet, due to the high pathloss in THz regime, directional transmission is required and therefore LWAs, whose radiation pattern can be easily controlled by frequency, and have been shown to have promising results also in multiplexing [16, 21] and link discovery [10, 11] become a good candidate.

A LWA can be realized by a parallel-plate waveguide with an opening slot on one of the plates, as shown in Fig. 1. The figure illustrates beam steering and depicts a transmitter steering between two different angles θ_1 to θ_2 by changing the input frequency (depicted by color).

2.2 LWA Transmission

For the parallel-plate waveguide, the dominant transverse electric (TE) mode is TE_1 mode [23], and the phase constant β of the TE_1 mode is

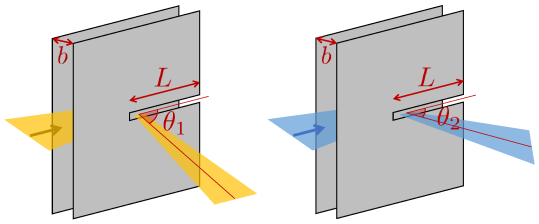

Figure 1: Terahertz leaky wave antenna beam steering leveraging frequency-angle coupling.

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

where $k_0 = \frac{2\pi f}{c}$ is the free-space wavenumber, f represents the frequency, c is the speed of light, and f_{co} is the cutoff frequency. By definition, frequencies below f_{co} cannot propagate in the waveguide, implying $f > f_{co}$. Also, the cutoff frequency for a parallel-plate waveguide depends on the plate separation b, specifically,

$$f_{co} = \frac{c}{2b}. \tag{2}$$

The guided TE_1 mode within the waveguide leaks out of the waveguide through the opening slot. The far-field radiation pattern G can be derived as [12, 30]

$$G(f,\theta) = L\,\mathrm{sinc}\left(\left[\beta(f) - j\alpha - k_0\cos\theta\right]\frac{L}{2}\right), \tag{3}$$

where α is the attenuation coefficient which parameterizes the loss of energy due to leakage through the slot into free space, β is the phase constant defined in Equation (1), L is the length of the slot opening, and θ is the emitting angle with respect to the guided mode propagation axis ($0° < \theta < 90°$), as shown in Fig. 1.

While Equation (3) 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 sinc because of the $\cos\theta$ term. Also, for a complex sinc function, the beamwidth is determined by the imaginary part α. 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 sinc function maximizes when

$$\mathrm{Re}\left\{\left(\beta(f) - j\alpha - k_0\cos\theta\right)\frac{L}{2}\right\} = 0. \tag{4}$$

Therefore, the maximum radiation happens at the angle

$$\theta_{max}(f) = \sin^{-1}\left(\frac{c}{2bf}\right), \tag{5}$$

and conversely

$$f_{max}(\theta) = \frac{c}{2b\sin\theta}. \tag{6}$$

These equations describe the peak angle of a certain frequency and peak frequency for a given angle, respectively. Specifically,

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 (5) and second, the angular spread of each single-tone frequency component determined by α.

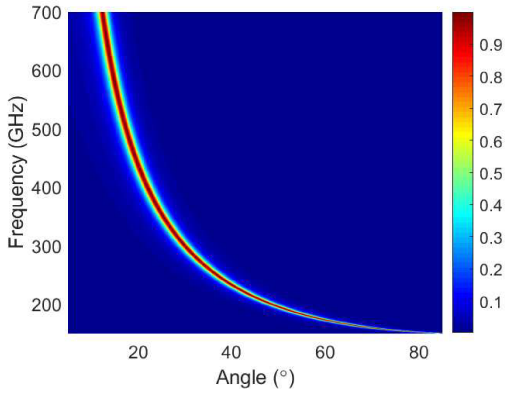

Figure 2: LWA frequency-angle coupling emitting behavior according to Equation (3). Plate separation $b = 1$ mm, slot length $L = 3$ cm, and $\alpha = 50$ rad/m

.

Fig. 2 shows an example LWA radiation pattern for a LWA with a plate separation of $b = 1$ mm, slot length $L = 3$ cm, $\alpha = 50$ rad/m, and cutoff frequency 150 GHz. Observe the nonlinear frequency-angle coupling relationship described by Equation (5): 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.

2.3 Steering from Alice to Bob

A transmitter (Alice) uses a LWA to transmit to a static receiver (Bob) with a THz broadband receiver located at θ_B, as illustrated in Fig. 3. Assume Alice has acquired Bob's angular location θ_B via a

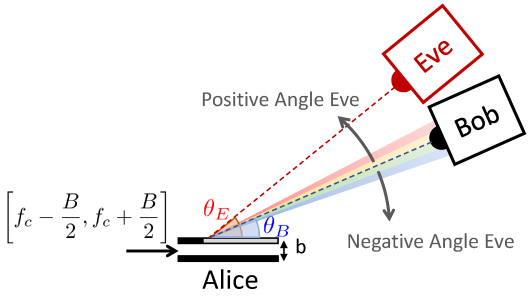

Figure 3: Leaky wave antenna transmission under passive eavesdropping.

path discovery phase [11]. Therefore, Alice can select the suitable frequency band for Bob according to the frequency-angle coupling described by Equation (6). Specifically, the center frequency f_c of the transmission is

$$f_c = f_{max}(\theta_B).$$

Let B represent the bandwidth of the transmission. 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 $\frac{B}{K}$. Alice transmits the same power P for all subchannels. The SNR of subchannel k is therefore

$$\text{SNR}_k^{Bob} = \frac{P\rho_B G(f_k, \theta_B)}{n},$$

where ρ_B is the channel gain from Alice to Bob, f_k is the center frequency of subchannel k, and n is the noise power, which is assumed to be flat across the whole transmission band.

2.4 Threat Model

As Alice transmits to Bob with the selected frequency band, an eavesdropper (Eve) tries to intercept the signals from Alice to Bob. We consider a single Eve located at angle θ_E. Eve's subchannel SNR can be expressed as

$$\text{SNR}_k^{Eve} = \frac{P\rho_E G(f_k, \theta_E)}{n},$$

where ρ_E is the channel gain from Alice to Eve.

We observe that Eve's subchannel SNR differs from Bob's subchannel SNR due to two factors: a potentially different pathloss, and a different radiation gain. The effect of pathloss is clear. Namely, Eve has an advantage for eavesdropping when the channel gain is higher (smaller pathloss) and thus resulting in a higher SNR. Therefore, without loss of generality, we consider equal pathloss, $\rho_E = \rho_B$.

In contrast, the effect of the LWA radiation is rather complicated, as it varies with different subchannels. In fact, varying radiation gain across frequencies has never been observed in the conventional directional links. For example, the radiation pattern of the phased-array antenna is determined by the phase of each antenna element and does not vary with frequency. As a result, the secrecy level across the transmission band is expected to be flat for conventional direction links. However, in THz bands with LWA steering, the secrecy level is expected to vary within the transmission band because LWA's radiation gain depends on frequency. This novel frequency-varying physical layer secrecy behavior is a key focus of this study.

2.5 Security Metric

Despite the broadcast nature of wireless channels, perfect secrecy is possible considering different channel conditions at Bob and Eve [6, 19, 35]. Specifically, when Eve has a worse channel condition than Bob, a positive rate with perfect secrecy can be achieved between Alice and Bob. That is, Eve's observation through her channel contains less information compared to Bob, and the information gap between Bob and Eve enables the secret transmission between Alice and Bob. The maximum 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 of the LWA to be the summation of subchannel secrecy capacity across independent subchannels [20]. Specifically, we define subchannel secrecy capacity for each subchannel k as [19]

$$C_S^k = \frac{B}{K}\left[\log_2\left(1+\mathrm{SNR}_k^{Bob}\right) - \log_2\left(1+\mathrm{SNR}_k^{Eve}\right)\right]^+, \quad (7)$$

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.

3 LWA LINK SECURITY PROPERTIES

From §2, we learn that a LWA link is expected to have non-uniform secrecy levels across the transmission band because the radiation pattern of each frequency is different. This is a unique characteristic that does not exist in conventional directional links. Therefore, in this section, we study LWA physical layer security properties and their differences from conventional directional links via the physics-based model described in §2.

3.1 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.

3.1.1 Subchannel Secrecy. From §2, 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. The LWA used in the numerical analysis has the same parameters as the example we show in Fig. 2, plate separation $b = 1$ mm, slot length $L = 3$ cm, and $\alpha = 50$ rad/m. 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. 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 §2.

Fig. 4 shows the subchannel secrecy capacity across the 27 GHz transmission band. Note first that, as also occurs without LWAs,

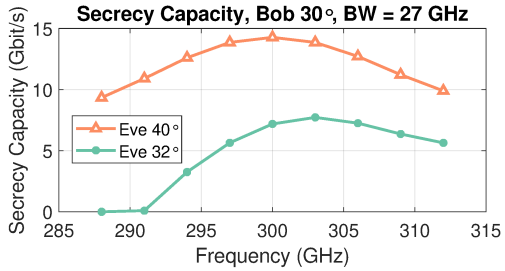

Figure 4: Non-uniform subchannel secrecy capacity of a LWA link for Bob located at 30° with a transmission bandwidth of 27GHz.

subchannel secrecy capacity is higher when Eve is at a greater angular distance from Bob. Indeed, the theoretical LWA radiation pattern in Equation (3) 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 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 break secrecy capacity into its components of Bob and Eve's SNRs. As shown in Fig. 5, Bob indeed receives the highest SNR at the center frequency as the center frequency is chosen so that the radiation pattern maximize 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.

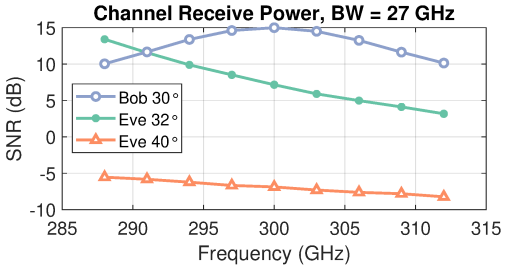

Figure 5: Bob and Eve subchannel SNR. Bob locates at 30° and the bandwidth for the transmission is 27GHz.

Fig. 5 shows that Eve's SNR decreases monotonically with frequency, for both Eve locations, with higher SNR when she is closer to Bob. Moreover, while it is always beneficial for Eve to be 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. 2. In fact, the single-tone half power beamwidth (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. 4. When Eve is at a positive angle with respect to Bob, she intercepts lower frequencies better. However, when Eve is far 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 suffers similarly, yielding a nearly flat but modestly decreasing secrecy capacity.

In summary, when Eve is farther 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.

3.1.2 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.

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 information that can be securely transferred from Alice to Bob.

Following the previous setup, we continue to study the case when Bob is at 30°, the bandwidth is 27 GHz, and the LWA parameters are the same as before, as shown in Fig. 2. Eve locates within 10° around Bob, both on the positive side and negative side. The normalized channel secrecy capacity is computed for all eavesdropping locations so that the insecure zone can be determined accordingly.

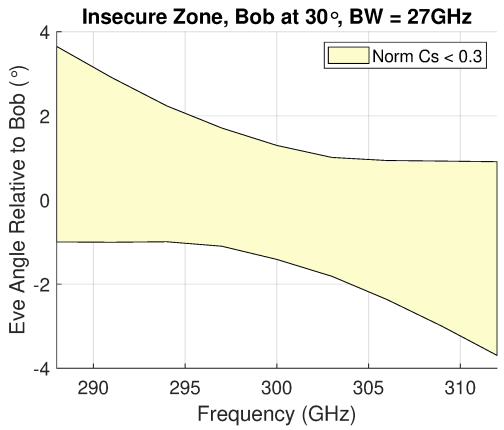

Figure 6: Insecure zone of each subchannel with a threshold of 0.3 illustrates vulnerable but complementary edge frequencies. Bob locates at 30° and the bandwidth for the transmission is 27GHz.

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 Eve locations than the center frequency. Specifically, lower frequency components remain insecure for a larger angle range for Eve having a greater angle than Bob, whereas higher frequency components are vulnerable under a wider range of locations when Eve has 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. For a conventional directional link, the radiation pattern does not change with frequency. Therefore, no frequency is more secure than other frequencies in the spatial domain. In contrast, the radiation pattern of a LWA varies with frequency. Consequently, the lower frequency components with a radiation pattern that peaks at a slightly larger angle than Bob's

location are more vulnerable to a positive angle Eve. Similarly, high frequency components 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 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 a great potential in realizing a secure link. In the most simplified form and to illustrate, we can assume that only half of the subchannels are exposed to a single Eve having a fixed location, whereas the other half of the subchannels remain secure, regardless of Eve's location. 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 [31]. 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. The above discussion omits many details, but the point is that when the secrecy level of different frequencies has a known coupling pattern, that information can be used by Alice and Bob to improve link security.

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 LWA link and has a great potential in realizing a secure transmission.

3.2 Bandwidth and Beamwidth Coupling

3.2.1 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 link directivity is based on the frequency-angle coupling property, the larger the bandwidth, the wider the angular span of the selected frequencies, resulting a wider beam. That is, bandwidth and beamwidth are coupled in the LWA system.

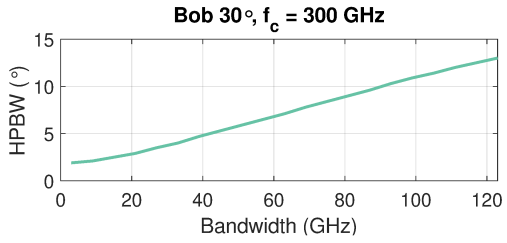

Figure 7: LWA link HPBW increases with bandwidth.

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 123 GHz. Fig. 7 illustrates the HPBW of the all-tone radiation pattern as the bandwidth increases for Bob at 30°. We observe that the beamwidth increases nearly linearly with bandwidth. Indeed, due to widening angular span as the total bandwidth of the selected frequencies increases, HPBW also increases.

This coupling 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.

3.2.2 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 can be securely transferred.

We further introduce a concept of "security separation" based on the normalized secrecy capacity. For a certain directional transmission, the closer Eve is to Bob, the lower the normalized secrecy capacity. To achieve a certain normalized secrecy capacity, Eve has to be located far 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 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. 8 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. 7. Thus, the x-axis in Fig. 8 also represents increasing bandwidth. In addition to the LWA link represented by solid lines, the dashed lines are also shown for comparison, representing a hypothetical link that has the exact same radiation pattern as the LWA link but no frequency-angle coupling property.

Fig. 8 shows the required security separation for two normalized secrecy capacity thresholds: 0.3 and 0.8. 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

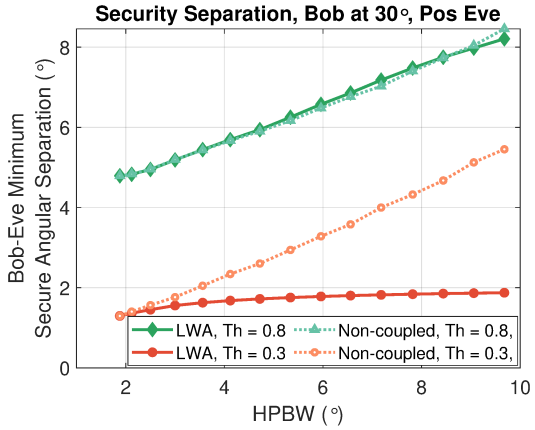

Figure 8: Minimum angular separation required to achieve a certain normalized secrecy capacity increases with link HPBW for positive angle Eve. However, the scaling is surprisingly slow for low target secrecy, especially compared to a link without the frequency-angle coupling property.

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 information has to be transferred securely, the required angular separation between Bob and Eve barely increases as the beam widens. In contrast, when transferring a larger portion of information securely is required, 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 can decode 70% of the information being transmitted, but barely benefits from a wider LWA beam. For comparison, the dashed lines, which represent 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 dashed orange line shows that in traditional systems, the security separation between Bob and Eve increases proportionally to the HPBW to maintain the goal of transferring 30% of the total information securely. In contrast, the LWA security separation curve 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, only one of the newly added edge frequencies is more accessible, while the other edge frequency falls out of reach.

In summary, it is still 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 information needs to be securely transferred. Based on these observations, Alice can almost choose whatever bandwidth she wants without concern about the security penalty when only a smaller portion of the information needs to be secure. However, if a higher portion of information needs to be secure, Alice still has to limit the transmission bandwidth in exchange for extra link secrecy.

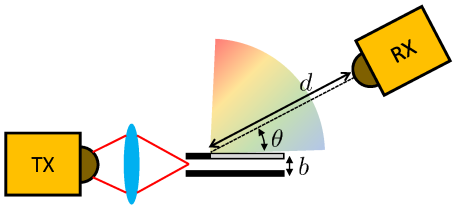

Figure 9: Experiment diagram.

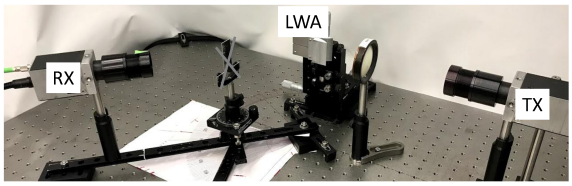

Figure 10: Experiment setup.

4 EXPERIMENTAL EVALUATION

In this section, we experimentally study the security of a LWA link and compare its properties with the above results based on models derived from Maxwell's equations.

4.1 Experimental Setup

We measure the radiation pattern of a custom LWA device for experimental validation. Specifically, the LWA consists of two 4 x 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 [7] 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 up to 6.4 THz with a frequency resolution of 3.13 GHz.

Fig. 9 illustrates the experiment diagram and Fig. 10 demonstrates the experiment setup. During the measurement, the transmitter couples the THz pulse into 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. The receiver has a lens with 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.

Once the time-domain samples at $12^\circ < \theta < 80^\circ$ 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. When focusing on each specific frequency component, the dataset can also be interpreted as the radiation pattern of each frequency components.

4.2 The Alice-Bob LWA Link

Equation (5) 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. 11. The results indicate an excellent match between frequencies of 169 and 388 GHz, with a slight deviation at the highest frequencies.

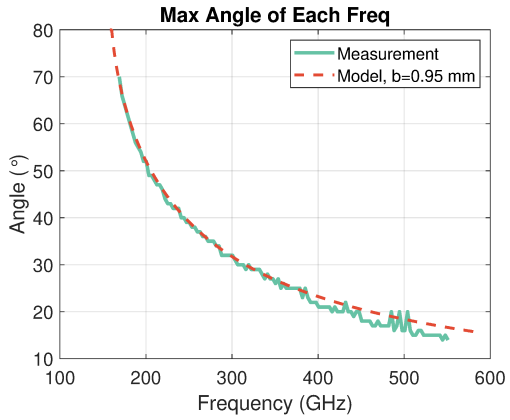

Figure 11: Maximum radiation angle of each frequency.

Next, we explore how the experimental system's radiation pattern is impacted by the input frequency. Namely, if we fix an input frequency, Equation (3) describes the resulting gain as a function of the transmission angle θ. In the experiment, we consider single tones of 207 GHz or 316 GHz and measure the received power at all angles. The model parameters are computed from the LWA's geometry with the exception of the attenuation constant α, which cannot be. Hence, we fit the best empirical value of $\alpha = 200$ rad/m. Fig. 12 shows the measurement results along with the values predicted by Equation (3).

Beginning with the lower frequency of 207 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 316 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 receive power by over 10 dB at some angles. Thus, the measured beam asymmetry is even greater than 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 are most likely due to experimental error.

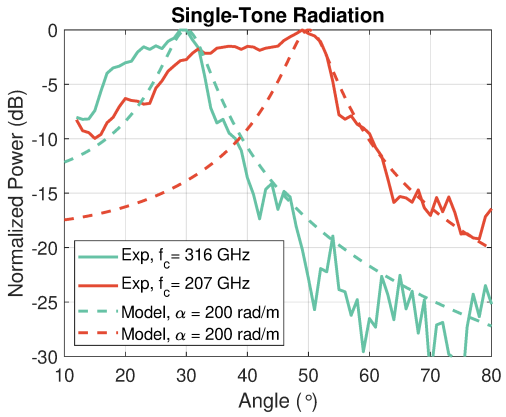

Figure 12: Measured single-tone radiation pattern, matched with model prediction when $\alpha = 200$ rad/m.

4.3 Empirical Security

Here, 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.

4.3.1 Asymmetry. Because beam asymmetry was 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 via the scenario in which Bob is at 30°, and Eve is either at a positive angle or negative angle from Bob. Analogous to the process in the numerical 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. 13 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.

First, observe that the experimental subchannel secrecy capacity follows the trend of the model predicted value. Despite the fluctuation likely due to 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. 12, the beam pattern decays more rapidly towards larger angles but decays much more slowly towards the smaller angles. This suggests that an

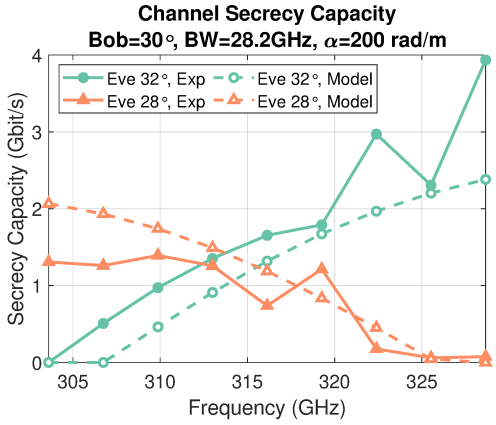

Figure 13: Experimental subchannel secrecy capacity when Bob is at 30° and Eve is at 28° or 32°.

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.

4.3.2 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 HPBW predictions are shown in 14, one with $\alpha = 50$ rad/m studied in §3.2, and the other is the best matching $\alpha = 200$ rad/m.

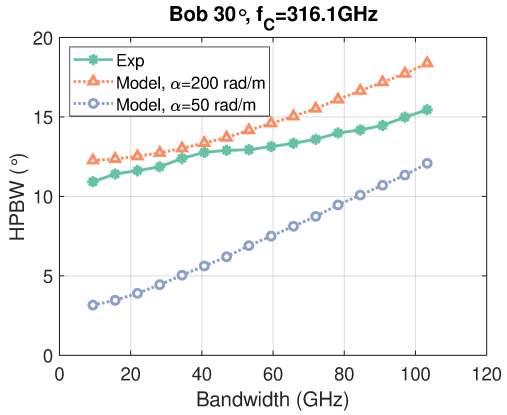

Figure 14: Experimental all-tone HPBW as bandwidth increases compared to the model.

First, focusing on the model's prediction, observe that α impacts beamwidth scaling. 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 less 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.

4.3.3 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. §3.2). Here, we experimentally study the minimum Bob-Eve separation required to achieve a particular security threshold, with two thresholds, 0.3 and 0.8. The results are shown in Figure 15 along with the model predictions.

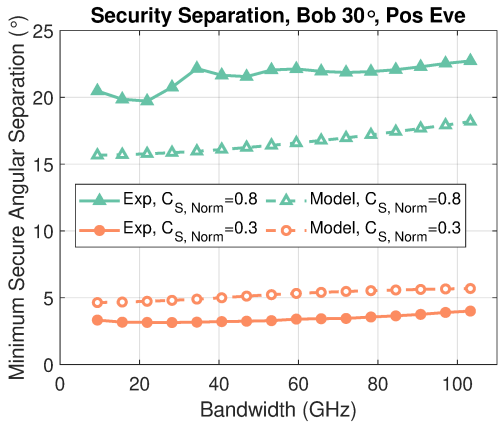

Figure 15: The experimental minimum Bob-Eve separation required for a certain secrecy level, showing that the model predicts the trend but might overestimate or underestimate the minimum secure separation.

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 0.8, the experiments show a similar trend of angular increase despite the irregular decrease and a sudden increase below a bandwidth of 40 GHz. Unlike the model, the measurement has larger experimental error especially when the receiver power is low. As a result, the measured radiation pattern can possesses unexpected side lobes. The irregular

fluctuation below 40 GHz suggests that some subchannels have especially evident side lobes so that when those subchannels are included in the transmission, the minimum security separation increases unexpectedly. Nevertheless, with increasing bandwidth, the irregularity in each subchannel also averages out and shows a trend similar to the model prediction. The increase of the minimum secure separation indicates the trade-off between bandwidth and security for a LWA link when the security requirement is high.

Finally, 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 0.8. 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.

5 CONCLUSIONS

This paper presents, for the first time, a study of the security of a THz link created by a leaky wave antenna. We perform an analytic and experimental investigation to show how the link's unique angle-frequency coupling impacts security, in some cases aiding the adversary (e.g., more vulnerable to Eve in the negative angle due to beam pattern asymmetry) and in other cases hindering the adversary (e.g., a wide-band transmission is also wide-angle, and therefore difficult to intercept all frequency band).

ACKNOWLEDGMENTS

This research was supported by Cisco, Intel, and by NSF grants CNS-1923782, CNS-1827940, CNS-1824529, CNS-1801857, CNS-1801865, CNS-1518916 and DOD: Army Research Laboratory grant W911NF-1920269.

REFERENCES

[1] Ian F Akyildiz, Josep Miquel Jornet, and Chong Han. 2014. Terahertz Band: Next Frontier for Wireless Communications. *Physical Communication* 12 (2014), 16–32.

[2] Grzegorz J Blinowski. 2016. Practical Aspects of Physical and MAC Layer Security in Visible Light Communication Systems. *International Journal of Electronics and Telecommunications* 62, 1 (2016), 7–13.

[3] Jiska Classen, Joe Chen, Daniel Steinmetzer, Matthias Hollick, and Edward Knightly. 2015. The Spy Next Door: Eavesdropping on High Throughput Visible Light Communications. In *Proceedings of the 2nd International Workshop on Visible Light Communications Systems.*

[4] U.S. Federal Communications Commission. 2019. FCC Opens Spectrum Horizons for New Services & Technologies. https://www.fcc.gov/document/fcc-opens-spectrum-horizons-new-services-technologies

[5] World Radiocommunication Conference. 2019. Resolution 731: Consideration of Sharing and Adjacent-Band Compatibility between Passive and Active Services above 71 GHz. https://www.itu.int/en/ITU-R/conferences/wrc/2019/Documents/PFA-WRC19-E.pdf

[6] Imre Csiszár and Janos Korner. 1978. Broadcast Channels with Confidential Messages. *IEEE Transactions on Information Theory* 24, 3 (1978), 339–348.

[7] Irl Duling and David Zimdars. 2009. Revealing Hidden Defects. *Nature Photonics* 3, 11 (2009), 630–632.

[8] John Federici and Lothar Moeller. 2010. Review of Terahertz and Subterahertz Wireless Communications. *Journal of Applied Physics* 107, 11 (2010), 6.

[9] Xiaojian Fu, Fei Yang, Chenxi Liu, Xiaojun Wu, and Tie Jun Cui. 2020. Terahertz Beam Steering Technologies: From Phased Arrays to Field-Programmable Metasurfaces. *Advanced Optical Materials* 8, 3 (2020), 1900628.

[10] Yasaman Ghasempour, Rabi Shrestha, Aaron Charous, Edward Knightly, and Daniel M Mittleman. 2020. Single-Shot Link Discovery for Terahertz Wireless Networks. *Nature Communications* 11, 1 (2020), 1–6.

[11] Yasaman Ghasempour, Chia-Yi Yeh, Rabi Shrestha, Daniel M Mittleman, and Edward Knightly. 2020. Single Shot Single Antenna Path Discovery in THz Networks. In *Proceedings of the 26th Annual International Conference on Mobile Computing and Networking.*

[12] Frank Gross. 2010. *Frontiers in Antennas: Next Generation Design & Engineering.* McGraw Hill Professional.

[13] Shulabh Gupta, Samer Abielmona, and Christophe Caloz. 2009. Microwave Analog Real-Time Spectrum Analyzer (RTSA) Based on the Spectral–Spatial Decomposition Property of Leaky-Wave Structures. *IEEE Transactions on Microwave Theory and Techniques* 57, 12 (2009), 2989–2999.

[14] Daniel Headland, Yasuaki Monnai, Derek Abbott, Christophe Fumeaux, and Withawat Withayachumnankul. 2018. Tutorial: Terahertz Beamforming, from Concepts to Realizations. *Apl Photonics* 3, 5 (2018), 051101.

[15] Josep Miquel Jornet and Ian F Akyildiz. 2011. Channel Modeling and Capacity Analysis for Electromagnetic Wireless Nanonetworks in the Terahertz Band. *IEEE Transactions on Wireless Communications* 10, 10 (2011), 3211–3221.

[16] Nicholas J Karl, Robert W McKinney, Yasuaki Monnai, Rajind Mendis, and Daniel M Mittleman. 2015. Frequency-Division Multiplexing in the Terahertz Range Using a Leaky-Wave Antenna. *Nature Photonics* 9, 11 (2015), 717.

[17] Thomas Kleine-Ostmann and Tadao Nagatsuma. 2011. A Review on Terahertz Communications Research. *Journal of Infrared, Millimeter, and Terahertz Waves* 32, 2 (2011), 143–171.

[18] Swen Koenig, Daniel Lopez-Diaz, Jochen Antes, Florian Boes, Ralf Henneberger, Arnulf Leuther, Axel Tessmann, René Schmogrow, David Hillerkuss, Robert Palmer, et al. 2013. Wireless Sub-THz Communication System with High Data Rate. *Nature Photonics* 7, 12 (2013), 977.

[19] S Leung-Yan-Cheong and M Hellman. 1978. The Gaussian Wire-Tap Channel. *IEEE Transactions on Information Theory* 24, 4 (1978), 451–456.

[20] Zang Li, Roy Yates, and Wade Trappe. 2010. Secrecy Capacity of Independent Parallel Channels. In *Securing Wireless Communications at the Physical Layer.* Springer US, Boston, MA, 1–18.

[21] Jianjun Ma, Nicholas J Karl, Sara Bretin, Guillaume Ducournau, and Daniel M Mittleman. 2017. Frequency-Division Multiplexer and Demultiplexer for Terahertz Wireless Links. *Nature Communications* 8, 1 (2017), 1–8.

[22] Jianjun Ma, Rabi Shrestha, Jacob Adelberg, Chia-Yi Yeh, Zahed Hossain, Edward Knightly, Josep Miquel Jornet, and Daniel M Mittleman. 2018. Security and Eavesdropping in Terahertz Wireless Links. *Nature* 563, 7729 (2018), 89–93.

[23] Rajind Mendis and Daniel M Mittleman. 2009. An Investigation of the Lowest-Order Transverse-Electric (TE 1) Mode of the Parallel-Plate Waveguide for THz Pulse Propagation. *Journal of the Optical Society of America B* 26, 9 (2009), A6–A13.

[24] Daniel M Mittleman. 2017. Perspective: Terahertz Science and Technology. *Journal of Applied Physics* 122, 23 (2017), 230901.

[25] Anamaria Moldovan, Prasanth Karunakaran, Ian F Akyildiz, and Wolfgang H Gerstacker. 2017. Coverage and Achievable Rate Analysis for Indoor Terahertz Wireless Networks. In *Proceedings of the 2017 IEEE International Conference on Communications (ICC).*

[26] Shahid Mumtaz, Josep Miquel Jornet, Jocelyn Aulin, Wolfgang H Gerstacker, Xiaodai Dong, and Bo Ai. 2017. Terahertz Communication for Vehicular Networks. *IEEE Transactions on Vehicular Technology* 66, 7 (2017), 5617–5625.

[27] Kosuke Murano, Issei Watanabe, Akifumi Kasamatsu, Safumi Suzuki, Masahiro Asada, Withawat Withayachumnankul, Toshiyuki Tanaka, and Yasuaki Monnai. 2016. Low-Profile Terahertz Radar Based on Broadband Leaky-Wave Beam Steering. *IEEE Transactions on Terahertz Science and Technology* 7, 1 (2016), 60–69.

[28] Tadao Nagatsuma, Shogo Horiguchi, Yusuke Minamikata, Yasuyuki Yoshimizu, Shintaro Hisatake, Shigeru Kuwano, Naoto Yoshimoto, Jun Terada, and Hiroyuki Takahashi. 2013. Terahertz Wireless Communications Based on Photonics Technologies. *Optics Express* 21, 20 (2013), 23736–23747.

[29] Daniel Steinmetzer, Joe Chen, Jiska Classen, Edward Knightly, and Matthias Hollick. 2015. Eavesdropping with Periscopes: Experimental Security Analysis of Highly Directional Millimeter Waves. In *Proceedings of the 2015 IEEE Conference on Communications and Network Security (CNS).*

[30] Adrian Sutinjo, Michal Okoniewski, and Ronald H Johnston. 2008. Radiation from Fast and Slow Traveling Waves. *IEEE Antennas and Propagation Magazine* 50, 4 (2008), 175–181.

[31] Wade Trappe and Lawrence C Washington. 2006. *Introduction to Cryptography with Coding Theory.* Pearson.

[32] Chao Wang and Hui-Ming Wang. 2016. Physical Layer Security in Millimeter Wave Cellular Networks. *IEEE Transactions on Wireless Communications* 15, 8

(2016), 5569–5585.

[33] Lifeng Wang, Maged Elkashlan, Trung Q Duong, and Robert W Heath. 2014. Secure Communication in Cellular Networks: The Benefits of Millimeter Wave Mobile Broadband. In *Proceedings of the 2014 IEEE 15th International Workshop on Signal Processing Advances in Wireless Communications (SPAWC)*.

[34] Wen-Qin Wang and Zhi Zheng. 2018. Hybrid MIMO and Phased-Array Directional Modulation for Physical Layer Security in mmWave Wireless Communications. *IEEE Journal on Selected Areas in Communications* 36, 7 (2018), 1383–1396.

[35] Aaron D Wyner. 1975. The Wire-Tap Channel. *Bell System Technical Journal* 54, 8 (1975), 1355–1387.

[36] Yongxu Zhu, Lifeng Wang, Kai-Kit Wong, and Robert W Heath. 2017. Secure Communications in Millimeter Wave Ad Hoc Networks. *IEEE Transactions on Wireless Communications* 16, 5 (2017), 3205–3217.