Physical Layer Defense against Eavesdropping Attacks on Low-Resolution Phased Arrays

Patel, Kartik ; Myers, N.J.; Heath, Robert W.

DOI
10.1109/ICC45855.2022.9838571

Publication date
2022

Document Version
Final published version

Published in
Proceedings European Control Conference (ECC) 2022

Physical Layer Defense against Eavesdropping Attacks on Low-Resolution Phased Arrays

Kartik Patel[†], Nitin Jonathan Myers[*], and Robert W. Heath Jr.[‡]
[†]Wireless Networking and Communications Group, The University of Texas at Austin, Austin, USA
[*]Delft Center for Systems and Control, Delft University of Technology, Delft, Netherlands
[‡] Department of Electrical and Computer Engineering, North Carolina State University, Rayleigh, USA
Email: kartikpatel@utexas.edu, N.J.Myers@tudelft.nl, rwheathjr@ncsu.edu

ICC 2022 - IEEE International Conference on Communications | 978-1-5386-8347-7/22/$31.00 ©2022 IEEE | DOI: 10.1109/ICC45855.2022.9838571

***Abstract*—Eavesdropping attacks are a severe threat to millimeter-wave (mmWave) networks that use low-resolution phased arrays. Although directional beamforming in mmWave phased arrays provides natural defense against eavesdropping, the use of low-resolution phase shifters induces energy leakage into unintended directions. This energy leakage can be exploited by the adversaries. In this paper, we propose a directional modulation (DM)-based defense against eavesdropping attacks on low-resolution phased arrays. Our defense technique applies random circulant shifts to the beamformer for every symbol transmission. By appropriately adjusting the phase of the transmitted symbol, the transmitter (TX) can maintain a high-quality link with the receiver while corrupting the symbols transmitted along unintended directions. We theoretically analyze the secrecy mutual information (SMI) achieved by the proposed defense mechanism and show that our defense induces artificial phase noise (APN) along unintended directions, which increases the SMI of the system. Finally, we numerically show the superiority of the proposed defense technique over the state-of-the-art defense techniques.**

I. Introduction

MmWave technology, currently deployed in 5G networks, is prone to eavesdropping attacks even with beamforming. Although directional beamforming used in mmWave communication concentrates the transmitted radio frequency (RF) signals towards the intended receiver (RX) and reduces the signals transmitted along *unintended directions* [1], the beams with practical mmWave hardware are far from directional due to two reasons. First, commodity mmWave radios use phased arrays to avoid the high power consumption with fully digital arrays [2]. Second, radios use low-resolution phase shifters which reduces the hardware complexity at mmWave frequencies [3]. The imperfections in the beam patterns result in leakage of the RF signal along unintended directions, which can be exploited by the eavesdropper [4]–[6].

Prior work has developed defense techniques for secure mmWave communication. One approach is to limit the energy leakage along the directions of the eavesdropper [4], [7]. An alternative approach is to transmit artificial noise (AN) along the unintended directions [8], [9]. Unfortunately, these AN-based methods also degrade the received signal power at the intended RX. A different approach to achieve secure mmWave communication is using DM. DM-based methods modify the beamformer at each symbol such that the constellation is maintained along the intended direction and distorted along other directions [10]–[13]. For example, the Antenna Subset Modulation (ASM) technique proposed in [10] is a DM-based method which uses randomized antenna switching to change the beamformer at each symbol. These DM-based methods, however, reduce the mainlobe gain under the per-antenna power constraint, thereby reducing the received power at the RX. Moreover, these methods do not provide adequate defense when using low-resolution phased arrays.

In this paper, we propose a novel DM-based defense technique that achieves high secrecy, even with low-resolution phased arrays, without impacting communication with the RX. We summarize our contributions below:

- We propose a DM-based defense method that circularly shifts the beamformer and adjusts the phase of the transmitted symbol. We show that our method distorts the symbols received along unintended directions.
- We provide an analytical expression of SMI along on-grid directions. Our analysis indicates that eavesdroppers cannot decode transmitted symbols even under the leakage effect with low-resolution phased arrays.
- We numerically study SMI with the proposed defense technique and discuss the benefits of using the proposed scheme over benchmarks from [10] and [11].

Notation: a is a scalar and $\mathbf{a}$ is a vector. $[\mathbf{a}]_k$ is the k^{th} entry of $\mathbf{a}$. The transpose and the conjugate-transpose of $\mathbf{a}$ are $\mathbf{a}^{\mathrm{T}}$ and $\mathbf{a}^*$. $|a|$ and $\measuredangle a$ denote the magnitude and the phase of a. $(b)_{\%N}$ denotes the modulo-N of an integer b. $\mathcal{CN}(\mu, \sigma^2)$ represents a circularly symmetric complex Gaussian random variable with mean μ and variance σ^2. $\mathrm{j} = \sqrt{-1}$. $[N]$ denotes the set $\{0, 1, ..., N-1\}$.

II. System Model

We consider an mmWave system in which the TX is equipped with a uniform linear array of N_{T} antennas. Each transmit antenna is associated with a phase shifter of q-bit resolution. In practice, $1 \leq q \leq 3$ to limit the hardware complexity [3], [14]. We consider a narrowband setup and assume

This material is based upon work supported in part by the National Science Foundation under the grant number CNS-1731658, by the Army Research Office under grant W911NF1910221 and by the Idaho National Labs.

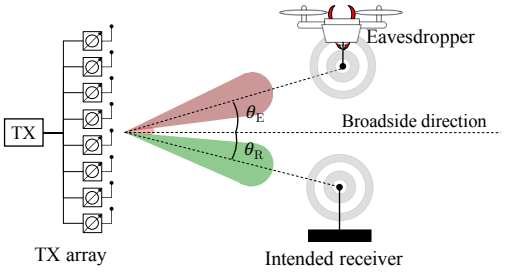

Fig. 1. A low-resolution phased array results in leakage of RF signals which can be exploited by an eavesdropper. The angle-of-departure of the dominant paths associated with the RX and the eavesdropper are θ_{R} and θ_{E}. This figure illustrates a line-of-sight scenario where the TX uses 1-bit phase shifters.

a single antenna RX. We also assume that the eavesdropper has a signal antenna.

A. Channel and signal model

We assume an half-wavelength spaced array at the TX and define the TX array response vector

$$\mathbf{a}(\theta) = \left[1, e^{-\mathrm{j}\pi \sin\theta}, \ldots, e^{-\mathrm{j}(N_{\mathrm{T}}-1)\pi \sin\theta}\right]^{\mathrm{T}}. \tag{1}$$

We consider a ray-based channel with L_{R} rays to model the propagation environment between the TX and the RX. We use $\alpha_{\mathrm{R},\ell}$ and $\theta_{\mathrm{R},\ell}$ to denote the complex gain and the angle of departure (AoD) of the ℓ-th path. The mmWave channel between the TX and the RX is then

$$\mathbf{h}_{\mathrm{R}} = \sum_{\ell=1}^{L_{\mathrm{R}}} \alpha_{\mathrm{R},\ell} \mathbf{a}^{\mathrm{T}}(\theta_{\mathrm{R},\ell}). \tag{2}$$

The channel $\mathbf{h}_{\mathrm{E}}$ between the TX and the eavesdropper is similarly defined using the parameters L_{E}, $\alpha_{\mathrm{E},\ell}$, and $\theta_{\mathrm{E},\ell}$ as

$$\mathbf{h}_{\mathrm{E}} = \sum_{i=1}^{L_{\mathrm{E}}} \alpha_{\mathrm{E},\ell} \mathbf{a}^{\mathrm{T}}(\theta_{\mathrm{E},\ell}). \tag{3}$$

The on-grid directions associated with the TX array are the θs for which $\mathbf{a}(\theta)$ is a column of the $N_{\mathrm{T}} \times N_{\mathrm{T}}$ discrete Fourier transform (DFT) matrix.

We use x_k to denote the k^{th} symbol transmitted by the TX such that $\mathbb{E}[|x_k|^2] = 1$. The TX applies a beamformer $\mathbf{f}_k$ to its phased array to transmit x_k. The phase of the entries in $\mathbf{f}_k$ can only take finite values from the set $\mathcal{B}_q = \left\{\frac{2\pi i}{2^q} : i \in [2^q]\right\}$. The signal received by the RX is then

$$y_{\mathrm{R},k} = \mathbf{h}_{\mathrm{R}} \mathbf{f}_k x_k + n_{\mathrm{R},k}, \tag{4}$$

where $n_{\mathrm{R},k} \sim \mathcal{CN}(0, \sigma^2)$ is independent and identically distributed (IID) noise. Similarly, the signal received at the eavesdropper for the k^{th} symbol transmission is

$$y_{\mathrm{E},k} = \mathbf{h}_{\mathrm{E}} \mathbf{f}_k x_k + n_{\mathrm{E},k}, \tag{5}$$

where $n_{\mathrm{E},k} \sim \mathcal{CN}(0, \sigma^2)$ is IID noise at the eavesdropper. Conventional beamforming techniques, which are agnostic to the eavesdropper, select a beamformer $\mathbf{f}_k$ from a codebook that maximizes $|\mathbf{h}_{\mathrm{R}} \mathbf{f}_k|^2$, i.e., the power received at the RX. However, not all beamformers can be applied in low-resolution analog antenna arrays. In the following section, we discuss practical beamformers for low-resolution phased arrays.

B. Practical beamformer design

We define a q-bit quantization function that rounds the phase to nearest value in set $\mathcal{B}_q$, i.e. $Q_q(x) = \arg\min_{\beta \in \mathcal{B}_q} |x - \beta|$. The q-bit phase quantized version of a beamformer $\mathbf{f}$ is

$$\left[\tilde{\mathbf{f}}\right]_i = \frac{1}{\sqrt{N_{\mathrm{T}}}} \exp\left(\mathrm{j} Q_q\left(\measuredangle [\mathbf{f}]_i\right)\right). \tag{6}$$

This approach of rounding the phase to the nearest value from the set $\mathcal{B}_q$ allows implementing a feasible beamformer in a q-bit phased array. The q-bit phase quantization of $\mathbf{f}$, however, introduces imperfections in the generated beam pattern. These imperfections introduce energy leakage in directions other than the direction of the RX, which makes the mmWave system susceptible to eavesdropping. For instance, the energy leaked along an unintended direction can be as high as the main lobe energy with one-bit phased arrays [15], [16]. Under such strong leakage, standard defense mechanisms that induce AN along the unintended directions do not suffice. Therefore, there is a need to develop new physical layer defense methods for secure communication with low-resolution phased arrays.

III. Circulant Shift-based beamforming

In this section, we first define the quantized DFT codebook and then describe our circulant shift-based beamforming (CSB) defense against eavesdropping attacks. Then, we analyze the statistics of the APN induced by CSB defense and derive the SMI with this approach.

A. DFT codebook and notation

The quantized DFT codebook is defined as

$$\tilde{\mathcal{F}} = \left\{\tilde{\mathbf{f}}_j : [\tilde{\mathbf{f}}_j]_i = \frac{1}{\sqrt{N_{\mathrm{T}}}} e^{\mathrm{j} Q_q\left(\frac{2\pi ij}{N_{\mathrm{T}}}\right)}, \forall i, j \in [N_{\mathrm{T}}]\right\}. \tag{7}$$

Our defense mechanism is applied on top of this quantized DFT codebook used for beamforming with low-resolution phased arrays.

To describe CSB defense, we first consider a single ray channel model for both the RX and the eavesdropper. We later discuss how our defense performs in a multi-path scenario in Sec. III-E. We define θ_{R} as the AoD of the ray to the RX and θ_{E} as the AoD of the ray to the eavesdropper. Under the single ray assumption, the TX-RX channel and the TX-eavesdropper channel are

$$\mathbf{h}_{\mathrm{R}} = \alpha_{\mathrm{R}} \mathbf{a}^{\mathrm{T}}(\theta_{\mathrm{R}}) \text{ and } \mathbf{h}_{\mathrm{E}} = \alpha_{\mathrm{E}} \mathbf{a}^{\mathrm{T}}(\theta_{\mathrm{E}}).$$

In our analysis, we assume that θ_{R} and θ_{E} are on-grid, i.e., $\frac{N_{\mathrm{T}}}{2} \sin\theta_{\mathrm{R}} = i_{\mathrm{R}}$ and $\frac{N_{\mathrm{T}}}{2} \sin\theta_{\mathrm{E}} = i_{\mathrm{E}}$ for some integers i_{R} and i_{E}. In our simulations, we evaluate CSB defense for a more realistic multi-path scenario where the AoDs can be off-grid.

B. Circulantly shifting a beamformer in CSB

The key idea behind our CSB technique is to apply circulant shifts of the quantized DFT beamformer to the phased array. We show that circularly shifting a beamformer at the TX affects the phase of the received signal differently along distinct directions in Lemma 1.

We define the circulant shift operator $\mathcal{P}_c$ which circularly shifts the input vector by c steps. Specifically, for an N_{T}-dimensional vector $\mathbf{a}$, $[\mathcal{P}_c(\mathbf{a})]_i = [\mathbf{a}]_{(i-c)_{\%N_{\mathrm{T}}}}$.

Lemma 1. *Let the AoD associated with the radio (RX or eavesdropper) be θ, such that $\frac{N_{\mathrm{T}}}{2}\sin\theta = i$. If $\tilde{\mathbf{f}} \in \tilde{\mathcal{F}}$, then for any integer pair $c \in [N_{\mathrm{T}}]$,*

$$\mathbf{a}^{\mathrm{T}}(\theta)\mathcal{P}_c(\tilde{\mathbf{f}}) = \mathbf{a}^{\mathrm{T}}(\theta)\tilde{\mathbf{f}}e^{-\mathrm{j}\frac{2\pi}{N_{\mathrm{T}}}ci} \tag{8}$$

Proof. We note that circularly shifting an N_{T} length vector by c-steps results in the element-wise multiplication of its DFT with $[1, e^{-\mathrm{j}\frac{2\pi c}{N_{\mathrm{T}}}}, e^{-\mathrm{j}\frac{4\pi c}{N_{\mathrm{T}}}}, \cdots, e^{-\mathrm{j}\frac{2\pi(N_{\mathrm{T}}-1)c}{N_{\mathrm{T}}}}]$. For an on-grid AoD θ, we observe that $\mathbf{a}^{\mathrm{T}}(\theta)\tilde{\mathbf{f}}$ and $\mathbf{a}^{\mathrm{T}}(\theta)\mathcal{P}_c(\tilde{\mathbf{f}})$ are the i^{th} entries of the DFT of $\tilde{\mathbf{f}}$ and $\mathcal{P}_c(\tilde{\mathbf{f}})$. We put these observations together to arrive at (8). □

From (8), we first observe that receivers at different angular coordinates θs, equivalently different is, observe different phase changes when circularly shifting the transmit beamformer. Therefore, the phase changes induced by circulantly shifting $\tilde{\mathbf{f}}$ are different at the RX and the eavesdropper, when the AoDs associated with their dominant paths are different. Second, we notice that N_{T} distinct circulant shifts can be applied at the TX for every standard beamformer $\tilde{\mathbf{f}}$. As a result, the phase at the eavesdropper can be randomized by choosing the applied circulant shift at random from $[N_{\mathrm{T}}]$. These properties form the crux of our CSB-based defense.

C. CSB-based defense

In our CSB-based defense technique, the TX circularly shifts the beamformer $\tilde{\mathbf{f}}$ by a uniform random integer in $[N_{\mathrm{T}}]$ for every transmitted symbol. The circulant shift chosen for the k^{th} symbol is defined as c_k. Then, the TX computes the phase change induced at the RX by circulantly shifting the beamformer. From (8), we observe that the received symbol gets multiplied with $\exp\left(-\mathrm{j}\frac{2\pi}{N_{\mathrm{T}}}c_k i_{\mathrm{R}}\right)$ due to the phase change, where $i_{\mathrm{R}} = N_{\mathrm{T}}\sin\theta_{\mathrm{R}}/2$. To compensate for this phase change, the TX transmits the phase adjusted symbol $x'_k = x_k \exp\left(\mathrm{j}\frac{2\pi}{N_{\mathrm{T}}}c_k i_{\mathrm{R}}\right)$ using the beamformer $\mathcal{P}_{c_k}(\tilde{\mathbf{f}})$. With this approach, we notice that the RX receives

$$y_{\mathrm{R},k} = \mathbf{h}_{\mathrm{R}}\mathcal{P}_{c_k}(\tilde{\mathbf{f}})x'_k + n_{\mathrm{R},k} \overset{(a)}{=} \alpha_{\mathrm{R}}\mathbf{a}^{\mathrm{T}}(\theta_{\mathrm{R}})\tilde{\mathbf{f}}x_k + n_{\mathrm{R},k}, \tag{9}$$

where (a) follows from (8). The symbol received by the RX is same as that obtained when the TX sends x_k using the beamformer $\tilde{\mathbf{f}}$.

We now show how that phase at the eavesdropper is random with CSB. When the eavesdropper is along an on-grid direction, i.e., $N_{\mathrm{T}}\sin\theta_{\mathrm{E}}/2 = i_{\mathrm{E}}$, the signal received by the eavesdropper with CSB can be written as

$$y_{\mathrm{E},k} = \mathbf{h}_{\mathrm{E}}\mathcal{P}_{c_k}(\tilde{\mathbf{f}})x'_k + n_{\mathrm{E},k} \tag{10}$$

$$= \alpha_{\mathrm{E}}\mathbf{a}^{\mathrm{T}}(\theta_{\mathrm{E}})\tilde{\mathbf{f}}x_k e^{\mathrm{j}\frac{2\pi c_k(i_{\mathrm{R}}-i_{\mathrm{E}})}{N_{\mathrm{T}}}} + n_{\mathrm{E},k}. \tag{11}$$

As the AoDs associated with the RX and the eavesdropper are assumed to be different, $i_{\mathrm{R}} \neq i_{\mathrm{E}}$. As a result, we observe from (11) that the phase of the symbol received by the eavesdropper is random when c_k is chosen at random. Due to randomness in the applied circulant shift, the eavesdropper cannot predict the phase error induced by CSB even with perfect information about the beamformer $\tilde{\mathbf{f}}$ and the AoD associated with the RX.

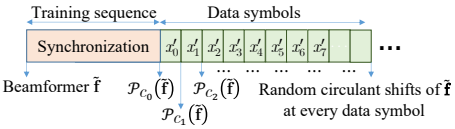

Fig. 2. In an IEEE 802.11ad system, CSB defense applies random circulant shifts of the beamformer $\tilde{\mathbf{f}}$ at every data symbol transmitted within the packet.

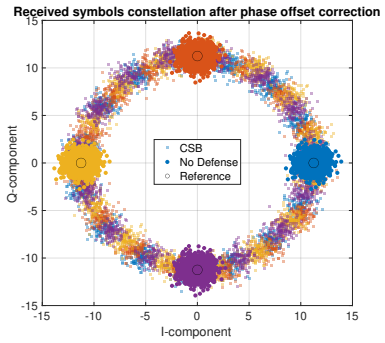

Fig. 3. Phase perturbed constellation at the eavesdropper due to APN induced by CSB defense. Proposed CSB defense applies random circulant shifts of the beamformer to induce APN along unintended directions.

In an IEEE 802.11ad system, a packet is transmitted using a particular beamformer. With CSB, this beamformer is circulantly shifted at random to transmit each symbol within the packet (see Fig. 2). The random phase shifts induced by CSB at the eavesdropper make symbol detection hard even after successful channel estimation. An example of the received constellation at the eavesdropper with the CSB technique is shown in Fig. 3. Our technique assumes that the switching time between the beamformers is negligible to ignore the phase shift induced by the oscillator phase noise. Our assumption is reasonable as the oscillator phase noise standard deviation at 28 GHz [17] is just 1.37^o for the beam switching time of 4 ns reported in [18].

The derivations in (9) and (11) assume that the eavesdropper and the RX are along on-grid directions. In Section IV, we show using simulations that our CSB technique performs well even when the on-grid conditions are not satisfied.

D. Statistical analysis of CSB and SMI

We analyze the phase perturbation induced by CSB, called APN, at the eavesdropper and derive the achievable SMI. We define $\Delta i = i_{\mathrm{R}} - i_{\mathrm{E}}$ as the difference in the on-grid indices of the AoDs associated with the RX and the eavesdropper. The error in the phase of the received symbols at the eavesdropper, i.e. the APN, can be expressed using (11) as $\Delta\Phi_k = \frac{2\pi}{N_{\mathrm{T}}}(c_k\Delta i)_{\%N_{\mathrm{T}}}$. In Lemma 2, we derive the statistics of this APN induced at the eavesdropper. In this derivation, we avoid the subscript k associated with the symbol index, for simplicity of notation.

Lemma 2. *Consider a uniformly distributed random variable C, distributed over $\Omega = [N_{\mathrm{T}}]$. We define $\Delta\Phi = \frac{2\pi}{N_{\mathrm{T}}}(C\Delta i)_{\%N_{\mathrm{T}}}$,*

$$\Omega_{\Phi_{\Delta i}} = \left\{ \frac{2\pi\,(p\Delta i)_{\%N_{\mathrm{T}}}}{N_{\mathrm{T}}} : \forall p \in \left[\frac{N_{\mathrm{T}}}{\gcd(\Delta i, N_{\mathrm{T}})} \right] \right\}. \quad (12)$$

Then,

$$\mathbb{P}(\Delta\Phi = \phi) = \begin{cases} \frac{\gcd(\Delta i, N_{\mathrm{T}})}{N_{\mathrm{T}}}, & \phi \in \Omega_{\Phi_{\Delta i}} \\ 0, & \text{otherwise} \end{cases}. \quad (13)$$

Proof. See Appendix A. □

Lemma 2 shows that the APN induced by CSB defense is uniformly distributed over $\Omega_{\Phi_{\Delta i}}$. With this result, we show in Lemma 3 that the APN introduced by CSB defense renders the eavesdropper unable to infer the transmitted symbol from the phase-corrupted received symbol.

Lemma 3. *Consider an M-PSK constellation with symbol set $\mathcal{M}$. We define partitions of $\mathcal{M}$ such that each partition contains $\gcd(|\Omega_{\Phi_{\Delta i}}|, M)$ number of symbols spaced uniformly in phase. The eavesdropper cannot distinguish between the symbols within a partition due to the APN induced by CSB defense. Additionally, there are $M/\gcd(|\Omega_{\Phi_{\Delta i}}|, M)$ number of symbols that can be accurately distinguished.*

Proof. See Appendix B. □

Example 1. *Consider a TX with $N_{\mathrm{T}} = 16$ that uses a QPSK constellation. In the high SNR regime at the eavesdropper, the mutual information transfer to the eavesdropper is $\log_2(4/\gcd(|\Omega_{\Phi_{\Delta i}}|, 4))$ bits/symbol. Thus, the mutual information is 0 bit/symbol when $\Delta i \notin \{0, 8\}$, and is 1 bit/symbol when $\Delta i = 8$. With CSB, the eavesdropper does not receive any useful information unless it is along the on-grid directions corresponding to $\Delta i = 0$ or 8.*

We now use Lemma 3 to derive the SMI achievable with CSB defense by considering an M-PSK constellation. The SMI, measured in bits/symbol, is defined as the difference between the information transferred over the TX-RX channel and the TX-eavesdropper channel. We denote the mutual information (MI) of the TX-RX channel by $\mathcal{I}_{\mathrm{R}}$ and MI of the TX-eavesdropper channel by $\mathcal{I}_{\mathrm{E}}$. Thus, we can define the SMI C_{S} as $C_{\mathrm{S}} = \max\{\mathbb{E}\left[\mathcal{I}_{\mathrm{R}} - \mathcal{I}_{\mathrm{E}}\right], 0\}$. We define $\mathcal{I}(\rho, M)$, measured in bits per symbol, as the spectral efficiency of the channel with SNR ρ and the input M-PSK constellation [19]. Then from Lemma 3, communication over CSB-secured TX-eavesdropper channel using M-PSK modulation is equivalent to communication over the unsecured TX-eavesdropper channel using $M/\gcd(\Delta i_k, M)$-PSK constellation. Thus, when the TX uses the beamformer $\tilde{\mathbf{f}}_k$, the SMI of CSB-secured communication system is

$$C_{\mathrm{S}} = \max\left\{ \mathbb{E}\left[\mathcal{I}\left(\frac{1}{\sigma^2}\left|\mathbf{h}_{\mathrm{R}}\tilde{\mathbf{f}}_k\right|^2, M \right) - \mathcal{I}\left(\frac{1}{\sigma^2}\left|\mathbf{h}_{\mathrm{E}}\tilde{\mathbf{f}}_k\right|^2, \frac{M}{\gcd(|\Omega_{\Phi_{\Delta i}}|, M)} \right) \right], 0 \right\}. \quad (14)$$

Without CSB defense, MI transferred to the eavesdropper depends only on the SNR at the eavesdropper. With CSB defense, MI transferred to the eavesdropper is reduced due to corruption in the constellation.

E. Multi-path scenario

We study the performance of CSB defense for a multi-path channel that comprises propagation paths with different AoDs.

We use ℓ_{R}^* to denote the index of the dominant path to the RX and ℓ_{E}^* to denote the index of the dominant path to the eavesdropper. We define $\theta_{\mathrm{R},\ell_{\mathrm{R}}^*} = \theta_{\mathrm{R}}$ and $\theta_{\mathrm{E},\ell_{\mathrm{E}}^*} = \theta_{\mathrm{E}}$. Using the notations from (4) and (5), the signal received at the RX after circularly shifting the beamformer by c_k-steps is

$$y_{\mathrm{R},k} = \mathbf{h}_{\mathrm{R}}\mathcal{P}_{c_k}(\tilde{\mathbf{f}})x'_k + n_{\mathrm{R},k} \quad (15)$$

$$= \sum_{\ell=1}^{L_{\mathrm{R}}} \alpha_{\mathrm{R},\ell}\mathbf{a}^{\mathrm{T}}(\theta_{\mathrm{R},\ell})\mathcal{P}_{c_k}(\tilde{\mathbf{f}})x'_k + n_{\mathrm{R},k} \quad (16)$$

$$= \alpha_{\mathrm{R}}\mathbf{a}^{\mathrm{T}}(\theta_{\mathrm{R}})\tilde{\mathbf{f}}x_k + \underbrace{\sum_{\ell\neq\ell_{\mathrm{R}}^*} \alpha_{\mathrm{R},\ell}\mathbf{a}^{\mathrm{T}}(\theta_{\mathrm{R},\ell})\mathcal{P}_{c_k}(\tilde{\mathbf{f}})x'_k}_{\text{Residue}} + n_{\mathrm{R},k}. \quad (17)$$

Thus, in a multi-path environment with different AoDs, the RX receives a combination of the desired constellation and a phase perturbed constellation. The perturbed constellation arises because the phase of the residual term in (17) is random. To see this, we first note that CSB adjusts the phase of the transmitted symbol according to the expected phase change along the dominant path. In this case, the remaining paths in the channel experience different phase shifts due to circulant shifting of the beamformer and these phase shifts are not compensated.

In scenarios where the power of the dominant path is substantially higher than that of the other paths, the residue is small compared to the first term in (17). As a result, the perturbations in the constellation at the RX are small. In Section IV, we study the robustness of CSB to multi-path, by varying the Rician factor in a multi-path environment.

IV. Numerical Results

We discuss the SMI achieved by CSB defense compared to two benchmark DM-based techniques: (1) original ASM [10], referred as *ASM*, (2) a modification to ASM in which a subset of antennas create destructive interference [11], referred as *DINT*. We then study the performance of CSB in terms of symbol error rate (SER) achieved at the RX and the eavesdropper. We denote the ASM technique by ASM-c where c denotes the fraction of active antennas at the TX [10]. Similarly, we denote DINT technique by DINT-c where c denotes the fraction of antennas used for coherent beamforming [11].

We consider a uniform linear half-wavelength spaced phased antenna array at the TX with $N_{\mathrm{T}} = 16$ antennas. We assume that the RX is located along 25° with respect to the broadside angle of the TX array. We assume a line-of-sight (LOS) scenario for the TX-RX and the TX-eavesdropper channels; the AoDs associated with both these channels are known to the

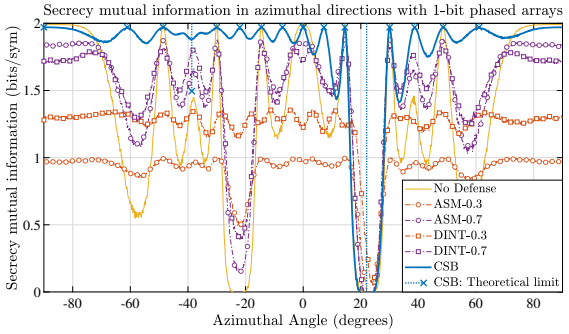

Fig. 4. SMI for different angular positions of the eavesdropper when the RX is at 25° with respect to the boresight of the 1-bit TX phased array: CSB defense achieves a large SMI as it preserves the SNR at the RX and induces APN along the other directions. The theoretical SMI shown for on-grid positions is derived from Lemma 3.

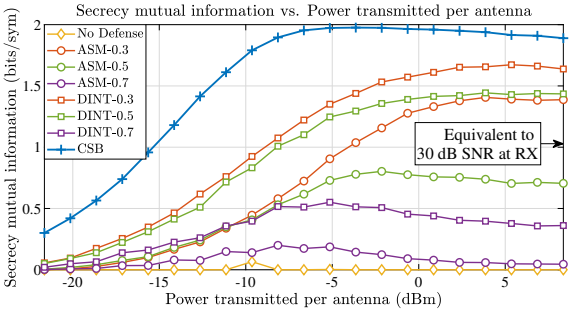

Fig. 5. SMI of the system with the transmitted power per antenna: We assume that the RX and the eavesdropper are equidistant from the TX, and the eavesdropper greedily positions itself along an angular direction with highest energy leakage. CSB defense achieves a better SMI than ASM and DINT. In the high power transmission regime, CSB results in a small degradation in SMI, due to non-uniform APN induced along the off-grid directions.

eavesdropper. We first plot the SMI for different angular positions of the eavesdropper located at the same radial distance from the TX as the RX. In Fig. 4, we show the SMI obtained numerically with CSB, ASM and DINT defenses. We notice that ASM and DINT perform poorly along the directions of the energy leakage. This poor performance is because the AN induced by ASM and DINT is small compared to the leakage energy of the RF signal when using low-resolution phased arrays. Thus, the defense by ASM and DINT gets weaker as the resolution of the phased arrays decreases. Furthermore, ASM and DINT result in a lower received power at the RX when compared to CSB, under the common per-antenna power constraint. Hence, the proposed CSB defense achieves a larger SMI as compared to ASM and DINT. We also observe a non-zero SMI with CSB defense along off-grid directions, which implies that APN is also induced along off-grid directions. We plot the theoretical mutual information transfer at high SNR for the on-grid positions of the eavesdropper using Lemma 3.

In Fig. 5, we show the SMI of the system with respect to the power transmitted per-antenna. We assume that the TX-RX and the TX-eavesdropper distance is 10 meters, and the eavesdropper adopts a greedy strategy of moving to the direction with the highest energy leakage. From Fig. 5, we observe that the SMI achieved by CSB defense is better than that of ASM and DINT. In the low transmit power regime,

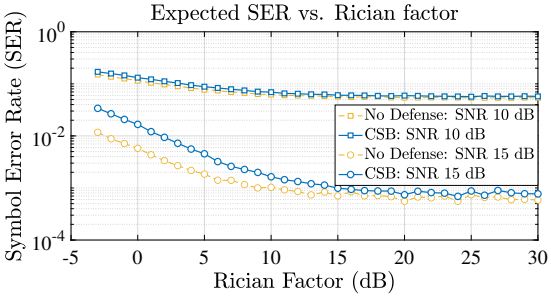

Fig. 6. SER at the RX for different Rician factors of the channel. A higher Rician factor corresponds to a stronger dominant path. As the Rician factor decreases, the SER with CSB defense increases because the interference from the perturbed constellation increases.

CSB achieves high MI at the RX while ASM and DINT lose power due to antenna switching and destructive interference, respectively. In the high transmit power regime, i.e., high SNR at the RX, CSB defense shows reduction in SMI due to non-uniform distortion in the constellation along off-grid directions. In the same regime, the SMI saturates with ASM and DINT because the AN induced by ASM and DINT also increases with the per-antenna transmit power.

To investigate the performance of CSB defense in a multi-path setting, we plot the SER at the RX as a function of the Rician factor of the channel in Fig. 6. The Rician factor is the ratio of the power of the dominant path and the total power of the non-dominant paths. For this simulation, we use NYUSIM to generate multi-path mmWave channels at 28 GHz [20]. The power of the non-dominant paths are scaled appropriately to generate a channel with a specific Rician factor. We then normalize the generated channel to evaluate the performance at a specific SNR. From Fig. 6, we notice that the SER achieved at the RX with CSB defense increases as the power of the non-dominant path increases. This observation is expected as the residual term in (17) increases for lower Rician factors.

V. Conclusions

We proposed a novel DM-based physical layer defense, called CSB defense, that applies random circulant shifts of the beamformer at every symbol transmission. Furthermore, the TX transmits phase-adjusted symbols such that the intended RX receives the correct symbol while eavesdroppers observe phase perturbed symbols. We analytically showed that our CSB defense induces APN along the on-grid directions and derived the statistics of this APN. The APN limits the information transferred to the eavesdropper even with perfect channel information. Finally, we showed that CSB defense preserves the power transmitted along the direction of the RX and achieves a larger SMI than comparable benchmarks.

Appendix

A. Proof of Lemma 2

The proof contains two steps: (i) For any $c \in [N_{\mathrm{T}}]$, $\Delta\Phi \in \Omega_{\Phi_{\Delta i}}$. (ii) If the random variable C is uniformly distributed over $[N_{\mathrm{T}}]$, then $\Delta\Phi$ is uniformly distributed over $\Omega_{\Phi_{\Delta i}}$.

We prove the first step (i) by induction. For the case $c = 0, \Delta\Phi = 0 \in \Omega_{\Phi_{\Delta i}}$. Next, we assume that for some $c \in [N_{\mathrm{T}}]$,

$\Delta\Phi = \frac{2\pi}{N_{\mathrm{T}}}(c\Delta i)_{\%N_{\mathrm{T}}} = \frac{2\pi}{N_{\mathrm{T}}}(\ell\Delta i)_{\%N_{\mathrm{T}}} \in \Omega_{\Phi_{\Delta i}}$, where ℓ is some integer in $[N_{\mathrm{T}}/\gcd(N_{\mathrm{T}}, \Delta i)]$. Then, for $c+1$ shifts,

$$\Delta\Phi' = \frac{2\pi}{N_{\mathrm{T}}}((c+1)\Delta i)_{\%N_{\mathrm{T}}} \tag{18}$$

$$= \frac{2\pi}{N_{\mathrm{T}}}\left((\ell\Delta i)_{\%N_{\mathrm{T}}} + (\Delta i)_{\%N_{\mathrm{T}}}\right)_{\%N_{\mathrm{T}}} \tag{19}$$

$$= \frac{2\pi}{N_{\mathrm{T}}}((\ell+1)\Delta i)_{\%N_{\mathrm{T}}} \in \Omega_{\Phi_{\Delta i}}. \tag{20}$$

Therefore, if there exists c such that $\Delta\Phi \in \Omega_{\Phi_{\Delta i}}$, then $\Delta\Phi'$ corresponding to $c+1$ shifts also belongs to $\Omega_{\Phi_{\Delta i}}$. Hence, it follows by induction that $\Delta\Phi \in \Omega_{\Phi_{\Delta i}}$ for every $c \in [N_{\mathrm{T}}]$.

To prove the second step (ii), we show that there are same number c such that $\Delta\Phi = \frac{2\pi}{N_{\mathrm{T}}}(\ell\Delta i)_{\%N_{\mathrm{T}}}$ for any ℓ. We denote by c_0 the smallest value of c that satisfies $(c\Delta i)_{\%N_{\mathrm{T}}} = (\ell\Delta i)_{\%N_{\mathrm{T}}}$, i.e., $c\Delta i = \ell\Delta i + kN_{\mathrm{T}}$, for some integer $k \geq 0$. Consider k_1 such that (i)$\frac{k_1 N_{\mathrm{T}}}{\Delta i}$ is an integer, (ii)$\frac{k_1 N_{\mathrm{T}}}{\Delta i} \leq N_{\mathrm{T}} - 1$. Then,

$$\left(c_0 + k_1\frac{N_{\mathrm{T}}}{\Delta i}\right)\Delta i = \ell\Delta i + (k+k_1)N_{\mathrm{T}}. \tag{21}$$

Thus, for each permissible k_1, there exists $c = c_0 + \frac{k_1 N_{\mathrm{T}}}{\Delta i}$ such that $\Delta\Phi = \frac{2\pi(\ell\Delta i)_{\%N_{\mathrm{T}}}}{N_{\mathrm{T}}}$. Observe that the number of permissible k_1's only depend on Δi and N_{T}, and *not* on ℓ. Therefore, for every ℓ, there are same number of c such that $\Delta\Phi = \frac{2\pi(\ell\Delta i)_{\%N_{\mathrm{T}}}}{N_{\mathrm{T}}}$. As a result, by choosing c uniformly from $[N_{\mathrm{T}}]$, $\Delta\Phi$ is uniformly distributed over $\Omega_{\Phi_{\Delta i}}$.

B. Proof of Lemma 3

To prove Lemma 3. we first find a condition when two symbols $e^{\mathrm{j}2\pi k_1/M}$ and $e^{\mathrm{j}2\pi k_2/M}$ in a constellation $\mathcal{M}$ cannot be distinguished due to the APN induced by CSB. For two symbols to be indistinguishable under APN, the difference in the phases of the both symbols must be in $\Omega_{\Phi_{\Delta i}}$. Equivalently,

$$\frac{k_1 - k_2}{M} = \frac{(\ell\Delta i)_{\%N_{\mathrm{T}}}}{N_{\mathrm{T}}} + p_1 \overset{(a)}{=} \frac{\ell\Delta i}{N_{\mathrm{T}}} + p_1 - p_2, \tag{22}$$

where p_1 is an integer and $\ell \in [N_{\mathrm{T}}/\gcd(N_{\mathrm{T}}, \Delta i)]$. (a) follows from $(\ell\Delta i)_{\%N_{\mathrm{T}}} + p_2 N_{\mathrm{T}} = \ell\Delta i$, for some integer p_2. We define $g = \gcd(\Delta i, N_{\mathrm{T}})$. Then, $N_{\mathrm{T}} = gu_1$ and $\Delta i = gu_2$, for some integers u_1, u_2. Additionally, note that $u_1 = |\Omega_{\Phi_{\Delta i}}|$. By re-arranging (22), we get

$$\frac{|\Omega_{\Phi_{\Delta i}}|}{M}(k_1 - k_2) - u_2\ell = |\Omega_{\Phi_{\Delta i}}|(p_1 - p_2). \tag{23}$$

To satisfy (23), $(k_1 - k_2)$ must be an integer multiple of $M/\gcd(M, |\Omega_{\Phi_{\Delta i}}|)$. We define partition of constellation $\mathcal{M}$, denoted by $\mathcal{M}_{k_1}$ containing the symbol $e^{\mathrm{j}\frac{2\pi k_1}{M}}$, and all symbols $e^{\mathrm{j}\frac{2\pi k_2}{M}}$ such that $k_1 - k_2$ satisfies (23). Specifically,

$$\mathcal{M}_{k_1} = \bigcup_{i \in [\gcd(M, |\Omega_{\Phi_{\Delta i}}|)]} \left\{\exp\left(\mathrm{j}\frac{2\pi k_1}{M} + \mathrm{j}\frac{2\pi i}{\gcd(M, |\Omega_{\Phi_{\Delta i}}|)}\right)\right\}. \tag{24}$$

Note that each partition contains $\gcd(M, |\Omega_{\Phi_{\Delta i}}|)$ number of symbols that cannot be distinguished from other symbols in that partition. Furthermore, there are $M/\gcd(M, |\Omega_{\Phi_{\Delta i}}|)$ number of partitions. As a result, out of the M symbols in the constellation $\mathcal{M}$, $M/\gcd(M, |\Omega_{\Phi_{\Delta i}}|)$ number of symbols are distinguishable under APN induced by CSB.

REFERENCES

[1] Y. Wu, A. Khisti, C. Xiao, G. Caire, K. Wong, and X. Gao, "A survey of physical layer security techniques for 5g wireless networks and challenges ahead," *IEEE J. Sel. Areas Commun.*, vol. 36, no. 4, pp. 679–695, April 2018.

[2] R. W. Heath, N. González-Prelcic, S. Rangan, W. Roh, and A. M. Sayeed, "An overview of signal processing techniques for millimeter wave MIMO systems," *IEEE J. Sel. Topics Signal Process.*, vol. 10, no. 3, pp. 436–453, 2016.

[3] A. S. Y. Poon and M. Taghivand, "Supporting and enabling circuits for antenna arrays in wireless communications," *Proc. IEEE*, vol. 100, no. 7, pp. 2207–2218, 2012.

[4] J.-H. Lee, J. Choi, W.-H. Lee, and J. Song, "Exploiting array pattern synthesis for physical layer security in millimeter wave channels," *Electronics*, vol. 8, no. 7, p. 745, Jul 2019.

[5] S. Balakrishnan, P. Wang, A. Bhuyan, and Z. Sun, "Modeling and analysis of eavesdropping attack in 802.11ad mmwave wireless networks," *IEEE Access*, vol. 7, pp. 70 355–70 370, 2019.

[6] C.-Y. Yeh and E. W. Knightly, "Eavesdropping in massive MIMO: New vulnerabilities and countermeasures," *IEEE Transactions on Wireless Communications*, vol. 20, no. 10, pp. 6536–6550, 2021.

[7] Y. Ju, H. Wang, T. Zheng, and Q. Yin, "Secure transmissions in millimeter wave systems," *IEEE Trans. Commun.*, vol. 65, no. 5, pp. 2114–2127, 2017.

[8] X. Tian, M. Li, Z. Wang, and Q. Liu, "Hybrid precoder and combiner design for secure transmission in mmwave MIMO systems," in *Proc. IEEE Global Commun. Conf.*, 2017, pp. 1–6.

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

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

[11] M. E. Eltayeb, J. Choi, T. Y. Al-Naffouri, and R. W. Heath, "On the security of millimeter wave vehicular communication systems using random antenna subsets," in *IEEE 84th Veh. Technol. Conf. (VTC-Fall)*, 2016, pp. 1–5.

[12] W.-Q. Wang and Z. Zheng, "Hybrid MIMO and phased-array directional modulation for physical layer security in mmwave wireless communications," *IEEE J. Sel. Areas Commun.*, vol. 36, no. 7, pp. 1383–1396, 2018.

[13] Z. Wei, C. Masouros, and F. Liu, "Secure directional modulation with few-bit phase shifters: Optimal and iterative-closed-form designs," *IEEE Trans. Commun.*, vol. 69, no. 1, pp. 486–500, 2021.

[14] J. Chen, "Hybrid beamforming with discrete phase shifters for millimeter-wave massive MIMO systems," *IEEE Trans. Veh. Technol.*, vol. 66, no. 8, pp. 7604–7608, 2017.

[15] M. Clenet and G. Morin, "Graphical investigation of quantisation effects of phase shifters on array patterns," Defence Research Establishment Ottawa (Ontario), Tech. Rep., 2000.

[16] S. Ebadi, R. V. Gatti, and R. Sorrentino, "Linear reflectarray antenna design using 1-bit digital phase shifters," in *Proc. of the 3rd IEEE European Conf. on Ant. and Prop. (EUCAP)*, 2009, pp. 3729–3732.

[17] A. Pitarokoilis, S. K. Mohammed, and E. G. Larsson, "Effect of oscillator phase noise on uplink performance of large MU-MIMO systems," in *Proc. of the 50th Annual Allerton Conf. on Commun., Control, and Comput.*, 2012, pp. 1190–1197.

[18] B. Sadhu, Y. Tousi, J. Hallin, S. Sahl, S. K. Reynolds, Ö. Renström, K. Sjögren, O. Haapalahti, N. Mazor, B. Bokinge *et al.*, "A 28-GHz 32-element TRX phased-array IC with concurrent dual-polarized operation and orthogonal phase and gain control for 5G communications," *IEEE J. of Solid-State Circuits*, vol. 52, no. 12, pp. 3373–3391, 2017.

[19] R. W. Heath, *Introduction to Wireless Digital Communication: A Signal Processing Perspective*. Pearson Education, 2017.

[20] S. Ju, O. Kanhere, Y. Xing, and T. S. Rappaport, "A millimeter-wave channel simulator NYUSIM with spatial consistency and human blockage," in *Proc. IEEE Global Commun. Conf.*, 2019, p. 1–6.