Circulant Shift-based Beamforming for Secure Communication with Low-resolution Phased Arrays

Patel, Kartik; Myers, Nitin Jonathan; Heath, Robert W.

DOI
10.1109/TWC.2022.3210649

Publication date
2023

Document Version
Final published version

Published in
IEEE Transactions on Wireless Communications

Circulant Shift-Based Beamforming for Secure Communication With Low-Resolution Phased Arrays

Kartik Patel, *Student Member, IEEE*, Nitin Jonathan Myers, *Member, IEEE*, and Robert W. Heath, Jr., *Fellow, IEEE*

***Abstract*— Millimeter wave (mmWave) technology can achieve high-speed communication due to the large available spectrum. Furthermore, the use of directional beams in mmWave system provides a natural defense against physical layer security attacks. In practice, however, the beams are imperfect due to mmWave hardware limitations such as the low-resolution of the phase shifters. These imperfections in the beam pattern introduce an energy leakage that can be exploited by an eavesdropper. To defend against such eavesdropping attacks, we propose a directional modulation-based defense technique where the transmitter applies random circulant shifts of a beamformer. We show that the use of random circulant shifts together with appropriate phase adjustment induces (APN) in the directions different from that of the target receiver. Our method corrupts the phase at the eavesdropper without affecting the communication link of the target receiver. We also experimentally verify the APN induced due to circulant shifts, using channel measurements from a 2-bit mmWave phased array testbed. Using simulations, we study the performance of the proposed defense technique against a greedy eavesdropping strategy in a vehicle-to-infrastructure scenario. The proposed technique achieves better defense than the antenna subset modulation, without compromising on the communication link with the target receiver.**

***Index Terms*— Millimeter wave (mmWave) communication, physical layer security, low-resolution phased arrays, directional modulation.**

I. Introduction

MILLIMETER wave (mmWave) communication uses directional beamforming where signals are transmitted or received along selected directions [1]. Directional beamforming also provides resilience against eavesdropping attacks as it concentrates the transmitted radio frequency (RF) signals along the direction of the intended user and reduces the signal transmitted along *unintended* directions, i.e. directions other than the direction of the intended user [2].

The directional beam patterns, in practice, are not perfect due to the design constraints in mmWave radios. Due to the high power consumption with fully digital arrays in a wideband setting, commodity mmWave radios are usually based on hybrid or analog antenna arrays that use RF phase shifters [1]. Moreover, the resolution of the RF phase shifters in these arrays is limited to few bits to reduce the hardware complexity [3]. The low resolution of phase shifters results in imperfections in the directed beam patterns which *leak* the RF signal along the unintended directions. In this paper, we study the RF signals leaked with such low resolution phased arrays and show that this leakage can be exploited by a mobile eavesdropper, such as an unmanned aerial vehicle (UAV) in a vehicle-to-infrastructure (V2I) scenario.

A standard approach to improve physical layer security (PLS) in an mmWave system is to reduce the energy leakage by appropriately designing a beamformer using channel state information (CSI) or the position of the eavesdropper [4], [5]. In [4], a precoding technique was proposed to reduce the energy leaked along the direction of the eavesdropper. In [5], defense mechanisms that exploit partial CSI to design precoders were developed to minimize the energy leakage. In this work, we claim that an eavesdropper can still breach such defenses that only focus on minimizing the energy leakage along potential eavesdropping directions. This is because a mobile eavesdropper can still achieve good received power by moving to a different direction, or by shifting closer to the transmitter (TX). The defense techniques in [4] and [5] also require fully digital antenna arrays and partial information about the eavesdropper, neither of which may be available in a practical system with analog or hybrid phased arrays.

Defense mechanisms that do not require fully digital arrays and are unaware of the eavesdropping location were proposed in [6] and [7]. In [6] and [7], hybrid beamformers were designed to transmit artificial noise (AN) along the unintended directions. Such AN-based defense techniques, however, degrade the performance at the intended receiver (RX). This is because either AN is induced at the RX or the power allocated for data transmission is reduced. An alternative approach that induces spatially selective AN requires

Manuscript received 13 July 2021; revised 11 January 2022 and 5 July 2022; accepted 17 September 2022. Date of publication 6 October 2022; date of current version 11 April 2023. This work was supported in part by the National Science Foundation under Grant CNS-1731658, in part by the Army Research Office under Grant W911NF1910221, and in part by the Idaho National Laboratory (INL) Laboratory Directed Research & Development (LDRD) Program under Department of Energy (DOE) Idaho Operations Office under Contract DE-AC07-05ID14517. The associate editor coordinating the review of this article and approving it for publication was K. Tourki. *(Corresponding author: Nitin Jonathan Myers.)*

Kartik Patel is with the Wireless Networking and Communications Group, The University of Texas at Austin, Austin, TX 78712 USA.

Nitin Jonathan Myers is with the Delft Center for Systems and Control, Delft University of Technology, 2628 CD Delft, The Netherlands (e-mail: n.j.myers@tudelft.nl).

Robert W. Heath, Jr., is with the Department of Electrical and Computer Engineering, North Carolina State University, Raleigh, NC 27695 USA.

Color versions of one or more figures in this article are available at https://doi.org/10.1109/TWC.2022.3210649.

Digital Object Identifier 10.1109/TWC.2022.3210649

partial CSI or position information of the eavesdropper which may not be available at the TX [8], [9], [10].

directional modulation (DM)-based physical layer defense techniques are also promising for secure mmWave communication. These methods modify the beamformer at every symbol such that the constellation is maintained along the intended direction and distorted along other directions [11], [12], [13], [14], [15], [16], [17], [18], [19], [20], [21]. Various algorithms to design DM-based symbol-level precoding have been proposed for secure multiple-input multiple-output (MIMO) communication with a digital antenna array [11], [12], [13], [14], [15], [16]. In the context of mmWave systems with hybrid or analog antenna array, DM-based methods have been proposed in [17], [18], [19], [20], and [21]. For instance, the Antenna Subset Modulation (ASM) technique proposed in [17] switches off a subset of antennas at every symbol. Switching at random changes the beamformer which affects the amplitude and phase of the transmitted symbol in all directions. By adjusting the phase of the transmitted symbol, the intended symbol is received at the RX while the symbol at the eavesdropper is distorted. A similar technique in [18] selects a random subset of antennas to destructively combine the RF signals at the unintended directions. Unfortunately, the methods in [17] and [18] reduce the mainlobe gain under the per-antenna power constraint. As a result, the RX observes a lower power when compared to the use of an ideal directional beam. In [19], a time-modulated DM-based technique was proposed for secure mmWave communication. Another DM-based technique for *actively driven* phased arrays, where an amplifier is cascaded after each low-resolution phase shifter, was developed in [20]. Our defense technique, in contrast, is designed for low-resolution phased arrays with passive phase shifters under the per-antenna power constraint. Our method also does not require CSI of the eavesdropper.

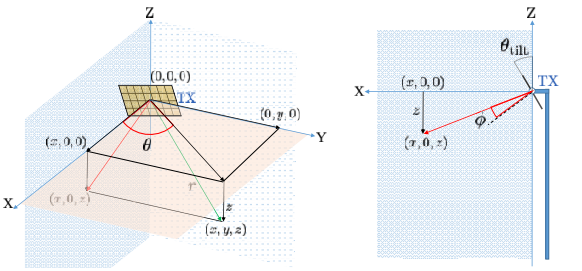
In this paper, we propose a novel DM-based approach to defend against an eavesdropper without impacting the communication performance at the RX. Our method called *Circulant Shift-based Beamforming* (CSB) applies a random circulant shift of the standard beamformer in every symbol duration. These random circulant shifts induce random phase changes in the symbols received along different directions. As the TX knows the phase change induced along the intended direction, it adjusts the transmitted symbol such that the RX receives the symbol without any phase distortion. The symbol observed along any other direction, however, is corrupted by APN. We characterize the statistical properties of the APN induced by CSB along the on-grid directions and show that the equivalent channel between the TX and the eavesdropper suffers from an ambiguity in the phase of the received symbol. As a result, coherent modulation techniques such as M-PSK cannot be decoded by an eavesdropper located along the on-grid directions even if the eavesdropper observes a high received power.

The proposed CSB has three key advantages over the techniques designed for mmWave systems. First, there is a smaller power loss at the RX compared to the ASM-based approach, as CSB activates all the antennas. Furthermore, circulantly shifting a beamformer does not change the beamforming gain at the discrete angles defined by the common DFT codebook. Second, our method is designed for low-resolution phased arrays without the assumption of active antenna elements as opposed to the prior work in [20]. Third, CSB has a lower complexity than other DM-based beamforming methods as CSB does not require any real-time optimization to compute the beamformer to achieve secure communication.

We would like to mention that our technique is different from recent PLS methods based on spatial modulation (SM) [22] and index modulation (IM) [23]. In the SM-based defense techniques [22], the TX selects a subset of antennas based on the CSI of the channel between itself and the RX. Then, the RX uses the CSI to decode the data symbols. An IM-based defense technique such as the one discussed in [23] uses rule-based mapping for index modulation in OFDM-IM. In contrast, our proposed CSB defense does not focus on antenna selection or IM. Our method only applies circulant shifts of the beamformer to corrupt the phase of the received symbols at the eavesdropper. The contributions of this paper can be summarized as follows:

- We propose CSB for secure communication under RF energy leakage due to low resolution phase shifters. Our technique applies random circulant shifts of the beamformer together with appropriate phase correction in the transmitted symbol, to introduce APN in the unintended directions. The phase correction ensures that the RX obtains the correct transmitted symbol. We characterize the induced APN for the case when the RX and the eavesdropper are located along on-grid directions, under the line-of-sight (LOS) channel assumption for the RX and the eavesdropper. Based on the statistical characteristics of APN, we derive the secrecy mutual information (SMI) of the proposed defense technique.
- We validate the key idea underlying the proposed defense mechanism using an mmWave phased array testbed. Considering the phase noise limitation of our phased arrays, we design an experiment to measure the phase change induced due to circulant shifts and show that circulant shifts indeed induce different phase shifts along different directions.
- We design a first of its kind mobile eavesdropping attack in a V2I mmWave system with low-resolution phased arrays. For this attack, we formulate a 2D trajectory optimization problem to track the directions of the RF energy leakage over time and use dynamic programming to solve the trajectory optimization problem. We numerically show how standard beamforming is vulnerable to such an attack, and discuss the use of CSB technique to defend this attack.

Organization: Section II contains the geometrical channel model and the definitions used in the paper. In Section III, we describe the proposed CSB for secure communication. Our experiment design to validate the proposed CSB is explained in Section IV. In Section V, we discuss our trajectory optimization-based mobile eavesdropping attack on the low-resolution phased array. Finally, we give simulation results in Section VI.



(a) 3D view

(b) Side view from positive Y-axis

Fig. 1. Conversion from rectangular coordinate (x, y, d) to modified spherical coordinate (r, θ, ϕ). The origin of both the coordinate systems is defined as the center of the TX antenna array.

Notations: $\mathbf{a}$ and $\mathbf{A}$ denote a vector and a matrix. a and A represent scalars. $\mathbf{A}^{\mathrm{T}}, \bar{\mathbf{A}}$, and $\mathbf{A}^{*}$ denote the transpose, conjugate and conjugate transpose of $\mathbf{A}$. The $(i, j)-$th element of $\mathbf{A}$ is $[\mathbf{A}]_{i,j}$. The inner product of matrices $\mathbf{A}$ and $\mathbf{B}$ is defined as $\langle \mathbf{A}, \mathbf{B} \rangle = \sum_{i,j} [\mathbf{A}]_{i,j} \left[\bar{\mathbf{B}}\right]_{i,j}$. We use $[N]$ to denote the set $\{0, 1, \ldots, N-1\}$. Finally, $\mathrm{j} = \sqrt{-1}$.

II. System Model

In this section, we describe the channel and the system model used in this paper. We also discuss the imperfections in the beams generated with low-resolution phased arrays.

A. Coordinate System

We consider the geometrical setup depicted in Fig. 1 where the TX is equipped with a planar antenna array centered at $(0, 0, 0)$. The plane of the TX array is perpendicular to the XZ-plane, and the array is tilted at an angle θ_{tilt} towards the ground. For ease of analysis, we convert the rectangular coordinate system into a modified spherical coordinate system shown in Fig. 1. The origin of the modified spherical coordinate system is defined as the center of the TX array. Consider a point (x, y, z) in the rectangular coordinate system, such that, $x \geq 0$ and $y, z \in \mathbb{R}$. The corresponding transformed coordinate (r, θ, ϕ), where r is the distance of the point from the origin, θ and ϕ are the azimuth and elevation angles, can be calculated as

$$r = \sqrt{x^2 + y^2 + z^2}, \theta = \arctan\left(\frac{y}{x}\right) \phi = \arctan\left(\frac{z}{x}\right) + \theta_{\mathrm{tilt}}. \tag{1}$$

We observe from the geometry that $r \geq 0$, $\theta \in [-\pi/2, \pi/2]$ and $\phi \in [-\pi/2 + \theta_{\mathrm{tilt}}, \pi/2]$. For simplicity of notation, we define the mapping S_1 such that, $(r, \theta, \phi) = S_1((x, y, z))$.

The modified spherical coordinate system defines the elevation angle as the angle between the projections of (x, y, z) and the perpendicular to the TX array on XZ-plane. In contrast, the conventional spherical coordinate system defines the elevation angle as the angle between the (x, y, z) and its projection on XY-plane. This modified coordinate system allows decoupling the phase variations in the array response matrix across two dimensions of the TX array.

We denote the RX coordinate in the rectangular and modified spherical systems by $(x_{\mathrm{R}}, y_{\mathrm{R}}, z_{\mathrm{R}})$ and $(r_{\mathrm{R}}, \theta_{\mathrm{R}}, \phi_{\mathrm{R}})$. These coordinates are defined under the assumption that the center of the TX is $(0, 0, 0)$. Similarly, we use $(x_{\mathrm{E}}, y_{\mathrm{E}}, z_{\mathrm{E}})$ and $(r_{\mathrm{E}}, \theta_{\mathrm{E}}, \phi_{\mathrm{E}})$ to represent the coordinates of the eavesdropper in the rectangular and the modified spherical systems. We also define the *angular coordinates* of the RX and the eavesdropper, relative to the TX, as $(\theta_{\mathrm{R}}, \phi_{\mathrm{R}})$ and $(\theta_{\mathrm{E}}, \phi_{\mathrm{E}})$.

B. Channel Model

In this paper, we model the mmWave channel between the TX and the RX as a narrowband line-of-sight (LoS) channel. The TX is equipped with a half-wavelength spaced uniform planar array (UPA) with $N_{\mathrm{T}} \times N_{\mathrm{T}}$ antenna elements. Although we assume an equal number of antennas along the azimuth and the elevation dimension for notational convenience, our design can also be generalized to other rectangular array geometries. The RX and the eavesdropper are assumed to be in the far field of the TX. For simplicity, we assume that the RX and the eavesdropper are equipped with a single mmWave antenna. The techniques discussed in this paper also apply to a multi-antenna RX and a multi-antenna eavesdropper under the far field assumption.

We now describe the array response matrices at the TX for the links associated with the RX and the eavesdropper. We define the Vandermonde vector

$$\mathbf{a}(\theta) = \left[1, e^{-\mathrm{j}\pi \sin\theta}, \ldots, e^{-\mathrm{j}(N_{\mathrm{T}}-1)\pi \sin\theta}\right]^{\mathrm{T}}. \tag{2}$$

As the angular coordinate of the RX relative to the TX is $(\theta_{\mathrm{R}}, \phi_{\mathrm{R}})$, the array response matrix between the TX and the RX can be expressed as

$$\mathbf{V}_{\mathrm{R}} = \mathbf{V}(\theta_{\mathrm{R}}, \phi_{\mathrm{R}}) = \mathbf{a}(\phi_{\mathrm{R}})\mathbf{a}^{\mathrm{T}}(\theta_{\mathrm{R}}). \tag{3}$$

The definition of the elevation angle ϕ_{R} in the modified spherical system allows the use of same array response function $\mathbf{a}(\cdot)$ along both dimensions of the antenna arrays. Similar to the RX, we define the array response matrix associated with the eavesdropper as

$$\mathbf{V}_{\mathrm{E}} = \mathbf{V}(\theta_{\mathrm{E}}, \phi_{\mathrm{E}}) = \mathbf{a}(\phi_{\mathrm{E}})\mathbf{a}^{\mathrm{T}}(\theta_{\mathrm{E}}). \tag{4}$$

Under the LoS assumption, the TX-RX and the TX-eavesdropper channels are just a scaled versions of the corresponding array response matrices.

C. Signal Model

We derive the signal model at a time instant t when the RX and the eavesdropper are located at $(r_{\mathrm{R},t}, \theta_{\mathrm{R},t}, \phi_{\mathrm{R},t})$ and $(r_{\mathrm{E},t}, \theta_{\mathrm{E},t}, \phi_{\mathrm{E},t})$. The TX array response matrices associated with the RX and the eavesdropper are denoted by $\mathbf{V}(\theta_{\mathrm{R},t}, \phi_{\mathrm{R},t})$ and $\mathbf{V}(\theta_{\mathrm{E},t}, \phi_{\mathrm{E},t})$. The TX applies a beamformer $\mathbf{F}_t$ to direct its signals towards the RX. We use x_t to denote the symbol transmitted by the TX. We assume that both the beamformer and the transmitted symbols are normalized, i.e. $||\mathbf{F}_t||_F^2 = 1$ and $\mathbb{E}[|x_t|^2] = 1$. We denote the phase offset due to the propagation delay between the TX and the RX by ν_{R}, the power received at the RX by $P_{r_{\mathrm{R},t}}$, and the independent

and identically distributed (IID) complex Gaussian noise by $n_{\mathrm{R},t} \sim \mathcal{CN}(0,\sigma^2)$. Then, the signal received by the RX at time t is

$$y_{\mathrm{R},t} = \sqrt{P_{r_{\mathrm{R},t}}} e^{\mathrm{j}\nu_{\mathrm{R}}} \langle \mathbf{V}(\theta_{\mathrm{R},t},\phi_{\mathrm{R},t}), \mathbf{F}_t \rangle x_t + n_{\mathrm{R},t}. \quad (5)$$

Similarly, let ν_{E} be the phase offset due to the propagation delay between the TX and the eavesdropper, $P_{r_{\mathrm{E},t}}$ be the power received by the eavesdropper, and $n_{\mathrm{E},t} \sim \mathcal{CN}(0,\sigma^2)$ be the IID complex Gaussian noise of the channel between the TX and the eavesdropper. Then, the signal received by an eavesdropper at $(r_{\mathrm{E},t}, \theta_{\mathrm{E},t}, \phi_{\mathrm{E},t})$ is

$$y_{\mathrm{E},t} = \sqrt{P_{r_{\mathrm{E},t}}} e^{\mathrm{j}\nu_{\mathrm{E}}} \langle \mathbf{V}(\theta_{\mathrm{E},t},\phi_{\mathrm{E},t}), \mathbf{F}_t \rangle x_t + n_{\mathrm{E},t}. \quad (6)$$

Conventional beamforming methods that are agnostic to the eavesdropper maximize the signal power at the RX. For example, $\mathbf{F}_t = \mathbf{V}(\theta_{\mathrm{R},t},\phi_{\mathrm{R},t})/N_{\mathrm{T}}$ results in the maximum signal-to-noise ratio (SNR) of $\rho_{\mathrm{R},t} = P_{r_{\mathrm{R},t}} N_{\mathrm{T}}^2/\sigma^2$ at the RX. Such a beamformer, however, cannot be applied in low resolution phased arrays due to the limited resolution of phase shifters. This is because the phase of the entries in $\mathbf{V}(\theta_{\mathrm{R},t},\phi_{\mathrm{R},t})$ do not necessarily take quantized values.

D. Practical Beamformer Design

We assume that the resolution of the phase shifters is q bits. In practice, q is a small number to limit the hardware complexity, e.g., $1 \le q \le 3$ [24], [25]. In this case, the entries of the beamformer $\mathbf{F}_t$ can only take finite phase values within the set $\mathcal{B}_q = \{\frac{2\pi i}{2^q} : i = 0, 1, \ldots, 2^q - 1\}$. Under this constraint, the phase of every element in the desired unquantized beamforming matrix is usually quantized to q levels for hardware compatibility. In this section, we describe the phase quantization procedure and its impact on the generated beam pattern.

The q-bit phase quantization function rounds the phase to the nearest element in $\mathcal{B}_q$, i.e., $Q_q(x) = \arg\min_{\beta\in\mathcal{B}_q} |\beta - x|$. We denote the phase of a complex number x as $\measuredangle(x)$. Thus, we can write the q-bit quantized beamformer corresponding to $\mathbf{F}_t$ as

$$\left[\tilde{\mathbf{F}}_t\right]_{k,\ell} = \frac{1}{N_{\mathrm{T}}} \exp\left\{\mathrm{j} Q_q\left(\measuredangle\left([\mathbf{F}_t]_{k,\ell}\right)\right)\right\}. \quad (7)$$

We would like to mention that this approach of rounding off the phase to the nearest element in $\mathcal{B}_q$ is one of many ways to calculate limited-resolution beamformer. Other methods to find the feasible beamformer are presented in [24], [25], and [26].

The quantization of the phase shifts introduces imperfections in the generated beam pattern. These imperfections cause energy leakage along the unintended directions, as shown in Fig. 2. We observe from Fig. 2 that the energy leakage is significant with low-resolution phased arrays using $q = 1$. Specifically, the beam patterns generated by one-bit phased arrays with a rectangular array geometry are mirror symmetric about the boresight direction (see Appendix A for proof).

An eavesdropper such as a mobile adversary can exploit the energy leakage by moving to the directions where the leakage is large, to eavesdrop on the TX. Furthermore, the eavesdropper can shift closer to the TX along this direction to receive a higher SNR. As a result, defense mechanisms that just minimize the energy leakage are not well suited in a mobile setting where the eavesdropper can re-position itself. Therefore, in this work, we propose a DM-based defense mechanism that corrupts the phase of the received symbols at the eavesdropper. Furthermore, the phase corruption due to our method is independent of the energy received by the eavesdropper.

III. Circulant Shift-Based Beamformer Design

In this section, we propose CSB as a defense against eavesdropping on a TX equipped with a low-resolution phased array.

A. Baseline 2D-DFT Codebook

Our CSB technique is applied on top of the standard 2D-DFT codebook used in uniform planar phased arrays. Due to the use of q-bit phase shifters, we define the quantized version of the 2D-DFT codebook as

$$\tilde{\mathcal{F}} = \left\{\tilde{\mathbf{F}}_{i,j} : \left[\tilde{\mathbf{F}}_{i,j}\right]_{k,\ell} = \frac{1}{N_{\mathrm{T}}} \exp\left(\mathrm{j} Q_q\left(\frac{2\pi}{N_{\mathrm{T}}}(ik + j\ell)\right)\right), \quad \forall i,j,k,\ell \in [N_{\mathrm{T}}]\right\}. \quad (8)$$

When a beamformer $\tilde{\mathbf{F}}_{i,j}$ is selected from the codebook $\tilde{\mathcal{F}}$ and applied to the phased array, it generates a directional beam pointing along the directions (θ,ϕ) such that $i = (N_{\mathrm{T}} \sin\theta/2)_{\%N_{\mathrm{T}}}$ and $j = (N_{\mathrm{T}} \sin\phi/2)_{\%N_{\mathrm{T}}}$, for $i,j \in [N_{\mathrm{T}}]$.

In the design of our defense mechanism, we assume that the RX and the eavesdropper are on-grid, i.e. $\frac{N_{\mathrm{T}} \sin\theta}{2}$ is an integer $\forall\theta \in \{\theta_{\mathrm{R},t}, \phi_{\mathrm{R},t}, \theta_{\mathrm{E},t}, \phi_{\mathrm{R},t}\}$. Although this assumption is required in the analysis of the proposed defense mechanism, we show in Section VI that our method works well even when the RX is off-grid provided the angular coordinate of the RX is known.

B. Circulantly Shifting a Beamformer

We define a matrix operator $\mathcal{P}_{m,n}$ that circularly shifts the input matrix by m steps along each column, and by n steps along every row. Specifically, for an $N \times N$ matrix $\mathbf{A}$,

$$[\mathcal{P}_{m,n}(\mathbf{A})]_{k,l} = [\mathbf{A}]_{(k-m)_{\%N},(l-n)_{\%N}}, \quad (9)$$

where $(\cdot)_{\%N}$ denotes the modulo-N operation. The matrix $\mathcal{P}_{m,n}(\mathbf{A})$ is interpreted as an (m,n) 2D-circulant shifted version of $\mathbf{A}$.

Now, we study the impact of circulantly shifting a beamformer on the received signal. We observe from (5) and (6) that the scaling introduced by the beamformer in the received symbol is $\langle \mathbf{V}(\theta,\phi), \mathbf{F} \rangle$. We define $\tilde{\mathcal{F}}$ as the set containing the $q-$bit quantized versions of the standard 2D-DFT beamformers. Our CSB technique is based on the key idea that circulantly shifting a beamformer at the TX affects the phase of the received signal differently in distinct directions. We discuss this property in Lemma 1. The proof of Lemma 1 follows from the circulant shifting property of the discrete Fourier transform [27].

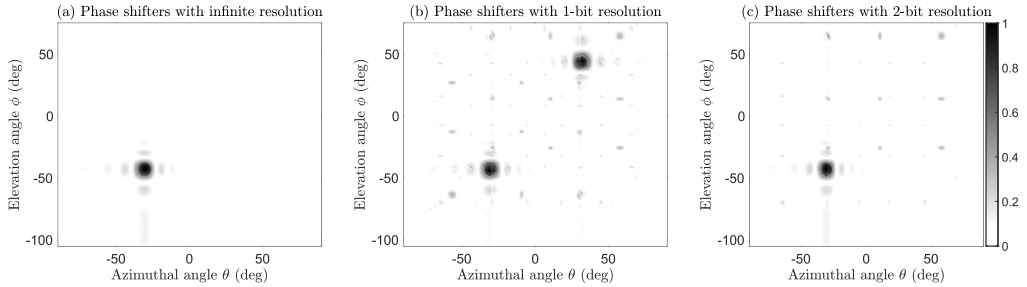


Fig. 2. The normalized amplitude of the received signal in the (θ, ϕ) space when beamforming is performed with (a) infinite-bit (b) 1-bit and (c) 2-bit resolution phased arrays. Here, the TX is equipped with a 16×16 half-wavelength spaced planar array. The array is tilted at 15° towards ground. The TX beamforms towards an RX whose angular coordinate is $(-30^\circ, -42^\circ)$.

Lemma 1: Let the angular coordinate of an on-grid receiver (RX or eavesdropper) be (θ, ϕ) *such that* $\frac{N_\mathrm{T}}{2}\sin\theta = i$ *and* $\frac{N_\mathrm{T}}{2}\sin\phi = j$. *If* $\tilde{\mathbf{F}} \in \tilde{\mathcal{F}}$, *then for any integer pair* $(m, n) \in [N_\mathrm{T}]^2$,

$$\left\langle \mathbf{V}(\theta,\phi), \mathcal{P}_{m,n}(\tilde{\mathbf{F}}) \right\rangle = \left\langle \mathbf{V}(\theta,\phi), \tilde{\mathbf{F}} \right\rangle e^{-\mathrm{j}\frac{2\pi}{N_\mathrm{T}}(mj+ni)} \quad (10)$$

Proof: Recall that $\mathbf{V}(\theta,\phi) = \mathbf{a}(\phi)\mathbf{a}^\mathrm{T}(\theta)$. For an on-grid receiver, the (k,ℓ)-th element of the array response matrix $\mathbf{V}(\theta,\phi)$ is $[\mathbf{V}(\theta,\phi)]_{k,\ell} = \frac{1}{N_\mathrm{T}} e^{-\mathrm{j}\frac{2\pi}{N_\mathrm{T}}(ik+j\ell)}$. In this case,

$$\left\langle \mathbf{V}(\theta,\phi), \tilde{\mathbf{F}} \right\rangle = \sum_{k,\ell} [\mathbf{V}(\theta,\phi)]_{k,\ell} \left[\tilde{\mathbf{F}}\right]_{k,\ell} \quad (11)$$

$$= \frac{1}{N_\mathrm{T}} \sum_{k,\ell} \left[\tilde{\mathbf{F}}\right]_{k,\ell} e^{-\mathrm{j}\frac{2\pi}{N_\mathrm{T}}(ik+j\ell)}. \quad (12)$$

Similarly, the inner product between the circularly shifted beamformer $\mathcal{P}_{m,n}(\tilde{\mathbf{F}})$ and $\mathbf{V}(\theta,\phi)$ is

$$\left\langle \mathbf{V}(\theta,\phi), \mathcal{P}_{m,n}(\tilde{\mathbf{F}}) \right\rangle = \sum_{k,\ell} [\mathbf{V}(\theta,\phi)]_{k,\ell} \left[\mathcal{P}_{m,n}(\tilde{\mathbf{F}})\right]_{k,\ell} \quad (13)$$

$$= \frac{1}{N_\mathrm{T}} \sum_{k,\ell} e^{-\mathrm{j}\frac{2\pi}{N_\mathrm{T}}(ik+j\ell)} \left[\tilde{\mathbf{F}}\right]_{(k-m)_{\%N},(\ell-n)_{\%N}}. \quad (14)$$

$$(14) \overset{(a)}{=} \frac{1}{N_\mathrm{T}} \sum_{k',\ell'} e^{-\mathrm{j}\frac{2\pi}{N_\mathrm{T}}\left(i\left(k'+m\right)_{\%N_\mathrm{T}} + j\left(\ell'+n\right)_{\%N_\mathrm{T}}\right)} \left[\tilde{\mathbf{F}}\right]_{k',\ell'}, \quad (15)$$

$$\overset{(b)}{=} \frac{1}{N_\mathrm{T}} \sum_{k',\ell'} e^{-\mathrm{j}\frac{2\pi}{N_\mathrm{T}}(i(k'+m)+j(\ell'+n))} \left[\tilde{\mathbf{F}}\right]_{k',\ell'}, \quad (16)$$

$$= e^{-\mathrm{j}\frac{2\pi}{N_\mathrm{T}}(mi+nj)} \left\langle \mathbf{V}(\theta,\phi), \tilde{\mathbf{F}} \right\rangle. \quad (17)$$

where (a) is based on the observation $k' = (k-m)_{\%N_\mathrm{T}}$ and $\ell' = (\ell-n)_{\%N_\mathrm{T}}$ and (b) follows from the fact that $\exp\left(-\mathrm{j}2\pi\,(i)_{\%N}/N\right) = \exp(-\mathrm{j}2\pi i/N)$ for any integer i. □

We make three key observations from Lemma 1. First, as $|\langle \mathbf{V}(\theta,\phi), \mathcal{P}_{m,n}(\tilde{\mathbf{F}})\rangle| = |\langle \mathbf{V}(\theta,\phi), \tilde{\mathbf{F}}\rangle|$, it follows that the beamforming gain at the RX remains the same for any circulant shift applied at the TX. Second, radios at different angular coordinates (θ,ϕ)'s, equivalently different 2D-DFT grid locations (i,j)'s, observe different phase changes when circularly shifting the transmit beamformer. Therefore, as long as the eavesdropper is not in the LoS path between the TX and the RX, the phase change induced at the RX and the eavesdropper are different when circularly shifting the beamformer. Third, we notice that N_T^2 distinct 2D-circulant shifts can be applied at the TX for every standard beamformer $\tilde{\mathbf{F}}$. As different circulant shifts induce different phase changes in any direction, our CSB-based defense can randomize the phase at the eavesdropper by applying a random circulant shift of $\tilde{\mathbf{F}}$. It is important to note that circularly shifting a beamformer at random also induces random phase changes at the RX which is undesirable.

Our CSB-based defense technique determines the phase change induced at the RX apriori, and adjusts the phase of the transmitted symbol accordingly. Such an approach ensures that the RX receives the correct transmitted symbol while the eavesdropper observes a phase perturbed symbol. We define x'_t as the symbol sent over the beamformer $\mathcal{P}_{m,n}(\tilde{\mathbf{F}}_t)$ to the RX at 2D-DFT grid location $(i_{\mathrm{R},t}, j_{\mathrm{R},t})$. In particular, with CSB, $x'_t = x_t \exp\left(\mathrm{j}\frac{2\pi}{N_\mathrm{T}}(mi_{\mathrm{R},t} + nj_{\mathrm{R},t})\right)$. The signal received by the RX can be simplified using Lemma 1 as

$$y_{\mathrm{R},t} = \sqrt{P_{r_{\mathrm{R},t}}} e^{\mathrm{j}\nu_\mathrm{R}} \left\langle \mathbf{V}(\theta_{\mathrm{R},t},\phi_{\mathrm{R},t}), \mathcal{P}_{m,n}(\tilde{\mathbf{F}}_t) \right\rangle x'_t + n_t, \quad (18)$$

$$= \sqrt{P_{r_{\mathrm{R},t}}} e^{\mathrm{j}\nu_\mathrm{R}} \left\langle \mathbf{V}(\theta_{\mathrm{R},t},\phi_{\mathrm{R},t}), \tilde{\mathbf{F}}_t \right\rangle x_t + n_t. \quad (19)$$

Therefore, by using the circularly shifted beamformer $\mathcal{P}_{m,n}(\tilde{\mathbf{F}}_t)$ and the phase rotated symbol x'_t, the received signal at the RX remains unchanged.

We now show that CSB perturbs the phase of the symbol received along the directions different from that of the RX. We assume an on-grid eavesdropper and use $(i_{\mathrm{E},t}, j_{\mathrm{E},t})$ to denote its 2D-DFT grid location. With the circularly shifted beamformer and the phase-adjusted transmitted symbol, the signal received by the eavesdropper is

$$y_{\mathrm{E},t}^{(m,n)} = \sqrt{P_{r_{\mathrm{E},t}}} e^{\mathrm{j}\nu_\mathrm{E}} \left\langle \mathbf{V}(\theta_{\mathrm{E},t},\phi_{\mathrm{E},t}), \mathcal{P}_{m,n}(\tilde{\mathbf{F}}_t) \right\rangle x'_t + n_t, \quad (20)$$

$$y_{\mathrm{E},t}^{(m,n)} = \sqrt{P_{r_{\mathrm{E},t}}} e^{\mathrm{j}\nu_\mathrm{E}} \left\langle \mathbf{V}(\theta_{\mathrm{E},t},\phi_{\mathrm{E},t}), \tilde{\mathbf{F}}_t \right\rangle \quad (21)$$

$$\times x_t \exp\Bigg(\mathrm{j}\frac{2\pi}{N_\mathrm{T}}(m(j_{\mathrm{R},t} - j_{\mathrm{E},t}) + n(i_{\mathrm{R},t} - i_{\mathrm{E},t}))\Bigg) + n_t. \quad (22)$$

As the eavesdropper and the RX are located along different directions, we have $(i_{\mathrm{R},t}, j_{\mathrm{R},t}) \neq (i_{\mathrm{E},t}, j_{\mathrm{E},t})$ for any t. In this case, we observe from (22) that the phase of the symbol received by the eavesdropper is random when the 2D-circulant

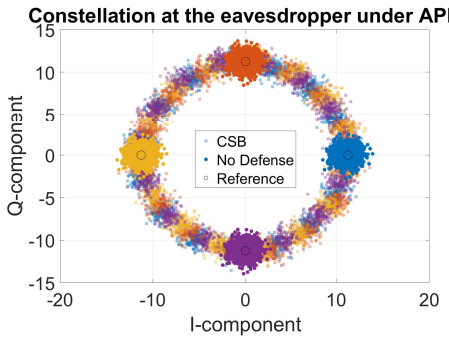


Fig. 3. Constellation at the eavesdropper in the presence of APN induced by CSB, compared to the case without any defense mechanism. CSB applies random circulant shifts of a beamformer to randomize the phase of the symbol at the eavesdropper.

shift (m,n) is chosen at random. Due to uncertainty in the applied 2D-circulant shift, the eavesdropper cannot predict the induced phase error even with the perfect information of the underlying 2D-DFT beamformer $\tilde{\mathbf{F}}_t$ and the position of the RX $(\theta_{\mathrm{R},t}, \phi_{\mathrm{R},t})$. Therefore, by randomizing the 2D-circulant shifts (m,n) at every symbol and appropriately adjusting the phase of the transmitted symbol, the received signal at the RX is preserved while the phase of the symbol at the eavesdropper is corrupted. An example of the received constellation at the eavesdropper with the CSB technique is shown in Fig. 3.

C. Achievable Secrecy Mutual Information

In this section, we first characterize the phase errors induced at the eavesdropper and then calculate the SMI achieved by CSB.

We call the phase errors induced by CSB as APN. We define $\Delta i_t = i_{\mathrm{R},t} - i_{\mathrm{E},t}$ and $\Delta j = j_{\mathrm{R},t} - j_{\mathrm{E},t}$ as the difference in the DFT grid coordinates corresponding to 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 (22) as

$$\Delta\Phi_t = \frac{2\pi}{N_{\mathrm{T}}} \left(m\Delta i_t + n\Delta j_t\right)_{\%N_{\mathrm{T}}}. \tag{23}$$

We also define $g_t = \gcd(\Delta i_t, \Delta j_t)$. In Lemma 2, we derive statistical properties of APN. We avoid the subscript t for simplicity of notation. For the theoretical analysis, we assume a noiseless channel between the TX and the eavesdropper to specifically focus on the effect of CSB.

Lemma 2: Consider independent random variables M_0 and N_0 that are uniformly distributed over $\Omega = [N_{\mathrm{T}}]$. We define $g = \gcd(\Delta i, \Delta j)$,

$$\Delta\Phi = \frac{2\pi}{N_{\mathrm{T}}} \left(M_0\Delta i + N_0\Delta j\right)_{\%N_{\mathrm{T}}}, \tag{24}$$

$$\Omega_{\Phi_g} = \left\{ \frac{2\pi \left(gi\right)_{\%N_{\mathrm{T}}}}{N_{\mathrm{T}}} : \forall i \in \left[\frac{N_{\mathrm{T}}}{\gcd(N_{\mathrm{T}}, g)} \right] \right\}. \tag{25}$$

Then,

$$\mathbb{P}\left(\Delta\Phi = \phi\right) = \begin{cases} \frac{\gcd(N_{\mathrm{T}},g)}{N_{\mathrm{T}}}, & \phi \in \Omega_{\Phi_g} \\ 0, & \text{otherwise} \end{cases}. \tag{26}$$

Proof:

The proof contains two steps: (i) For any pair $(m,n) \in [N_{\mathrm{T}}]^2$, $\Delta\Phi \in \Omega_{\Phi_g}$. (ii) If the random variables M_0, N_0 are uniformly distributed, then $\Delta\Phi$ is uniformly distributed over Ω_{Φ_g}.

We prove the first step (i) by induction. For the case $(m,n) = (0,0)$, $\Delta\Phi = 0 \in \Omega_{\Phi_g}$. We assume that for the pair (m,n), $\Delta\Phi = \frac{2\pi}{N_{\mathrm{T}}}\left(m\Delta i + n\Delta j\right)_{\%N_{\mathrm{T}}} = \frac{2\pi(g\ell)_{\%N_{\mathrm{T}}}}{N_{\mathrm{T}}}$, where ℓ is some integer. Then, for the pair $(m+1,n)$,

$$\Delta\Phi' = \frac{2\pi}{N_{\mathrm{T}}} \left((m+1)\Delta i + n\Delta j\right)_{\%N_{\mathrm{T}}} \tag{27}$$

$$= \frac{2\pi}{N_{\mathrm{T}}} \left(\left(m\Delta i + n\Delta j\right)_{\%N_{\mathrm{T}}} + \left(\Delta i\right)_{\%N_{\mathrm{T}}}\right)_{\%N_{\mathrm{T}}} \tag{28}$$

$$\overset{(a)}{=} \frac{2\pi}{N_{\mathrm{T}}} \left(\left(g\ell\right)_{\%N_{\mathrm{T}}} + \left(gk\right)_{\%N_{\mathrm{T}}}\right)_{\%N_{\mathrm{T}}} \tag{29}$$

$$= \frac{2\pi}{N_{\mathrm{T}}} \left(g(\ell+k)\right)_{\%N_{\mathrm{T}}} \in \Omega_{\Phi_g}, \tag{30}$$

where the equality (a) uses the fact that $\Delta i = gk$ for some integer k if $g = \gcd(\Delta i, \Delta j)$. Therefore, if there exists a pair (m,n) such that $\Delta\Phi \in \Omega_{\Phi_g}$, $\Delta\Phi'$ corresponding to the pair $(m+1,n)$ belongs to Ω_{Φ_g}. Similarly, it can be shown that $\Delta\Phi'$ corresponding to $(m,n+1)$ also belongs to Ω_{Φ_g}. Therefore, it follows by induction that $\Delta\Phi \in \Omega_{\Phi_g}$ for every $(m,n) \in [N_{\mathrm{T}}]^2$.

We now prove the second step (ii) in Lemma 2. To show that $\Delta\Phi$ is uniformly distributed over Ω_{Φ_g}, we prove that there are same number of (m,n) pairs such that $\Delta\Phi = \frac{2\pi(g\ell)_{\%N_{\mathrm{T}}}}{N_{\mathrm{T}}}$ for any ℓ. We denote by m_0, n_0 as the smallest values of m,n that satisfy $(m\Delta i + n\Delta j)_{\%N_{\mathrm{T}}} = (g\ell)_{\%N_{\mathrm{T}}}$, i.e., $m_0\Delta i + n_0\Delta j = g\ell + kN_{\mathrm{T}}$, for some integer $k \geq 0$. We also consider an integer pair (k_1,k_2), such that (i) $\frac{k_1 N_{\mathrm{T}}}{\Delta i}, \frac{k_2 N_{\mathrm{T}}}{\Delta j} \leq N_{\mathrm{T}} - 1$, (ii) $\frac{k_1 N_{\mathrm{T}}}{\Delta i}$, $\frac{k_2 N_{\mathrm{T}}}{\Delta j}$ are integers, and (iii) $k_1/\Delta i + k_2/\Delta j$ is an integer. Then,

$$\left(m_0 + k_1\frac{N_{\mathrm{T}}}{\Delta i}\right)\Delta i + \left(n_0 + k_2\frac{N_{\mathrm{T}}}{\Delta j}\right)\Delta j = g\ell + (k+r)N_{\mathrm{T}}, \tag{31}$$

where r is some integer. Thus, for each permissible pair (k_1,k_2), there exists a pair $(m,n) = (m_0 + \frac{k_1 N_{\mathrm{T}}}{\Delta i}, n_0 + \frac{k_2 N_{\mathrm{T}}}{\Delta j})$ such that $\Delta\Phi = \frac{2\pi(g\ell)_{\%N_{\mathrm{T}}}}{N_{\mathrm{T}}}$. Observe that the number of permissible pairs (k_1,k_2) only depend on $\Delta i, \Delta j, N_{\mathrm{T}}$, and *not* on ℓ. Therefore, for every ℓ, there are same number of (m,n) pairs, such that $\Delta\Phi = \frac{2\pi(g\ell)_{\%N_{\mathrm{T}}}}{N_{\mathrm{T}}}$. As a result, by choosing the pair (m,n) uniformly from $[N_{\mathrm{T}}]^2$, it can be ensured that $\Delta\Phi$ is uniformly distributed over Ω_{Φ_g}. □

Lemma 2 shows that the APN induced by CSB is uniformly distributed over Ω_{Φ_g}. With this result, we show in Lemma 3 that the APN introduced by CSB renders the eavesdropper unable to distinguish the transmitted symbol from the phase-corrupted received symbol.

Lemma 3: Consider an M-PSK constellation with the symbol set $\mathcal{M}$. We define partitions of $\mathcal{M}$ such that each partition contains $\gcd\left(\left|\Omega_{\Phi_g}\right|, M\right)$ number of symbols spaced uniformly in phase. The eavesdropper cannot distinguish between the symbols within a partition due to the APN induced by CSB.

Additionally, there are $M/\gcd(|\Omega_{\Phi_g}|, M)$ number of symbols that can be accurately distinguished.

Proof: To prove this lemma, 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 Ω_{Φ_g}. Equivalently,

$$\frac{2\pi k_1}{M} - \frac{2\pi k_2}{M} = \frac{2\pi\,(g\ell)_{\%N_{\mathrm{T}}}}{N_{\mathrm{T}}} + 2\pi p_1, \tag{32}$$

where p_1 is an integer and $\ell \in \left[\frac{N_{\mathrm{T}}}{\gcd(N_{\mathrm{T}},g)}\right]$. Observe that $(g\ell)_{\%N_{\mathrm{T}}} + p_2 N_{\mathrm{T}} = g\ell$, for some integer p_2. As a result, we can write

$$\frac{k_1 - k_2}{M} - \frac{g\ell}{N_{\mathrm{T}}} = p_1 - p_2 := p_3. \tag{33}$$

We define $g' = \gcd(g, N_{\mathrm{T}})$. Then $N_{\mathrm{T}} = g'u_1$ and $g = g'u_2$, for some integers u_1, u_2. Additionally, note that $u_1 = |\Omega_{\Phi_g}|$. By re-arranging (33), we get

$$\frac{|\Omega_{\Phi_g}|}{M}(k_1 - k_2) - u_2\ell = |\Omega_{\Phi_g}|p_3. \tag{34}$$

To satisfy (34), $(k_1 - k_2)$ must be an integer multiple of $M/\gcd(M, |\Omega_{\Phi_g}|)$. We define a 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 (34). Specifically,

$$\mathcal{M}_{k_1} = \left\{\exp\left(\mathrm{j}\frac{2\pi k_1}{M} + \mathrm{j}\frac{2\pi i}{\gcd(M, |\Omega_{\Phi_g}|)}\right) : i \in \left[\gcd(M, |\Omega_{\Phi_g}|)\right]\right\}. \tag{35}$$

Note that each partition contains $\gcd(M, |\Omega_{\Phi_g}|)$ number of symbols that cannot be distinguished from other symbols in that partition. Furthermore, there are $M/\gcd(M, |\Omega_{\Phi_g}|)$ number of partitions. As a result, out of the M symbols in the constellation $\mathcal{M}$, $M/\gcd(M, |\Omega_{\Phi_g}|)$ number of symbols are distinguishable under APN. We explain the interpretation of this lemma using Example 1. □

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 $\log_2(4/\gcd(|\Omega_{\Phi_{g_t}}|, 4))$ bits/symbol. If $g_t \notin \{0, 8\}$, the mutual information between the TX and the eavesdropper is 0 bit/symbol. Alternatively, if $g_t = 8$ the mutual information between the TX and the eavesdropper is 1 bit/symbol. Therefore, with CSB defense, the eavesdropper can only receive meaningful information along the certain directions associated with $g_t = 8$ and $g_t = 0$. Combined with directional beam patterns, the performance of the eavesdropper is limited by low energy leakage or high phase corruption.

Remark 1: It is worth pointing out that CSB does not require perfect CSI at the TX or the RX. CSB only requires the best 2D-DFT beam index associated with the intended RX. Such information is periodically acquired in IEEE 802.11ad and 5G devices using beam search. Furthermore, CSB defense does not require knowledge of the eavesdropper's location, neither does it require eavesdropper to be along on-grid directions. We assume the eavesdropper is on-grid to analyze the statistical characteristics of APN as a function of the eavesdropper's location. We show numerically the performance of the CSB defense when the eavesdropper is located along on-grid and off-grid directions.

We now use Lemma 3 to derive the SMI 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 mutual information (MI) of the channel between TX and RX by $\mathcal{I}_{\mathrm{R}}$, and MI of the channel between TX and eavesdropper by $\mathcal{I}_{\mathrm{E}}$. Thus, we can define the SMI C_{S} at time t as

$$C_{\mathrm{S}}(t) = \max\left\{\mathcal{I}_{\mathrm{R}} - \mathcal{I}_{\mathrm{E}}, 0\right\} \tag{36}$$

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 [28]. Additionally, if the eavesdropper is located at an on-grid position at time t such that $\gcd(\Delta i_t, \Delta j_t) = g_t$, then from Lemma 3, communication over the CSB-secured TX-eavesdropper channel using M-PSK modulation is equivalent to communication over the unsecured TX-eavesdropper channel using $M/\gcd(g_t, M)$-PSK constellation. Thus, if the angular coordinate of the RX at time t is $(\theta_{\mathrm{R},t}, \phi_{\mathrm{R},t})$, and that of the eavesdropper is $(\theta_{\mathrm{E},t}, \phi_{\mathrm{E},t})$, then using beamformer $\tilde{\mathbf{F}}_t$ at time t, we can calculate the SMI with CSB defense as

$$C_{\mathrm{S}}(t) = \max\Bigg\{\mathcal{I}\left(\frac{P_{r_{\mathrm{R},t}}}{\sigma^2}\left|\left\langle \mathbf{V}(\theta_{\mathrm{R},t}, \phi_{\mathrm{R},t}), \tilde{\mathbf{F}}_t\right\rangle\right|^2, M\right) - \mathcal{I}\left(\frac{P_{r_{\mathrm{E},t}}}{\sigma^2}\left|\langle \mathbf{V}(\theta_{\mathrm{E},t}, \phi_{\mathrm{E},t}),\rangle\, \tilde{\mathbf{F}}_t\right|^2, \frac{M}{\gcd\left(|\Omega_{\Phi_{g_t}}|, M\right)}\right), 0\Bigg\}. \tag{37}$$

For an effective eavesdropping attack, the eavesdropper attempts to minimize $C_{\mathrm{S}}(t)$ by positioning itself to appropriate $(\theta_{\mathrm{E},t}, \phi_{\mathrm{E},t})$. In the presence of CSB defense, the position of the eavesdropper, however, affects not only the SNR at the eavesdropper but also $|\Omega_{\Phi_{g_t}}|$, i.e., the equivalent constellation observed by the eavesdropper. Thus, CSB defense reduces information transfer to the eavesdropper by corrupting the constellation.

Remark 2: For the design of CSB defense, we considered a narrowband single-path channel. In a multi-path environment with different angle of departures, the RX receives a combination of desired constellation and a phase perturbed constellation. Due to the use of directional beams at the TX the signals received from the non-dominant paths will have significantly less energy, thereby resulting in small perturbations in the constellation at the RX. We discuss the performance of CSB defense in a multi-path environment in Section VI.

D. Implementing CSB - A Packet Level Overview

In this part, we describe the details related to implementation of CSB. Fig. 4 describes a typical PHY layer packet structure in IEEE 802.11ad protocol [29]. The training sequences, mainly short training field (STF) and channel

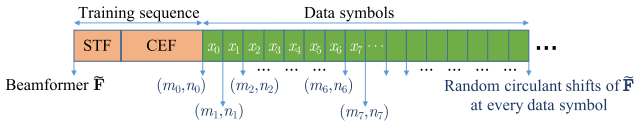


Fig. 4. IEEE 802.11ad packet structure: CSB defense uses (m, n)-2D circularly shifted beamformers, where (m, n) are IID random variables from the set $[N_{\mathrm{T}}]^2$. Circularly shifting a beamformer at every data symbol distorts the constellation at the eavesdropper, even with perfect CFO correction and channel estimation.

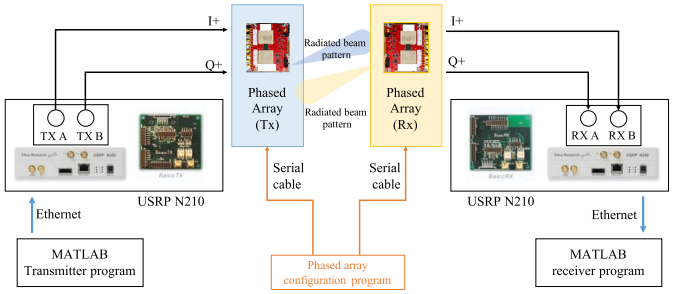


Fig. 5. Block diagram of the experimental setup used to validate the key idea in CSB defense.

estimation field (CEF), are used for the frame synchronization, carrier frequency offset (CFO) and phase offset correction. Then, data symbols are transmitted by the TX, followed by another packet or a short beam training field.

We propose to use CSB defense during the data symbol transmission. Specifically, the TX uses a fixed beamformer $\tilde{\mathbf{F}}$ for transmission of the training sequence. It allows the RX to perform frame synchronization, CFO and phase offset corrections, and channel estimation. Then, during data transmission, the TX circularly shifts the beamformer by (m, n) units. Here, (m, n) is chosen at random from the set $[N_{\mathrm{T}}]^2$ for each data symbol. For a particular (m, n) shift, the phase of the transmitted symbol is adjusted such that the phase of the symbol received in the direction of the RX remains unchanged. Thus, the RX receives the data symbols in a way that is agnostic to the circulant shifts applied at the TX. The eavesdropper, however, suffers from phase errors induced due to circulant shifting. Although using a fixed beamformer to transmit the training sequence allows the eavesdropper to equalize the channel, the symbols received by the eavesdropper are distorted due to circulant shifting of the beamformer.

In case of an OFDM-based operation with IEEE 802.11ad, CSB introduces the same phase error across all the sub-carriers as analog beams are frequency flat. Under a constant phase perturbation, the eavesdropper can correct the phase of the received OFDM symbol using pilot sub-carriers. To overcome this loophole, the TX can leverage the large symbol period of an OFDM symbol to circularly shift the beamformer multiple times within a symbol period. By adjusting the phase of the transmitted symbol after every shift of the beamformer, the received OFDM symbol is corrupted along all directions other than the direction of the RX.

E. Complexity Analysis

CSB defense circularly shifts the beamformer at each data symbol and adjusts the phase of the transmitted symbol such that the RX receives the symbol without distortion. Given the use of directional beamforming, the position of the RX is available at the TX. Furthermore, given the position of the RX, the CSB defense only requires $O(1)$ computation to find the change in the phase of the transmitted symbol for each circulant shift of the beamformer.

It is worth pointing out that the CSB defense can be extended to hybrid antenna arrays by independently implementing it on each RF chain. Given that CSB defense only requires a one-step phase adjustment for each RF chain, the complexity of implementing CSB scales linearly the number of RF chains in a hybrid array.

IV. Experimental Validation

In this section, we design an experiment to validate the premise of CSB defense. Specifically, our experiment estimates the phase change induced by circularly shifting a beamformer and shows that the estimated phase change is consistent with the result in Lemma 1.

A. Hardware Setup

We use two N210 USRPs, each as the baseband processor at the TX and the RX. Each USRP is connected to a separate SiBEAM Sil6342 phased array operating at 60.48 GHz. These phased arrays are uniform linear arrays with 12-antenna elements. Each element is connected to a 2-bit phase shifter that can be configured independent of the others. A block diagram of our hardware is shown in Fig. 5. We use the following procedure to setup the TX: (i) A MATLAB instance runs the transmitter program and generates the I/Q samples that are sent to USRP via Ethernet cable. (ii) The USRP then generates the baseband signal that is fed into the TX phased array. (iii) The phased array configuration program (external to the TX program) sets the configuration of the phase shifters using a universal asynchronous receiver-transmitter (UART) protocol. (iv) The baseband signal is upconverted to 60.48 GHz and the upconverted signal is phase shifted with the set configuration of the phased array. Finally, the 12×1 phase shifted signals are transmitted over the channel. A similar setup (i) – (iv) is built at the RX.

The SiBEAM Sil6342 phased arrays allow reconfiguration of the phase shifters using a UART protocol. The phase shifter of each antenna element can be set to one of the four phase states. The combination of the phase states applied to the 12×1 phased array realizes a specific beamformer. For the experiment, we emulate a one-bit phased array by using only two states out of four available phase states. Using one-bit phased array allows us to analytically predict the leaked RF signal which is mirror symmetric to the target direction as proven in Appendix A. Unlike ideal phased arrays, the off-the-shelf phased array used in our experiment does not provide the precise phase shifts of $\{0, \pi\}$ due to hardware imperfections. The phase offsets from 0 and π are estimated at each antenna using the calibration procedure described in [30]. With the

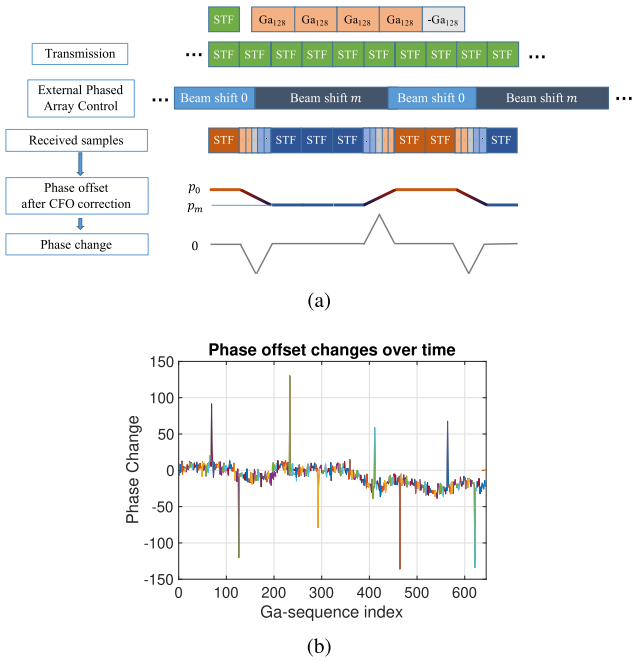


Fig. 6. (a) The figure describes our experimental procedure in which the phased arrays are externally controlled. It also shows the phase offset induced due to change in the beamformer. (b) This plot shows the phase difference between consecutive Ga-sequences in a packet. The spikes indicates changes in the beamformer and second, fourth, and sixth spike indicates transition from the test beamformer to its m-circulant shift.

knowledge of the phase offsets associated with the phase states, the phase of every entry in the beamformer is mapped to the nearest phase offset available at that antenna element.

B. Experimental Procedure

In Fig. 6(a), we describe the packet structure and the experimental procedure. A packet consists of a group of 130 short training fields (STF) where each STF contains five 128-length Golay sequences. The TX transmits an uninterrupted stream of identical packets while the RX captures one packet at a time. To accurately measure the phase change due to circulant shifting of the beamformer, it is vital to maintain coherence across measurements acquired before and after the circulant shift. Any interruption during packet reception must be avoided as it introduces a phase noise that cannot be corrected. To this end, we design our experiment by separating the receiver operation and the circulant shifting of the transmit beamformer. Specifically, the RX acquires a packet without any interruption, while an external program periodically applies beamformers by alternating between a beamformer and its m-circulant shift within the same packet.

To estimate the phase change due to the change in the beamformer, we first correct the frequency offset of each STF, and calculate the phase offset of each Ga-sequence in an STF. As a result, any significant change in the phase offsets of consecutive Ga-sequences can be attributed to circulantly shifting the beamformer. The measured phase change is either due to (i) the transition from the test beamformer to its m-circularly shifted beamformer or (ii) the transition from the m-circularly shifted beamformer to the test beamformer.

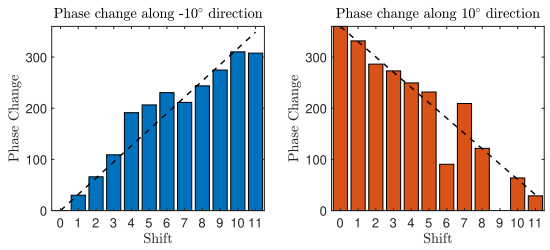


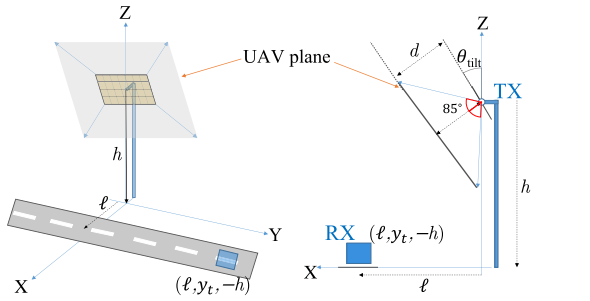
Fig. 7. Phase change corresponding to different circulant shifts in the beamformer when the RX is at 10° and -10° with respect to the boresight of the transmit phased array. The estimated slopes of the dotted lines are 31.7° and -29.9° per shift. These estimates are close to their theoretical values of 30° and -30° per shift.

To distinguish between the two phase changes, we use different dwell durations for the test beamformer and its m-circulant shift. In particular, we implement the test beamformer for $1/3$rd of the period duration and its m-circulant shift for $2/3$rd of the period duration. Under such a setting, if two consecutive phase changes occur at a lag of $1/3$rd of the period duration, we can conclude that the later phase change is due to the transition from the test beamformer to its m-circulant shift.

In Fig. 6(b), we show the difference between the phase offsets of consecutive Ga-sequences within a packet. The periodic pairs of spikes indicate sudden changes in the phase offset of consecutive Ga-sequences. These jumps are due to change in the beamformer. Furthermore, the long duration after the second, fourth and sixth spike is due to the transition from the beamformer to its m-circulant shift. By measuring the changes in the phase offsets and averaging them, we get the phase change due to the transition from the test beamformer to its m-circulant shift along a direction. Similarly, we measure the phase shift along different directions for every $m \in \{1, 2, \ldots, 11\}$.

C. Experimental Results

We collected IQ measurements using our mmWave testbed. For the experiment, we use a one-bit quantized beamformer ($q = 1$) for directional beamforming along 10° relative to the boresight. Due to the one-bit quantization, the beam pattern is symmetric about the boresight, i.e., the beam has two main lobes at 10° and -10°. Different circulant shifts of this beamformer are applied at the TX. In each case, the raw IQ samples are captured by a RX placed at 10°. Then, the phase change induced due to each circulant shift is estimated by following the procedure described in Fig. 6(a). The experiment is repeated by moving the RX to -10°. From Fig. 7, we observe that the phase change is linear with applied circulant shift m as derived in Lemma 1. The slope of this linear variation is also consistent with the angle from the boresight, as shown in Fig. 7. As the phase change induced at the RX by circulantly shifting a transmit beamformer can be predicted, the phase of the transmitted symbols can be adjusted at the TX for correct decoding along the direction of the RX. Such an adjustment, however, does not correct the phase perturbation at the eavesdropper. This is because the



(a) 3D view of the system (b) Side view from positive y-axis

Fig. 8. We assume that the UAV moves on a plane parallel to the plane of TX antenna array at a distance d. The angle subtended by the UAV plane at the center of the TX antenna array is $\beta/2 = 85°$.

phase change induced by circulant shifting a beamformer is different along different directions.

V. AirSpy: An Attack on V2I Network

In this section, we describe an attack, called *AirSpy*, on a planar low-resolution phased array TX in a downlink V2I network. We assume a mobile UAV eavesdropper that is aware of the resolution of the RF phased array at the TX and the position of the RX. The attack is achieved by computing a UAV flight path that efficiently taps the leaked RF signals in a mechanically feasible manner. We first define the secrecy rate of the link between the TX and the RX. Then, we develop an attack by formulating a trajectory search problem under the mechanical constraints on the UAV. Finally, we discuss a dynamic programming-based algorithm for trajectory search.

A. Secrecy Rate

To measure the severity of a physical layer attack, we define the secrecy rate corresponding to a beamformer $\tilde{\mathbf{F}}_t$ as

$$\mathcal{C}(\tilde{\mathbf{F}}_t, (r_{\mathrm{E},t}, \theta_{\mathrm{E},t}, \phi_{\mathrm{E},t})) \tag{38}$$

$$= \left[\log\left(1 + \frac{P_{r_{\mathrm{R},t}}}{\sigma^2}\left|\left\langle \mathbf{V}(\theta_{\mathrm{R},t}, \phi_{\mathrm{R},t}), \tilde{\mathbf{F}}_t\right\rangle\right|^2\right) - \log\left(1 + \frac{P_{r_{\mathrm{E},t}}}{\sigma^2}\left|\left\langle \mathbf{V}(\theta_{\mathrm{E},t}, \phi_{\mathrm{E},t}), \tilde{\mathbf{F}}_t\right\rangle\right|^2\right)\right]. \tag{39}$$

A greedy attack strategy is one that finds an optimal eavesdropping position $(\theta_{\mathrm{E}}, \phi_{\mathrm{E}}) \neq (\theta_{\mathrm{R},t}, \phi_{\mathrm{R},t})$ which minimizes the secrecy rate at every time instant. Such a greedy approach, however, may be mechanically infeasible under a finite velocity constraint. A good attack strategy is one that identifies and tracks multiple RF leakage signals over time for long term exploitation under the velocity constraint.

B. Learning Algorithm for Eavesdropping Trajectory Design

In this section, we define a trajectory and the set of feasible trajectories that satisfies the mechanical constraints on the motion of the UAV. Then, we propose an efficient dynamic programming-based algorithm that finds a UAV trajectory to eavesdrop on the TX. Our design assumes perfect knowledge of the RX location over a time interval, and minimizes the sum secrecy rate in this interval.

We consider a TX equipped with a planar antenna array situated at a height h from the ground. We assume that the RX is a vehicular RX that travels on a linear ground trajectory defined by the line $\{x = \ell, z = -h\}$. To incorporate the mechanical constraints on the eavesdropping UAV and design a numerically efficient algorithm, we limit the motion of the UAV to a virtual plane called the *UAV Plane*. This plane is parallel to the plane of the TX antenna array at a distance d, as shown in Fig. 8. The azimuth and elevation angles subtended by the UAV plane at the center of the TX antenna array are both equal to β, where $\beta \in (0, \pi)$. We use $\mathcal{P}_d$ to denote the set of points on the UAV plane, i.e.,

$$\begin{aligned}\mathcal{P}_d = \{\, &(x, y, z) : x\cos\theta_{\mathrm{tilt}} - z\sin\theta_{\mathrm{tilt}} = d,\\ &\phi = \arctan(z/x) + \theta_{\mathrm{tilt}} \in [-\beta/2, \beta/2],\\ &\theta = \arctan(y/x) \in [-\beta/2, \beta/2]\}\end{aligned} \tag{40}$$

For any angular coordinate of the eavesdropper $(\theta_{\mathrm{E}}, \phi_{\mathrm{E}}) \in [-\beta/2, \beta/2]^2$, there is a unique 2D-coordinate on the UAV plane. With the UAV plane constraint, the eavesdropper trajectory design problem is simplified from 3D to 2D.

We use a 2D coordinate system centered at the UAV plane to denote points on the UAV plane. The 2D-coordinate (u, v) corresponding to $(x, y, z) \in \mathcal{P}_d$ is computed from $x_u = ud\tan(\beta/2)\sin\theta_{\mathrm{tilt}} + d\cos\theta_{\mathrm{tilt}}$, $y_v = vd\tan(\beta/2)$, $z_u = ud\tan(\beta/2)\cos\theta_{\mathrm{tilt}} - d\sin\theta_{\mathrm{tilt}}$, where $u, v \in [-1, 1]$. For notational convenience, we define a mapping $S_2 : [-1, 1]^2 \to \mathcal{P}_d$ such that $(x_u, y_v, z_u) = S_2(u, v)$. We discretize the time index t with a sampling period T_{s}, and minimize the sum secrecy rate over discrete time instances for computational tractability. For that, we define a trajectory in Definition 1.

Definition 1: A discrete trajectory of length N, denoted by $\tau_{N,d}$, is a sequence of (u_t, v_t) pairs, where $(u_t, v_t) \in [-1, 1]^2$ and $t = 0, 1, \ldots, N-1$, such that t-th element of the sequence represents the coordinate of the UAV with respect to the center of the UAV plane at time tT_{s}. We denote t-th element of the trajectory $\tau_{N,d}$ by $\tau_{N,d}(t) = (u_t, v_t)$.

We would like to mention that only a subset of the trajectories in Definition 1 are permissible for the UAV. First, the trajectory must meet the maximum permissible velocity constraint on the UAV. Second, the UAV following this trajectory should not block the LoS path between the TX and the RX at any time instant. Based on these constraints, we define the set of permissible trajectories in Definition 2. Recall that the mapping S_1 converts rectangular coordinates to modified spherical coordinates, and S_2 changes the reference from the center of the UAV plane to the center of the TX antenna array.

Definition 2: Let $v_{\max}$ be the maximum permissible velocity of the UAV, $(\theta_{\mathrm{R},t}, \phi_{\mathrm{R},t})$ be the angular coordinate of the RX with respect to TX at time t, and (r_t, θ_t, ϕ_t) denote the angular coordinate of the UAV such that $(r_t, \theta_t, \phi_t) = S_1(S_2(u_t, v_t))$. Then, a discrete trajectory $\tau_{N,d}$ is a permissible trajectory, if for $\epsilon > 0$ and $\forall t > 0$,

$$\begin{aligned}&(1)\quad v(t) = \frac{\|\tau_{N,d}(t) - \tau_{N,d}(t-1)\|_2}{T_{\mathrm{s}}} \leq \frac{v_{\max}}{2d\tan(\beta/2)},\\ &(2)\qquad |\theta_t - \theta_{\mathrm{R},t}|^2 + |\phi_t - \phi_{\mathrm{R},t}|^2 > \epsilon^2.\end{aligned} \tag{41}$$

We use $\mathcal{T}_{N,d,\epsilon}$ to denote the set of all permissible trajectories.

Algorithm 1 Value Function Estimation and Optimal Trajectory

Initialize array H as $H(\mathbf{s}) = 0$ for all $\mathbf{s}$
for $n = N-1, N-2 \ldots, 1$ **do**
  $H(\mathbf{s}) \leftarrow \max_{\mathbf{s}':(\mathbf{s},\mathbf{s}')\in\mathcal{A}} R(\mathbf{s}') + H^*(\mathbf{s}')\ \forall \mathbf{s} = (u, v, n)$
Output: A trajectory τ of length N, such that $\tau(0) = \arg\max_{\mathbf{s}=(u,v,0)} H^*(\mathbf{s})$ and $\tau(t+1) = \arg\max_{(\mathbf{s},\mathbf{s}')\in\mathcal{A},\mathbf{s}_t=\tau(t)}\ R(\mathbf{s}') + H^*(\mathbf{s}')$.

The parameter ϵ in (41) characterizes the minimum permissible angular distance between the RX and the UAV, with respect to the TX. The constraint in (41) prevents the UAV from blocking the LoS path between the TX and the RX.

We now formulate the discrete trajectory optimization problem. The eavesdropper first computes the q-bit quantized beamformer $\tilde{\mathbf{F}}_t$ corresponding to the RX for all t. Then, the function $\mathcal{C}_t(\tilde{\mathbf{F}}_t, \tau(t))$ is evaluated over a discrete time grid. Finally, the optimal trajectory $\tau^*_{N,d,\epsilon}$ can be defined as

$$\tau^*_{N,d,\epsilon} := \underset{\tau\in\mathcal{T}_{N,d,\epsilon}}{\arg\min} \sum_{t=0}^{(N-1)T_s} \mathcal{C}_t(\tilde{\mathbf{F}}_t, \tau(t)). \tag{42}$$

The problem in (42) finds an optimal trajectory from a set of permissible trajectories that minimizes the total secrecy rate over time T.

We solve the optimization problem in (42) using a dynamic programming-based trajectory search. For that, we first define the state space, actions and reward as follows:

1) *State:* The state of the UAV at time index t is given by $\mathbf{s} = (u, v, t)$ where $(u, v) \in [-1, 1]^2$ and $t \in [N]$. We also define the state at time t as $\mathbf{s}_t = (u, v)$. We use a discrete $G \times G$ spatial grid to represent the coordinates $(u, v) \in \{-1 + 2i/G : i \in [G]\}^2$.
2) *Action:* An action $a_t = (\mathbf{s}, \mathbf{s}')$ at time t is defined as the transition from state $\mathbf{s} = (u, v, t)$ to $\mathbf{s}' = (u', v', t+1)$. An action $a_t = (\mathbf{s}, \mathbf{s}')$ is a valid action if there exists a permissible trajectory $\tau \in \mathcal{T}_{N,d,\epsilon}$ that makes a transition from state $\mathbf{s}$ to $\mathbf{s}'$. We denote the set of all valid actions by $\mathcal{A}$.
3) *Reward:* As the goal of the eavesdropper is to minimize (39), we define the reward R associated with an action $a_t = (\mathbf{s}, \mathbf{s}')$ as

$$R(a_t) = \log\left(1 + \frac{P_{r_{t+1}}}{\sigma^2}\left|\left\langle \mathbf{V}(\theta_{t+1}, \phi_{t+1}), \tilde{\mathbf{F}}_{t+1}\right\rangle\right|^2\right), \tag{43}$$

where $(r_{t+1}, \theta_{t+1}, \phi_{t+1}) = S_1(S_2(\mathbf{s}'))$. Since the definition of the reward solely depends on the next state, we denote $R(a_t) = R(\mathbf{s}')$ where $a_t = (\mathbf{s}, \mathbf{s}')$.

We now describe an adaption of dynamic programming called value iteration to solve (42) [31]. The value function is defined as

$$H^*(\mathbf{s}) = \max_{\mathbf{s}':(\mathbf{s},\mathbf{s}')\in\mathcal{A}} \left[R(\mathbf{s}') + H^*(\mathbf{s}')\right]. \tag{44}$$

An algorithm to estimate the value function is given in Algorithm 1.

We would like to highlight that our trajectory optimization algorithm requires the knowledge of the sequence of standard beamformers, i.e., $\{\tilde{\mathbf{F}}_t\}_{t=0}^T$, which can be computed from the trajectory of the RX. Furthermore, in a V2I system, the trajectory of the RX can be estimated based on the traffic geometry and vehicle dynamics. Given this knowledge at the eavesdropper, we use dynamic programming approach to solve the trajectory optimization problem because the problem has the following properties: (1) optimal sub-structure: the problem can be divided into sub-problems of finding *optimal* step from a state $\mathbf{s}$ and each of these sub-problems can be solved optimally, (2) overlapping sub-problems: multiple potential trajectories may require solving a sub-problem of finding the optimal step from a state $\mathbf{s}$ [32]. Thus, under these two assumptions, the proposed dynamic programming-based Algorithm 1 finds the global optimal sequence of states that maximizes the rewards. Equivalently, the optimal trajectory is found using global optimal sequence of states [32]. We discuss the performance of the proposed trajectory search algorithm in Section VI.

Although the design of sophisticated real-time attacks that are agnostic to the resolution of phase shifters and incorporate additional mechanical constraints such as the acceleration and power of the UAV is an interesting research direction, it is not within the scope of this work.

VI. Numerical Results

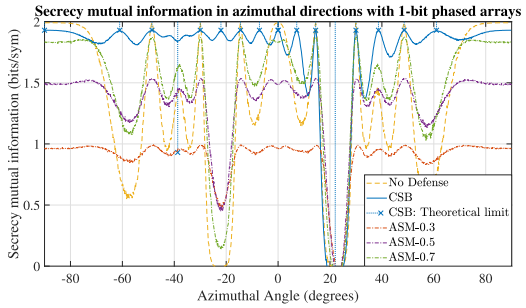
In this section, we show the severity of the proposed attack and the benefit of the proposed CSB defense. Specifically, we first discuss the SMI achieved by CSB defense compared to the benchmark DM-based technique, ASM [17]. We then show the severity of the *AirSpy* attack on a V2I TX, and explain the benefits of using CSB against such an attack.

We emphasize that our design of CSB is focused on passive phased arrays. CSB, however, can also be implemented on active phased arrays that require a higher hardware complexity than passive phased arrays. As characterizing the trade-off between the hardware complexity and the performance of defense techniques is beyond the scope of this paper, we focus on passive phased arrays and benchmark the performance of CSB against the techniques designed for such arrays.

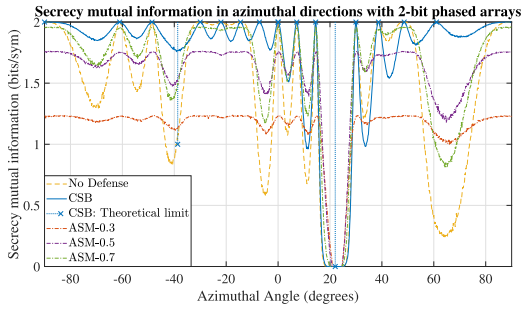
A. Performance of the Defense Technique

In this part, we compare the CSB technique with ASM in terms of the SMI. To this end, we consider a 16×1 linear phased antenna array at the TX and the use of the QPSK modulation. We consider an RX located at 25° with respect to the broadside angle of TX array. We plot the SMI for different angular positions of the eavesdropper located at the same radial distance from TX as the RX. We denote the ASM technique by ASM-c where c denotes the fraction of active antennas at the TX.

In Fig. 9, we show the numerically estimated SMI of CSB defense, and ASM defense with 0.3, 0.5 and 0.7 fraction of active antennas. We notice that ASM performs poorly along the directions of the energy leakage. This is due to the fact that the AN induced by ASM is small when compared to the RF



(a) 1-bit phased array



(b) 2-bit phased array

Fig. 9. SMI along different directions when the RX is at 25° with respect to the boresight of the TX 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.

signal leakage with low-resolution phased arrays. Furthermore, ASM defense also suffers from lower received power at the RX under the common per-antenna power constraint. In contrast, CSB defense achieves better SMI as compared to ASM.

We also plot the theoretical SMI for on-grid positions of the eavesdropper as characterized in Lemma 3. We emphasize that the SMI characterized in Lemma 3 is derived for the case with high SNR at the eavesdropper. In practice, however, the SMI along on-grid directions is higher due to low energy leakage along the on-grid directions. In conclusion, unless the directions corresponding to the high energy leakage coincides with the direction with limited APN (such as -38.6° in Example 1), CSB defense can maintain high secrecy communication.

Notably, CSB defense, like all DM-based defenses, cannot provide secrecy benefits when the eavesdropper is located exactly along the direction of the legitimate user. In practice, such eavesdroppers located along this direction are likely to block the propagation path to the RX, which can be detected by the RX [33], [34]. An alternate approach to address this issue is by focusing power in a spatial region around the intended RX, using large antenna arrays at the TX. Such spatial focusing achieves a higher secrecy rate.

B. Severity of AirSpy Attack

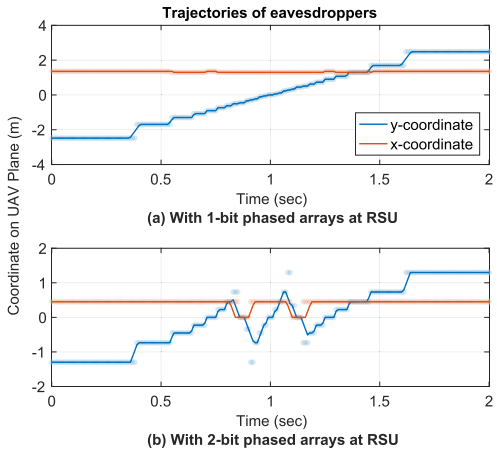
In this part, we numerically show the severity of the proposed attack. We first provide the trajectory of the UAV calculated with our trajectory design algorithm. Then, we study the secrecy rate of the system corresponding to the designed trajectory.

We consider a downlink V2I scenario, shown in Fig. 8, where the TX is equipped with a planar mmWave phased array with 16×16 elements. The TX array is located at $h = 8\,\mathrm{m}$ above the ground and is tilted downward by 15°. A vehicular RX travels on a straight lane at a distance of $\ell = 3$ m from the TX at a speed of 20 m/s. We assume that the RX is in a connected mode with this TX when the transceiver distance along the $y-$dimension is within 10 m, i.e., $y_t \in [-10, 10]$. As the vehicle moves at 20 m/s, the RX is connected to the TX for 1 second. We call this 1 second duration *episode*. We assume that the UAV eavesdropper traverses on a plane at a distance $d = 1$ m from the TX array. For the simulation, we consider a bounded region of the plane such that the angle subtended by the region at the center of TX antenna array is $\beta = 160^\circ$. We limit the speed of the UAV to 17 m/s [35]. In this setting, we first plot the eavesdropping trajectory designed using our dynamic programming-based algorithm when the RX moves from point $(3, -10, 8)$ to $(3, 10, 8)$ in an episode. The trajectories derived for attacks on 1-bit and 2-bit phased arrays are shown in Fig. 10(a).

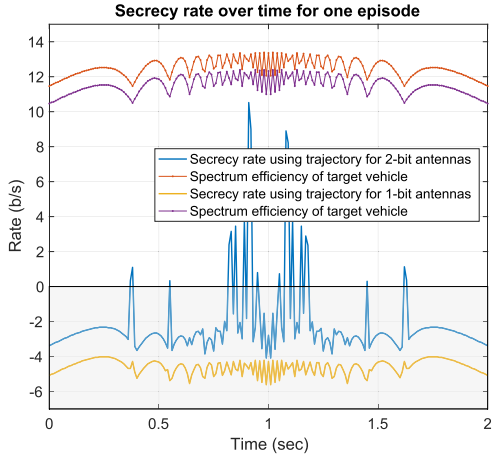
We notice that the optimal trajectory for eavesdropping on a one-bit phased array TX is consistent with the analytical solution derived in Appendix A. The solution can be explained from the observation that the beams generated with a one-bit phased array are mirror symmetric about the boresight direction. In case of 2-bit phased arrays, however, the optimal eavesdropping trajectory derived with our method exhibits an interesting phenomenon. The UAV diverges from the direction of the strongest side-lobe at about 0.8 seconds and 1.2 seconds. This divergence is important to minimize the sum secrecy rate over an episode. Such a change results in better eavesdropping than a feasible greedy trajectory that simply follows the strongest sidelobe. We illustrate this observation using a video that is available on our website [36].

In Fig. 10(b), we show the evolution of the secrecy rate as the eavesdropper follows the trajectory shown in Fig. 10(a) during one episode. The secrecy rate when using one-bit phased arrays at TX is consistently 0 because the energy received at the UAV eavesdropper is higher than the energy received at the RX. This is because the UAV eavesdropper is closer to the TX than the RX. The secrecy rate using the trajectory designed for 2-bit phased arrays at the TX is also below 0 for the same reason, except during the time when the eavesdropper deviates from the path traced out by the strongest side-lobe.

In both the one-bit and the two-bit scenarios, the rate at the eavesdropper is significantly higher than the rate at the RX. In such a case, any defense strategy that slightly reduces the leaked RF signals does not help in minimizing the secrecy rate. Furthermore, strategies that null the leaked RF signal in a particular direction are also not useful. This is because a mobile eavesdropper can optimize its trajectory in the new setup to track the other side-lobes. Therefore, any defense technique that reduces the energy leakage cannot tackle the issue of eavesdropping with a mobile eavesdropper. Our CSB defense corrupts the phase of the symbols along the directions other than the direction of the RX, instead of reducing the energy leakage.



(a) Trajectory of the eavesdropper



(b) Secrecy rate over an episode

Fig. 10. The figure depicts attacks using *AirSpy*. In (a), we show the optimal trajectory of the eavesdropper on the UAV plane, and the strongest sidelobe with dots. For one-bit phased arrays, the eavesdropper just tracks the strongest sidelobe. For 2-bit phased arrays, however, the eavesdropper follows a different path to avoid sudden transitions that arise when tracing the strongest side-lobe. This is because such sudden transitions are mechanically infeasible. The evolution of the secrecy rate over an episode is illustrated in (b). AirSpy is a good attack that substantially reduces the secrecy rate in low resolution phased array systems.

Remark: Although the secrecy rate is a non-negative quantity, we plot negative values in Fig. 10 to show the large difference between the rates at the RX and the eavesdropper over an episode.

C. Defense Against AirSpy

We describe the benefits of using CSB defense over ASM in a low-resolution phased array under the AirSpy attack. We use a system setup similar to the one used to analyze the attack. For the simulation of CSB and ASM defense, we consider both the RX and the eavesdropper perform perfect synchronization and we only focus on the performance during the data transmission. Additionally, we consider that the TX corrects the phase change as characterized in Lemma 1 when the RX is along an on-grid direction or an off-grid direction. Since the nearest on-grid direction associated with the RX is known to the TX in the form of the beam selected from the DFT codebook, our defense method does not require additional information to maintain the communication performance at the RX. Note that the phase change due to circulant shifts characterized in Lemma 1 is only valid along the on-grid directions. We will show using simulations that the phase correction based on nearest on-grid direction still maintains the performance at the RX along the off-grid directions.

In Fig. 11(a), we show the average SER at the RX and the eavesdropper as the function of the SNR received at the RX. Note that the SER at the RX is higher than the SER at the eavesdropper when using ASM-0.6 for the defense. This is due to two reasons. First, the received power at the eavesdropper is higher than the received SNR at the RX as the TX-eavesdropper distance is much smaller than the TX-RX distance. Second, the AN induced by ASM which adds to the noise at the eavesdropper is not sufficient enough to perturb the constellation at the eavesdropper. Thus, the effective signal power received at the eavesdropper due to the signal leakage from the low-resolution phased arrays is higher than the AN induced by ASM. In contrast, CSB defense scrambles the phase of the signal along the directions other than that of the RX, thus, corrupting the signal irrespective of the signal power.

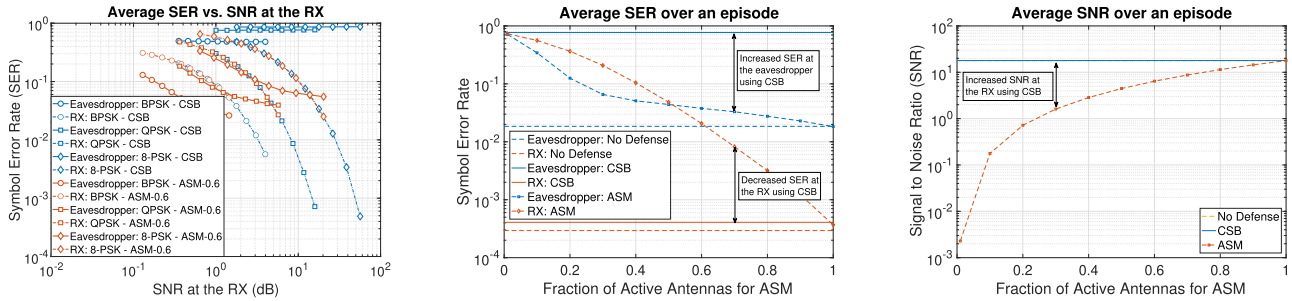
In Fig. 11(b), we show the average SER at the eavesdropper and the RX for different ASM parameter c. The SER at the eavesdropper when using CSB defense is higher than ASM defense for any parameter c. Additionally, the SER at the RX is also consistently lower when using CSB as compared to using ASM. It can also be observed from Fig. 11(c) that the use of CSB defense also provides an increased SNR at the RX when compared to ASM. From Fig. 11(b) and Fig. 11(c), we can conclude that CSB achieves a large SER at the eavesdropper, while the SER and the SNR at the RX is maintained without any significant degradation from the standard case.

D. Impact of the Phase Jitter at the RX

We analyze the impact of the phase jitter on the performance at the RX. Note that the phase corruption that is independent of the induced APN only worsens the signal quality at the eavesdropper. We consider two sources of phase jitter in the TX-RX communication: (1) the phase noise due to the jitter at the oscillators which induces random phase offsets at the RX and (2) the error between the actual phase shifts and the applied phase shifts on the phase shifters, defined as jitter at the phase shifters, that perturbs the phase of each element of the beamforming vector. In Fig. 12(a), we show the average phase error as a function of the maximum jitter at the phase shifters for different levels of jitter at the oscillators. Note that the phase error at the RX is dominated by the phase noise in the oscillator. Furthermore, this phase error due to phase noise in the oscillator is fundamental to the hardware of the communication system and is independent of the proposed CSB defense technique.

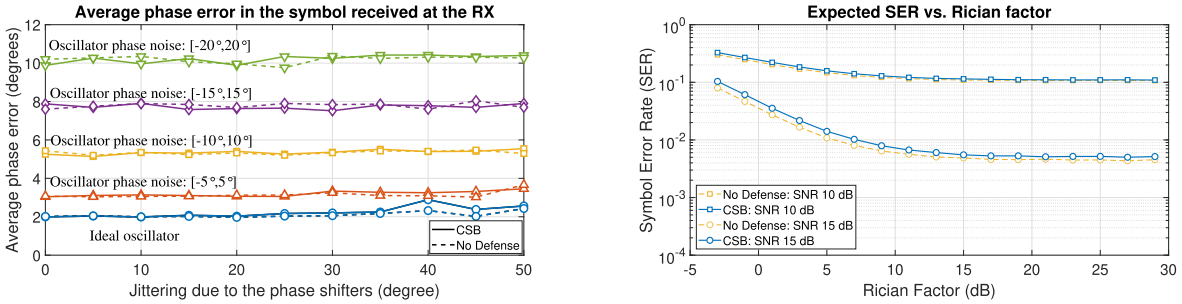
E. Performance of CSB in a Multi-Path Setting

We study the robustness of CSB in a multi-path channel setting through SER at the RX for varying Rician factors.



(a) SER at the eavesdropper with SNR at the RX (b) SER at the eavesdropper and the RX for different ASM parameters (c) SNR at the RX for different ASM parameters

Fig. 11. The plots show the SER and SNR performance of CSB defense as compared to ASM when the TX with 2-bit phased array is under the AirSpy attack. ASM provides lower SER to the eavesdropper as compared to CSB. CSB also provides higher SNR at the RX as compared to ASM.



(a) Impact of phase jitters (b) Impact of multi-path components on CSB

Fig. 12. (a) The average phase error in the symbol received at the RX as a function of the maximum phase jitter at phase shifters: The jitters at the phase shifters have minimal effect on the phase error, while the jitters at the oscillator have significant effect on the phase error. (b) With CSB defense, SER at the RX increases with the power of the non-dominant paths. This is due to increased interference from the phase perturbed symbols received along the non-dominant directions.

Note that the Rician factor characterizes the ratio of the power of LoS and non-LoS channel paths. We obtain channel paths from the NYUSIM simulator [37] and vary the Rician factor by scaling the non-LoS channel paths. From Fig. 12(b), we notice that the SER increases as the relative power of the non-dominant path increases. This is due to increased interference from the phase perturbed symbols transmitted along non-dominant directions.

VII. Conclusion

In this paper, we developed a directional modulation-based beamformer design technique called *CSB*, to defend against an eavesdropping attack on low-resolution phased arrays. The proposed CSB defense applies random circulant shifts of the low resolution beamformer to scramble the phase of the received symbol in the unintended directions. As a result, CSB blinds an eavesdropper that taps the leaked RF signals. We characterized the phase ambiguity introduced at the eavesdropper and derived the secrecy mutual information. We also designed an experiment on an mmWave testbed using 60 GHz phased arrays and showed that circulantly shifting a beamformer induces different but predictable phase shifts along different directions. The predictability of the phase shifts allows the TX to adjust the phase of the transmitted symbol to maintain the communication between the TX and the RX. Finally, we developed an eavesdropping attack for low-resolution phased arrays in a V2I network and evaluated the performance of CSB under such an attack. Our results indicate that CSB achieves a better defense than similar state-of-the-art benchmark techniques.

Appendix

A. Proof That the Beams With One-Bit Phased Arrays Are Mirror Symmetric About the Boresight

We use $\tilde{\mathbf{F}}_t$ to denote a one-bit beamformer which maximizes $|\langle \mathbf{V}(\theta_{\mathrm{R},t}, \phi_{\mathrm{R},t}), \tilde{\mathbf{F}}_t \rangle|^2$, i.e., the energy of the beam in the direction of the RX. We observe that the entries of the one-bit beamformer are $\pm 1/N_{\mathrm{T}}$. The energy leakage in the mirror symmetric direction to the RX, i.e., $(-\theta_{\mathrm{R},t}, -\phi_{\mathrm{R},t})$, is determined by $|\langle \mathbf{V}(-\theta_{\mathrm{R},t}, -\phi_{\mathrm{R},t}), \tilde{\mathbf{F}}_t \rangle|^2$. This is the same as $|\langle \bar{\mathbf{V}}(\theta_{\mathrm{R},t}, \phi_{\mathrm{R},t}), \tilde{\mathbf{F}}_t \rangle|^2$, by the property that $\bar{\mathbf{V}}(-\theta, -\phi) = \mathbf{V}(\theta, \phi)$. Now, we observe that $(\bar{\tilde{\mathbf{F}}}_t) = \tilde{\mathbf{F}}_t$ as the one-bit beamformer has real entries. As a result,

$$\left| \left\langle \mathbf{V}(-\theta_{\mathrm{R},t}, -\phi_{\mathrm{R},t}), \tilde{\mathbf{F}}_t \right\rangle \right|^2 = \left| \left\langle \bar{\mathbf{V}}(\theta_{\mathrm{R},t}, \phi_{\mathrm{R},t}), \bar{\tilde{\mathbf{F}}}_t \right\rangle \right|^2 \quad (45)$$

$$= \left| \left\langle \mathbf{V}(\theta_{\mathrm{R},t}, \phi_{\mathrm{R},t}), \tilde{\mathbf{F}}_t \right\rangle \right|^2 . \quad (46)$$

Therefore, the beam pattern with a one-bit phased array has an equal amount of energy along the directions $(\theta_{\mathrm{R},t}, \phi_{\mathrm{R},t})$ and $(-\theta_{\mathrm{R},t}, -\phi_{\mathrm{R},t})$. Due to this property, we observe that a reasonable eavesdropping strategy is one that traces the mirror-symmetric path corresponding to the RX.

REFERENCES

[1] R. W. Heath, Jr., 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, Apr. 2016.

[2] Y. Wu, A. Khisti, C. Xiao, G. Caire, K.-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, Apr. 2018.

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

[6] 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. (GLOBECOM)*, Dec. 2017, pp. 1–6.

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

[8] Q. Li and W.-K. Ma, "Spatially selective artificial-noise aided transmit optimization for MISO multi-eves secrecy rate maximization," *IEEE Trans. Signal Process.*, vol. 61, no. 10, pp. 2704–2717, May 2013.

[9] W.-C. Liao, T.-H. Chang, W.-K. Ma, and C.-Y. Chi, "QoS-based transmit beamforming in the presence of eavesdroppers: An optimized artificial-noise-aided approach," *IEEE Trans. Signal Process.*, vol. 59, no. 3, pp. 1202–1216, Mar. 2011.

[10] S. Gerbracht, C. Scheunert, and E. A. Jorswieck, "Secrecy outage in MISO systems with partial channel information," *IEEE Trans. Inf. Forensics Security*, vol. 7, no. 2, pp. 704–716, Apr. 2012.

[11] Y. Ding and V. F. Fusco, "A vector approach for the analysis and synthesis of directional modulation transmitters," *IEEE Trans. Antennas Propag.*, vol. 62, no. 1, pp. 361–370, Jan. 2014.

[12] M. Hafez, M. Yusuf, T. Khattab, T. Elfouly, and H. Arslan, "Secure spatial multiple access using directional modulation," *IEEE Trans. Wireless Commun.*, vol. 17, no. 1, pp. 563–573, Jan. 2018.

[13] A. Kalantari, M. Soltanalian, S. Maleki, S. Chatzinotas, and B. Ottersten, "Directional modulation via symbol-level precoding: A way to enhance security," *IEEE J. Sel. Topics Signal Process.*, vol. 10, no. 8, pp. 1478–1493, Dec. 2016.

[14] A. Kalantari, M. Soltanalian, S. Maleki, S. Chatzinotas, and B. Ottersten, "Secure M-PSK communication via directional modulation," in *Proc. IEEE Int. Conf. Acoust., Speech Signal Process. (ICASSP)*, Mar. 2016, pp. 3481–3485.

[15] F. Shu, L. Xu, J. Wang, W. Zhu, and Z. Xiaobo, "Artificial-noise-aided secure multicast precoding for directional modulation systems," *IEEE Trans. Veh. Technol.*, vol. 67, no. 7, pp. 6658–6662, Jul. 2018.

[16] R. M. Christopher and D. K. Borah, "Iterative convex optimization of multi-beam directional modulation with artificial noise," *IEEE Commun. Lett.*, vol. 22, no. 8, pp. 1712–1715, Aug. 2018.

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

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

[19] 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, Jul. 2018.

[20] 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, Jan. 2021.

[21] M. P. Daly and J. T. Bernhard, "Directional modulation technique for phased arrays," *IEEE Trans. Antennas Propag.*, vol. 57, no. 9, pp. 2633–2640, Sep. 2009.

[22] X. Wang, X. Wang, and L. Sun, "Spatial modulation aided physical layer security enhancement for fading wiretap channels," in *Proc. IEEE 8th Int. Conf. Wireless Commun. Signal Process. (WCSP)*, Yangzhou, China, Oct. 2016, pp. 1–5.

[23] Y. Lee, H. Jo, Y. Ko, and J. Choi, "Secure index and data symbol modulation for OFDM-IM," *IEEE Access*, vol. 5, pp. 24959–24974, 2017.

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

[25] H. Seleem, A. I. Sulyman, and A. Alsanie, "Hybrid precoding-beamforming design with Hadamard RF codebook for mmWave large-scale MIMO systems," *IEEE Access*, vol. 5, pp. 6813–6823, 2017.

[26] Z. Wang, M. Li, Q. Liu, and A. Lee Swindlehurst, "Hybrid precoder and combiner design with low-resolution phase shifters in mmWave MIMO systems," *IEEE J. Sel. Topics Signal Process.*, vol. 12, no. 2, pp. 256–269, May 2018.

[27] A. Oppenheim, A. Willsky, S. Nawab, W. Hamid, and I. Young, *Signals & Systems* (signal processing series). Upper Saddle River, NJ, USA: Prentice-Hall, 1997.

[28] R. W. Heath, Jr., *Introduction to Wireless Digital Communication: A Signal Processing Perspective*. London, U.K.: Pearson Education, 2017.

[29] T. Nitsche, C. Cordeiro, A. B. Flores, E. W. Knightly, E. Perahia, and J. C. Widmer, "IEEE 802.11ad: Directional 60 GHz communication for multi-gigabit-per-second Wi-Fi," *IEEE Commun. Mag.*, vol. 52, no. 12, pp. 132–141, Dec. 2014.

[30] Y. Zhang, K. Patel, S. Shakkottai, and R. W. Heath, Jr., "Side-information-aided noncoherent beam alignment design for millimeter wave systems," in *Proc. 20th ACM Int. Symp. Mobile Ad Hoc Netw. Comput.*, Jul. 2019, pp. 341–350.

[31] R. S. Sutton and A. G. Barto, *Reinforcement Learning: An Introduction*. Cambridge, MA, USA: MIT Press, 2018.

[32] J. Guttag, *Introduction to Computation and Programming Using Python, third edition: With Application to Computational Modeling and Understanding Data*. Cambridge, MA, USA: MIT Press, 2021.

[33] H. Xie, N. Gonzalez-Prelcic, and T. Shimizu, "Blockage detection and channel tracking in wideband mmWave MIMO systems," in *Proc. IEEE Int. Conf. Commun. (ICC)*, Jun. 2021, pp. 1–6.

[34] M. E. Eltayeb, T. Y. Al-Naffouri, and R. W. Heath, Jr., "Compressive sensing for blockage detection in vehicular millimeter wave antenna arrays," in *Proc. IEEE Global Commun. Conf. (GLOBECOM)*, Dec. 2016, pp. 1–6.

[35] GreenSight. *Announcing the Dreamer Drone With 60 Minutes of Usable Flight Time*. [Online]. Available: http://www.greensightag.com/logbook/announcing-the-dreamer-drone-with-60-minutes-of-flight-time/

[36] K. Patel, N. J. Myers, and R. W. Heath, Jr. (2022). *CSB-AirSpy*. [Online]. Available: https://www.kartikpatel.in/publications/csb-airspy/

[37] 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. (GLOBECOM)*, Dec. 2019, pp. 1–6.

Kartik Patel (Student Member, IEEE) received the B.Tech. degree in electronics and communication engineering from the Indian Institute of Technology (IIT) Roorkee in 2017 and the M.S. degree in electrical and computer engineering (ECE) from The University of Texas at Austin (UT Austin) in 2020, where he is currently pursuing the Ph.D. degree with the ECE Department. His research interests lie at the intersection of wireless networks, sensing, and machine learning with active focus on validating proposed solution on experimental testbed.

Nitin Jonathan Myers (Member, IEEE) received the B.Tech. and M.Tech. degrees in electrical engineering from the Indian Institute of Technology (IIT) Madras in 2016 and the Ph.D. degree in electrical and computer engineering (ECE) from The University of Texas at Austin (UT Austin) in 2020.

He is currently an Assistant Professor with the Delft Center for Systems and Control, Delft University of Technology (TU Delft). Prior to joining TU Delft, he was a Senior Engineer with the 5G Modem Research and Development Team, Samsung Semiconductor Inc., San Diego. His research interests include optimization and multi-dimensional signal processing, with applications to communications and sensing. He received the DAAD WISE Scholarship in 2014 and a Silver Medal, Institute Merit Prize, in 2016, during his bachelor's days at IIT Madras. At UT Austin, he received the University Graduate Continuing Fellowship (2019–2020), the 2018 and 2019 ECE Research Awards, and the 2018 ECE Professional Development Award from the Cockrell School of Engineering. He was recognized as an Exemplary Reviewer by the IEEE TRANSACTIONS ON COMMUNICATIONS in 2019 and the IEEE WIRELESS COMMUNICATIONS LETTERS in 2018. His bachelor's mentees at UT Austin won the First Runner-Up Prize in the IEEE ICASSP 2020 Video Contest. His Ph.D. Advisee at TU Delft won the Best Student Paper Award at IEEE SPAWC 2022. Recently, he was recognized by TU Delft as the Best Lecturer in the second year of the bachelor's program in mechanical engineering (2021–2022).

Robert W. Heath, Jr. (Fellow, IEEE) received the B.S. and M.S. degrees from the University of Virginia, Charlottesville, VA, USA, in 1996 and 1997, respectively, and the Ph.D. degree from Stanford University, Stanford, CA, USA, in 2002, all in electrical engineering.

From 1998 to 2001, he was a Senior Member of the Technical Staff and a Senior Consultant at Iospan Wireless Inc., San Jose, CA, USA, where he worked on the design and implementation of the physical and link layers of the first commercial MIMO-OFDM communication system. From 2002 to 2020, he was with The University of Texas at Austin, most recently as the Cockrell Family Regents Chair of Engineering and the Director of UT SAVES. He is currently the Lampe Distinguished Professor at North Carolina State University and the Co-Founder of 6GNC. He is also the President and the CEO of MIMO Wireless Inc. He has authored *Introduction to Wireless Digital Communication* (Prentice Hall, 2017) and *Digital Wireless Communication: Physical Layer Exploration Lab Using the NI USRP* (National Technology and Science Press, 2012) and coauthored *Millimeter Wave Wireless Communications* (Prentice Hall, 2014) and *Foundations of MIMO Communication* (Cambridge University Press, 2018). He has been the coauthor of a number award winning journals and conference papers, including recently the 2017 Marconi Prize Paper Award, the 2019 IEEE Communications Society Stephen O. Rice Prize, the 2020 IEEE Signal Processing Society Overview Paper Award, and the 2021 IEEE Vehicular Technology Society Neal Shepherd Memorial Best Propagation Paper Award. Other notable awards include the 2017 EURASIP Technical Achievement Award, the 2019 IEEE Kiyo Tomiyasu Award, and the 2021 IEEE Vehicular Technology Society James Evans Avant Grade Award. In 2017, he was selected as a fellow of the National Academy of Inventors. He is a Member-at-Large on the IEEE Communications Society Board-of-Governors (2020–2022). He was a Past Member-at-Large on the IEEE Signal Processing Society Board-of-Governors (2016–2018). He was the Editor-in-Chief of *IEEE Signal Processing Magazine* (2018–2020). He is also a Licensed Amateur Radio Operator, a Private Pilot, and a Registered Professional Engineer in Texas.