Angularly Dispersive Terahertz Links with Secure Coding: From Theoretical Foundations to Experiments

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

Alejandro Cohen
Technion

Rafael G. L. D'Oliveira
MIT

Muriel Médard
MIT

Daniel M. Mittleman
Brown University

Edward W. Knightly
Rice University

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 to channelize the wideband transmission in frequency, and perform secure coding across frequency channels. With 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.

CCS CONCEPTS

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

KEYWORDS

terahertz, angular dispersion, security, experiment

ACM Reference Format:
Chia-Yi Yeh, Alejandro Cohen, Rafael G. L. D'Oliveira, Muriel Médard, Daniel M. Mittleman, and Edward W. Knightly. 2022. 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), May 16–19, 2022, San Antonio, TX, USA.* ACM, New York, NY, USA, 6 pages. https://doi.org/10.1145/3507657.3528553

1 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 [12], and from antenna structures such as the leaky-wave antenna (LWA) [14]. To date, angular dispersion has been shown to enable a novel, yet simple, beam steering mechanism via frequency selection [7, 10]. 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 [3–5, 13].

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 [11], 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 study of secure transmission strategies on angularly dispersive links to address the challenge of securing wideband transmissions with angular dispersion. In particular, we propose to frequency channelize the wideband transmission and perform 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 [15]. 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 [9] 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. While our results are based on LWAs, the findings can be generalized to other angularly dispersive links.

With over-the-air experiments, first, we show that Alice can utilize encoding of her data across different sub-bands to dramatically

Permission to make digital or hard copies of all or part of this work for personal or classroom use is granted without fee provided that copies are not made or distributed for profit or commercial advantage and that copies bear this notice and the full citation on the first page. Copyrights for components of this work owned by others than ACM must be honored. Abstracting with credit is permitted. To copy otherwise, or republish, to post on servers or to redistribute to lists, requires prior specific permission and/or a fee. Request permissions from permissions@acm.org.
WiSec '22, May 16–19, 2022, San Antonio, TX, USA
© 2022 Association for Computing Machinery.
ACM ISBN 978-1-4503-9216-7/22/05…$15.00
https://doi.org/10.1145/3507657.3528553

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 (∼ 30%) under a bandwidth increment of more than 40 GHz, as opposed to more than 190% 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. 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. Moreover, we find that without SCADL, the baseline strategy ICB is significantly impacted by the practical beam asymmetry and irregularities, resulting in an unexpectedly large and asymmetry insecure region.

2 SYSTEM MODEL

2.1 Angularly Dispersive 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 [15] is employed for THz directional transmission. We denote the known frequency-dependent emission angle relationship by $\theta_{max}(f)$, and the electric field generated by the LWA by $G(f, \theta)$, both can be obtained before the deployment using an analytical model [6, 14] or via over-the-air measurements.

Assuming a transmitter Alice knows the location of a static user Bob, in the line-of-sight (LoS) scenario, Alice employs the LWA described above to transmit to 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 $k \in \{1, \cdots, K\}$.

2.2 Threat Model

In this work, we study how Alice can leverage coding to secure the angularly dispersive links against a potential eavesdropper Eve. To this end, we model Eve's interception as a function of her location and define link secrecy for a given encoding process by the protected spatial region.

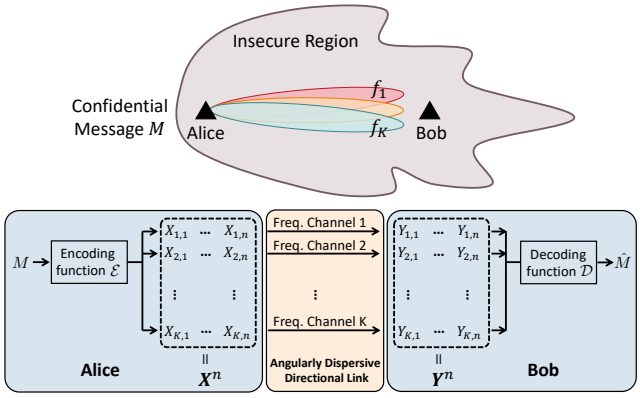


Figure 1: Wideband angularly dispersive link channelized into K frequency channels.

2.2.1 LWA Wiretap Channel Model. Using a LWA, a transmitter Alice wants to transmit a confidential message M, which can be either in plaintext or ciphertext, 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.

We model the LWA link eavesdropping scenario as K parallel additive white Gaussian noise (AWGN) wiretap channels. 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 $n_{E,k}$):

$$y_k = h_{B,k}\, x_k + n_{B,k} \quad \text{and} \quad z_k = h_{E,k}\, x_k + n_{E,k}. \tag{1}$$

The noise at Bob and Eve, $n_{B,k}$ and $n_{E,k}$, are assumed to be independent, with zero mean and the same 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 $k \in \{1, \cdots, K\}$. The SNR at Bob and Eve depends on the signal attenuation they experience, which is frequency and location dependent for the LWA link:

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

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

2.2.2 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. 1, 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 $\mathbf{X}^n$ to an estimated message $\hat{M}$.

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

$$\lim_{n\to\infty} \mathbb{P}(M \neq \hat{M}) = 0 \text{ (reliability);} \tag{3}$$

$$\lim_{n\to\infty} \frac{1}{n} I(M; \mathbf{Z}^n) = 0 \text{ (secrecy),} \tag{4}$$

where $\mathbb{P}$ represents probability and I denotes mutual information. Note that Eq. (4) follows the weak secrecy defined in the literature [1], 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. (3). 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. (2).

2.2.3 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. (4) is satisfied:

$$\mathcal{R}_{\text{sec}} = \left\{ (d_E, \theta_E) \mid \lim_{n\to\infty} \frac{1}{n} I(M; \mathbf{Z}^n) = 0 \right\}. \tag{5}$$

The rest of the Eve locations forms the insecure region, $\mathcal{R}_{\text{ins}} = \mathcal{R}^c_{\text{sec}}$. In addition to examining the secure regions, we also quantify the security level of the angularly dispersive link by secrecy outage in the spatial domain by insecure area:

$$\mathcal{A}_{\text{ins}} = \text{area}(\mathcal{R}_{\text{ins}}). \tag{6}$$

3 SECURE CODING

To secure the angularly dispersive LWA link as defined in Sec. 2, 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 [15]. 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 [9]. 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. In this paper, we conjecture that the results in the noise-based prior works [8, 9] can be generalized to our signal-strength-based model, and leave the proof for future.

3.1 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:

$$\mathcal{R}^{\text{Joint}}_{\text{sec}} = \left\{ j \mid R \le R^{\text{Joint}}_S(j) \right\} \text{ and } \mathcal{R}^{\text{Joint}}_{\text{ins}} = \left\{ j \mid R > R^{\text{Joint}}_S(j) \right\}, \tag{7}$$

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

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. (7) 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. (7) and is adapted from [9] based on Gaussain codebooks for a transmission with secrecy rate R.

Codebook generation. Randomly and independently generate K Gaussian codebooks $C_k, k = \{1, \cdots, K\}$. The Gaussian codebook 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 $C = C_1 \times \cdots \times C_K$ into 2^{nR} bins.

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

Decoding at the legitimate receiver. By construction, with high probability all K codebooks $C_1, \cdots, C_K$ 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.

3.2 ICB

As a baseline to the proposed cross-channel coding strategy, we specify ICB that must code each frequency channel independently. 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:

$$\mathcal{R}^{\text{Ind}}_{\text{sec},k} = \left\{ j \mid R_k \le R^{\text{Ind}}_{S,k}(j) \right\} \text{ and } \mathcal{R}^{\text{Ind}}_{\text{ins},k} = \left\{ j \mid R_k > R^{\text{Ind}}_{S,k}(j) \right\}, \quad (8)$$

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

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 $\mathcal{R}^{\text{Ind}}_{\text{ins}}$:

$$\mathcal{R}^{\text{Ind}}_{\text{sec}} = \bigcap_{k=1}^{K} \mathcal{R}^{\text{Ind}}_{\text{sec},k} \quad \text{and} \quad \mathcal{R}^{\text{Ind}}_{\text{ins}} = \bigcup_{k=1}^{K} \mathcal{R}^{\text{Ind}}_{\text{ins},k}. \quad (9)$$

Eq. (9) 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. (9). Similar to SCADL, ICB is also based on Gaussian codebooks and is adapted from [9]. 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 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 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 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 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. 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.

4 OVER THE AIR EXPERIMENTS

4.1 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 and are separated by 0.95 mm. We create a slot on one of the plate, with a slot length of 3 cm and a slot width of 1 mm.

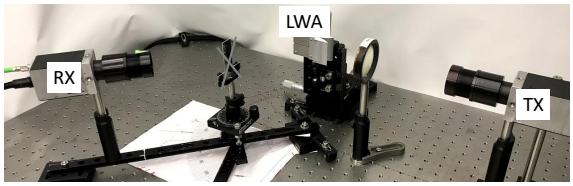


Figure 2: Experiment setup.

To measure the radiation pattern of the LWA, we use T-Ray 4000 TD-THz System [2] for generating and receiving THz signals. Fig. 2 demonstrates the experiment setup. During the measurement, the transmitter couples the THz pulse into the LWA, with frequency components span from below 150GHz to above 1.5 THz. 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. With a sampling rate of 12.8 THz (1 sample every 78 femtoseconds) and 4096 time-domain samples, the detector can measure the THz signals with a frequency resolution of 3.13 GHz. We place the receiver at $12^\circ < \theta < 80^\circ$ with 1° resolution in the measurement. For each frequency component, the measurements over angular locations describe the radiation pattern, and thus we obtain a real-world LWA radiation pattern.

In the following, we consider Alice employs a uniform power per frequency channel, and the resulting SNR at Bob and Eve in each frequency channel follows Eq. (2). Alice's transmit power is chosen to yield an SNR of 25 dB at Bob for the center frequency channel. In addition, we define the normalized secrecy rate $0 < \eta < 1$ as the ratio between the total secrecy rate R and Bob's total achievable communication rate R^*_B, $\eta = R/R^*_B$, to normalize the effect of increasing bandwidth. 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 $R_k = \eta R^*_{B,k}$. In the following, we arbitrarily choose $\eta = 0.2$ in the evaluation.

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. 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.

4.2 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 $\theta_B = 40^\circ$ and a distance

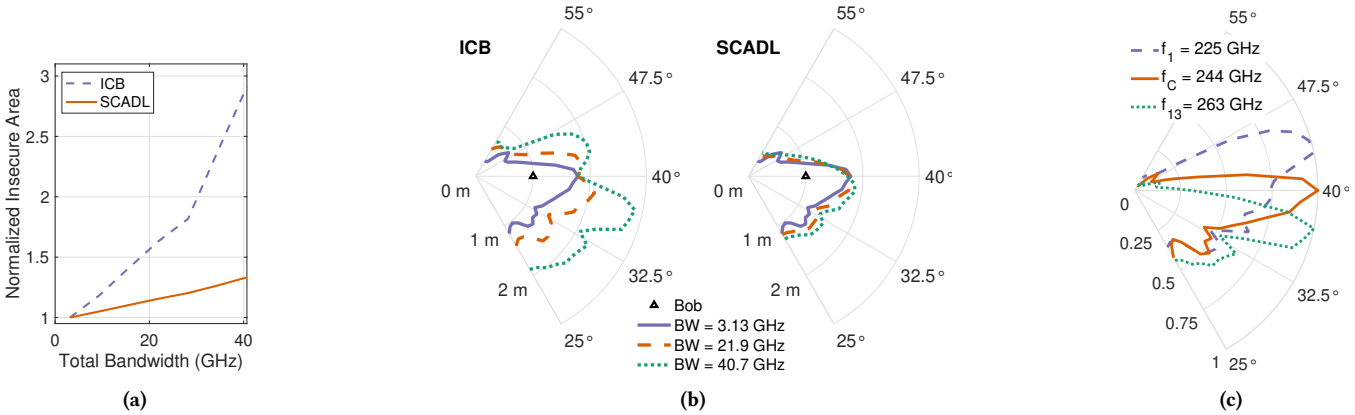


Figure 3: (a) Insecure area scaling with transmission bandwidth when SCADL and ICB are employed, with a normalized secrecy rate $\eta = 0.2$ for Bob at 40°. (b) Boundary of insecure regions when the total transmission bandwidth scales from 3.13 GHz to 40.7 GHz, with a normalized secrecy rate $\eta = 0.2$ for Bob at 40°. (c) 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.

of $d_B = 1$ m. Fig. 3a 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. To show the scaling, the insecure area is normalized to the single-channel transmission scenario, as SCADL and ICB converge to the same strategy for the single-channel scenario.

From Fig. 3a, we observe that when the independently coded baseline strategy ICB is employed (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. 3a clearly 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.

4.3 Empirical Insecure Region Characterization

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

Fig. 3b shows the spatial region near Bob in the polar coordinate. The origin represents Alice's location, the black triangle represent Bob at $\theta_B = 40^\circ$ 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. 3b 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), interestingly, 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. To understand the insecure region expansion, recall that when employing ICB, the transmission is secure only when all sub-messages 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. (9). 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. 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. 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.

In addition, 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 ($\theta > 40^\circ$).

To understand the uneven insecure region expansion when employing the independently-coded strategy ICB, we examine the measured LWA beam pattern. Fig. 3c illustrates the measured LWA radiation pattern for the center (f_C, red solid curve), the lowest (f_1, blue dashed curve) and the highest frequency channel (f_{13},

green dotted curve), when 13 frequency channels are used for the transmission (total bandwidth of 40.7 GHz).

Fig. 3c clearly shows LWA's angular dispersion property: higher frequencies emit towards smaller angles, as we expect. However, the measured LWA radiation pattern 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 than the lower frequency channels.

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. 3b when SCADL is employed for the LWA transmission. 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.

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. 3b 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.

5 CONCLUSIONS

This paper presents the first study of 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 experimentally demonstrate 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.

ACKNOWLEDGMENTS

CY and EK's research was supported by Cisco, Intel, NSF grants CNS-1955075, CNS-1923782, CNS-1824529, CNS-1801857, and DOD: Army Research Laboratory grant W911NF-19-2-0269. RD's research was supported by Portuguese Science and Technology Foundation grant MPP2030 and Lincoln Laboratory. DM's research was supported by Air Force Research Laboratory grant FA8750-19-1-0500 and NSF grant NSF-1954780 and NSF-1923782.

REFERENCES

[1] Matthieu Bloch and Joao Barros. 2011. *Physical-Layer Security: From Information Theory to Security Engineering.* Cambridge University Press.
[2] Irl Duling and David Zimdars. 2009. Revealing Hidden Defects. *Nature Photonics* 3, 11 (2009), 630–632.
[3] 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.
[4] Yasaman Ghasempour, Chia-Yi Yeh, Rabi Shrestha, Yasith Amarasinghe, Daniel M Mittleman, and Edward W Knightly. 2020. LeakyTrack: Non-Coherent Single-Antenna Nodal and Environmental Mobility Tracking with a Leaky-Wave Antenna. In *SenSys*. 56–68.
[5] 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*.
[6] Frank Gross. 2010. *Frontiers in Antennas: Next Generation Design & Engineering.* McGraw Hill Professional.
[7] 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.
[8] Yingbin Liang, Gerhard Kramer, H Vincent Poor, and Shlomo Shamai. 2009. Compound Wiretap Channels. *EURASIP Journal on Wireless Communications and Networking* 2009 (2009), 1–12.
[9] Tie Liu, Vinod Prabhakaran, and Sriram Vishwanath. 2008. The Secrecy Capacity of a Class of Parallel Gaussian Compound Wiretap Channels. In *2008 IEEE International Symposium on Information Theory*. IEEE, 116–120.
[10] 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.
[11] 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.
[12] WQ Malik, DJ Edwards, and CJ Stevens. 2006. Angular-Spectral Antenna Effects in Ultra-Wideband Communications Links. *IEE Proceedings-Communications* 153, 1 (2006), 99–106.
[13] Hooman Saeidi, Suresh Venkatesh, Xuyang Lu, and Kaushik Sengupta. 2021. 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).
[14] 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.
[15] Chia-Yi Yeh, Yasaman Ghasempour, Yasith Amarasinghe, Daniel M. Mittleman, and Edward W. Knightly. 2020. 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).*