Securing Angularly Dispersive Terahertz Links with Coding

Chia-Yi Yeh, *Member, IEEE,* Alejandro Cohen, *Member, IEEE,* Rafael G. L. D'Oliveira, Muriel Médard, *Fellow, IEEE,* Daniel M. Mittleman, *Fellow, IEEE,* and Edward W. Knightly, *Fellow, IEEE*

***Abstract*—With the large bandwidths available in the terahertz regime, directional transmissions can exhibit angular dispersion, i.e., frequency-dependent radiation direction. Unfortunately, angular dispersion introduces new security threats as increased bandwidth necessarily yields a larger signal footprint in the spatial domain and potentially benefits an eavesdropper. This paper is the first study of secure transmission strategies on angularly dispersive links. Based on information theoretic foundations, we propose a transmission strategy that channelizes the wideband transmission in frequency, and performs secure coding across frequency channels. With model-driven evaluations and over-the-air experiments, we show that the proposed method exploits the properties of angular dispersion to realize secure wideband transmissions, despite the increased signal footprint and even for practical irregular beams with side lobes and asymmetry. In contrast, without the proposed cross-channel coding strategy, angularly dispersive links can suffer from significant security degradation when bandwidth increases. In addition, we find that the security degradation due to bandwidth increment for angularly dispersive links is secondary compared to other factors including the selected secrecy rate or the directivity of the link. Nonetheless, we find that a higher angular dispersion level, i.e., a larger angular spread with the same bandwidth, results in a higher security degradation as bandwidth increases.**

***Index Terms*—Terahertz, Angular Dispersion, Leaky Wave Antenna, Physical Layer Security**

I. Introduction

Angularly dispersive links are characterized by frequency dependent radiation direction. In practice, this property manifests from wide bandwidths, as are expected in the terahertz (THz) regime [2], and from antenna structures such as the leaky-wave antenna (LWA) [3]. To date, angular dispersion has been shown to enable a novel, yet simple, beam steering mechanism via frequency selection [4], [5]. Additionally, path discovery, a key element for directional transmission in mobile THz networks, leveraged angular dispersion by analyzing how different frequencies travel at different angles and thus different paths [6]–[9].

A preliminary version of this paper was accepted at ACM WiSec 2022 [1]. This extended version (i) provides model-driven analysis, (ii) explores the interplay of additional factors including the selected secrecy rate, beam directivity, and angular dispersion level, and (iii) experimentally demonstrates link secrecy for Bob at different angular locations. (Corresponding author: Chia-Yi Yeh, e-mail: cyyeh@mit.edu.)

C-Y. Yeh and E. W. Knightly are with the Department of Electrical and Computer Engineering, Rice University, Houston, TX 77005 USA.

A. Cohen is with the Department of Electrical and Computer Engineering, Technion, Haifa, 3200003, Israel.

R. G. L. D'Oliveira is with the School of Mathematical and Statistical Sciences, Clemson University, Clemson, SC 29634 USA.

M. Médard is with the department of Electrical Engineering and Computer Science, MIT, Cambridge, MA 02139 USA.

D. M. Mittleman is with School of Engineering, Brown University, Providence, RI 02912 USA (e-mail: daniel_mittleman@brown.edu).

While angular dispersion provides new opportunities for THz communications, it also introduces new security threats via unique link characteristics that potentially benefit an eavesdropper. Namely, the transmitter Alice obtains maximum SNR to the receiver Bob at one frequency as dictated by angular dispersion. Unfortunately, with angular dispersion, to send a wider band transmission to Bob necessarily expands the spatial footprint of the transmission, potentially aiding an eavesdropper Eve. Since higher directivity, or a narrower signal footprint, has been shown to be more resilient against eavesdropping [10], an increasingly larger signal footprint of an angularly dispersive link creates security concerns as bandwidth (and data rate) increases: will THz links be fast (wideband) or secure (small footprint), but not both?

This paper is the first to study secure transmission strategies for angularly dispersive links to address the challenge of securing wideband transmissions with angular dispersion. In particular, we propose a transmission strategy that frequency channelizes the wideband transmission and performs coding across frequency channels to secure the angularly dispersive link. The idea is to exploit the fact that for angularly dispersive links, Eve only intercepts a subset of frequency channels well, when she is at a different angular location from Bob [11]. Frequency channelization and cross-channel coding together force Eve to obtain high enough signal strength across the *entire* transmission band to decode the message Alice transmits, and thus limit Eve's chance of interception.

To demonstrate our idea, we establish angularly dispersive THz links using a parallel-plate LWA and specify a cross-channel coding strategy termed SCADL (**S**ecure **C**oding for **A**ngularly **D**ispersive **L**inks), which is adapted from [12] and based on information theory. As a baseline, we specify ICB (**I**ndependently **C**oded **B**aseline), which requires Alice to code independently per frequency channel. We obtain bandwidth-scalable link secrecy in SCADL by ensuring that for a subset of the channels, Eve receives a weaker signal than Bob, as a result of angular dispersion. In contrast, ICB ensures link secrecy only when Eve receives a weaker signal than Bob for all frequency channels. Using prior work in secure coding [12] as a foundation, we for the first time apply the coding scheme for links with angular dispersion and examine in both model-driven simulations and experiments. Also, while our results are based on LWAs, the findings can be generalized to other angularly dispersive links. Using a mix of theoretical analysis, model-driven evaluations, and over-the-air experiments, we make the following contributions.

First, we show that Alice can utilize encoding of her data across different sub-bands to dramatically reduce the security disadvantage due to a widening signal footprint for angularly

dispersive links. In particular, we find that when the proposed cross-coding strategy, SCADL, is employed, the insecure area, i.e., the area of eavesdropping locations where Eve can obtain significant amount of information about the message Alice sends to Bob, only has a modest increase ($< 15\%$) under a bandwidth increment of almost 20 GHz, as opposed to more than 200% growth when the baseline strategy ICB is employed. Indeed, when each frequency channel *independently* codes a sub-message via the baseline strategy, Eve is increasingly likely to decode at least one sub-message when the number of frequency channels increases. Thus, the insecure region expands with the larger signal footprint when the transmission bandwidth increases, such that the baseline strategy must severely compromise security to increase data rate. In contrast, SCADL exploits the *a priori* known angular dispersion characteristics of the antenna so that the transmission remains secure when Eve receives only a subset of frequency channels well.

Next, surprisingly, we find that the shape of the insecure region can be significantly different from the spatial footprint for the angularly dispersive links: With SCADL, the insecure region remains almost fixed as bandwidth increases, despite the widening signal footprint. Perhaps even more unexpected, when ICB is employed, the insecure region forms an unusual two-lobe shape around Bob when the bandwidth increases, instead of uniformly expanding in angle according to the signal footprint. That is, the angularly dispersive transmission becomes more vulnerable at an angle slightly larger or smaller than Bob's angle, in contrast to without angularly dispersive, in which the link is most vulnerable at the emission direction towards Bob. The differences in the insecure region characteristics highlight the importance of evaluating secure transmission strategies in the spatial domain for angularly dispersive links.

We further evaluate the impact of bandwidth (and thus the beamwidth) on secure transmissions compared to other factors, and find that once SCADL is employed, angularly dispersive link's security degradation due to bandwidth increment is insignificant compared to other factors including the selected secrecy rate or single-tone beam directivity. Yet, when all other factors are fixed, we find that a higher angular dispersion level, i.e., a larger angular span given the same bandwidth, indicates a larger insecure area growth under the same bandwidth increment and thus a less secure link.

Finally, we perform the first experimental study of secure coding on over-the-air angularly dispersive links. By measuring a wideband THz transmission from a LWA, we obtain the frequency-dependent radiation pattern for angularly dispersive transmissions. Despite the beam asymmetry and irregularities in the measured LWA radiation pattern, we demonstrate that the proposed cross-channel secure coding successfully manages the widening spatial footprint as observed in the model-driven approach. In contrast, the baseline strategy ICB is significantly impacted by the practical beam asymmetry and irregularities, resulting in an unexpectedly large and asymmetry insecure region. The experimental results demonstrate that our proposed cross-channel coding approach can secure wideband angularly dispersive transmissions even in practical settings. We further examine the insecure region for Bob at different angular locations, which correspond to different angular dispersion levels. We find that, in addition to a wider angular span, Bob at a larger angle is further subject to stronger sidelobes in the experiment, resulting in a stronger dependency on Bob's angular location than in the model-driven results.

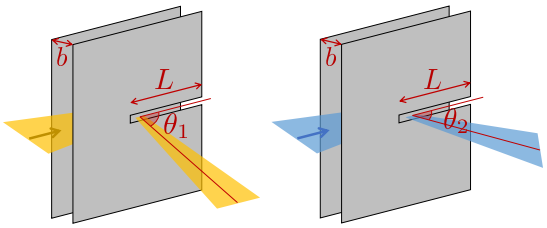

Fig. 1. Terahertz beam steering using a parallel-plate leaky wave antenna with frequency-angle coupling.

II. System Model

A. Angularly Dispersive Leaky-Wave Antenna Link

To understand the security performance of angularly dispersive link, in this paper, a parallel-plate leaky-wave antenna (LWA) with the angular dispersion property, as shown in Fig. 1, is employed for THz directional transmission. The LWA consists of two parallel plates placed at a separation b with a slot opening of length L on one plate. When different frequencies are coupled into the parallel plates, they leak out from the slot towards different angles θ ($0^\circ < \theta < 90^\circ$) dictated by the boundary condition between the parallel-plate waveguide and the opening slot, so that lower frequency emits towards a larger angle and vice versa. We denote this known frequency-dependent emission angle relationship by $\theta_{max}(f)$, and denote the electric field generated by the LWA by $G(f, \theta)$, both of which can be obtained before the deployment using an analytical model [3], [13] or via over-the-air measurements. In this project, we consider the radiation patterns $G(f, \theta)$ to be known and fixed, which Alice cannot change or adapt after she has selected her antenna, including the angular dispersion behavior and radiation null position, if any.

Assuming a transmitter Alice knows the location of a static user Bob in the training phase [6], in the line-of-sight (LoS) scenario, a transmitter Alice employs the LWA described above to transmit to a static user Bob located at an angle θ_B and a distance d_B via frequency selection. 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, $\theta_{max}(f_C) = \theta_B$. For the transmission, Alice uses a transmission band from f_L to f_H (centered at f_C) and divides the band uniformly into K frequency channels, each with a subchannel bandwidth $w = (f_H - f_L)/K$ and centered at f_k for $k \in \{1, \cdots, K\}$.

In contrast to conventional non-angularly dispersive links, the LWA link results in a frequency-dependent emission in the spatial domain due to LWA's angularly dispersive radiation, as illustrated in Fig. 2. To model the resulting signal strength in space, we assume the subchannel bandwidth w is narrow enough so that we can approximate the received signal strength

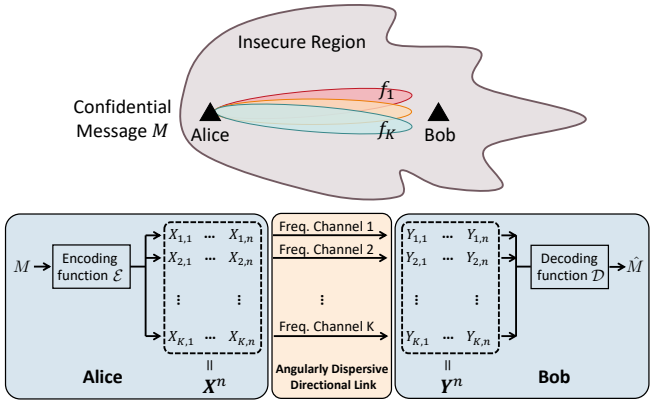

Fig. 2. Wideband angularly dispersive link channelized into K frequency channels.

S in the k-th frequency channel $[f_k - \frac{w}{2}, f_k + \frac{w}{2}]$ at the center frequency f_k. Assume Alice employs a uniform transmit power P for each frequency channel $k \in \{1, \cdots, K\}$, in the LoS scenario, the received signal strength S at location at location (d, θ) in the k-th frequency can then be represented as

$$S_{(d,\theta)}(f_k) = P \cdot \gamma(d, f_k) \cdot |G(f_k, \theta)|^2, \tag{1}$$

where $\gamma(d, f)$ is the channel gain from the transmitter to the receiver, which is assume to follow the free-space pathloss, $\gamma(d, f) = (4\pi df/c)^2$.

When an angularly dispersive antenna is employed, the signal strength model described in Eq. (1) characterizes a widening signal footprint when the frequency channels increases, since $G(f_k, \theta)$ is maximized at different angles for different frequency channels. This unique spatial characteristic of angularly dispersive links creates security concerns for wideband transmissions.

B. Threat Model

In this work, we study how Alice can leverage coding to secure the angularly dispersive links against a potential eavesdropper Eve at a location unknown to Alice and Bob. To this end, we model Eve's interception as a function of her location, define the link secrecy condition, and further define a security metric termed *secure region* as the spatial region in which Eve fails to compromise the link secrecy given an encoding process.

1) LWA Wiretap Channel Model: Using a LWA, a transmitter Alice wants to transmit a confidential message M reliably to a legitimate receiver Bob while keeping it secret from an eavesdropper Eve. We assume Bob and Eve both have a LoS path from Alice and are located at angle and distance (θ_B, d_B) and (θ_E, d_E) with respect to Alice. To reach Bob at θ_B, Alice selects a frequency band emitting towards Bob and channelizes in a frequency-division manner which yields K parallel frequency channels, as described in Sec. II-A.

We model the LWA link eavesdropping scenario as K parallel additive white Gaussian noise (AWGN) wiretap channels. As opposed to the conventional wiretap channel, the LWA wiretap channel depends on Bob's location and Eve's location, and the SNR of each frequency channel inherently follows LWA's frequency-dependent radiation. In each frequency channel $k \in \{1, \cdots, K\}$, Alice transmits x_k, while Bob and Eve receive y_k and z_k respectively, with a location-dependent attenuation ($h_{B,k}$ or $h_{E,k}$) and an i.i.d. additive Gaussian noise ($n_{B,k}$ or $n_{E,k}$):

$$y_k = h_{B,k}\, x_k + n_{B,k} \quad \text{and} \quad z_k = h_{E,k}\, x_k + n_{E,k}. \tag{2}$$

The noise at Bob and Eve, $n_{B,k}$ and $n_{E,k}$, are assumed to be independent, with zero mean and the same noise power σ^2, that is, $n_{B,k} \sim \mathcal{N}(0, \sigma^2)$ and $n_{E,k} \sim \mathcal{N}(0, \sigma^2)$ for all $k \in \{1, \cdots, K\}$. Unlike traditional wiretap schemes considered in the literature [14, Chapter 5], here with the same noise power, the SNR at Bob and Eve thus depends on the signal attenuation they experience, which is frequency and location dependent for the LWA link as modeled in Eq. (1):

$$\begin{aligned} \text{SNR}_{B,k} &= \frac{P \cdot \gamma(d_B, f_k) \cdot |G(f_k, \theta_B)|^2}{\sigma^2} \\ \text{SNR}_{E,k} &= \frac{P \cdot \gamma(d_E, f_k) \cdot |G(f_k, \theta_E)|^2}{\sigma^2}. \end{aligned} \tag{3}$$

Notice that SNR profile at Bob and Eve does not directly determine if a link is secure. Instead, the security of the transmission depends on how Alice and Bob encode and decode the message, as well as the secrecy definition, which we describe next.

2) LWA Link Secrecy Condition: To formally define the security of the LWA transmission, we assume that Alice uses the LWA n times to transmit a message M with a length of m bits, resulting a secrecy data rate $R := m/n$ (bit per use), which is bounded by the communication capacity of the Alice-Bob LWA link. As shown in Fig. 2, when Alice uses the LWA at time $t \in \{1, \cdots, n\}$, she sends K signals, one in each frequency channel, denoted by $X_t = [X_{1,t}; \cdots; X_{K,t}] \in \mathbb{R}^{K \times 1}$. The overall transmitted signal for all time $t \in \{1, \cdots, n\}$ is denoted by $\mathbf{X}^n = [X_1, \cdots, X_n] \in \mathbb{R}^{K \times n}$, and the corresponding received signals at Bob and Eve is denoted by $\mathbf{Y}^n \in \mathbb{R}^{K \times n}$ and $\mathbf{Z}^n \in \mathbb{R}^{K \times n}$, respectively. We note that the mapping from the m-bit message M to the transmitted signal $\mathbf{X}^n$ is characterized by an encoding function $\mathcal{E}$. Similarly, a decoding function $\mathcal{D}$ describes how Bob maps the received signals $\mathbf{Y}^n$ to an estimated message $\hat{M}$.

Now, we define the conditions that determine whether a secure LWA transmission is achieved. Given that the coding process ($\mathcal{E}$ and $\mathcal{D}$) is public information and thus is also known to Eve, the secrecy rate R achieves reliability condition at Bob and the secrecy condition at Eve if:

$$\lim_{n \to \infty} \mathbb{P}(M \neq \hat{M}) = 0 \text{ (reliability)}; \tag{4}$$

$$\lim_{n \to \infty} \frac{1}{n} I(M; \mathbf{Z}^n) = 0 \text{ (secrecy)}, \tag{5}$$

where $\mathbb{P}$ represents probability and I denotes mutual information. Note that Eq. (5) follows the weak secrecy defined in the literature [14, Chapter 3], indicating that Eve's observation does not contain significant amount of information of the confidential message M. Since Alice knows Bob's location and Bob's SNR profile, Alice can choose an appropriate coding process that accommodates Bob's SNR to achieve

the reliability condition in Eq. (4). Thus, whether the LWA link with secrecy rate R is achieved is determined by Eve's observation $\mathbf{Z}^n$, which is a function of location as described in Eq. (3).

We note that the achievable secrecy rate is bounded by the achievable communication rate between Alice and Bob, as the latter requires only the reliability condition while the former requires both reliability and secrecy conditions. Particularly, for frequency channel k, the per-channel achievable communication rate $R^*_{B,k}$ follows Gaussian channel model by [15, Chapter 9]:

$$R^*_{B,k} = \frac{1}{2}\log_2\left(1 + \text{SNR}_{B,k}\right). \tag{6}$$

Then, the total achievable communication rate follows parallel Gaussian channels and is the summation of the per-channel achievable communication rate [15, Chapter 9]: $R^*_B = \sum_{k=1}^{K} R^*_{B,k}$. In the following, Alice only employs a secrecy rate $0 < R < R^*_B$ since any rate higher than R^*_B is infeasible.

3) Secure Region As the Metric: In practice, Alice has to choose her encoding function $\mathcal{E}$ without the knowledge of Eve's location (and thus Eve's SNR profile). Therefore, Alice is motivated to preserve the link secrecy for as large an eavesdropping location set as possible. To this end, we characterize LWA link's security in the spatial domain by the secure region, defined as the set of Eve locations where the secrecy condition in Eq. (5) is satisfied:

$$\mathcal{R}_{\text{sec}} = \left\{(d_E, \theta_E) \mid \lim_{n\to\infty} \frac{1}{n} I(M; \mathbf{Z}^n) = 0\right\}. \tag{7}$$

The rest of the Eve locations forms the insecure region, $\mathcal{R}_{\text{ins}} = \mathcal{R}^c_{\text{sec}}$.

Since angularly dispersive links have a unique frequency-dependent spatial signature, the secure region dependency on coding strategies and major transmission factors are yet to be understood. Indeed, as we show in Sec. V, the shape of the secure region can vary dramatically when different coding functions are employed. Thus, examining the secure region provides us insights on the vulnerable region for angularly dispersive directional transmissions.

In addition to examining the secure regions, we also study how the security level of the LWA link scales with major transmission factors. To this end, we define the insecure area $\mathcal{A}_{\text{ins}}$ as the secrecy outage in the spatial domain:

$$\mathcal{A}_{\text{ins}} = \text{area}(\mathcal{R}_{\text{ins}}). \tag{8}$$

Using the insecure area $\mathcal{A}_{\text{ins}}$, we can quantify the security level of the angularly dispersive link, with a smaller insecure area being more secure.

III. Secure Coding

To secure the angularly dispersive LWA link as defined in Sec. II, we propose to perform cross-channel coding for the frequency-channelized transmission, leveraging the property that Eve only receives a subset of frequency channels well, but not all [11]. To demonstrate our idea, we specify a cross-channel coding scheme, which we term SCADL (**S**ecure **C**oding for **A**ngularly **D**ispersive **L**inks), based on information theory and is adapted from prior work [12]. As a comparison, we specify a baseline coding strategy, termed ICB (**I**ndependently **C**oded **B**aseline), which must code independently in each frequency channel.

Given the similarities of our LWA wiretap channel defined in Sec. II-B and the Gaussian compound wiretap channels studied in [16] (degraded) and [12] (non-degraded), we apply the coding schemes in these prior works to obtain the secure region. However, unlike prior wiretap channel models [14, Remark 5.2] where link secrecy is based on a larger noise at Eve compared to Bob, in our model, the link secrecy is obtained by a weaker received signal at Eve, as a result of a weaker antenna gain or a higher pathloss. In this paper, we conjecture that the results in these noise-based prior works can be generalized to our signal-strength-based model, and leave the proof for future.

A. SCADL

First, we specify the cross-channel coding strategy SCADL to be applied to secure the angularly dispersive transmission. Instead of employing an arbitrary coding strategy, the idea is to make SCADL achieve the information theoretic limit so that employing SCADL results in the maximum secure region among all possible cross-channel coding strategies.

We can obtain the region where secrecy is possible when a secrecy rate R is chosen. Namely, the secure region $\mathcal{R}^{\text{Joint}}_{\text{sec}}$ is the set of all locations j that yield an achievable secrecy rate $R^{\text{Joint}}_S(j)$ larger than the secrecy rate R selected by Alice, while the insecure region $\mathcal{R}^{\text{Joint}}_{\text{ins}}$ consists of locations that cannot support the selected secrecy rate R:

$$\mathcal{R}^{\text{Joint}}_{\text{sec}} = \left\{j \mid R \le R^{\text{Joint}}_S(j)\right\} \text{ and } \mathcal{R}^{\text{Joint}}_{\text{ins}} = \left\{j \mid R > R^{\text{Joint}}_S(j)\right\}, \tag{9}$$

where

$$R^{\text{Joint}}_S(j) = \sum_{k=1}^{K} \frac{1}{2}\left[\log_2\left(1 + \text{SNR}_{B,k}\right) - \log_2\left(1 + \text{SNR}^j_{E,k}\right)\right]^+. \tag{10}$$

Here, $\mathcal{R}^{\text{Joint}}_{\text{sec}}$ is the region in which the secrecy rate R is feasible (but not guaranteed), whereas $\mathcal{R}^{\text{Joint}}_{\text{ins}}$ is the region in which the LWA link with a secrecy rate R can *never* be secure regardless of the coding process. That is, Eq. (9) describes the limit on secure and insecure region for angularly dispersive secure transmissions with cross-channel coding, which we examine in later sections, along with the corresponding insecure area $\mathcal{A}^{\text{Joint}}_{\text{ins}} = \text{area}(\mathcal{R}^{\text{Joint}}_{\text{ins}})$.

Here, we specify the coding construction of SCADL, which achieves the secure region in Eq. (9) and is adapted from [12] based on Gaussain codebooks for a transmission with secrecy rate R.

Codebook generation. Randomly and independently generate K Gaussian codebooks $\mathcal{C}_k, k = \{1, \cdots, K\}$. The Gaussian codebook $\mathcal{C}_k$ consists of $2^{n[R^*_{B,k} - \epsilon]}$ codewords, each of length n, where $R^*_{B,k}$ is the achievable communication rate between Alice and Bob in frequency channel k and $\epsilon > 0$ is small. Next, randomly partition the product of codebook $\mathcal{C} = \mathcal{C}_1 \times \cdots \times \mathcal{C}_K$ into 2^{nR} bins.

Encoding. For a given message $M \in \{1, \cdots, 2^{nR}\}$, randomly choose a codeword from $\mathcal{C}$ in the M-th bin and send the corresponding codeword in $\mathcal{C}_k$ via frequency channel k.

Decoding at the legitimate receiver. By construction, with high probability all K codebooks $\mathcal{C}_1, \cdots, \mathcal{C}_K$ can be decoded from the received signal at Bob. Thus, the transmitted message M can be decoded at Bob with high probability. Notice that decoding the message M requires observations across all K frequency channels.

B. ICB

As a baseline to the proposed cross-channel coding strategy, we specify ICB that must code each frequency channel independently. To make SCADL and ICB comparable, we let ICB have a similar construction as SCADL but without cross-channel coding. Thus, the comparison between ICB and SCADL reflects solely the differences between cross-channel coding and independently-coded per channel. Similar to SCADL, our goal is make ICB achieve the information theoretic limit, but in a per channel manner, instead of across all frequency channels as in SCADL.

For an independently coded strategy, each frequency channel must deliver its own sub-message independently, i.e., the transmitted signal in a frequency channel cannot be affected by the sub-messages in other frequency channels. To this end, Alice divides the message M into sub-message M_k for $k \in \{1, \cdots, K\}$, each to be transmitted in the corresponding frequency channel, resulting in a per-channel secrecy rate of R_k in channel k.

We can obtain the region where secrecy is possible when the per-channel secrecy rates $[R_1, \cdots, R_k]$ are chosen. First, for channel k with a selected secrecy rate R_k, the set of all Eve locations j that yield an achievable secrecy rate $R^{\text{Ind}}_{S,k}(j)$ larger than the secrecy rate R_k forms the per-channel secure region $\mathcal{R}^{\text{Ind}}_{\text{sec},k}$, while the per-channel insecure region $\mathcal{R}^{\text{Ind}}_{\text{ins},k}$ consists of locations that cannot support the selected per-channel secrecy rate R_k:

$$\mathcal{R}^{\text{Ind}}_{\text{sec},k} = \left\{j \mid R_k \le R^{\text{Ind}}_{S,k}(j)\right\} \text{ and } \mathcal{R}^{\text{Ind}}_{\text{ins},k} = \left\{j \mid R_k > R^{\text{Ind}}_{S,k}(j)\right\}, \tag{11}$$

where

$$R^{\text{Ind}}_{S,k}(j) = \frac{1}{2}\Big[\log_2\left(1 + \text{SNR}_{B,k}\right) - \log_2\left(1 + \text{SNR}^{j}_{E,k}\right)\Big]^{+}. \tag{12}$$

Here, $\mathcal{R}^{\text{Ind}}_{\text{sec},k}$ is the region in which the transmission in frequency k with a secrecy rate R_k is feasible (but not guaranteed), whereas $\mathcal{R}^{\text{Ind}}_{\text{ins},k}$ is the region in which the channel-k transmission with a secrecy rate R_k can *never* be secure regardless of the coding process.

Next, when considering the collective transmission across all K frequency channels, a transmission with per-channel secrecy rates $[R_1, \cdots, R_K]$ is only achievable when the per-channel transmissions in all K frequency channels are feasible. In contrast, the transmission is certainly insecure if the transmission in any of the frequency channels is insecure. Thus, the per-channel secrecy rates $[R_1, \cdots, R_K]$ result in a secure region $\mathcal{R}^{\text{Ind}}_{\text{sec}}$, in which the selected rate vector is achievable, whereas the rest of the locations form the insecure region $\mathcal{R}^{\text{Ind}}_{\text{ins}}$:

$$\mathcal{R}^{\text{Ind}}_{\text{sec}} = \bigcap_{k=1}^{K} \mathcal{R}^{\text{Ind}}_{\text{sec},k} \quad \text{and} \quad \mathcal{R}^{\text{Ind}}_{\text{ins}} = \bigcup_{k=1}^{K} \mathcal{R}^{\text{Ind}}_{\text{ins},k}. \tag{13}$$

Eq. (13) describes the limit on secure and insecure region when coding independently per channel is required, which we explore in later sections for the angularly dispersive links, along with the resulting insecure area $\mathcal{A}^{\text{Ind}}_{\text{ins}} = \text{area}(\mathcal{R}^{\text{Ind}}_{\text{ins}})$.

Here, we specify the coding construction of ICB that achieves the secure region in Eq. (13). Similar to SCADL, ICB is also based on Gaussian codebooks and is adapted from [12]. Given that Alice has chosen the per-channel rates $[R_1, \cdots, R_K]$ in all K channels, Alice codes independently in each frequency channel as follows:

Codebook generation. For frequency channel k, randomly generate a Gaussian codebook $\mathcal{C}_k$ consisting of $2^{n[R^*_{B,k}-\epsilon]}$ codewords, each of length n, where $R^*_{B,k}$ is the achievable communication rate between Alice and Bob in frequency channel k and $\epsilon > 0$ is small. Randomly partition the codebook $\mathcal{C}_k$ into 2^{nR_k} bins.

Encoding. For a given message $M_k \in \{1, \cdots, 2^{nR_k}\}$, Alice randomly chooses a codeword from $\mathcal{C}_k$ in the M_k-th bin and send it through frequency channel k.

Decoding at the legitimate receiver. By construction, with high probability the codebook $\mathcal{C}_k$ can be decoded from the received signal at Bob. Thus, for all channel $k \in \{1, \cdots, K\}$, the transmitted message M_k can be decoded at Bob with high probability, and therefore the entire message M can be decoded at Bob with high probability.

When comparing the coding constructions of ICB and SCADL, we observe that the two share the same codebook generation procedure and only diverge in the binning process, so that one codes independently per channel while the other codes cross channels. This distinction makes ICB vulnerable even when Eve receives a strong signal in only one frequency channel, as Eve is able to decode a sub-message and thus a significant part of the total message. Unfortunately, for angularly dispersive links, Eve is likely to receive a subset of frequency channels well. Indeed, we provide the proof of SCADL being more secure than ICB in the Supplementary Materials. In the following, ICB serves as the baseline to the proposed SCADL, demonstrating the link secrecy when cross-channel coding is not used for angularly dispersive links.

IV. Model-Driven Performance Evaluation

In this section, we study the security of angularly dispersive links with the proposed cross-channel coding strategy SCADL, and compare it with the independently coded baseline strategy ICB. We examine the secure coding strategies for the key factor of transmission bandwidth, as a larger bandwidth necessarily yields a wider signal footprint for angularly dispersive links. To characterize the link secrecy, the secure region as described in Eq. (9) and Eq. (13) is investigated.

A. Methodology

1) Analytical LWA radiation model: The radiation pattern of a parallel-plate LWA has been characterized using a simplified model, which has been shown to match well to over-the-air LWA measurements [6], [8], and thus is employed in our analysis. In particular, the parallel-plate LWA is abstracted as a uniform finite aperture of length L with an emission distribution at the aperture determined by an attenuation constant α and 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 LWA which has a dominant transverse electric (TE) mode of TE_1 mode [17], the phase constant β relates to the plate separation b by

$$\beta(f) = k_0\sqrt{1-\left(\frac{f_{co}}{f}\right)^2}, \tag{14}$$

for frequency $f > f_{co}$ and $k_0 = \frac{2\pi f}{c}$ is the free-space wavenumber. As for the attenuation constant α, it can be engineered [18] but the designed parameters have not been formally characterized. With the abstracted model, the E-field of the LWA for frequency f towards angle θ is [3], [19]

$$G(f,\theta) = L\,\mathrm{sinc}\left(\left[\beta(f) - j\alpha - k_0\cos\theta\right]\frac{L}{2}\right). \tag{15}$$

Eq. (15) describes a sinc-like radiation pattern for a given frequency f where the maximum emission direction varies with frequency.

LWA's angular dispersion property can be better described by the maximum radiation angle θ_{max} for a frequency f, which can be derived from Eq. (15):

$$\theta_{max}(f) = \sin^{-1}\left(\frac{c}{2bf}\right). \tag{16}$$

Eq. (16) shows that LWA's maximum radiation direction is a non-linear function of the input frequency, with a higher frequency emitting towards a smaller angle, providing the foundation for LWA beam steering for users at different angles by selecting the corresponding frequencies, as described in Sec. II-A.

2) Setup: For the model-driven evaluation, we explore the security of angularly dispersive links using an ideal LWA with radiation as modeled in Eq. (15). In particular, the LWA has a plate separation of $b = 1$ mm, a slot length $L = 3$ cm, and an attenuation constant α of 50 m^{-1}. Using the above LWA, Alice transmits to Bob located at angle $\theta_B = 30°$ and distance $d_B = 1$ m with respect to Alice. To reach Bob, Alice employs a transmission band centered at 300 GHz, which has a maximum radiation towards Bob's angle at $30°$. The subchannel bandwidth of the transmission w is 0.5 GHz and Alice selects an integer number of subchannels yielding total bandwidth ranging from 0.5 GHz to 19.5 GHz (from 1 channel to 39 channels). Alice employs a uniform power per frequency channel, and the resulting SNR at Bob and Eve in each frequency channel follows Eq. (3). Alice's transmit power is chosen to yield an SNR of 25 dB at Bob for the center frequency channel.

To transmit the confidential message to Bob, Alice employs a secrecy rate R, which is bounded by Bob's total achievable communication rate R_B^*. Notice that Bob's total communication rate R_B^* increases with more frequency channels, indicating a higher total secrecy rate R can be supported. To compare scenarios with different bandwidth, the total secrecy rate R is scaled to Bob's total communication rate R_B^*. That is, the ratio between the secrecy rate R and Bob's total communication rate R_B^* is fixed, which we define as the normalized secrecy rate η:

$$\eta = R/R_B^*. \tag{17}$$

The normalized total secrecy rate η falls between 0 and 1 and reflects the fraction of the channel capacity being used for secrecy transmission. For ICB, the total secrecy rate is the summation of the per-channel secrecy rate, $R = \sum_{k=1}^{K} R_k$, and the per-channel secrecy rate R_k is allocated by $R_k = \eta R_{B,k}^*$ so that Eq. (17) is met. In the following, we arbitrarily choose $\eta = 0.2$ in the evaluation.

B. Insecure Area Scaling with Total Bandwidth

In this subsection, we study how the insecure area scales with increasing bandwidth for angularly dispersive links. For a non-angularly dispersive link, the insecure area is expected to remain the same with increasing bandwidth as the transmission footprint does not change with a larger bandwidth. However, a key property of angularly dispersive links is that the signal footprint widens with a larger transmission band, suggesting a larger insecure area and thus a less secure transmission when the bandwidth is larger. In the following, we examine SCADL against ICB for the LWA angularly dispersive link, and show that, contrary to our expectation, the insecure area increase can be surprisingly slow when widening the transmission band.

Fig. 3 shows the scaling of insecure area for SCADL and ICB when the transmission bandwidth increases from 0.5 GHz to 19.5 GHz for Bob located at an angle of $30°$ and a distance of 1 m from Alice. As described in the setup, Alice and Bob communicate securely at a rate R that is 20% of Bob's total achievable communication rate R_B^*, that is, at a normalized secrecy rate $\eta = 0.2$. To quantify the insecure area scaling, we use the single-channel case (i.e., the total bandwidth is 0.5 GHz) as the basis. When Alice and Bob employ only one channel, SCADL and ICB converge to the same strategy and result in the same insecure area, which is used as the basis for comparison. Thus, we define the normalized insecure area as the insecure area compared to the single-channel case, to explore the area scaling in Fig. 3.

In Fig. 3, we observe that when the independently-coded baseline strategy ICB is employed, the insecure area expands by more than 3 times as the bandwidth increases from 0.5 GHz to 19.5 GHz. The insecure area increase matches our expectation for the angularly dispersive link, showing that a wider signal footprint translates into a larger insecure area.

However, when SCADL is employed, we observe that the insecure area remains almost constant and yields only a 1.14 times increase in the insecure area under the same bandwidth

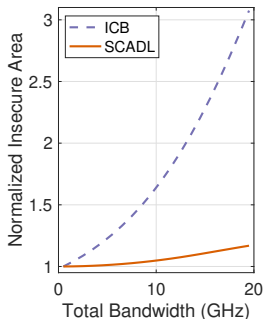

Fig. 3. Insecure area scaling with transmission bandwidth when SCADL and ICB are employed, with a normalized secrecy rate $\eta = 0.2$.

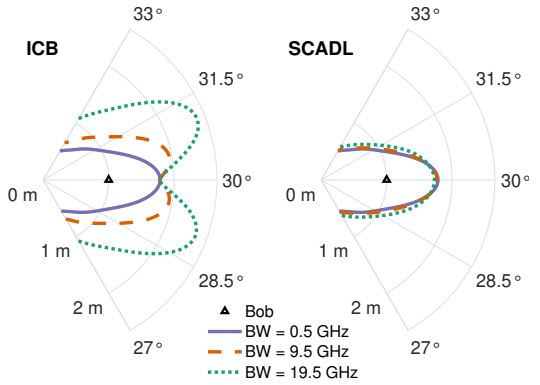

Fig. 4. Boundary of insecure regions when the total transmission bandwidth scales from 0.5 GHz to 19.5 GHz, with a normalized secrecy rate $\eta = 0.2$ for Bob at 30°.

increment. That is, the insecure area increases significantly slower for SCADL compared to ICB despite the fact that the two strategies yield the *same* spatial footprint, i.e., the same SNR profile in space. We also stress that both ICB and SCADL employ secrecy capacity achieving codes, indicating that the gap is a fundamental difference between coding per channel and coding across channels, not due to a suboptimal coding design.

The fact that the insecure area can remain almost constant when employing SCADL is striking, as it shows that achieving a higher secrecy rate with little sacrifice in secrecy outage is possible for angularly dispersive links. In addition, the insecure area scaling difference in Fig. 3 indicates the importance of cross-channel coding for angularly dispersive links, especially when a large bandwidth is employed.

While Fig. 3 shows the insecure area scaling with bandwidth, it is not clear how the insecure region varies in the spatial domain with increasing bandwidth. That is, we yet to known which spatial regions become secure or insecure when the bandwidth widens, which we study in the next subsection.

C. Insecure Region Characterization

Using the same transmission scenario as in Fig. 3, we examine the spatial regions that are vulnerable to eavesdropping when the bandwidth widens.

Fig. 4 shows the insecure region for SCADL and ICB when the transmission bandwidth increases from 0.5 GHz to 19.5 GHz. Fig. 4 depicts space as a polar plot with the origin being Alice's location and the black triangle represents Bob at 30° and 1 m from Alice. The curves depict the boundaries of insecure regions for bandwidths of 0.5, 9.5, and 19.5 GHz. When Eve locates within the enclosed region, she is able to learn about the confidential message Alice sends to Bob so that the secrecy condition in Eq. (5) is violated. Since the transmission beamwidth is narrow in all three cases, we expand the region near Bob in the plot to illustrate the insecure region's change in the angular region of interest.

First, we examine the insecure region for ICB shown in the left of Fig. 4. We start with the blue solid curve which depicts the boundary of the insecure region for the single channel scenario. As we expect, the blue curve encloses a region corresponding to the directional radiation pattern around Bob, indicating that when a single frequency channel is employed, locations that are angularly close to Bob and radially close to Alice is vulnerable to eavesdropping. In particular, Eve is most advantageous when she is at the same angle as Bob at 30°, where she can obtain knowledge about the confidential message up to a distance of 1.8 m. Yet, since the transmission is highly directional, even Eve moves only by 2°, her range of interception is significantly reduced to 0.7 m.

Interestingly, as the bandwidth increases to 9.5 GHz, the orange dashed curve shows that the insecure region no longer retains the one-lobe shape. Instead, the insecure region expands in the angles except for Bob's angle and results in two lobes at angles slightly off Bob's angle. In particular, the orange dashed curve shows that the maximum angles happens at 29.5° and 30.5°, where message leakage happens up to 1.95 m. We observe that the same insecure region expansion continues when the transmission bandwidth further increases. As depicted by the dotted green curve, when the bandwidth widens to 19.5 GHz, the maximum angles shift to 29° and 31°, where message leakage happens up to an even further distance of 2.5 m.

To understand the insecure region variation, recall that when employing ICB, the transmission is secure only when all submessages over the K frequency channels are secure. As a result, the total insecure region when employing ICB is the union of the per-channel insecure region as described in Eq. (13). When new frequency channels are added for an angularly dispersive link, they create per-channel insecure regions that appear angularly misaligned with the existing insecure region, and thus widen the collective insecure region. In addition, the newly added frequencies have a longer range of interception so that the angles corresponding to the maximum range of interception diverge from Bob's angle.

We emphasize that the growth in the maximum distance of leakage is not due to Alice's transmit power since Alice employs a uniform transmit power across the K frequency channels. Indeed, Bob's SNR across the K frequency channels peaks at the center frequency channel at 25 dB and decreases towards the edge frequency channels, indicating the same trend for Bob's achievable communication rate (per frequency channel). Therefore, when Alice employs ICB, she employs a lower per-channel secrecy rate R_k towards the edge frequency channels. Yet, despite a lower per-channel secrecy rate R_k in the edge frequencies, the longest distance of leakage increases,

resulting in the two-lobe insecure region.

This two-lobe shape of insecure region, which is not due to side lobes, is rather unusual and is uniquely observed for the angularly dispersive link. Indeed, for a conventional non-angularly dispersive directional link whose signal footprint is independent of the total bandwidth, the insecure region should retain a single lobe shape with increasing bandwidth. This unique insecure region characteristic suggests that angularly dispersive links can be more vulnerable to eavesdropping *off* the transmission axis, contrasting to typical directional transmissions which are vulnerable along the Alice-Bob axis. This implies that Eve may not have to be aligned with Bob to intercept an angularly dispersive link, which potentially lowers the chance of blocking Bob's received signal and thus being detected. While we see a unique two-lobe insecure region for an angularly dispersive link when employing ICB, we note that it is not always the case for angularly dispersive links, as we see next for SCADL.

Next, we examine the insecure region of the proposed cross-coding strategy, SCADL, shown on the right of Fig. 4. As before, we start with the blue solid curve which depicts the boundary of the insecure region for the single channel case. Since ICB and SCADL converge to the same strategy in the single channel case, we observe that the insecure area for the single channel scenario is the same for ICB and SCADL.

However, the insecure region of SCADL becomes significantly different from ICB when the bandwidth increases. Surprisingly, we observe that the insecure region remains almost *identical* with increasing bandwidth, despite the widening signal footprint of the angularly dispersive link. Yet, when examining closely, we can still observe some changes in the insecure region when the bandwidth increases. In general, for angles further away from Bob's angle, the minimum secure distance expands with a larger bandwidth. In contrast, for angles closer to Bob's angle, the minimum secure distance even *decreases* with a larger bandwidth.

To understand why the insecure region remains almost identical with increasing bandwidth when SCADL is employed, we examine a location j before and after the bandwidth increment and argue that location j remains secure with a high probability if it is secure before the bandwidth increment. We roughly divide locations into three sectors: larger than Bob's angle, smaller than Bob's angle, and close to Bob's angle. First, when Eve locates at an angle close to Bob's angle, she receives a similar SNR profile across the frequency channels as Bob. Therefore, if the angularly dispersive link is secure before the bandwidth increment, Eve must receive a lower SNR than Bob across the frequency channels. When new frequency channels are added, Eve must also receives a lower SNR for the newly added channels, and thus the angularly dispersive link remains secure after the bandwidth increment. Next, when Eve is in the larger angle sector, she receives stronger signals for the lower frequency channels and weaker signals for the higher frequency channels. Therefore, when the transmission band widens symmetrically from the center frequency, Eve only intercepts half of the newly added frequency channels (the higher frequency portion). Meanwhile, Bob enjoys the capacity increment from all the newly added frequency channels. This knowledge increment gap between Bob and Eve retains the secrecy of the transmission when bandwidth widens. A similar argument holds when Eve is in the smaller angle sector. Thus, when SCADL is employed for an angularly dispersive link, any location that is previously secure is likely to remain so when the bandwidth widens, despite the widening signal footprint.

Comparing the insecure region for ICB and SCADL in Fig. 4, we find that exploiting the non-uniform signal strength in the frequency domain is the key to combat the widening signal footprint for wide-bandwidth angularly dispersive links. SCADL exploits the location-dependent non-uniform signal strength property via requiring the receiver to decode the message using the observations across all K frequency channels. Therefore, when Eve receives a strong signal in some frequency bands, as long as she receives a weak signal in the rest of the frequency channels, the confidential message remains unknown to Eve. In comparison, ICB does not exploit the signal strength coupling property and thus suffers from the widening signal footprint. As a result, when Eve receives a strong signal in some frequency bands, she gains knowledge about the sub-messages sent in those frequency channels, resulting in an insecure transmission.

The insecure area scaling in Fig. 3 and the insecure region characterization in Fig. 4 for SCADL alleviate concerns about angularly dispersive directional links being less secure compared to a conventional directional link, especially when employing a wide bandwidth with a wider spatial footprint. That is, one would expect that the insecure region remains the same for a non-angularly dispersive link but expands for an angularly dispersive link when the transmission bandwidth increases. In contrast, Fig. 3 and Fig. 4 show that the insecure area can remain almost constant and the insecure region of an angularly dispersive link can remain almost identical to the single channel scenario when SCADL is employed. Yet, we point out that employing the cross-channel coding strategy is essential to achieve this.

D. Security of General Angular Dispersive Links

In the previous subsections, Fig. 3 and Fig. 4 demonstrate the security characteristic of one specific angularly dispersive link. Here, we further explore the interplay between angularly dispersive link secrecy and three major factors: secrecy rate, transmission beamwidth, and angular dispersive level. In particular, we examine how the insecure area varies with the three factor, as well as how these three factors affect the scaling of the insecure area when the bandwidth increases.

1) Normalized Secrecy Rate: We first examine how selecting different secrecy rates impacts the security of an angularly dispersive link. To this end, four levels of normalized secrecy rate η ranging from low ($\eta = 0.2$) to high ($\eta = 0.8$) are employed using the same setup as in Fig. 3. For each normalized secrecy rate, we obtain the insecure area when the total bandwidth is 0.5 GHz (single channel) and 19.5 GHz (39 channels). To focus on the scaling of the insecure area, we normalize the insecure area to the smallest insecure area among all examined settings, which is the single-channel transmission with $\eta = 0.2$ in this case.

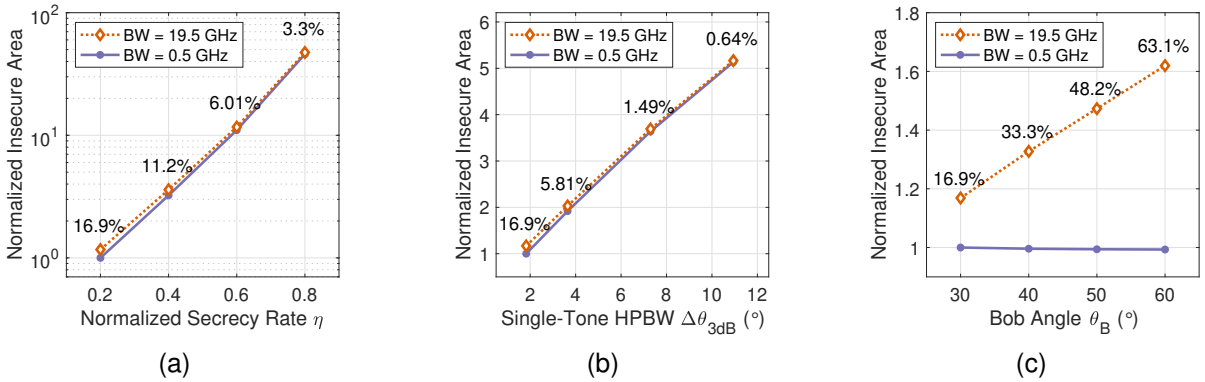

Fig. 5. Insecure area variation with three transmission factors when SCADL is employed for an angularly dispersive link. (a) Normalized secrecy rate η, (b) single-tone beamwidth $\Delta\theta_{3\text{dB}}$, and (c) Bob angle θ_B which reflects angular dispersion level. The percentage shows the insecure area growth from the single-channel 0.5 GHz bandwidth transmission.

Fig. 5a shows the normalized insecure area variation when different normalized secrecy rates are employed for the angularly dispersive transmission using SCADL. First, we examine the blue solid line for the single channel transmission. From the blue solid line, we observe that when a larger normalized secrecy rate is employed for the transmission, the insecure area expands. In addition, we note that the Y axis of Fig. 5a is in log scale, indicating that the insecure area scales exponentially with the secrecy rate. Indeed, we expect a wireless transmission, not limited to an angularly dispersive one, to be more vulnerable to eavesdropping when Alice chooses to transmit the confidential message at a higher secrecy rate. And since the secrecy rate increases logarithmic with decreasing Eve's SNR (which scales inversely with Eve's distance), the insecure area grows exponentially with the secrecy rate.

Next, we examine the orange diamond curve for a larger bandwidth transmission of 19.5 GHz. We observe that the orange diamond curve follows the blue solid line closely with a slight increase, indicating that the insecure area expands with a larger transmission band, as we expect for an angularly dispersive link due to a widening signal footprint.

To further compare the two transmissions with different bandwidths, the percentage number shown above each diamond marker indicates the insecure area growth compared to the single channel transmission. The growth percentage in Fig. 5a shows a larger insecure area growth when a lower normalized secrecy rate is employed, which is due to a smaller referenced area. That is, the insecure area of the single-channel transmission sets the basis for the area growth comparison, and a smaller area basis makes the same area change appear larger in ratio, which happens when a smaller normalized secrecy rate η is employed. Nevertheless, we observe the insecure area growth due to bandwidth scaling is small to moderate: all below 20% in Fig. 5a.

When comparing the insecure area growth due to a larger secrecy rate vs. a larger bandwidth, we observe that the effect of the secrecy rate dominates. The order of magnitude difference in insecure area scaling indicates that selecting the secrecy rate is the primary consideration for an angularly dispersive secrecy transmission, compared to the total bandwidth employed.

2) Single-Tone Beamwidth: Next, we examine how the security of an angularly dispersive link varies when the LWA exhibits a different beamwidth. Secrecy Transmission on Parallel Channels

We point out that the collective beamwidth (i.e., the beamwidth considering the radiation of all frequency channels) of an angularly dispersive link depends on both the single-tone beamwidth and the total bandwidth employed. Therefore, to isolate the beamwidth discussion from the bandwidth factor for angularly dispersive links, we use the single-tone beamwdith, $\Delta\theta_{3\text{dB}}$, as the metric in the following.

To explore angularly dispersive links with different single-tone beamwdith, the same setup as in Fig. 3 is used except that we vary the LWA attenuation constant α. When the LWA has a higher attenuation constant α along the LWA aperture, the single-tone beamwdith $\Delta\theta_{3\text{dB}}$ becomes wider. Previously, α is chosen as $50m^{-1}$ and results in a single-tone beamwidth of $1.8°$. Here, we further increase α to as large as $300m^{-1}$, yielding a single-tone beamwidth of $10.9°$, which is 6 times larger than before. To focus on the scaling as in Fig 5a, we normalize the insecure area to one specific transmission setup, which is the single-channel transmission with the smallest LWA attenuation constant $\alpha = 50m^{-1}$ in this case.

Fig. 5b shows the insecure area of an angularly dispersive link when the LWA exhibits different single-tone beamwidths. First, we examine the blue solid line for the single-channel transmission. We observe that the insecure area increases linearly with a larger single-tone beamwidth, which is expected and directly reflects the larger signal footprint of the transmission.

Next, we examine the orange diamond curve for a angularly dispersive transmission with a larger bandwidth of 19.5 GHz. We observe that the orange diamond curve follows the solid blue line closely with only a slight increase, again showing the unique insecure area growth with bandwidth increment when the link is angularly dispersive. The percentage number shown above each diamond marker indicates the insecure area growth in percentage due to the bandwidth increment, showing an insecure area growth less than 20% when the transmission bandwidth increases to 19.5 GHz. We also observe a larger

insecure area growth when the single-tone beamwdith is smaller, which is due to a smaller referenced area in the single-channel transmission as we also observed in Fig. 5a.

The insecure area scaling in Fig. 5a and Fig. 5b has many similarities, indicating that just like the factor of secrecy rate, the factor of single-tone beamwdith also has a dominant effect the insecure area compared to the transmission bandwidth. We note that Fig. 5a and Fig. 5b have different scales in the Y axis: one is in log scale while the other is not. Nonetheless, the finding is similar: the impact of bandwidth to link secrecy is secondary compared to the secrecy rate or the single-tone beamwidth for an angularly dispersive link.

3) Angular Dispersion Level: Last, we examine how the angular dispersion level impact the secrecy of the angularly dispersive transmission. We define the angular dispersion level as the radiation direction change given a unit change in frequency. In the context of a LWA transmission, the angular dispersion level varies with Bob's angle. For Bob at a smaller angle, such as $\theta_B = 30°$, the radiation direction changes by $0.11°$ (from $30°$ to $29.89°$ or $30.11°$) when the frequency change by 1 GHz from the center frequency 300 GHz. In contrast, for Bob at a larger angle, such as $\theta_B = 60°$, with the same frequency change of 1 GHz from the center frequency (which becomes 173 GHz), the radiation direction changes by $0.57°$, which is a larger change compared to Bob at a smaller angle, and thus a higher angular dispersion level.

To explore the impact of angular dispersion level on security, we use the same setup as in Fig. 3 for Bob at different angles, ranging from $30°$ to $60°$. As before, to focus on the scaling as in Fig 5a, we normalize the insecure area to one specific transmission setup, which is the single-channel transmission to Bob at $\theta_B = 30°$ in this case.

Fig. 5c shows the insecure area for the angularly dispersive transmission when Bob is at different angular locations. First, the blue solid line illustrates a consistent insecure area when a single frequency channel is employed regardless of Bob's angular location. This indicates that the single-tone radiation from the LWA is similar across different transmission angles, and thus results in a consistent security level for Bob at different angles.

However, when the transmission bandwidth increases to 19.5 GHz, as shown by the orange dashed line, the insecure area expands more for Bob at a larger angle. For Bob at $60°$, the insecure area expands by 63.1%, as opposed to 16.9% for Bob at $30°$. Indeed, as we point out earlier, with the same bandwidth, the overall radiation is more spread-out in the angular domain for Bob at a larger angle. As a result, the edge frequencies are more vulnerable to eavesdropping, yielding a larger insecure area.

From Fig. 5c, we observe that a higher angular dispersion is indeed associated with a less secure link. In particular, a more angularly dispersive link results in a larger security degradation due to bandwidth increment, despite employing a cross-channel coding such as SCADL that exploits the non-uniformity across the frequencies. Thus, when a directional link exhibits high angular dispersion, we still cannot avoid the trade-off between bandwidth and security.

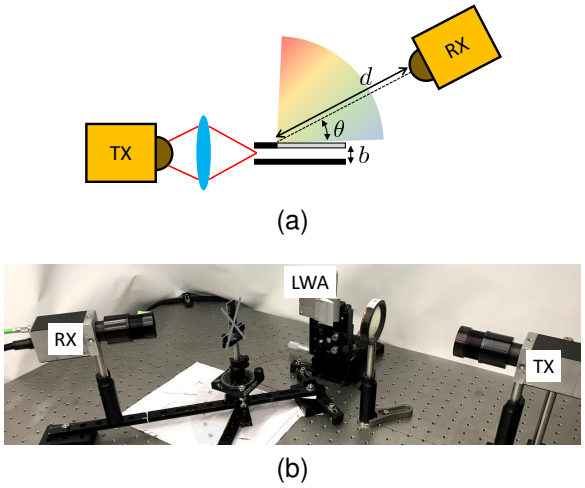

Fig. 6. (a) Experiment diagram, (b) Experiment setup.

V. Over the Air Experiments

In Sec. IV, we examine the security properties of LWA angularly dispersive links using a model-driven approach. In this section, we further study the angularly dispersive link security using real-world LWA measurements. The security performance difference between the model-driven simulation and the over-the-air experiment reflects the impact due to the hardware. In this paper, we focus on angular dispersion and the antenna radiation pattern. Other hardware impairments, as considered in the literature, for example, in [20], are left for future study.

A. Experimental Setup

We measure the radiation pattern of a custom parallel-plate 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 [21] 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 measure the THz signals with a frequency resolution of 3.13 GHz.

Fig. 6a illustrates the experiment diagram and Fig. 6b 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. We place the receiver at $12° < \theta < 80°$ with $1°$ resolution in the measurement.

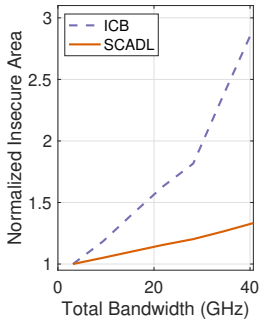

Fig. 7. Insecure area scaling with transmission bandwidth when SCADL and ICB are employed, with a normalized secrecy rate $\eta = 0.2$ for Bob at $40°$.

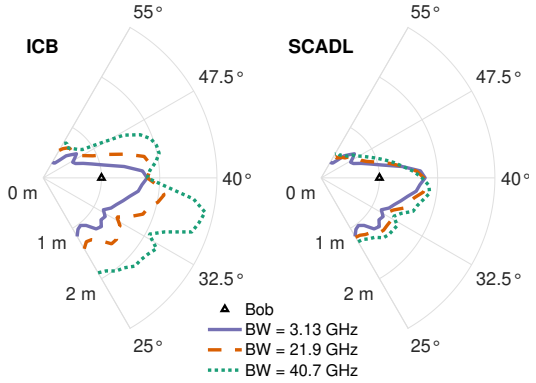

Fig. 8. Boundary of insecure regions when the total transmission bandwidth scales from 3.13 GHz to 40.7 GHz, with a normalized secrecy rate $\eta = 0.2$ for Bob at $40°$.

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. For each frequency component, the measurements over angular locations $12° < \theta < 80°$ describe the radiation pattern, and thus we obtain a real-world LWA radiation pattern.

In the following, the same methodology as in the model-driven analysis is used, except that the LWA radiation pattern is based on the over-the-air measurement. In addition, since the frequency resolution of our measurement is 3.13 GHz, the subchannel bandwidth w for the experimental evaluation is chosen accordingly, i.e., $w = 3.13$ GHz, instead of $w = 0.5$ GHz as in the model-driven analysis. In the following analysis, the number of frequency channels varies from 1 to 13, so that the total bandwidth ranges from 3.13 GHz to 40.7 GHz.

B. Empirical Insecure Area Scaling

For the experimental evaluation, we first examine the scaling of insecure area when the transmission bandwidth increases. We examine the scenario where Bob is at an angle $\theta_B = 40°$ and a distance of $d_B = 1$ m. Fig. 7 shows the insecure area scaling when the transmission bandwidth increases from 3.13 GHz to 40.7 GHz when a normalized secrecy rate $\eta = 0.2$ is employed. As before, the insecure area is normalized to the single-channel transmission scenario to show the scaling.

From Fig. 7, we observe that when the independently coded baseline strategy ICB is employed for an angularly dispersive link (blue dashed curve), the insecure area expands with increasing bandwidth. In comparison, when SCADL is employed for the angularly dispersive link (orange solid curve), the insecure area scales significantly slower with increasing bandwidth although the transmitted signal has the same widening angular footprint as the ICB transmission.

While the irregular beam pattern of a real LWA introduces some local variations, Fig. 7 clearly shows the same trend as in Fig. 3 based on the model-driven approach, validating our discussion based on the model-driven approach in Sec. IV. Specifically, Fig. 7 shows that the secrecy of an angularly dispersive link can suffer from a wider angular footprint when the transmission bandwidth increases if ICB is employed. Yet, if SCADL is employed, angularly dispersive link's secrecy degradation due to the widening signal footprint can be alleviated, providing a relatively consistent secrecy level as the bandwidth increases.

C. Empirical Insecure Region Characterization

Next, we examine the insecure region of the LWA link based on measurements, which illustrates how the beam pattern irregularity of an real angularly dispersive antenna affects the performance of secure coding in the spatial domain.

Fig. 8 shows the spatial region near Bob in the polar coordinate. As in Fig. 4, the origin represents Alice's location, the black triangle represent Bob at $\theta_B = 40°$ and $d_B = 1$ m. The three curves represent the boundaries of insecure regions when three different bandwidths are employed for the angularly dispersive transmission.

First, we examine the left figure in Fig. 8 for the baseline strategy ICB. The single-channel transmission shown by the blue solid curve illustrates that the measured LWA has an asymmetric beam pattern: the antenna gain declines much slower towards the smaller angle than towards the larger angles. As a result, the insecure region extends more towards the smaller angles than towards the larger angles, indicating that the single-channel transmission is more vulnerable towards the smaller angles.

As the bandwidth increases to 21.9 GHz (orange dashed curve) and 40.7 GHz (green dotted curve), we observe that the insecure region expands towards both sides of angles *unevenly*. In particular, the insecure area expands more in the smaller angles than in the larger angles. Moreover, the longest range of leakage towards the larger angles vs. towards the smaller angles is dramatically different. For a transmission bandwidth of 40.7 GHz, the longest leakage distance is 2.03 m (at $43°$) for angles larger than $40°$. In comparison, for angles smaller than $40°$, the longest leakage distance is 2.84 m (at $37°$), which is almost 40% longer than 2.03 m from the larger angles ($\theta > 40°$).

To understand the uneven insecure region expansion as the bandwidth increases when employing the independently-coded strategy ICB, we examine the measured LWA beam pattern. Fig. 9 illustrates the measured LWA radiation pattern for 3 frequency channels. Initially, when only a single channel is used for the transmission, Alice employs only the center

frequency channel at 244 GHz shown by the red solid curve, which has a strongest emission towards Bob at $40°$. As the transmission bandwidth increases, more frequency channels are used. For a total bandwidth of 40.7 GHz, 13 frequency channels are used for the transmission, and the blue dashed curve and the green dotted curve in Fig. 9 illustrate the radiation pattern of the lowest frequency channel (f_1) and the highest frequency channel (f_{13}), respectively. Fig. 9 clearly shows LWA's angular dispersion property: higher frequencies emit towards smaller angles, as we expect.

Yet, unlike the analytical LWA model, the measured LWA radiation pattern in Fig. 9 exhibits irregularities and asymmetry. In particular, the antenna gain declines slower towards the smaller angle compared to the larger angles. As a result, when the transmission band widens equally from the center frequency, Bob receives a stronger signal for the lower frequency channel compared to the higher frequency channels. For the 13-channel transmission towards Bob at $40°$, the normalized antenna gain of the lowest frequency channel f_1 is 0.74 (or -1.3 dB) while the gain of the highest frequency channel f_{13} is only 0.31 (or -5.1 dB). Bob's SNR disadvantage in the higher frequency channels thus yields a larger insecure region expansion compared to the lower frequency channels, despite the fact that ICB allocates a lower per-channel secrecy rate R_k for the higher frequency channel due to its lower communication capacity.

Based on the discussion above, we find that the security performance of ICB is significantly impacted by the asymmetry and irregularities in the radiation pattern. In particular, ICB is sensitive to the lowest SNR at Bob because the frequency channel with the lowest SNR yields the most notable insecure region. When the radiation pattern exhibits asymmetry and irregularities, Bob's SNR is more likely to suffer in at least one frequency channel, which can significantly reduce the security of the transmission when ICB is employed.

Next, we examine the right figure in Fig. 8 when SCADL is employed for the LWA transmission. In the right figure, we observe that SCADL yields the same insecure region as ICB for the single-channel transmission, showing local fluctuations due to beam irregularity. Yet, unlike ICB, when the bandwidth increases, the insecure region remains comparable to the single-channel transmission when SCADL is employed. In addition, the insecure region boundary appears to be smoother with increasing bandwidth.

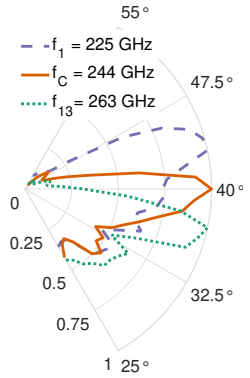

Fig. 9. LWA measured radiation pattern at 3 frequencies: the lowest, center, and highest frequency channel of a 13-channel transmission to Bob at $40°$ with a total bandwidth of 40.7 GHz.

To understand the insecure region behavior, we note that both angular dispersion and beam irregularity result in a non-uniform SNR across the frequency channel for both Bob and Eve, which SCADL exploits for security. For angular dispersion, SCADL exploits the difference between higher and lower frequency so that the insecure region does not expand much despite a widening signal footprint when the bandwidth increases. In terms of beam irregularities, SCADL exploits the fact that a strong side-lobe does not happen at the same angle for all frequency channels. Therefore, the effect of a strong side-lobe in one frequency channel becomes averaged out when more frequency channels are added to the transmission, resulting a smoother insecure region boundary.

From the result in Fig. 8 and the above discussion, we find that employing SCADL for angularly dispersive link can effectively reduce the disadvantage from the widening signal footprint, even under practical beam irregularities.

D. Empirical Link Secrecy Across Angular Locations

In the previous subsection, we investigate the secrecy of a LWA link for Bob at $40°$. Here, we further examine how LWA's link secrecy varies across Bob's angular location using the experimental LWA measurements. As characterized in the analytical model, LWA has a nonlinear frequency-angle dependency which results in different angular dispersion levels when transmitting towards different angular locations, i.e., different angular signal footprint given the same bandwidth. In addition, there can be other angle-dependent beam pattern behaviors in the experimental LWA measurements. Thus, to study the LWA link secrecy dependency on Bob's angle, the same methodology as in Fig. 7 is employed for a set of Bob angles $\theta_B = \{30°, 40°, 50°, 60°\}$ using the LWA measurements.

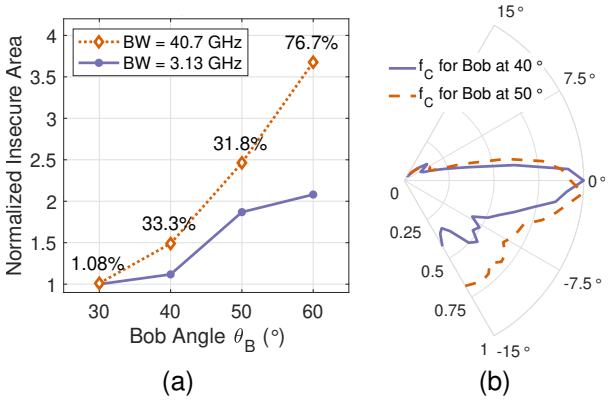

Fig. 10. (a) Insecure area variation with Bob's angle θ_B (reflecting angular dispersion level) when SCADL is employed. The percentage shows the insecure area growth from the single-channel 3.13 GHz transmission. (b) Measured LWA radiation pattern at the center frequencies for Bob at $40°$ and $50°$.

Fig. 10a shows the insecure area of LWA transmissions towards different Bob angular locations when SCADL is employed. As before, the insecure area is normalized to the

single-channel transmission for Bob at 30° to show the scaling. First, we examine the single-channel transmission shown by the solid blue line. We observe that the insecure area for the single-channel transmission varies for different angular locations. In particular, the single-channel insecure area becomes larger towards Bob at a larger angle. This experimental result contrasts to the model-driven result in Fig. 5c which shows a consistent insecure area for single-channel transmission across different Bob angles. While the model-driven radiation pattern illustrates a similar beam pattern for all frequencies (all sinc-like but emitting towards different angles), in the LWA measurements as shown in Fig. 10b, however, we observe more beam irregularities and stronger sidelobes for the lower frequencies which emit towards the smaller angles. Thus, when transmitting using a single frequency channel, the insecure area is larger for Bob at a larger angle according to the LWA measurements.

Next, we examine the LWA transmission with a bandwidth of 40.7 GHz (13 frequency channels), shown by the orange dotted line. We observe that the insecure area is larger when transmitting to Bob at a larger angle given the same transmission bandwidth of 40.7 GHz, which is similar to the observation based on the model-driven approach in Fig. 5c. Yet, when comparing the experimental results (Fig. 10a) to the model-driven results (Fig. 5c), we find that the model-driven approach yields a almost linear increase with Bob's angle, contrasts to an escalating growth observed in the experimental results. Indeed, in the model-driven approach, the larger insecure area for Bob at a larger angle *only* accounts for the wider angular span due to a larger angular dispersive level. In comparison, in the experimental result, the larger insecure area for Bob at a larger angle is due to *both* a wider angular span and a stronger sidelobes, as we observe also for the single-channel transmission, resulting an escalating insecure growth with Bob's angle.

When we examine the insecure area growth percentage compared to the single-channel transmission, as shown by the numbers above the orange diamond markers, we observe a generally larger percentage growth for Bob at a larger angle, matching our observations based on the model-driven approach in Fig. 5c. Yet, due to the beam pattern irregularities in the measured LWA, the insecure area growth percentage is not necessarily larger with a higher angular dispersion level.

From the empirical insecure area results for different Bob angles in Fig. 10a, we conclude that the insecure area of an practical angularly dispersive transmission depends on the angular dispersive level as we learn from the analytical model. Yet, due to beam irregularities in practical antennas, the insecure area may have higher variations compared to the analytical model.

VI. Related Works

Here, we present a survey of the literature on experimental study for directional link and security schemes.

Experimental Study for Directional Link Security: Prior works have experimentally investigate in the security of directional links for mmWave [22], THz [10], and visible light communications [23]. Security of a highly directional link using a large antenna array has also been studied experimentally [24]. These prior works showed potential eavesdropping vulnerabilities despite the highly-directional transmission for a specific frequency channel. In comparison, we study a composite directional link with multiple frequency channels which exhibits an angular dispersion property and results in a unique angular spread in space with increasing bandwidth.

Security of angularly dispersive links was first studied in our prior work [11], which demonstrated unique security properties of angularly dispersive link. Based on the findings, in this work, we further propose to secure the angularly dispersive links using cross-channel coding strategy. Compared to the preliminary conference version of this paper [1] which demonstrated a subset of experimental results for Bob at a fixed angular location, this extended version additionally provides model-driven analysis, explores the interplay of key factors (including the selected secrecy rate, beam directivity, and angular dispersion level), and further experimentally study the link secrecy for Bob at different angular locations.

Eavesdropping Countermeasures for Directional Links: To thwart eavesdropping of directional links, prior works have studied strategies including beamforming [25], generating artificial noise for Eve [26], [27] or transmitting time-modulated signals in a per-symbol basis to scramble the received constellation at Eve [28]–[30]. However, these strategies rely on multiple antennas at the transmitter, which cannot be applied to the single antenna system we study. In contrast, for the single-element LWA link, we leverage the existing secure coding development [12] and propose SCADL which exploits the non-uniform SNR across frequency channels for security.

Cross-Channel Coding: Applying coding across parallel channels is commonly used in wireless networks for reliability purposes, such as countering frequency selective channels for orthogonal frequency-division multiplexing (OFDM) systems [31], [32]. Yet, coding for reliability only considers the Alice-Bob link but not Eve. Cross-channel coding for wireless security was also studied in prior work for fading channels [33]. While prior work focused on temporal characteristics, in this work, we study a system with an unique frequency-dependent spatial domain characteristics.

VII. Conclusions

This paper studies secure transmission strategies on angularly dispersive links. To address the security challenge of widening signal footprint with a larger bandwidth, we propose to frequency channelize the wideband transmission, and perform secure coding across frequency channels based on information theoretic foundations. To demonstrate our idea, we specify a cross-channel coding strategy SCADL, and compare it with a independently coded baseline approach ICB. Using an LWA with the angular dispersion property, we demonstrate both with model-driven approach and experiments that SCADL enables secure wideband angularly dispersive transmissions, even under practical beam asymmetry and irregularities, by exploiting the fact that Eve does not receive all frequency channels equally well. In comparison, the

independently coded per channel strategy ICB exposes the vulnerability of angularly dispersive links since the transmission becomes insecure as long as Eve intercepts some frequency channels well. Further, we examine the interplay between multiple factors, showing that the security degradation due to angular dispersion can be secondary to the selected secrecy rate and radiation beamwidth once SCADL is employed.

ACKNOWLEDGMENTS

This research was partially supported by NSF grant CNS-2148132. CY and EK's research was supported by NSF grants CNS-1955075, CNS-1923782, CNS-1824529, and DOD: Army Research Laboratory grant W911NF-19-2-0269. AC, RD and MM's research was supported by Air Force Contract No. FA8702-15-D-0001, and MIT Portugal Program [Project SNOB-5G with Nr. 045929(CENTRO-01-0247-FEDER-045929)]. DM's research was supported by Air Force Research Laboratory grant FA8750-19-1-0500 and NSF grants NSF-1954780 and NSF-1923782.

REFERENCES

[1] 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 *Proceedings of the 15th ACM Conference on Security and Privacy in Wireless and Mobile Networks (WiSec '22)*, 2022.

[2] W. Malik, D. Edwards, and C. Stevens, "Angular-Spectral Antenna Effects in Ultra-Wideband Communications Links," *IEE Proceedings-Communications*, vol. 153, no. 1, pp. 99–106, 2006.

[3] A. Sutinjo, M. Okoniewski, and R. H. Johnston, "Radiation from Fast and Slow Traveling Waves," *IEEE Antennas and Propagation Magazine*, vol. 50, no. 4, pp. 175–181, 2008.

[4] 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 Photonics*, vol. 9, no. 11, p. 717, 2015.

[5] J. Ma, N. J. Karl, S. Bretin, G. Ducournau, and D. M. Mittleman, "Frequency-Division Multiplexer and Demultiplexer for Terahertz Wireless Links," *Nature Communications*, vol. 8, no. 1, pp. 1–8, 2017.

[6] Y. Ghasempour, C.-Y. Yeh, R. Shrestha, D. M. Mittleman, and E. Knightly, "Single Shot Single Antenna Path Discovery in THz Networks," in *Proceedings of the 26th Annual International Conference on Mobile Computing and Networking*, 2020.

[7] Y. Ghasempour, R. Shrestha, A. Charous, E. Knightly, and D. M. Mittleman, "Single-Shot Link Discovery for Terahertz Wireless Networks," *Nature Communications*, vol. 11, no. 1, pp. 1–6, 2020.

[8] Y. Ghasempour, C.-Y. Yeh, R. Shrestha, Y. Amarasinghe, D. M. Mittleman, and E. W. Knightly, "LeakyTrack: Non-Coherent Single-Antenna Nodal and Environmental Mobility Tracking with a Leaky-Wave Antenna," in *SenSys*, 2020, pp. 56–68.

[9] 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 Journal of Solid-State Circuits*, 2021.

[10] J. Ma, R. Shrestha, J. Adelberg, C.-Y. Yeh, Z. Hossain, E. Knightly, J. M. Jornet, and D. M. Mittleman, "Security and Eavesdropping in Terahertz Wireless Links," *Nature*, vol. 563, no. 7729, pp. 89–93, 2018.

[11] C.-Y. Yeh, Y. Ghasempour, Y. Amarasinghe, D. M. Mittleman, and E. W. Knightly, "Security in Terahertz WLANs with Leaky Wave Antennas," in *Proceedings of the 13th Conference on Security and Privacy in Wireless and Mobile Networks (WiSec '20)*, 2020.

[12] T. Liu, V. Prabhakaran, and S. Vishwanath, "The Secrecy Capacity of a Class of Parallel Gaussian Compound Wiretap Channels," in *2008 IEEE Int. Symp. on Inf. Theory*. IEEE, 2008, pp. 116–120.

[13] C. Caloz, D. R. Jackson, and T. Itoh, "Leaky-Wave Antennas," in *Frontiers in Antennas: Next Generation Design & Engineering*, F. B. Gross, Ed. McGraw Hill Professional, 2011, ch. 9.

[14] M. Bloch and J. Barros, *Physical-Layer Security: From Information Theory to Security Engineering*. Cambridge University Press, 2011.

[15] T. M. Cover and J. A. Thomas, *Elements of Information Theory*. John Wiley & Sons, 2012.

[16] Y. Liang, G. Kramer, H. V. Poor, and S. Shamai, "Compound Wiretap Channels," *EURASIP Journal on Wireless Communications and Networking*, vol. 2009, pp. 1–12, 2009.

[17] 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," *Journal of the Optical Society of America B*, vol. 26, no. 9, pp. A6–A13, 2009.

[18] H. Guerboukha, R. Shrestha, J. Neronha, O. Ryan, M. Hornbuckle, Z. Fang, and D. Mittleman, "Efficient Leaky-Wave Antennas at Terahertz Frequencies Generating Highly Directional Beams," *Applied Physics Letters*, vol. 117, no. 26, p. 261103, 2020.

[19] F. Gross, *Frontiers in Antennas: Next Generation Design & Engineering*. McGraw Hill Professional, 2010.

[20] V. Shahiri, A. Kuhestani, and L. Hanzo, "Short-Packet Amplify-and-Forward Relaying for the Internet-of-Things in the Face of Imperfect Channel Estimation and Hardware Impairments," *IEEE Transactions on Green Communications and Networking*, vol. 6, no. 1, pp. 20–36, 2021.

[21] I. Duling and D. Zimdars, "Revealing Hidden Defects," *Nature Photonics*, vol. 3, no. 11, pp. 630–632, 2009.

[22] D. Steinmetzer, J. Chen, J. Classen, E. Knightly, and M. Hollick, "Eavesdropping with Periscopes: Experimental Security Analysis of Highly Directional Millimeter Waves," in *Proceedings of the 2015 IEEE Conference on Communications and Network Security (CNS)*, 2015.

[23] J. Classen, J. Chen, D. Steinmetzer, M. Hollick, and E. Knightly, "The Spy Next Door: Eavesdropping on High Throughput Visible Light Communications," in *Proceedings of the 2nd International Workshop on Visible Light Communications Systems*, 2015.

[24] C.-Y. Yeh and E. W. Knightly, "Eavesdropping in Massive MIMO: New Vulnerabilities and Countermeasures," *IEEE wireless comm.*, 2021.

[25] E. Yaacoub and M. Al-Husseini, "Achieving Physical Layer Security with Massive MIMO Beamforming," in *2017 11th European conference on antennas and propagation (EUCAP)*. IEEE, 2017, pp. 1753–1757.

[26] N. Anand, S.-J. Lee, and E. W. Knightly, "STROBE: Actively Securing Wireless Communications Using Zero-Forcing Beamforming," in *2012 Proceedings IEEE INFOCOM*. IEEE, 2012, pp. 720–728.

[27] M. Ragheb, S. M. S. Hemami, A. Kuhestani, D. W. K. Ng, and L. Hanzo, "On the Physical Layer Security of Untrusted Millimeter Wave Relaying Networks: A Stochastic Geometry Approach," *IEEE Transactions on Information Forensics and Security*, vol. 17, pp. 53–68, 2021.

[28] N. Valliappan, A. Lozano, and R. W. Heath, "Antenna subset modulation for secure millimeter-wave wireless communication," *IEEE Transactions on communications*, vol. 61, no. 8, pp. 3231–3245, 2013.

[29] K. Sengupta, X. Lu, S. Venkatesh, and B. Tang, "Physically Secure Sub-THz Wireless Links," in *2020 IEEE International Conference on Communications Workshops (ICC Workshops)*. IEEE, 2020, pp. 1–7.

[30] S. Venkatesh, X. Lu, B. Tang, and K. Sengupta, "Secure space-time-modulated millimetre-wave wireless links that are resilient to distributed eavesdropper attacks," *Nature Electronics*, vol. 4, no. 11, pp. 827–836, 2021.

[31] R. D. Wesel and J. M. Cioffi, "Fundamentals of Coding for Broadcast OFDM," in *Conference Record of the Twenty-Ninth Asilomar Conference on Signals, Systems and Computers*, vol. 1. IEEE, 1996, pp. 2–6.

[32] H. Bolcskei, "MIMO-OFDM Wireless Systems: Basics, Perspectives, and Challenges," *IEEE wireless comm.*, vol. 13, no. 4, pp. 31–37, 2006.

[33] M. Baldi, F. Chiaraluce, N. Laurenti, S. Tomasin, and F. Renna, "Secrecy Transmission on Parallel Channels: Theoretical Limits and Performance of Practical Codes," *IEEE Transactions on Information Forensics and Security*, vol. 9, no. 11, pp. 1765–1779, 2014.