Artificial Noise Aided Hybrid Precoding Design for Secure mmWave MISO Systems With Partial Channel Knowledge

Yahia R. Ramadan, *Student Member, IEEE*, and Hlaing Minn, *Fellow, IEEE*

***Abstract*—In this letter, we propose a hybrid analog–digital precoder design to enhance the physical layer security of millimeter-wave (mmWave) multiple-input single-output (MISO) systems with partial channel knowledge. We derive a closed-form expression for the average signal-to-interference-and-noise ratio (SINR) of the eavesdropper (Eve) as a function of the hybrid precoder. Using the average SINRs of Eves, we derive a secrecy rate lower bound. Then, we propose a low-complexity artificial-noise-aided (AN-aided) hybrid precoder design to maximize the secrecy rate lower bound. Numerical results show that the proposed AN-aided hybrid precoder achieves comparable performance to that of the fully digital precoder, with much lower hardware complexity. Moreover, the proposed AN-aided hybrid precoder outperforms the existing hybrid precoder design. Effect of finite-resolution phase shifters on the proposed precoder is also investigated.**

***Index Terms*—Artificial noise (AN), hybrid precoding, millimeter-wave (mmWave), partial channel knowledge, physical layer security.**

I. Introduction

Physical layer security is typically introduced by precoding schemes at the transmitter (Alice). For millimeter-wave (mmWave) communications [1], some of existing works consider radio-frequency (RF) precoding with a single RF chain in line-of-sight (LOS) channels [2]–[4] or non-line-of-sight (NLOS) channels [5]. The works in [6]–[8] apply secure baseband precoding with full RF chains. For mmWave systems, hybrid analog-digital precoders are preferred due to the hardware complexity and power consumption concern [9]. Secure hybrid precoding schemes are developed in [10]–[13]. The work in [10] relies on the beamforming strategy with no artificial noise (AN) which results in secrecy performance degradation at moderate and high signal-to-noise ratios (SNRs). The works in [11]–[13] develop an AN-aided hybrid precoder. However, the optimal power allocation between the confidential signal and AN was not considered in [11], but addressed in [12] when the number of RF chains is greater than the number of antennas of Eve for Rayleigh fading channels and in [13] for mmWave LOS channels. Moreover, [11] and [12] consider only the case that Alice does not have any knowledge of the channels to Eves. For cellular systems, base station (Alice) may know the directional information of other active users (Eves) and exploiting such partial channel knowledge to enhance secure communication is much desirable. To the best of our knowledge, secure AN-aided hybrid precoding for mmWave NLOS systems with partial channel knowledge has not been developed in the literature.

In this letter, we propose an AN-aided hybrid precoder design to maximize the average secrecy rate with partial channel knowledge. We derive a closed-form expression for the average signal-to-interference-and-noise ratio (SINR) of Eve as a function of the hybrid precoder. Using the average SINRs of Eves, we obtain a secrecy rate lower bound. Since the hybrid precoder design problem is non-convex, we propose a suboptimal solution. Numerical results show that the proposed AN-aided hybrid precoder achieves comparable performance to that of the fully digital precoder, with much lower hardware complexity. Moreover, the proposed AN-aided hybrid precoder outperforms the maximum-ratio-transmission (MRT) hybrid precoder of [14].

We use the following notation: $\mathbf{A}$ is a matrix, $\|\mathbf{A}\|_{\mathrm{F}}$ is its Frobenius norm, and $\mathrm{Tr}\left[\mathbf{A}\right]$ is its trace. $\mathbf{a}$ is a vector, and $\|\mathbf{a}\|$ is its $l2$-norm. a is a scalar. $(\cdot)^T$ and $(\cdot)^H$ are the transpose and conjugate transpose operators. $\mathbf{I}_N$ is the identity matrix of order N. $\boldsymbol{\mathcal{E}}_{\max}\left[\mathbf{A}\right]$ is the principal eigenvector of $\mathbf{A}$, while $\boldsymbol{\mathcal{E}}_{1:\mathrm{N}}\left[\mathbf{A}\right]$ is the first N principal eigenvectors of $\mathbf{A}$. $\mathrm{diag}\left(a_1, a_2, \ldots, a_N\right)$ returns the diagonal concatenation, while $\mathrm{blkdiag}\left(\mathbf{A}_1, \mathbf{A}_2, \ldots, \mathbf{A}_N\right)$ returns the block diagonal concatenation. $\mathbb{P}\left(x\right)$ and $\mathbb{E}\left(x\right)$ denote the probability and expectation of x. $\mathbf{x} \sim \mathcal{CN}\left(0, \Sigma\right)$ means that $\mathbf{x}$ is a circularly-symmetric complex Gaussian random vector with zero mean and covariance matrix Σ. $[\mathbf{a}]_i$ is the $i\mathrm{th}$ element of $\mathbf{a}$, while $[\mathbf{a}]_{(i:j)}$ consists of the $i\mathrm{th}$ to the $j\mathrm{th}$ elements of $\mathbf{a}$.

II. System and Channel Models

A. System Model

We consider a secrecy mmWave MISO system with K single-antenna receivers. The transmitter (Alice) sends a confidential message to the first receiver (Bob), while the rest $K-1$ receivers are eavesdroppers (Eves). Alice is equipped with a large-scale uniform linear array with N_{T} antennas $\left(N_{\mathrm{T}} \gg K\right)$. The spacing between antennas is half the wavelength. To reduce the hardware complexity and the power consumption, the antenna array is connected via an analog RF precoder to N_{RF} RF chains $\left(N_{\mathrm{RF}} < N_{\mathrm{T}}\right)$, which process the digitally precoded streams.

We consider a narrow-band transmission, where the received signal y_k at the $k\mathrm{th}$ receiver is given by

$$y_k = \mathbf{h}_k \mathbf{x} + n_k, \tag{1}$$

where $\mathbf{h}_k \in \mathbb{C}^{1\times N_{\mathrm{T}}}$ is the mmWave channel to the $k\mathrm{th}$ receiver, $n_k \sim \mathcal{CN}(0, \sigma^2)$ is the additive white complex Gaussian noise with zero mean and variance σ^2 at the $k\mathrm{th}$ receiver, and $\mathbf{x} \in$

Manuscript received August 10, 2017; accepted September 4, 2017. Date of publication September 11, 2017; date of current version October 11, 2017. The associate editor coordinating the review of this manuscript and approving it for publication was Prof. Yong Xiang. *(Corresponding author: Yahia R. Ramadan.)*

Y. R. Ramadan and H. Minn are with the Department of Electrical and Computer Engineering, University of Texas at Dallas, Richardson, TX 75080 USA (e-mail: yahia.ramadan@utdallas.edu; hlaing.minn@utdallas.edu).

Color versions of one or more of the figures in this letter are available online at http://ieeexplore.ieee.org.

Digital Object Identifier 10.1109/LSP.2017.2751459

$\mathbb{C}^{N_\mathrm{T}\times 1}$ is the transmit signal vector given by

$$\mathbf{x} = \sqrt{\phi}\,\mathbf{F}_\mathrm{RF}\mathbf{f}_\mathrm{BB}s + \sqrt{1-\phi}\,\mathbf{F}_\mathrm{RF}\mathbf{U}_\mathrm{BB}\mathbf{z}, \tag{2}$$

where ϕ is the power fraction allocated to the confidential signal, $(1-\phi)$ is the power fraction allocated to AN, $\mathbf{F}_\mathrm{RF} \in \mathbb{C}^{N_\mathrm{T}\times N_\mathrm{RF}}$ is the analog RF precoder, $s \sim \mathcal{CN}(0, P)$ is the coded confidential signal, $\mathbf{f}_\mathrm{BB} \in \mathbb{C}^{N_\mathrm{RF}\times 1}$ is the signal digital baseband precoder, $\mathbf{z} \sim \mathcal{CN}(0, P\mathbf{I}_{N_\mathrm{RF}})$ is the noise vector artificially generated by Alice, and $\mathbf{U}_\mathrm{BB} \in \mathbb{C}^{N_\mathrm{RF}\times N_\mathrm{RF}}$ is the AN digital baseband precoder. To maintain the power constraint $\mathbb{E}\{\mathbf{x}^H\mathbf{x}\} = P$, where P is the transmit power, we should have $\|\mathbf{F}_\mathrm{RF}\mathbf{f}_\mathrm{BB}\|^2 = \|\mathbf{F}_\mathrm{RF}\mathbf{U}_\mathrm{BB}\|_\mathrm{F}^2 = 1$. Using (1) and (2), the achievable rate R_k of the kth receiver is given by

$$R_k = \log_2\left(1 + \frac{\phi\gamma\left|\mathbf{h}_k\mathbf{F}_\mathrm{RF}\mathbf{f}_\mathrm{BB}\right|^2}{(1-\phi)\,\gamma\left\|\mathbf{h}_k\mathbf{F}_\mathrm{RF}\mathbf{U}_\mathrm{BB}\right\|^2 + 1}\right), \tag{3}$$

where $\gamma = P/\sigma^2$ is the transmit signal-to-noise ratio (SNR). The average secrecy rate $\bar{R}_\mathrm{sec}$ is given by [15]

$$\bar{R}_\mathrm{sec} = \mathbb{E}\left\{R_1 - \max_k\{R_k\}_{k=2}^K\right\}, \tag{4}$$

where the expectation is performed over the channels to Bob and Eves.

The RF precoder $\mathbf{F}_\mathrm{RF}$ is usually implemented using analog phase shifters. We consider the subarray structure [14], where each RF chain is connected to $\frac{N_\mathrm{T}}{N_\mathrm{RF}}$ antennas via analog phase shifters. Therefore, $\mathbf{F}_\mathrm{RF}$ has to be expressed as $\mathbf{F}_\mathrm{RF} = \mathrm{blkdiag}\left(\mathbf{f}_{\mathrm{RF},1}, \mathbf{f}_{\mathrm{RF},2}, \ldots, \mathbf{f}_{\mathrm{RF},N_\mathrm{RF}}\right)$, where $\mathbf{f}_{\mathrm{RF},r} \in \mathbb{C}^{\frac{N_\mathrm{T}}{N_\mathrm{RF}}\times 1}$ $\forall r \in \{1, 2, \ldots, N_\mathrm{RF}\}$ and $|[\mathbf{f}_{\mathrm{RF},r}]_m| = \frac{1}{\sqrt{N_\mathrm{T}/N_\mathrm{RF}}}$ $\forall r, m$ [14]. Therefore, we have $\mathbf{F}_\mathrm{RF}^H\mathbf{F}_\mathrm{RF} = \mathbf{I}_{N_\mathrm{RF}}$. Moreover, the power constraint is reduced to $\|\mathbf{f}_\mathrm{BB}\|^2 = \|\mathbf{U}_\mathrm{BB}\|_\mathrm{F}^2 = 1$. Let $\mathcal{F}_\mathrm{RF}$ be the set of analog RF precoders satisfying the constraints of subarray structure, then we should have $\mathbf{F}_\mathrm{RF} \in \mathcal{F}_\mathrm{RF}$.

B. Channel Model

mmWave channels are expected to have limited scattering [16], [17]. We adopt a sparse geometric multipath channel model where the channel vector $\mathbf{h}_k$ to the kth user is given by

$$\mathbf{h}_k = \sqrt{\frac{N_\mathrm{T}}{L}}\sum_{l=1}^{L}\alpha_{l,k}\mathbf{a}_{l,k}^H, \tag{5}$$

where L is the number of propagation paths, $\alpha_{l,k}$ is the complex channel gain of the lth path to the kth user, $\mathbf{a}_{l,k}$ is the transmit steering vector of the lth path to the kth user with azimuth angle of departure (AoD) of $\varphi_{l,k}$, and

$$\mathbf{a}_{l,k} = \frac{1}{\sqrt{N_\mathrm{T}}}\left[1, e^{-j\pi\cos(\varphi_{l,k})}, \ldots, e^{-j\pi(N_\mathrm{T}-1)\cos(\varphi_{l,k})}\right]^T. \tag{6}$$

Denoted by $\mathbf{A}_{\mathrm{T},k} \in \mathbb{C}^{N_\mathrm{T}\times L}$, the transmit array response matrix to the kth receiver is given by $\mathbf{A}_{\mathrm{T},k} = [\mathbf{a}_{1,k}, \mathbf{a}_{2,k}, \ldots, \mathbf{a}_{L,k}]$. Since each resolvable path consists of several paths, similar to [6, Sec. II-B] and [18, Sec. III-E], the channel gains $\{\alpha_{l,k}\}$ are assumed to be independent complex Gaussian random variables with zero mean and unit variance.

III. AN-Aided Hybrid Precoding Design

We design the hybrid precoder to maximize the average secrecy rate $\bar{R}_\mathrm{sec}$ for a given transmit SNR γ. We assume that Alice has full knowledge of the channel to Bob but has partial knowledge of the channels to Eves. Similar to [5], [6], and [10], Alice has knowledge only of the AoDs of the paths to Eves. Bob and Eves have full knowledge of their channels to Alice. These assumptions become realistic if Eves are active nodes, which have communicated with Alice [19]–[24]. We also assume that Eves do not cooperate.

With full knowledge of the channel to Bob and partial knowledge of the channels to Eves, maximizing the secrecy rate R_sec given by

$$R_\mathrm{sec} = R_1 - \mathbb{E}\left\{\max_k\{R_k\}_{k=2}^K\right\}, \tag{7}$$

where the expectation is performed over the unknown channel gains of Eves, is equivalent to maximizing the average secrecy rate $\bar{R}_\mathrm{sec}$ [25]. Since it is difficult to get R_sec in a closed form, we derive a secrecy rate lower bound $\tilde{R}_\mathrm{sec}$ as

$$\begin{aligned} R_\mathrm{sec} &= R_1 - \mathbb{E}\left\{\log_2\left(1 + \max_k\{\mathrm{SINR}_k\}_{k=2}^K\right)\right\} \\ &\geq R_1 - \log_2\left(1 + \mathbb{E}\left\{\max_k\{\mathrm{SINR}_k\}_{k=2}^K\right\}\right) \\ &\geq R_1 - \log_2\left(1 + \sum_{k=2}^{K}\mathbb{E}\left\{\mathrm{SINR}_k\right\}\right) \triangleq \tilde{R}_\mathrm{sec}, \end{aligned} \tag{8}$$

where $\mathbb{E}\{\mathrm{SINR}_k\} = \mathbb{E}\{\frac{\gamma\phi|\mathbf{h}_k\mathbf{F}_\mathrm{RF}\mathbf{f}_\mathrm{BB}|^2}{\gamma(1-\phi)\|\mathbf{h}_k\mathbf{F}_\mathrm{RF}\mathbf{U}_\mathrm{BB}\|^2+1}\}$ is the average SINR of the kth receiver; the first inequality holds due to Jensen's inequality, and the second inequality holds since $\max_k\{x_k\}_{k=2}^K \leq \sum_{k=2}^K x_k$. We need to evaluate $\mathbb{E}\{\mathrm{SINR}_k\}$ to get $\tilde{R}_\mathrm{sec}$. It can be rewritten as

$$\mathbb{E}\left\{\mathrm{SINR}_k\right\} = \mathbb{E}\left[\frac{\phi\boldsymbol{\alpha}_k^H\mathbf{A}_k\boldsymbol{\alpha}_k}{(1-\phi)\,\boldsymbol{\alpha}_k^H\mathbf{B}_k\boldsymbol{\alpha}_k + \delta}\right], \tag{9}$$

where $\boldsymbol{\alpha}_k = [\alpha_{1,k}, \alpha_{2,k}, \ldots, \alpha_{L,k}]^T$, $\mathbf{A}_k = \mathbf{A}_{\mathrm{T},k}^H\mathbf{F}_\mathrm{RF}\mathbf{f}_\mathrm{BB}\mathbf{f}_\mathrm{BB}^H\mathbf{F}_\mathrm{RF}^H\mathbf{A}_{\mathrm{T},k}$, $\mathbf{B}_k = \mathbf{A}_{\mathrm{T},k}^H\mathbf{F}_\mathrm{RF}\mathbf{U}_\mathrm{BB}\mathbf{U}_\mathrm{BB}^H\mathbf{F}_\mathrm{RF}^H\mathbf{A}_{\mathrm{T},k}$, and $\delta = \frac{L}{\gamma N_\mathrm{T}}$. We can notice that $\mathbb{E}\{\mathrm{SINR}_k\}$ in (9) is the expected value of a ratio of quadratic forms of $\boldsymbol{\alpha}_k$. Moreover, $\boldsymbol{\alpha}_k$ is a circularly symmetric complex Gaussian random vector with a probability density function (PDF) $f_{\boldsymbol{\alpha}_k}(\boldsymbol{\alpha}_k)$ given by [26]

$$f_{\boldsymbol{\alpha}_k}(\boldsymbol{\alpha}_k) = \pi^{-L}e^{-\boldsymbol{\alpha}_k^H\boldsymbol{\alpha}_k}. \tag{10}$$

Let w_1 and w_2 be two random variables such that $\mathbb{P}(w_2 > 0) = 1$. In [27], it was shown that

$$\mathbb{E}\left[\frac{w_1}{w_2}\right] = \int_0^\infty\left[\frac{\partial}{\partial s}M_{w_1,w_2}(s, -r)\right]_{s=0}dr, \tag{11}$$

where $M_{w_1,w_2}(s, r)$ is the joint moment generating function of w_1 and w_2. Define $w_1 = \phi\boldsymbol{\alpha}_k^H\mathbf{A}_k\boldsymbol{\alpha}_k$ and $w_2 = (1-\phi)\boldsymbol{\alpha}_k^H\mathbf{B}_k\boldsymbol{\alpha}_k + \delta$. Then, we obtain $M_{w_1,w_2}(s, -r)$ as in (12) shown at the bottom of the next page. Therefore, we get

$$\begin{aligned} \mathbb{E}\left\{\mathrm{SINR}_k\right\} &= \int_0^\infty\left[\frac{\partial}{\partial s}M_{w_1,w_2}(s, -r)\right]_{s=0}dr \\ &= \int_0^\infty e^{-\delta r}\left|\mathbf{I}_L + (1-\phi)\,\mathbf{B}_k r\right|^{-1} \\ &\quad\times \mathrm{Tr}\left[\left(\mathbf{I}_L + (1-\phi)\,\mathbf{B}_k r\right)^{-1}\phi\mathbf{A}_k\right]dr, \end{aligned} \tag{13}$$

which can be simplified to (14) shown at the bottom of this page, where $\{\lambda_{k,l}\}_{l=1}^{L}$ and $\mathbf{U}_k \in \mathbb{C}^{L\times L}$ are the eigenvalues and the eigenvectors matrix of $\mathbf{B}_k$, respectively, and the integral $I_{k,l}$ in (14) is obtained in a closed form in the appendix. Therefore, we can write $\tilde{R}_{\rm sec}$ in a closed form.

Using the secrecy rate lower bound $\tilde{R}_{\rm sec}$, the AN-aided hybrid precoder design problem is expressed as

$$\max_{\phi,\mathbf{F}_{\rm RF},\mathbf{f}_{\rm BB},\mathbf{U}_{\rm BB}} \tilde{R}_{\rm sec},$$
$$\text{s.t. } \mathbf{F}_{\rm RF}\in\mathcal{F}_{\rm RF},\ 0\le\phi\le 1, \|\mathbf{f}_{\rm BB}\|^2=1,\ \|\mathbf{U}_{\rm BB}\|_{\rm F}^2=1. \tag{15}$$

The optimization problem in (15) is nonconvex since the objective function and the RF precoder constraint are nonconvex. Therefore, we propose a suboptimal AN-aided hybrid precoder design to maximize the secrecy rate lower bound $\tilde{R}_{\rm sec}$. To get an efficient solution and decouple the hybrid precoder and the power fraction ϕ designs, we put $\phi = 1$ (no AN) and design the hybrid precoder. Then, we get ϕ maximizing $\tilde{R}_{\rm sec}$ by any efficient one-dimensional (1-D) search.

With $\phi = 1$ (no AN), $\mathbb{E}\{\text{SINR}_k\}$ in (14) is simplified to

$$\mathbb{E}\{\text{SINR}_k\} = \frac{\gamma N_{\rm T}}{L}\left\|\mathbf{A}_{{\rm T},k}^H\mathbf{F}_{\rm RF}\mathbf{f}_{\rm BB}\right\|^2. \tag{16}$$

Therefore, $\tilde{R}_{\rm sec}$ in (8) can be written while applying the power constraint $\|\mathbf{f}_{\rm BB}\|^2 = 1$ as

$$\tilde{R}_{\rm sec} = \log_2\left(\frac{\mathbf{f}_{\rm BB}^H\left(\mathbf{I}_{N_{\rm RF}}+\gamma\mathbf{F}_{\rm RF}^H\mathbf{h}_1^H\mathbf{h}_1\mathbf{F}_{\rm RF}\right)\mathbf{f}_{\rm BB}}{\mathbf{f}_{\rm BB}^H\left(\mathbf{I}_{N_{\rm RF}}+\frac{\gamma N_{\rm T}}{L}\sum_{k=2}^{K}\mathbf{F}_{\rm RF}^H\mathbf{A}_{{\rm T},k}\mathbf{A}_{{\rm T},k}^H\mathbf{F}_{\rm RF}\right)\mathbf{f}_{\rm BB}}\right). \tag{17}$$

Using the generalized eigenvector decomposition, we obtain $\mathbf{f}_{\rm BB}$ maximizing (17) as a function of $\mathbf{F}_{\rm RF}$ as

$$\mathbf{f}_{\rm BB} = \boldsymbol{\mathcal{E}}_{\max}\left[\left(\mathbf{I}_{N_{\rm RF}}+\frac{\gamma N_{\rm T}}{L}\sum_{k=2}^{K}\mathbf{F}_{\rm RF}^H\mathbf{A}_{{\rm T},k}\mathbf{A}_{{\rm T},k}^H\mathbf{F}_{\rm RF}\right)^{-1} \times\left(\mathbf{I}_{N_{\rm RF}}+\gamma\mathbf{F}_{\rm RF}^H\mathbf{h}_1^H\mathbf{h}_1\mathbf{F}_{\rm RF}\right)\right]. \tag{18}$$

If a fully digital precoder $\mathbf{f}_{\rm FD}$ (i.e., $\mathbf{F}_{\rm RF} = \mathbf{I}_{N_{\rm T}}$) was used, (18) would be written as

$$\mathbf{f}_{\rm FD} = \boldsymbol{\mathcal{E}}_{\max}\left[\left(\mathbf{I}_{N_{\rm T}}+\frac{\gamma N_{\rm T}}{L}\sum_{k=2}^{K}\mathbf{A}_{{\rm T},k}\mathbf{A}_{{\rm T},k}^H\right)^{-1} \times\left(\mathbf{I}_{N_{\rm T}}+\gamma\mathbf{h}_1^H\mathbf{h}_1\right)\right]. \tag{19}$$

We propose to obtain the RF precoder $\mathbf{F}_{\rm RF}$ as

$$\mathbf{f}_{{\rm RF},r} = \frac{1}{\sqrt{N_{\rm T}/N_{\rm RF}}}\exp\left(j\angle\left[\mathbf{f}_{\rm FD}\right]_{(r-1)\frac{N_{\rm T}}{N_{\rm RF}}+1:r\frac{N_{\rm T}}{N_{\rm RF}}}\right)\forall r, \tag{20}$$

which satisfies the constraints of the subarray structure and is a good approximation to $\mathbf{f}_{\rm FD}$.

Now, we design the AN baseband precoder $\mathbf{U}_{\rm BB}$ to be in the null space of the equivalent channel to Bob $\hat{\mathbf{h}}_1 = \mathbf{h}_1\mathbf{F}_{\rm RF}$ and directed to Eves as

$$\mathbf{U}_{\rm BB} = \Pi_{\hat{\mathbf{h}}_1}\mathbf{V}/\left\|\Pi_{\hat{\mathbf{h}}_1}\mathbf{V}\right\|_{\rm F}, \tag{21}$$

where $\Pi_{\hat{\mathbf{h}}_1} = (\mathbf{I}_{N_{\rm RF}} - \hat{\mathbf{h}}_1^H(\hat{\mathbf{h}}_1\hat{\mathbf{h}}_1^H)^{-1}\hat{\mathbf{h}}_1) \in \mathbb{C}^{N_{\rm RF}\times N_{\rm RF}}$ is the orthogonal complement projector of $\hat{\mathbf{h}}_1$, and $\mathbf{V} = \boldsymbol{\mathcal{E}}_{1:\min(N_{\rm RF},(K-1)L)}[\Pi_{\hat{\mathbf{h}}_1}^H\mathbf{F}_{\rm RF}^H\mathbf{A}_{\rm T,Eves}\mathbf{A}_{\rm T,Eves}^H\mathbf{F}_{\rm RF}\Pi_{\hat{\mathbf{h}}_1}]$, where $\mathbf{A}_{\rm T,Eves} = [\mathbf{A}_{\rm T,2}, \mathbf{A}_{\rm T,3}, \ldots, \mathbf{A}_{{\rm T},K}] \in \mathbb{C}^{N_{\rm T}\times(K-1)L}$. Note that $\mathbf{U}_{\rm BB}$ is normalized to satisfy the power constraint $\|\mathbf{U}_{\rm BB}\|_{\rm F}^2 = 1$. Finally, we obtain the power fraction ϕ by any efficient 1-D search (e.g., golden section search) as

$$\phi = \arg\max_{\phi} \tilde{R}_{\rm sec},\ \text{s.t. } 0\le\phi\le 1, \tag{22}$$

where $\tilde{R}_{\rm sec}$ is given by (8) using $\mathbb{E}\{\text{SINR}_k\}$ in (14). The computational complexity of the proposed AN-aided hybrid precoder is $\mathcal{O}(N_{\rm T}^3 + N_{\rm T}^2KL + N_{\rm RF}^3 + KL^3)$.

IV. Numerical Results

We assume that Alice has 32 antennas and 4 RF chains. All channels follow the mmWave channel model described in Section II-B with six propagation paths, and the angles of departure $\{\varphi_{l,k}\}$ are uniformly distributed within $[0\ 2\pi)$. We consider four baseline algorithms. The first algorithm is the MRT hybrid precoder of [14], which designs the hybrid precoder to maximize the rate of Bob while ignoring Eves. The second baseline algorithm (denoted by "Reduced Fully Digital Precoder") applies random antenna selection for each RF chain from its own

$$M_{w_1,w_2}(s,-r) = \int_{-\infty}^{\infty}\pi^{-L}e^{-\boldsymbol{\alpha}_k^H\boldsymbol{\alpha}_k}e^{\phi\boldsymbol{\alpha}_k^H\mathbf{A}_k\boldsymbol{\alpha}_k s-(1-\phi)\boldsymbol{\alpha}_k^H\mathbf{B}_k\boldsymbol{\alpha}_k r-\delta r}d\boldsymbol{\alpha}_k$$
$$= \frac{e^{-\delta r}}{|\mathbf{I}_L-\phi\mathbf{A}_k s+(1-\phi)\mathbf{B}_k r|}\underbrace{\int_{-\infty}^{\infty}\pi^{-L}|\mathbf{I}_L-\phi\mathbf{A}_k s+(1-\phi)\mathbf{B}_k r|e^{-\boldsymbol{\alpha}_k^H(\mathbf{I}_L-\phi\mathbf{A}_k s+(1-\phi)\mathbf{B}_k r)\boldsymbol{\alpha}_k}d\boldsymbol{\alpha}_k}_{=1\text{ (area under PDF)}}. \tag{12}$$

$$\mathbb{E}\{\text{SINR}_k\} = \mathbf{f}_{\rm BB}^H\mathbf{F}_{\rm RF}^H\mathbf{A}_{{\rm T},k}\mathbf{U}_k\text{diag}\left(\left\{\underbrace{\int_0^{\infty}\frac{\phi e^{-\delta r}dr}{(1+(1-\phi)\lambda_{k,l}r)\prod_{m=1}^{L}(1+(1-\phi)\lambda_{k,m}r)}}_{=I_{k,l}\text{ (obtained in a closed form in the appendix)}}\right\}_{l=1}^{L}\right)\mathbf{U}_k^H\mathbf{A}_{{\rm T},k}^H\mathbf{F}_{\rm RF}\mathbf{f}_{\rm BB}. \tag{14}$$

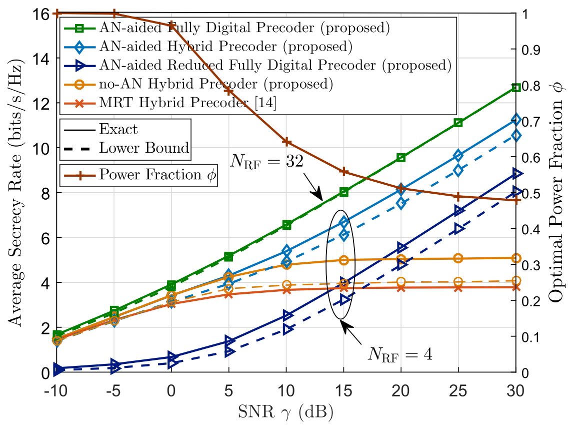

Fig. 1. Achievable average secrecy rate $\bar{R}_{\rm sec}$ and optimal power fraction ϕ with four Eves ($K = 5$).

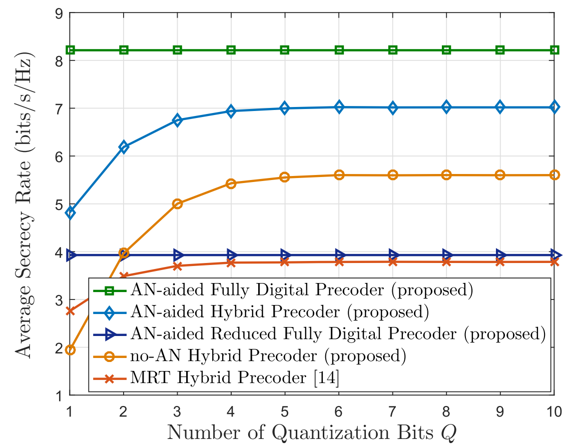

Fig. 2. Effect of finite-resolution phase shifters on the average secrecy rate $\bar{R}_{\rm sec}$ with four Eves ($K = 5$) and transmit SNR $\gamma = 15$ dB.

antenna subset and performs the proposed AN-aided digital precoding (i.e., $N_{\rm T} = N_{\rm RF} = 4$). The third baseline algorithm is the no-AN hybrid precoder which is based on the proposed hybrid precoder with no AN. The fourth baseline algorithm (denoted by "Fully Digital Precoder") is the fully digital precoder that applies the proposed AN-aided precoding with full RF chains (i.e., $N_{\rm T} = N_{\rm RF} = 32$). Note that the first, second, and third baseline algorithms are expected to be performance lower bounds, whereas the fourth baseline algorithm is expected to be a performance upper bound.

Fig. 1 shows the achievable average secrecy rate (left y-axis) and the optimal power fraction ϕ (right y-axis) as a function of the transmit SNR γ with four Eves ($K = 5$). As expected, the AN-aided fully digital precoding achieves the highest average secrecy rate due to the use of one RF chain per antenna (very large hardware complexity). The proposed AN-aided hybrid precoder achieves comparable performance to that of the AN-aided fully digital precoder, with much lower hardware complexity (only four RF chains are used). The performance loss is due to the modulus constraint and the limited number of RF chains. The proposed AN-aided hybrid precoder outperforms the AN-aided reduced fully digital precoder, which verifies the effectiveness of the proposed RF precoder design. The SNR gap between the proposed AN-aided hybrid precoder and the AN-aided reduced fully digital precoder is about 7.5 dB at high transmit SNRs. We also observe that the derived secrecy rate lower bound predicts the performance behavior efficiently. The MRT hybrid precoder achieves the worst average secrecy rate at moderate and high transmit SNRs due to ignoring Eves. At low transmit SNRs, the optimal power fraction ϕ is approximately 1 (no AN) that is why the proposed AN-aided hybrid precoder and the no-AN hybrid precoder have approximately the same performance at low transmit SNRs. As transmit SNR increases, the optimal power fraction ϕ decreases, which means allocating more power to the AN. That is why the performance of no-AN hybrid precoder degrades significantly at moderate and high transmit SNRs. On the contrary, the secrecy rate achieved by the proposed AN-aided hybrid precoder linearly increases with transmit SNR, thanks to the optimal power allocation to AN. The same above performance behavior is observed when increasing the number of Eves.

With finite-resolution phase shifters, Fig. 2 shows the achievable average secrecy rate versus different numbers of quantization bits for the phase shifters with four Eves ($K = 5$) and transmit SNR $\gamma = 15$ dB. After designing the RF precoder, the phases of the RF precoder are quantized into Q bits such that $\angle[\mathbf{f}_{{\rm RF},r}]_m \in \{0, \frac{2\pi}{2^Q}, \ldots, \frac{2\pi 2^{Q-1}}{2^Q}\}\forall r, m$. We observe that four quantization bits are sufficient for the proposed AN-aided hybrid precoder with secrecy rate loss less than 0.01 bits/s/Hz. With the same number of quantization bits, the proposed AN-aided hybrid precoder outperforms the other hybrid precoders.

V. Conclusion

We proposed an AN-aided hybrid precoder design to enhance the physical layer security. The proposed AN-aided hybrid precoder achieves comparable secrecy rate to that of the fully digital precoder, with much lower hardware complexity. Moreover, the proposed AN-aided hybrid precoder outperforms the conventional MRT hybrid precoder. With finite-resolution phase shifters, we showed that four quantization bits are sufficient for the proposed AN-aided hybrid precoder with secrecy rate loss less than 0.01 bits/s/Hz.

Appendix
Evaluating the Integral $I_{k,l}$ in (14)

Defining $\mu_{k,l} = \frac{1}{(1-\phi)\lambda_{k,l}}$, the integral $I_{k,l}$ in (14) can be written as $I_{k,l} = \phi \mu_{k,l} (\prod_{m=1}^{L} \mu_{k,m}) \tilde{I}_{k,l}$, where

$$\begin{aligned}\tilde{I}_{k,l} &= \int_0^\infty \frac{e^{-\delta r} dr}{(r+\mu_{k,l}) \prod_{m=1}^{L} (r+\mu_{k,m})} \\ &= \int_0^\infty \left(\frac{a_{k,l} e^{-\delta r}}{(r+\mu_{k,l})^2} + \frac{b_{k,l} e^{-\delta r}}{(r+\mu_{k,l})} + \sum_{m=1,\, m\neq l}^{L} \frac{c_{k,m} e^{-\delta r}}{(r+\mu_{k,m})} \right) dr \\ &= a_{k,l} \left(\delta e^{\mu_{k,l}\delta} \mathrm{Ei}\left(-\mu_{k,l}\delta\right) + \frac{1}{\mu_{k,l}} \right) - b_{k,l} e^{\mu_{k,l}\delta} \mathrm{Ei}\left(-\mu_{k,l}\delta\right) \\ &\quad - \sum_{m=1,\, m\neq l}^{L} c_{k,m} e^{\mu_{k,m}\delta} \mathrm{Ei}\left(-\mu_{k,m}\delta\right) \end{aligned} \tag{23}$$

where $\mathrm{Ei}(x) = -\int_{-x}^{\infty} \frac{e^{-t}}{t} dt$ is the exponential integral, and the partial fraction coefficients are obtained as $a_{k,l} = \frac{1}{\prod_{n=1,\, n\neq l}^{L} (\mu_{k,n} - \mu_{k,l})}$, $b_{k,l} = [\frac{\partial}{\partial r} \frac{1}{\prod_{n=1,\, n\neq l}^{L} (r+\mu_{k,n})}]_{r=-\mu_{k,l}}$, and $c_{k,m} = \frac{1}{(\mu_{k,l}-\mu_{k,m}) \prod_{n=1,\, n\neq m}^{L} (\mu_{k,n}-\mu_{k,m})}$.

REFERENCES

[1] T. Rappaport *et al.*, "Millimeter wave mobile communications for 5G cellular: It will work!"*IEEE Access*, vol. 1, pp. 335–349, May 2013.

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

[3] L. Wang, M. Elkashlan, T. Q. Duong, and R. W. Heath, "Secure communication in cellular networks: The benefits of millimeter wave mobile broadband," in *Proc. 2014 IEEE 15th Int. Workshop Signal Process. Adv. Wireless Commun.*, Jun. 2014, pp. 115–119.

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

[5] Y. Ramadan, A. Ibrahim, and M. Khairy, "RF beamforming for secrecy millimeter wave MISO-OFDM systems," in *Proc. 2016 IEEE Int. Conf. Commun.*, May 2016, pp. 1–6.

[6] 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.

[7] C. Wang and H. M. Wang, "Physical layer security in millimeter wave cellular networks," *IEEE Trans. Wireless Commun.*, vol. 15, no. 8, pp. 5569–5585, Aug. 2016.

[8] S. Vuppala, S. Biswas, and T. Ratnarajah, "An analysis on secure communication in millimeter/micro-wave hybrid networks," *IEEE Trans. Commun.*, vol. 64, no. 8, pp. 3507–3519, Aug. 2016.

[9] O. Ayach, R. Heath, S. Abu-Surra, S. Rajagopal, and Z. Pi, "Low complexity precoding for large millimeter wave MIMO systems," in *Proc. 2012 IEEE Int. Conf. Commun.*, Jun. 2012, pp. 3724– 3729.

[10] Y. Ramadan, H. Minn, and A. Ibrahim, "Hybrid analog-digital precoding design for secrecy mmWave MISO-OFDM systems," *IEEE Trans. Commun.*, to be published, doi: 10.1109/TCOMM.2017.2734666.

[11] N. Yang, L. Wang, G. Geraci, M. Elkashlan, J. Yuan, and M. D. Renzo, "Safeguarding 5G wireless communication networks using physical layer security," *IEEE Commun. Mag.*, vol. 53, no. 4, pp. 20–27, Apr. 2015.

[12] J. Zhu, W. Xu, and N. Wang, "Secure massive MIMO systems with limited RF chains," *IEEE Trans. Veh. Technol.*, vol. 66, no. 6, pp. 5455–5460, Jun. 2017.

[13] M. Eltayeb, J. Choi, T. Al-Naffouri, and R. W. Heath, "Enhancing secrecy with multi-antenna transmission in millimeter wave vehicular communication systems," *IEEE Trans. Veh. Technol.*, to be published, doi: 10.1109/TVT.2017.2681965

[14] S. Park, A. Alkhateeb, and R. W. Heath, "Dynamic subarrays for hybrid precoding in wideband mmWave MIMO systems," *IEEE Trans. Wireless Commun.*, vol. 16, no. 5, pp. 2907–2920, May 2017.

[15] S. Shafiee and S. Ulukus, "Achievable rates in Gaussian MISO channels with secrecy constraints," in *Proc. 2007 IEEE Int. Symp. Inf. Theory*, Jun. 2007, pp. 2466–2470.

[16] S.-K. Yong, P. Xia, and A. Valdes-Garcia, *60 GHz Technology for Gbps WLAN and WPAN: From Theory to Practice* New York, NY, USA: Wiley, 2010.

[17] H. Xu, V. Kukshya, and T. S. Rappaport, "Spatial and temporal characteristics of 60-GHz indoor channels," *IEEE J. Sel. Areas Commun.*, vol. 20, no. 3, pp. 620–630, Apr. 2002.

[18] M. R. Akdeniz *et al.*, "Millimeter wave channel modeling and cellular capacity evaluation," *IEEE J. Sel. Areas Commun.*, vol. 32, no. 6, pp. 1164–1179, Jun. 2014.

[19] X. Zhou, L. Song, and Y. Zhang, *Physical Layer Security in Wireless Communications*. Boca Raton, FL, USA: CRC Press, 2013.

[20] J. Wang, P. Ding, M. Zoltowski, and D. Love, "Space-time coding and beamforming with partial channel state information," in *Proc. 2005 IEEE Global Telecommun. Conf.*, Dec. 2005, pp. 3149–3153.

[21] J. W. Wallace and M. A. Jensen, "Time-varying MIMO channels: Measurement, analysis, and modeling," *IEEE Trans. Antennas Propag.*, vol. 54, no. 11, pp. 3265–3273, Nov. 2006.

[22] Y. Ramadan, A. Ibrahim, and M. Khairy, "Minimum outage RF beamforming for millimeter wave MISO-OFDM systems," in *Proc. 2015 IEEE Wireless Commun. Netw. Conf.*, Mar. 2015, pp. 557–561.

[23] M. F. Tang, S. Y. Wang, and B. Su, "Beamforming designs for multiuser transmissions in FDD massive MIMO systems using partial CSIT," in *Proc. 2016 IEEE Sensor Array Multichannel Signal Process. Workshop*, Jul. 2016, pp. 1–5.

[24] Z. Li, S. Han, and A. F. Molisch, "Optimizing channel-statistics-based analog beamforming for millimeter-wave multi-user massive MIMO downlink," *IEEE Trans. Wireless Commun.*, vol. 16, no. 7, pp. 4288–4303, Jul. 2017.

[25] S. Gerbracht, A. Wolf, and E. A. Jorswieck, "Beamforming for fading wiretap channels with partial channel information," in *Proc. 2010 Int. ITG Workshop Smart Antennas*, Feb. 2010, pp. 394–401.

[26] H. Stark and J. Woods, *Probability, Statistics, and Random Processes for Engineers*. Englewood Cliffs, NJ, USA: Prentice-Hall, 2012.

[27] J. Magnus, "The exact moments of a ratio of quadratic forms in normal variables," *Annales d'Economie et de Statistique*, vol. 4, pp. 95–109, Oct./Dec. 1986.