Exploiting Multi-Path for Safeguarding mmWave Communications Against Randomly Located Eavesdroppers

Rohith Talwar, Nancy Amala, George Medina, Akshadeep Singh Jida, and Mohammed E. Eltayeb

Department of Electrical & Electronic Engineering

California State University, Sacramento, USA

Emails: {rohithtalwar, nancyamalajosephraj, gm739, asjida, mohammed.eltayeb}@csus.edu

Abstract—Communication in the millimeter-wave (mmWave) band has recently been proposed to enable giga-bit-per-second data rates for next generation wireless systems. Physical layer security techniques have emerged as a simple and yet effective way to safeguard these systems against eavesdropping attacks. These techniques make use of the large antenna arrays available in mmWave systems to provide an array gain at the target receiver and degrade the signal quality at the eavesdropper. Despite their effectiveness, the majority of these techniques are based on line-of-sight communication links between the transmitter and the receiver, and may fail in the presence of blockages or non-line-of-sight links. This paper builds upon previous work and extends physical layer security to the non-line-of-sight communication case and randomly located eavesdroppers. Specifically, the large dimensional antenna arrays in mmWave systems and the intrinsic characteristics of wireless channel are exploited to induce noise-like signals that jam eavesdroppers with sensitive receivers. Numerical results show that the proposed techniques provide higher secrecy rate when compared to conventional array and physical layer techniques based on line-of-sight links.

Keywords–Millimeter-Wave; Physical layer security; Beamforming.

I. INTRODUCTION

The abundance of bandwidth in the millimeter-wave (mmWave) band enables high-speed, low latency, communication to support next generation systems [1]-[3]. These systems rely on directional communication with large antenna arrays to achieve sufficient link budget [4][5]. Securing these systems against eavesdropping and privacy attacks is one major challenge [6]-[8].

Security in wireless communications can be mainly grouped into cryptographic and Physical Layer Security (PLS) strategies, where the previous incorporates key-based approaches normally applied at higher system layers. The limited transmit RF-chains, higher path-loss, and directional communication requirement of mmWave systems, however, makes the implementation of classical cryptographic techniques inefficient for these systems [4][8][9]. For this reason, physical layer security has emerged as a simple but yet effective way to secure these systems and complement key-based cryptographic techniques [6][8][10]. Further, the implementation of PLS in mmWave is considered a productive strategy as it can result in higher communication speed, narrow communication beam and shorter transmission separation [11]. Physical layer security techniques utilize the large antenna arrays to enhance the communication signal (via beamforming) at the target receiver and degrade the signal quality at the eavesdropper. Directional beamforming, however, relies on Line-of-Sight (LoS) communication, and assumes the eavesdropper is not along the direction of communication. In practice, the passive eavesdropper could be located in the direction of communication, and, in the case of Non-Light-of-Sight (NLoS) communication, scatters can enable the eavesdropper to intercept the communication signal via multipath, hence rendering PHY layer security techniques ineffective. Therefore, it is critical to develop PHY layer security techniques that preserve privacy in both the LoS and NLoS cases.

Several strategies have been adopted in the literature to enhance the secrecy of mmWave wireless systems. Switched array based schemes [8] [12]-[14] employ random antenna subsets to induce artificial noise that jams potential eavesdroppers in non-receiver directions. In addition to this, the work in [8] proposed the use of prior information obtained from sensors to opportunistically inject noise in potential eavesdropper locations. In [15] and [16], low-complexity PLS techniques based on analog cooperative beamforming are proposed. These techniques enhanced the secrecy rate as distributed antenna nodes result in narrower beamwidth and increased artificial noise. The work in [17] built upon the techniques in [15] and [16] and proposed a beamforming solution with null steering. This solution is shown to improve the secrecy performance when the eavesdropper is in close proximity to the target receiver. Despite their capability in enhancing the transmission secrecy, those techniques require a LoS link to the target receiver and fail if the eavesdropper and the target receiver paths overlap. For instance, path overlap can occur if the eavesdropper is located along the transmission direction of the receiver or it is in close proximity to the receiver. Scatters close to the transmitter can cause blockages and lead to NLoS links. Overlapped common channel paths (as a result of NLoS links) between the receiver and the eavesdropper increase the risk of information leakage to the eavesdropper. To safeguard mmWave systems with possible overlapped common channel paths with the eavesdropper, the work in [18]-[21] considered the problem of aligned transmitter, eavesdropper, and target receiver in the mainlobe path, i.e., mainlobe security. In [18], a dual beam transmission technique that ensures the mainlobe is coherent only at the target receiver's location is proposed. The work in [19] proposed a dynamic rotated angular beamforming technique which uses a set of frequency offset modulator to

generate angle and range based transmission. The work in [21] utilized channel knowledge of eavesdroppers to enhance the secrecy rate of the target receiver. It should be noted that eavesdroppers in general are passive and their presence is unknown. The work in [20] proposed the use of maximum ratio combining and artificial noise injection in the null space of the receiver's channel to safeguard transmission. Maximum ratio combining, however, only increases the Signal-to-Noise Ratio (SNR) at the target receiver, but does not safeguard the communication link against an eavesdropper with a sensitive receiver. Moreover, noise injection requires complex antenna architectures which might be impractical to implement in mmWave systems.

In this paper, we address the problem of overlapped communication channel paths between the receiver and an arbitrary eavesdropper and propose two transmission techniques that enhance the security of mmWave systems with NLoS channels. Unlike [18]-[21], the proposed techniques do not necessarily require a LoS channel path between the transmitter and the receiver, and can be applied using a simple analog antenna architecture with a single RF chain at the transmitter. The first technique enhances secrecy by employing a path hopping technique, while the second technique uses random antenna subsets to beamform along multiple transmission paths. The proposed techniques facilitate secure transmission to the receiver without the need for complex antenna architectures and reduce the likelihood of information leakage to potential eavesdropper with common receiver communication paths.

The rest of the paper is structured as follows. In Section II, we introduce the system model. In Section III, we describe the proposed PLS techniques and analyze their performance in Section IV. We present some numerical results in Section V and conclude the work in Section VI.

II. SYSTEM MODEL

We consider a mmWave system where the transmitter communicates with a receiver via NLoS communications paths $L > 1$ in the presence of an eavesdropper. The transmitter consists of one RF chain and N antennas and the receiver is equipped with N_R antennas. To transmit the kth information symbol $s(k)$, where $E[|s(k)|^2] = 1$, to the receiver, the transmitter multiplies $s(k)$ by unit norm transmit vector $\mathbf{f} = [f_1, f_2, f_3, \ldots f_N] \in \mathcal{C}^N$, where f_n denotes the complex weight (or phase-shift) associated with the nth transmitting antenna. At the receiver, the received signals on all receive antennas are combined using a combining vector $\mathbf{w} \in \mathcal{C}^{N_R}$. Assuming a narrowband block fading channel, the received signal at the receiver is given by

$$y(k) = \mathbf{w}^* \mathbf{H} \mathbf{f} s(k) + z(k), \quad (1)$$

where $\mathbf{H}$ represents the mmWave channel matrix between the transmitter and the receiver, and $z(k) \sim \mathcal{CN}(0, \sigma^2)$ is the additive noise at the receiver. Adopting a geometric channel model with L scatters, where each scatter is assumed to contribute to a single channel path between the transmitter and the receiver, the channel $\mathbf{H}$ is given by [4]

$$\mathbf{H} = \sqrt{\frac{N N_R}{L}} \sum_{l=1}^{L} \alpha_l \mathbf{a}_R(\phi_l) \mathbf{a}_T^*(\theta_l) \quad (2)$$

where ϕ_l is Angle-of-Arrival (AoA) at the receiver associated with the lth Angle-of-Departure (AoD) θ_l from the transmitter, α_l is the complex gain of the lth path and $\mathbf{a}_R(\phi_l)$ and $\mathbf{a}_T(\theta_l)$ represent the receiver's and transmitter's array response defined in [4]. For ease of exposition, we assume a uniform linear array at the transmitter and a single antenna at the receiver. Hence, the the channel in (2) becomes

$$\mathbf{h} = \sqrt{\frac{N}{L}} \sum_{l=1}^{L} \alpha_l \mathbf{a}_T(\theta_l), \quad (3)$$

where $\mathbf{a}_T(\theta_l) = \frac{1}{\sqrt{N}}[e^{-j(\frac{N-1}{2})2\pi \frac{d}{\lambda} \cos(\theta_l)}, \ldots, e^{j(\frac{N-1}{2})2\pi \frac{d}{\lambda} \cos(\theta_l)}]$ and the signal in (1) simplifies to

$$y(k) = \mathbf{h}^* \mathbf{f} s(k) + z(k). \quad (4)$$

III. MILLIMETER WAVE SECURE TRANSMISSION

In this section, we introduce simple transmission techniques suitable for mmWave systems with analog antenna architecture (single RF chain). Nonetheless, the proposed techniques can also be applied in systems with advanced antenna architectures. The key idea is to exploit the intrinsic randomness of the wireless channel to distort transmission to eavesdroppers, with possible overlapping channels with the receiver, without the need for a fully digital array or prior channel information of eavesdroppers. With the assumption of local scatters at both the transmitter and receiver, the receiver's channel becomes unique at the transmitter, i.e., function of its location and scatters. This property has been exploited in finger-printing and localization techniques, see example [22]-[24] and references therein, to uniquely identify the location of the receiver. In this paper, with the assumption of full channel knowledge at the both the transmitter and the receiver, we exploit this property to jam an eavesdropper with an overlapping communication channel, i.e., eavesdropper shares a communication path with the target receiver. Instead of transmitting data symbols using the strongest channel path, the proposed transmission techniques select a random set of paths to transmit each data symbol (or data packet) to the target receiver. With the assumption that the receiver knows a-priori the selected transmission paths (this could be preprogrammed in the system) the receiver receives coherent signal, whereas, the eavesdropper receives a noise-like signal. This noise-like signal, which we term artificial noise, is a result of the randomized beam pattern observed at the eavesdropper. In the following sections, we further elaborate on those transmission techniques.

A. Enhancing secrecy with random path selection

In this technique, the transmitter transmits each data symbol along a random path (or AoD). Specifically, let $\theta_l \in \Phi$ be the lth AoD towards the target receiver and the set Φ represents all possible AoDs towards the target receiver. The transmitter's inter-antenna phase shifts are set as [13]

$$\Upsilon_n(k) = \left(\frac{N-1}{2} - n\right) 2\pi \frac{d}{\lambda} \cos(\theta_l) \quad (5)$$

where θ_l represents the lth selected AoD for the kth data symbol. Based on this, the nth entry of the beamforming vector $\mathbf{f}(k)$ (i.e., nth antenna weight) becomes $f_n(k) = \frac{1}{\sqrt{N}} e^{j \Upsilon_n(k)}$.

Using (4), the received signal at the receiver along AoD θ_l becomes

$$y_{\mathrm{R}}(k, \theta_l) = \mathbf{h}^* \mathbf{f}(k) s(k) + z_{\mathrm{R}}(k)$$

$$= \sqrt{\frac{N}{L}} \alpha_l \mathbf{a}_{\mathrm{T}}^*(\theta_l) \mathbf{f}(k) s(k) + z_{\mathrm{R}}(k) = \frac{1}{\sqrt{LN}} \alpha_l s(k) \times$$

$$\left(\sum_{n=0}^{N-1} e^{-j\left(\frac{N-1}{2}-n\right)\frac{2\pi d}{\lambda}\cos\theta_l} e^{j\left(\frac{N-1}{2}-n\right)\frac{2\pi d}{\lambda}\cos\theta_l} \right) + z_{\mathrm{R}}(k), \quad (6)$$

$$= \underbrace{s(k)}_{\substack{\text{information} \\ \text{symbol}}} \underbrace{\alpha_l \sqrt{\frac{N}{L}}}_{\substack{\text{effective channel} \\ \text{and array gain}}} + \underbrace{z_{\mathrm{R}}(k)}_{\substack{\text{additive} \\ \text{noise}}}.$$

where α_l is the lth path gain gain at the receiver, and $z_{\mathrm{R}}(k) \sim \mathcal{CN}(0, \sigma_{\mathrm{R}}^2)$ is the additive noise at the receiver.

Similarly, the received signal at an eavesdropper along an AoD θ_{E} is given by

$$y_{\mathrm{E}}(k, \theta_{\mathrm{E}}) = \mathbf{h}^* \mathbf{f}(k) s(k) + z_{\mathrm{E}}(k)$$

$$= \sqrt{\frac{N}{L}} \alpha_l \mathbf{a}_{\mathrm{T}}^*(\theta_{\mathrm{E}}) \mathbf{f}(k) s(k) + z_{\mathrm{E}}(k) = \frac{1}{\sqrt{LN}} \alpha_{\mathrm{E}} s(k) \times$$

$$\left(\sum_{n=0}^{N-1} e^{-j\left(\frac{N-1}{2}-n\right)\frac{2\pi d}{\lambda}\cos\theta_{\mathrm{E}}} e^{j\left(\frac{N-1}{2}-n\right)\frac{2\pi d}{\lambda}\cos\theta_l} \right) + z_{\mathrm{E}}(k) \quad (7)$$

$$= \underbrace{s(k)}_{\substack{\text{information} \\ \text{symbol}}} \underbrace{\alpha_{\mathrm{E}}}_{\substack{\text{channel} \\ \text{gain}}} \underbrace{\sqrt{1/LN} B(\theta_l)}_{\substack{\text{artifical} \\ \text{noise}}} + \underbrace{z_{\mathrm{E}}(k)}_{\substack{\text{additive} \\ \text{noise}}},$$

where $\theta_l \in \Phi$, $z_{\mathrm{E}}(k) \sim \mathcal{CN}(0, \sigma_{\mathrm{E}}^2)$ is the additive noise at the eavesdropper and the random variable $B(\theta_l)$ (due to random selection of θ_l) is

$$B(\theta_l) = \sum_{n=0}^{N-1} e^{-j\left(\frac{N-1}{2}-n\right)\frac{2\pi d}{\lambda}\cos\theta_{\mathrm{E}}} e^{j\left(\frac{N-1}{2}-n\right)\frac{2\pi d}{\lambda}\cos\theta_l} \quad (8)$$

$$= \sum_{n=0}^{N-1} e^{-j\left(\frac{N-1}{2}-n\right)\frac{2\pi d}{\lambda}(\cos(\theta_{\mathrm{E}})-\cos(\theta_l))} \quad (9)$$

$$= N \frac{\sin(N(\frac{\pi d}{\lambda}(\cos(\theta_{\mathrm{E}}) - \cos(\theta_l))))}{\sin((\frac{\pi d}{\lambda}(\cos(\theta_{\mathrm{E}}) - \cos(\theta_l))))}. \quad (10)$$

Observe when the eavesdropper is located along one of the AoDs in the set Φ, i.e., $\theta_{\mathrm{E}} = \theta_l$, then $B(\theta_l)$ becomes deterministic with the value of N. Note this event occurs with probability $\frac{1}{L}$, where L is the number of paths. Hence, it is important to have large number of paths L for this technique to be efficient.

B. Enhancing secrecy with joint path and antenna selection

The secrecy performance of the random path selection technique deteriorates with limited number of scatters, i.e., low number of transmit path L. To improve the secrecy in a low scattering environment, we propose a joint antenna selection and path selection technique. The idea is to associate a set of M antennas for the strongest transmission path and the remaining $N-M$ antennas for another randomly selected path. For each transmit symbol (or packet), different sets of antennas are associated with the strongest path and a random secondary transmit path. Selecting the strongest path maximizes the receive SNR at the receiver. This dual antenna and path

selection technique results in controlled interference in both the main and secondary transmission paths. The interference results from the contribution of the side-lobes of each transmit beam in all paths. The random antenna selection ensures that the side-lobe levels are perturbed for each transmit symbol. As the target receiver is aware of its channel, the transmit path identity, and the set of selected antennas for each path (can be preprogrammed a priori), it is able to decode the received symbol. As the eavesdropper does not have knowledge of these parameters, it can not precancel the interference due to the perturbed side-lobes. This reduces its rate and enhances the overall secrecy rate.

Let $\mathcal{I}_M(k)$ be a random subset of M antennas used to transmit the kth symbol along the strongest path (AoD θ_{S}), and $\mathcal{I}_L(k)$ be subset that contains the indices of the remaining antennas used to transmit the kth symbol along a secondary path (AoD θ_i). The nth antenna phase shift is set as

$$\Upsilon_n(k) = \left\{ \begin{array}{ll} \left(\frac{N-1}{2} - n\right) 2\pi \frac{d}{\lambda} \cos(\theta_{\mathrm{S}}), & n \in \mathcal{I}_M(k) \\ \left(\frac{N-1}{2} - n\right) 2\pi \frac{d}{\lambda} \cos(\theta_i), & n \in \mathcal{I}_L(k) \end{array} \right. \quad (11)$$

and the received signal at the target receiver becomes

$$y_{\mathrm{R}}(k, \theta_{\mathrm{S}}, \theta_i) = \mathbf{h}^* \mathbf{f}(k) s(k) + z_{\mathrm{R}}(k) = \frac{1}{\sqrt{LN}} s(k) \times$$

$$\left(\sum_{n\in\mathcal{I}_M(k)} \alpha_{\mathrm{S}} e^{-j\left(\frac{N-1}{2}-n\right)\frac{2\pi d}{\lambda}\cos\theta_{\mathrm{S}}} e^{j\left(\frac{N-1}{2}-n\right)\frac{2\pi d}{\lambda}\cos\theta_{\mathrm{S}}} \right.$$

$$+ \sum_{n\in\mathcal{I}_L(k)} \alpha_{\mathrm{S}} e^{-j\left(\frac{N-1}{2}-n\right)\frac{2\pi d}{\lambda}\cos\theta_{\mathrm{S}}} e^{j\left(\frac{N-1}{2}-n\right)\frac{2\pi d}{\lambda}\cos\theta_i}$$

$$+ \sum_{n\in\mathcal{I}_L(k)} \alpha_i e^{-j\left(\frac{N-1}{2}-n\right)\frac{2\pi d}{\lambda}\cos\theta_i} e^{j\left(\frac{N-1}{2}-n\right)\frac{2\pi d}{\lambda}\cos\theta_i}$$

$$\left. + \sum_{n\in\mathcal{I}_M(k)} \alpha_i e^{-j\left(\frac{N-1}{2}-n\right)\frac{2\pi d}{\lambda}\cos\theta_i} e^{j\left(\frac{N-1}{2}-n\right)\frac{2\pi d}{\lambda}\cos\theta_{\mathrm{S}}} \right)$$

$$+ z_{\mathrm{R}}(k)$$

$$= \underbrace{s(k)}_{\substack{\text{information} \\ \text{symbol}}} \underbrace{\frac{1}{\sqrt{LN}} \left(\alpha_{\mathrm{S}} M + \alpha_i (N - M) + \beta_{\mathrm{R}} \right)}_{\substack{\text{effective beamforming and} \\ \text{channel gain}}} + \underbrace{z_{\mathrm{R}}(k)}_{\substack{\text{additive} \\ \text{noise}}},$$

$$(12)$$

where β_{R} is given by

$$\beta_{\mathrm{R}} = \sum_{n\in\mathcal{I}_L(k)} \alpha_{\mathrm{S}} e^{j\left(\frac{N-1}{2}-n\right)\frac{2\pi d}{\lambda}(\cos\theta_i-\cos\theta_{\mathrm{S}})} +$$

$$\sum_{n\in\mathcal{I}_M(k)} \alpha_i e^{j\left(\frac{N-1}{2}-n\right)\frac{2\pi d}{\lambda}(\cos\theta_{\mathrm{S}}-\cos\theta_i)}. \quad (13)$$

Note β_{R} can be precalculated at the receiver since it has prior knowledge of the channel and the transmit antenna set along each path.

The eavesdropper can intercept the transmitted signal via the transmitter's side lobe or main lobe (this occurs when the eavesdropper is located along the the transmitter's main lobe). We will investigate these two scenarios separately. Assuming the eavesdropper can only intercept communication via the side lobe, the received signal at the eavesdropper along its

AoD $\theta_{\mathrm{E}} \notin \Phi$ is given by

$$
y_{\mathrm{E}}(k,\theta_{\mathrm{S}},\theta_i,\theta_{\mathrm{E}}) = \mathbf{h}^*\mathbf{f}(k)s(k) + z_{\mathrm{E}}(k) = \frac{1}{\sqrt{LN}}s(k)\alpha_{\mathrm{E}}\times
$$

$$
\left(\sum_{n\in\mathcal{I}_M(k)} e^{-j\left(\frac{N-1}{2}-n\right)\frac{2\pi d}{\lambda}\cos\theta_{\mathrm{E}}}e^{j\left(\frac{N-1}{2}-n\right)\frac{2\pi d}{\lambda}\cos\theta_{\mathrm{S}}} + \right.
$$

$$
\left. \sum_{n\in\mathcal{I}_L(k)} e^{-j\left(\frac{N-1}{2}-n\right)\frac{2\pi d}{\lambda}\cos\theta_{\mathrm{E}}}e^{j\left(\frac{N-1}{2}-n\right)\frac{2\pi d}{\lambda}\cos\theta_i} \right) + z_{\mathrm{E}}(k)
$$

$$
= \underbrace{s(k)}_{\substack{\text{information}\\\text{symbol}}} \quad \underbrace{\alpha_{\mathrm{E}}\beta_{\mathrm{E}}}_{\substack{\text{effective artificial}\\\text{noise}}} \quad + \underbrace{z(k)}_{\substack{\text{additive}\\\text{noise}}}, \tag{14}
$$

where the noise term β_{E} is given by

$$
\beta_{\mathrm{E}} = \frac{1}{\sqrt{LN}}\sum_{n\in\mathcal{I}_L(k)} e^{j\left(\frac{N-1}{2}-n\right)\frac{2\pi d}{\lambda}(\cos\theta_{\mathrm{S}}-\cos\theta_{\mathrm{E}})} +
$$

$$
\sum_{n\in\mathcal{I}_M(k)} e^{j\left(\frac{N-1}{2}-n\right)\frac{2\pi d}{\lambda}(\cos\theta_i-\cos\theta_{\mathrm{E}})}. \tag{15}
$$

From (15) we observe that the noise term β_{E} is random since the eavesdropper is unaware of the transmit angles θ_i and θ_s and the associated transmit antenna sets $\mathcal{I}_L(k)$ and $\mathcal{I}_M(k)$. This induces artificial noise that jams the eavesdropper. We also observe from (14) that high channel gain α_{E} increases the artificial noise at the eavesdropper, hence, no significant rate gain is expected with high channel gain.

Considering the second scenario, where we assume the eavesdropper can only intercept the communication link via the main lobe, the received signal at the eavesdropper along an AoD $\theta_{\mathrm{E}} = \theta_{\mathrm{S}}$ becomes

$$
y_{\mathrm{E}}(k,\theta_{\mathrm{S}},\theta_i,\theta_{\mathrm{E}}) = \mathbf{h}^*\mathbf{f}(k)s(k) + z_{\mathrm{E}}(k) = \frac{1}{\sqrt{LN}}s(k)\alpha_{\mathrm{E}}\times
$$

$$
\left(\sum_{n\in\mathcal{I}_M(k)} e^{-j\left(\frac{N-1}{2}-n\right)\frac{2\pi d}{\lambda}\cos\theta_{\mathrm{E}}}e^{j\left(\frac{N-1}{2}-n\right)\frac{2\pi d}{\lambda}\cos\theta_{\mathrm{S}}} + \right.
$$

$$
\left. \sum_{n\in\mathcal{I}_L(k)} e^{-j\left(\frac{N-1}{2}-n\right)\frac{2\pi d}{\lambda}\cos\theta_{\mathrm{E}}}e^{j\left(\frac{N-1}{2}-n\right)\frac{2\pi d}{\lambda}\cos\theta_i} \right) + z_{\mathrm{E}}(k)
$$

$$
= \underbrace{s(k)}_{\substack{\text{information}\\\text{symbol}}} \quad \underbrace{\frac{\alpha_{\mathrm{E}}\hat{\beta}_{\mathrm{E}}}{\sqrt{LN}}}_{\substack{\text{effective artificial}\\\text{noise}}} \quad + \underbrace{z_{\mathrm{E}}(k)}_{\substack{\text{additive}\\\text{noise}}}, \tag{16}
$$

where the noise term $\hat{\beta}_{\mathrm{E}}$ is given by

$$
\hat{\beta}_{\mathrm{E}} = \begin{cases} M + \sum_{n\in\mathcal{I}_L(k)} e^{-j\left(\frac{N-1}{2}-n\right)\gamma(\theta_i,\theta_{\mathrm{E}})}, & \text{if } \theta_{\mathrm{E}} = \theta_{\mathrm{S}} \\ N - M + \sum_{n\in\mathcal{I}_M(k)} e^{-j\left(\frac{N-1}{2}-n\right)\gamma(\theta_{\mathrm{S}},\theta_{\mathrm{E}})}, & \text{if } \theta_{\mathrm{E}} = \theta_i \end{cases} \tag{17}
$$

and $\gamma(\theta_x,\theta_{\mathrm{E}}) = \frac{2\pi d}{\lambda}(\cos\theta_x - \cos\theta_{\mathrm{E}})$. From (17) we observe that the noise term $\hat{\beta}_{\mathrm{E}}$ consists of a constant term and a random term (function of transmit antenna sets and AoD). Hence, to maintain the randomness of the term $\hat{\beta}_{\mathrm{E}}$ both transmit subsets should be sufficiently large. This maximizes the randomness of $\hat{\beta}_{\mathrm{E}}$ and, as a result, the artificial noise at the eavesdropper.

IV. PERFORMANCE EVALUATION

In this section, we evaluate the performance of the proposed transmission techniques in terms of the achievable secrecy rate R (bits/s/Hz). It is assumed that all communication takes place during a fixed coherence interval in which the channel is assumed to known to both the transmitter and target receiver. Furthermore, for ease of exposition, we take a pessimistic approach and assumed that the eavesdropper is aligned with one of the transmitter's L paths.

The secrecy rate R is defined as

$$
R = [\log_2(1 + \mathrm{SNR}_{\mathrm{R}}) - \log_2(1 + \mathrm{SNR}_{\mathrm{E}})]^+, \tag{18}
$$

where $\mathrm{SNR}_{\mathrm{R}}$ is the SNR at the target receiver, $\mathrm{SNR}_{\mathrm{E}}$ is the SNR at the eavesdropper, and a^+ denotes $\max\{0,a\}$. In the following, we derive the average SNR expressions for the proposed transmission techniques.

A. Random path selection

From (6), the SNR at the receiver can be expressed as

$$
\mathrm{SNR}_{\mathrm{R}} = \frac{(\mathbb{E}[\alpha_i\sqrt{N/L}])^2}{\sigma_{\mathrm{R}}^2} = \frac{N\bar{\alpha}^2}{L\sigma_{\mathrm{R}}^2} = \frac{N\rho_{\mathrm{R}}}{L}, \tag{19}
$$

where $\bar{\alpha}$ is the average channel gain of all transmit paths, and $\rho_{\mathrm{R}} = \frac{(\mathbb{E}[\alpha_i])^2}{\sigma_{\mathrm{R}}^2}$. From (19) we observe that the SNR at the target receiver deteriorates with increasing number of paths. This results as the total transmit power is spread among all L paths and weaker links will be utilized for transmission. However, as we will show in the derivation of the $\mathrm{SNR}_{\mathrm{E}}$ (see (20)), increasing the number of paths increases the artificial noise at the eavesdropper. Hence there is an optimal number of paths L that enhances the secrecy rate.

Similar to (19), the SNR at an eavesdropper can be expressed as (see (7))

$$
\mathrm{SNR}_{\mathrm{E}} = \frac{1}{L}\left(\frac{\alpha_{\mathrm{E}}^2 N}{L\sigma_{\mathrm{E}}^2}\right) + \left(1 - \frac{1}{L}\right)\left(\frac{\alpha_{\mathrm{E}}^2(\mathbb{E}[B(\theta_l)])^2/LN}{\alpha_{\mathrm{E}}^2\mathrm{var}[B(\theta_l)]/LN + \sigma_{\mathrm{E}}^2}\right)
$$

$$
= \frac{\rho_{\mathrm{E}}N}{L^2} + \left(1 - \frac{1}{L}\right)\left(\frac{\rho_{\mathrm{E}}(\mathbb{E}[B(\theta_l)])^2}{\rho_{\mathrm{E}}\mathrm{var}[B(\theta_l)] + LN}\right) \tag{20}
$$

where $\rho_{\mathrm{E}} = \frac{\alpha_{\mathrm{E}}^2}{\sigma_{\mathrm{E}}^2}$, $\mathrm{var}[\alpha_{\mathrm{E}}B(\theta_l)/\sqrt{LN}] = \alpha_{\mathrm{E}}^2/LN\mathrm{var}[B(\theta_l)]$ represents the artificial noise variance, $\theta_l \in \Phi$, and

$$
\mathbb{E}[B(\theta_l)] = \frac{N}{L}\sum_{l=1}^{L} \frac{\sin(N(\frac{\pi d}{\lambda}(\cos(\theta_{\mathrm{E}}) - \cos(\theta_l))))}{\sin((\frac{\pi d}{\lambda}(\cos(\theta_{\mathrm{E}}) - \cos(\theta_l))))}, \tag{21}
$$

and

$$
\mathrm{var}[B(\theta_l)] = \mathbb{E}[B(\theta_l)^2] - (\mathbb{E}[B(\theta_l)])^2. \tag{22}
$$

The first term of (20) captures the eavesdropper SNR when it is aligned with one of the transmitter's AoD, i.e., $\theta_{\mathrm{E}} = \theta_l$. This occurs with probability $1/L$ as it is assumed that θ_{E} overlaps with one of the receiver's AoDs, and there are a total of L AoDs. The second term of (20) captures the eavesdropper SNR when it is not aligned with the transmitter's AoD, i.e., $\theta_{\mathrm{E}} \neq \theta_l$. This occurs with probability $1 - 1/L$. It is not difficult to observe from (20) that the eavesdropper's SNR deteriorates with increasing number of transmission paths.
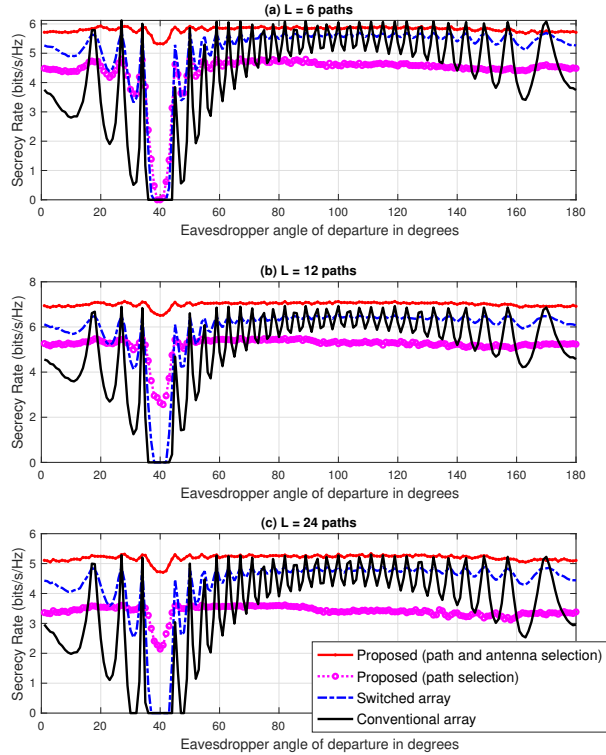
Figure 1. Secrecy rate versus the eavesdropper's angle of departure θ_E for different number of transmission paths; $N = 32$ transmit antennas, $\rho_R = 10$ dB, and $\rho_E = 15$ dB.

B. Joint path and antenna selection

Using (12), the SNR at the target receiver can be expressed as

$$
\text{SNR}_R = \frac{(\mathbb{E}[\alpha_s M + \alpha_i(N - M) + \beta_R])^2}{LN\sigma_R^2} \quad (23)
$$

$$
= \frac{\alpha_s^2 M^2}{LN\sigma_R^2} + \frac{(\bar{\bar{\alpha}}(N - M)^2}{LN\sigma_R^2} + \frac{(\mathbb{E}[\beta_R])^2}{LN\sigma_R^2}, \quad (24)
$$

where $\bar{\bar{\alpha}}$ is the average channel gain of all transmit paths, excluding the strongest path.

Similarly, using (14) and (16), the SNR at the eavesdropper can be expressed as

$$
\text{SNR}_E = \frac{2}{L}\left(\frac{\alpha_E^2(\mathbb{E}[\hat{\beta}_E])^2}{LN\sigma_E^2}\right) + \left(1 - \frac{2}{L}\right)\left(\frac{\alpha_E^2(\mathbb{E}[\beta_E])^2}{\alpha_E^2\text{var}[\beta_E] + LN\sigma_E^2}\right)
$$

$$
= \frac{2\rho_E(\mathbb{E}[\hat{\beta}_E])^2}{L^2 N} + \left(1 - \frac{2}{L}\right)\left(\frac{\rho_E(\mathbb{E}[\beta_E])^2}{\rho_E\text{var}[\beta_E] + LN}\right), \quad (25)
$$

where the expectation is over all transmit antennas and AoDs. The first term of (25) captures the eavesdropper SNR when it is aligned with one of the transmitter AoDs, i.e., $\theta_E = \theta_s$ or $\theta_E = \theta_i$, and $\theta_i, \theta_s \in \Phi$. This occurs with probability $2/L$. The second term of (25) captures the eavesdropper SNR when it is not aligned with the transmitter's AoD, i.e., $\theta_E \neq \theta_i, \theta_s$. This occurs with probability $1 - 2/L$. It is not difficult to see that $(\mathbb{E}[\hat{\beta}_E])^2 < N^2$ in (25), and hence the first SNR term is lower than the first SNR term in (20).
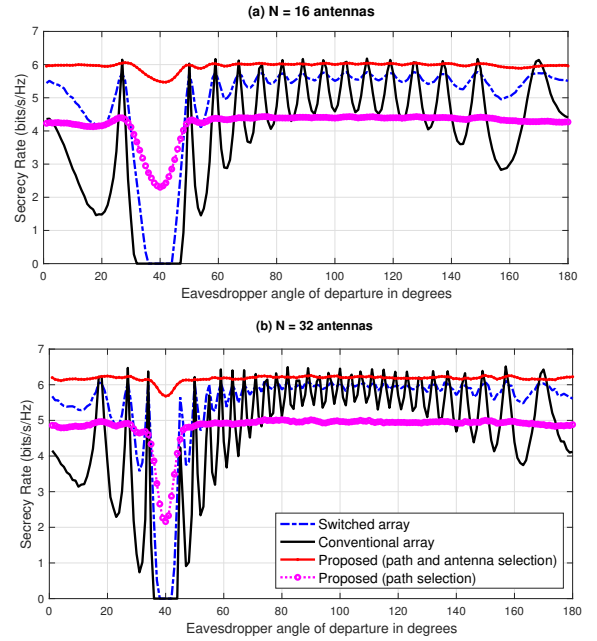

Figure 2. Secrecy rate versus the eavesdropper's angle of departure θ_E; $L = 12$ transmit path, $\rho_R = 10$ dB, and $\rho_E = 15$ dB.

V. NUMERICAL RESULTS AND DISCUSSIONS

In this section, we conduct numerical simulations to evaluate the efficacy of the proposed techniques. We consider a setup where a transmitter is communicating with a receiver in the presence of an eavesdropper. Both the transmitter and receiver are unaware of the eavesdropper's location. In this setup, the transmitter is equipped with a uniform linear array, with half wavelength separation, and the transmitter, receiver and eavesdropper have perfect knowledge of their channels. To benchmark the performance of the proposed techniques, we compare the secrecy rate achieved by the proposed techniques with the secrecy rate achieved when using conventional transmit antenna array, i.e., no action is taken at the transmitter, and the switched array technique proposed in [13] since it can be applied on analog antenna architectures. For all setups, we assume that the strongest transmit path to the target receiver is along a fixed AoD $\theta_R = 40$ degrees, i.e., $\theta_R = 40 \in \Phi$, and the remaining entries of Φ are randomly selected from the set $[1, 180]$ degrees. The channel gains are assumed to be normally distributed with zero mean and unit variance. Both the conventional array and switch antenna techniques always transmit along AoD $\theta_R = 40$ degrees. When simulating the joint angle and antenna selection techniques, we assume that the secondary link is selected from the set of $L_S = 5$ strongest paths and $M = N/2$.

To examine the performance of the proposed techniques, we plot the achievable secrecy rate when using the proposed techniques versus the eavesdropper AoD θ_E in Figure 1. For all cases, we observe that the secrecy rate is higher when the eavesdropper AoD θ_E does not overlap with the transmission AoD $\theta_R = 40$ degrees. However, when $\theta_E = 40$ degrees, i.e., the eavesdropper is located along one of the transmission path to the target receiver, we observe that all techniques suffer

a performance hit, with the conventional technique and the switched array technique achieving zero secrecy rate for all values of L. The proposed path selection technique is shown to achieve higher secrecy rate for higher number of paths while the proposed path and antenna selection technique achieves the best performance for all cases. The reason for this is that for low number of paths, the probability of intercepting a direct link when using the path selection technique is higher. This reduces the secrecy rate. The proposed path and antenna selection technique achieves the best performance as it randomizes both the transmit angle and antennas associated with each angle, thereby resulting in higher artificial noise at the eavesdropper.

In Figure 2, we examine the effect of the number of transmit antennas on the secrecy rate. For all techniques, we observe that increasing the number of antennas increases the secrecy rate and the proposed techniques achieve non-zero secrecy rates at $\theta_E = 40$ degrees. This is achieved as higher number of antennas result in narrower beams and increased number of sidelobes. The increased number of sidelobe levels increases the variance of the artificial noise. The path selection technique is shown to achieve lower secrecy rate when the eavesdropper is not located along the main transmission path $\theta_E \neq 40$ degrees. This rate loss is experienced as the path selection technique does not always use the best transmission path, but rather, it transmits along a set of paths, which contain weaker paths, to enhance the secrecy rate of the system.

To investigate the effect of the eavesdropper channel strength on the secrecy rate, we plot the secrecy rate versus the eavesdropper's average channel gain to noise ratio ρ_E when the eavesdropper is located along the transmitter's AoD $\theta_E = \theta_R = 40$ degrees in Figure 3, and when the eavesdropper is located along the transmitters sidelobe, i.e., $\theta_E \neq \theta_R$ in Figure 4. When the eavesdropper's communication link is weak, Figure 3 shows that all techniques achieve high secrecy rate. However, when the eavesdropper channel is stronger, the performance of both the switched-array and conventional array techniques plummet to zero, while the performance of the path selection technique deteriorates at a slower rate and the joint path and antenna selection technique deteriorates at a much slower rate as it achieves a higher artificial noise. When the eavesdropper is not located along the transmitter's AoD, Figure 4 shows that all techniques, except the conventional array technique, achieve high secrecy rate. The proposed joint path and antenna selection technique achieves the highest secrecy rate as it randomizes both the transmit AoD and transmit antenna sets, followed by the switched-array technique, and the proposed path selection technique. The path selection technique achieves a lower secrecy rate as it uses all paths (with potentially weaker paths) for communications, while the path and antenna selection technique always uses the strongest path and an auxiliary path for transmission. This results in a higher secrecy rate.

VI. CONCLUSION

This paper addressed the problem of PLS in the presence of an eavesdropper with overlapped channel paths with the target receiver. Two transmission techniques suitable for mmWave systems with analog antenna architectures are proposed. Both techniques use random transmission paths, instead of a single
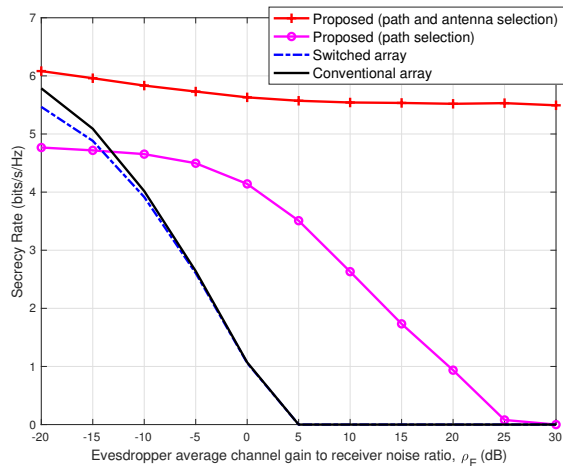

Figure 3. Secrecy rate versus ρ_E; $N = 32$ transmit antennas, $\rho_R = 10$ dB, and $L = 12$ paths. Eavesdropper is located along AoD $\theta_E = 40$ degrees.

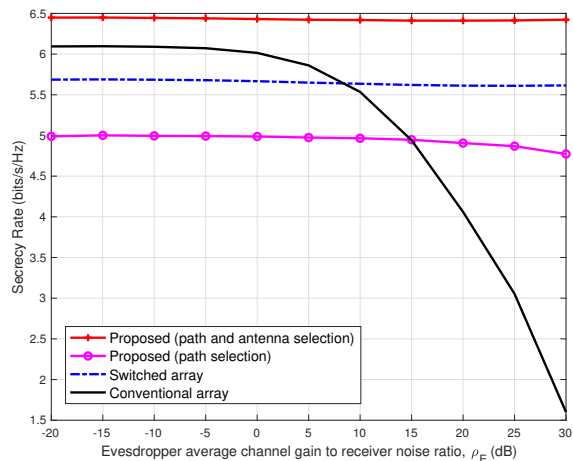

Figure 4. Secrecy rate versus ρ_E; $N = 32$ transmit antennas, $\rho_R = 10$ dB, and $L = 12$ paths. Eavesdropper is located along AoD $\theta_E = 55$ degrees.

or all paths, for data transmission. This results in noise-like signals at an arbitrary eavesdropper and improves the secrecy of the communication system. Numerical results show that in the presence of scatters, the proposed techniques achieve significantly higher secrecy rate when compared to conventional and switched array techniques. Note that the proposed techniques require the number of paths $L > 1$. For single path, i.e., LoS link, passive relays can be used to increase the number of transmission paths and induce randomness in the communication channel. Future work would focus on implementing a hardware prototype to investigate the efficacy of the proposed techniques.

REFERENCES

[1] F. Boccardi, R. Heath, A. Lozano, T. Marzetta, and P. Popovski, "Five disruptive technology directions for 5G," *IEEE Commun. Mag., vol. 52, no. 2, pp. 74-80, Feb. 2014.*

[2] Z. Pi and F. Khan, "An introduction to millimeter-wave mobile broadband systems", *IEEE Commun. Mag.,* vol. 49, no. 6, pp. 101-107, 2011.

[3] S. Pulipati et al., "Xilinx RF-SoC-based Digital Multi-Beam Array Processors for 28/60 GHz Wireless Testbeds," *2020 Moratuwa Engineering Research Conference (MERCon)*, Srilanka, Jul. 2020, pp. 1-6

[4] A. Alkhateeb, O. Ayach, and R. W. Heath Jr., "Channel estimation and hybrid precoding for millimeter wave cellular systems," *IEEE J. on Select. Areas in Commun.*, vol. 8, no. 5, pp. 831-846, Oct. 2014.

[5] M. E. Eltayeb, A. Alkhateeb, R. W. Heath Jr., and T. Y. Al-Naffouri, "Opportunistic Beam Training with Hybrid Analog/Digital Codebooks for mmWave Systems," *in IEEE Global Conference on Signal and Information Processing (GlobalSIP),* Dec. 2015, Orlando, Florida, USA.

[6] R. Khan, P. Kumar, D. N. K. Jayakody and M. Liyanage, "A Survey on Security and Privacy of 5G Technologies: Potential Solutions, Recent Advancements, and Future Directions," *in IEEE Communications Surveys & Tutorials,* vol. 22, no. 1, pp. 196-248, 2020.

[7] X. Wang et al., "Privacy-Preserving Content Dissemination for Vehicular Social Networks: Challenges and Solutions," *in IEEE Communications Surveys & Tutorials,* vol. 21, no. 2, pp. 1314-1345, 2019.

[8] M. E. Eltayeb, J. Choi, T. Y. Al-Naffouri, and R. W. Heath Jr., "Enhancing Secrecy With Multiantenna Transmission in Millimeter Wave Vehicular Communication Systems," *in IEEE Transactions on Vehicular Technology*, vol. 66, no. 9, pp. 8139-8151, Sept. 2017.

[9] A. N. Mohammed, M. E. Eltayeb, and I. Kostanic, "Channel Estimation in Millimeter Wave Systems with Inter Cell Interference," *in the 2019 IEEE 90th Vehicular Technology Conference,* Honolulu, HI, USA, 2019, pp. 1-5.

[10] H. M. Madni, M. S. Solaija, and H. Arslan, "Intelligent Physical Layer Security Approach for V2X Communication," arXiv:1905.05075, 2019.

[11] X. Sun, W. Yang, Y. Cai, L. Tao, and C. Cai, "Physical Layer Security in Wireless Information and Power Transfer Millimeter Wave Systems," *in the 2018 24th Asia-Pacific Conference on Communications (APCC),* Ningbo, China, 2018, pp. 83-87.

[12] 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 the 2016 IEEE 84th Vehicular Technology Conference*, Montreal, QC, 2016, pp. 1-5.

[13] N. Valliappan, A. Lozano, and R. W. Heath, "Antenna Subset Modu-lation for Secure Millimeter-Wave Wireless Communication," *in IEEE Transactions on Communications,* vol. 61, no. 8, pp. 3231-3245, August 2013.

[14] Y. Hong, X. Jing, and H. Gao, "Programmable Weight Phased-Array Transmission for Secure Millimeter-Wave Wireless Communications," *in IEEE Journal of Selected Topics in Signal Processing,* vol. 12, no. 2, pp. 399-413, May 2018.

[15] H. Jung and I. Lee, "Secrecy Rate of Analog Collaborative Beamforming With Virtual Antenna Array Following Spatial Random Distributions," *in IEEE Wireless Communications Letters,* vol. 7, no. 4, pp. 626-629, Aug. 2018.

[16] H. Jung and I. Lee, "Secrecy Performance Analysis of Analog Cooperative Beamforming in Three-Dimensional Gaussian Distributed Wireless Sensor Networks," *in IEEE Transactions on Wireless Communications,* vol. 18, no. 3, pp. 1860-1873, Mar. 2019.

[17] H. Jung and I. Lee, "Distributed Null-Steering Beamformer Design for Physical Layer Security Enhancement in Internet-of-Things Networks," *in IEEE Systems Journal*, doi: 10.1109/JSYST.2020.2967404.

[18] M. E. Eltayeb and R. W. Heath Jr., "Securing mmWave Vehicular Communication Links with Multiple Transmit Antennas," *in the 2018 IEEE International Conference on Communications Workshops (ICC Workshops)*, Kansas City, MO, 2018, pp. 1-6.

[19] Y. Hong, X. Jing, Y. He, and J. Mu, "Dynamic Rotated Angular Beamforming Using Frequency Diverse Phased-Array for Secure MmWave Wireless Communications," Electronics 2020.

[20] Y. Ju, H. Wang, T. Zheng, Q. Yin, and M. H. Lee, "Safeguarding Millimeter Wave Communications Against Randomly Located Eavesdroppers," *in IEEE Transactions on Wireless Communications,* vol. 17, no. 4, pp. 2675-2689, April 2018.

[21] Y. R. Ramadan and H. Minn, "Artificial Noise Aided Hybrid Precoding Design for Secure mmWave MISO Systems With Partial Channel Knowledge," *in IEEE Signal Processing Letters,* vol. 24, no. 11, pp. 1729-1733, Nov. 2017.

[22] P. Bahl and V. N. Padmanabhan, "RADAR: an in-building RF-based user location and tracking system," *in Proc. of the IEEE INFOCOM,* Mar. 2000, pp. 775-784.

[23] A. Alkhateeb, "DeepMIMO: A Generic Deep Learning Dataset for Millimeter Wave and Massive MIMO Applications", arXiv:1902.06435, Feb. 2019.

[24] V. Va, J. Choi, T. Shimizu, G. Bansal, and R. W. Heath, "Inverse Multipath Fingerprinting for Millimeter Wave V2I Beam Alignment," *in IEEE Transactions on Vehicular Technology,* vol. 67, no. 5, pp. 4042-4058, May 2018.