Hybrid Analog-Digital Precoding Design for Secrecy mmWave MISO-OFDM Systems

Yahia R. Ramadan, *Student Member*, *IEEE*, Hlaing Minn, *Fellow*, *IEEE*, Ahmed S. Ibrahim, *Member*, *IEEE*

***Abstract*—Millimeter-wave large-scale antenna systems typically apply hybrid analog-digital precoders to reduce hardware complexity and power consumption. In this paper, we design hybrid precoders for physical-layer security under two types of channel knowledge. With full channel knowledge at transmitter, we provide sufficient conditions on the minimum number of RF chains needed to realize the performance of the fully digital precoding. Then, we design the hybrid precoder to maximize the secrecy rate. By maximizing the average projection between the fully digital precoder and the hybrid precoder, we propose a low-complexity closed-form hybrid precoder. We extend the conventional projected maximum ratio transmission scheme to realize the hybrid precoder. Moreover, we propose an iterative hybrid precoder design to maximize the secrecy rate. With partial channel knowledge at transmitter, we derive a secrecy outage probability upper-bound. The secrecy throughput maximization is converted into a sequence of secrecy outage probability minimization problems. Then, the hybrid precoder is designed to minimize the secrecy outage probability by an iterative hybrid precoder design. Performance results show the proposed hybrid precoders achieve performance close to that of the fully digital precoding at low and moderate signal-to-noise ratios (SNRs), and sometimes at high SNRs depending on the system parameters.**

***Index Terms*—Millimeter-wave, hybrid precoding, physical layer security, partial channel knowledge, outage.**

I. Introduction

NEXT generation wireless communication systems demand an exponential increase in data rate. The spectrum available in the microwave band is too scarce to answer such data rate need. This leads to a potential use of the underutilized millimeter-wave (mmWave) band. Millimeter-wave communications can support multiple Gbps data rates, but since the carrier frequencies are so high, mmWave links suffer higher propagation path loss. Antenna arrays can be used to compensate such losses [1]. Tens of antennas can be packed into a small area in mmWave transceivers due to the tiny wavelength. However, implementing a separate radio-frequency (RF) chain for each antenna is impractical due to the high cost and power of mixed-signal devices. An efficient solution to reduce the hardware complexity and the power consumption is the hybrid analog-digital precoding, where the antenna array with N_{T} elements is connected via an analog RF precoder to N_{RF} RF chains ($N_{\mathrm{RF}} < N_{\mathrm{T}}$) which process the digitally-precoded transmitted stream [2].

Due to the broadcast nature of wireless links, wireless communication is susceptible to eavesdropping. As a result, physical layer security has recently gained a lot of interest in the literature especially for multiple-antenna systems and 5G wireless communication networks [3]. The spatial degrees of freedom can be exploited to enhance the main channel and degrade the channels to eavesdroppers (Eves). This enhances the secrecy rate which is defined as the minimum difference between the achievable rate of the main channel and each achievable rate of the channels to Eves [4]. This paper develops hybrid precoding designs for physical layer security in large-scale mmWave systems.

A. Related Works

With full channel knowledge at the transmitter (Alice), the beamforming strategy was proven to achieve the secrecy capacity when the intended receiver (Bob) has a single antenna in presence of a single Eve [5]. A semidefinite programming (SDP) framework was developed in [6] to maximize the secrecy rate with perfect or imperfect channel knowledge and multiple eavesdroppers with multiple antennas. The generation of artificial noise (AN) on the null space of the main channel was also introduced to degrade only the channels to Eves. If Alice does not have any knowledge of the channels to Eves, AN is uniformly spread on the null space of the main channel (isotropic AN) [7]. With partial channel knowledge at Alice, spatially-selective AN on the null space of the main channel is generated to effectively degrade the channels to Eves [8], [9]. We note that the works in [5]–[9] were restricted to secure baseband precoding with full RF chains.

As for secure RF precoding, previous works have focused on directional modulation (DM). In [10], [11], the RF precoder is designed such that the transmitted symbol is correctly modulated along the desired direction while the signal constellation is distorted along the other directions. The antenna subset modulation (ASM) proposed in [12] adopts the same idea besides choosing a different subset of antennas at each symbol. Using this approach, an additional randomness in the constellation along the other directions is introduced. In [13], two different transmission modes were used to analyze the secrecy throughput, and the impact of large antenna arrays on the secrecy throughput was also examined. In [14], the impact

Manuscript received March 6, 2016; revised June 4, 2017 and July 20, 2017; accepted July 21, 2017. The work of Y. R. Ramadan and H. Minn is supported in part by National Science Foundation under Award No. AST-1547048. The work of A. S. Ibrahim is supported in part by National Science Foundation under Award No. CNS-1618692. The associate editor coordinating the review of this paper and approving it for publication was Zhiguo Ding. *(Corresponding author: Hlaing Minn.)*

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-mails: {yahia.ramadan, hlaing.minn}@utdallas.edu. A. S. Ibrahim is with the Department of Electrical and Computer Engineering, Florida International University, Miami, FL 33174, USA, e-mail: aibrahim@fiu.edu.

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

Digital Object Identifier 10.1109/TCOMM.2017.0000000

of random blockage, mmWave frequencies, and number of transmit antennas on the secrecy rate was analyzed. However, previous works in [10]–[14] consider only the case that Alice has a single RF chain and the channels are line-of-sight (LOS) or dominated by a single propagation path while neglecting the small-scale fading. The first work to consider secure RF precoding for frequency-selective mmWave channels was in [15], where the RF precoder is designed to maximize the secrecy rate with full or partial channel knowledge at Alice. However, the work in [15] considers only the case that Alice has a single RF chain, and lacks designing the hybrid precoder if Alice has multiple RF chains.

With partial channel knowledge at Alice, the sparse structure of mmWave channels was exploited in [16] to generate spatially-selective AN to minimize the secrecy outage probability. However, the work in [16] was also restricted to secure baseband precoding with full RF chains. The only works that consider secure hybrid precoding are in [3], [17], where the baseband preocder is designed to generate isotropic AN, and the RF precoder is designed to enhance the main channel. However, the works in [3], [17] consider only the case that Alice does not have any knowledge of the channels to Eves and the channels are flat fading. The security aspect for two-way relaying was considered in [18], where the source nodes have multiple antennas connected to a single RF chain while the relay has multiple antennas connected to two RF chains, and the secure RF precoders are designed to maximize the secrecy rate. The works in [3], [16]–[18] were restricted to flat fading channels, but mmWave channels are likely to be frequency-selective due to the large transmission bandwidth [19]. To the best of our knowledge, secure hybrid precoding for frequency-selective mmWave channels with full or partial channel knowledge has not been developed in the literature. For flat fading channels, the hybrid precoder can be designed per symbol. However, for frequency-selective channels, the RF precoder has to be fixed across the subcarriers of orthogonal frequency division multiplexing (OFDM) symbol as it is applied in the time domain, while the baseband precoder is designed per subcarrier [20], thus creating a different design problem. Since we assume that Alice has some knowledge of the channels to Eves, we consider secure hybrid precoding using the beamforming strategy. Incorporation of AN in our framework requires a different development than the existing AN works, and hence we leave it as our future work.

B. Contributions

In this paper, we investigate the hybrid precoder design in mmWave multiple-input single-output (MISO) systems for physical layer security. We consider two types of channel knowledge at the transmitter. With full channel knowledge at Alice, we design the hybrid precoder to maximize the secrecy rate. With partial channel knowledge at Alice, we design the hybrid precoder to maximize the secrecy throughput. Our main contributions are summarized as follows:

- With full channel knowledge at Alice, we provide sufficient conditions on the minimum number of RF chains needed to realize the performance of the fully digital precoding.
- By maximizing the average projection between the fully digital precoder and the hybrid precoder, we propose a low-complexity closed-form hybrid precoder design which achieves exactly the same performance of the alternating minimization algorithms in [21].
- We extend the conventional projected maximum ratio transmissions (P-MRT) scheme to realize the hybrid precoder. We propose two P-MRT schemes. The first P-MRT scheme nulls the channels to Eves at time domain (TD-PMRT), while the second P-MRT scheme nulls the channels to Eves at frequency domain (FD-P-MRT). The two schemes TD-P-MRT and FD-P-MRT have different regions of feasibility. We define our P-MRT as an adaptive scheme that applies the one with higher secrecy rate between TD-P-MRT and FD-P-MRT for each channel realization.
- We propose an iterative hybrid precoder design to maximize the secrecy rate. The optimal baseband preocder is obtained as a function of the RF precoder. As a result, we write the secrecy rate as a function of the RF precoder only. Then, we propose a simple gradient ascent algorithm to design the RF precoder.
- With partial channel knowledge, where Alice has full knowledge of the channel to Bob but has knowledge only of the angles of departure (AoDs) of the propagation paths to Eves, we derive a secrecy outage probability upper bound. We convert the secrecy throughput maximization problem into a sequence of secrecy outage probability minimization problems, each is solved for a fixed target secrecy rate. Then, we propose an alternating minimization algorithm, based on gradient descent, to minimize the secrecy outage probability.
- We present extensive simulation results to show that the proposed hybrid precoding designs achieve performance close to that of the fully digital precoding at low and moderate signal-to-noise ratios (SNRs), and sometimes at high SNRs depending on the system parameters.

C. Notations and Organization

We use the following notation throughout this paper: $\mathbf{A}$ is a matrix, $\mathbf{a}$ is a vector, $\|\mathbf{a}\|$ is its $l2$-norm, and a is a scalar, whereas $(\cdot)^T$ and $(\cdot)^H$ are the transpose and conjugate transpose operators respectively. $\mathbf{I}_N$ is the identity matrix of order N. $\mathrm{Tr}[\mathbf{A}]$ denotes the trace of $\mathbf{A}$, $\boldsymbol{\mathcal{E}}_{\max}[\mathbf{A}]$ is the principal eigenvector of $\mathbf{A}$, and $\lambda_{\max}[\mathbf{A}]$ is the corresponding maximum eigenvalue, while $\boldsymbol{\mathcal{E}}_{1:\mathrm{N}}[\mathbf{A}]$ is the first N principal eigenvectors of $\mathbf{A}$. $\mathcal{N}[\mathbf{A}]$ returns the orthonormal basis of the null space of $\mathbf{A}$. $\mathrm{diag}(a_1, a_2, \ldots, a_N)$ returns the diagonal concatenation of elements $a_1, a_2, \ldots, a_N$, while $\mathrm{blkdiag}(\mathbf{A}_1, \mathbf{A}_2, \ldots, \mathbf{A}_N)$ returns the block diagonal concatenation of matrices $\mathbf{A}_1, \mathbf{A}_2, \ldots, \mathbf{A}_N$. $\gcd(a_1, a_2)$ is the greatest common divisor of a_1 and a_2. $\mathbb{P}(x)$ and $\mathbb{E}(x)$ denote the probability and expectation of x. We use MATLAB notations, where $\mathbf{a}(i:j)$ consists of the i^{th} to the j^{th} elements of $\mathbf{a}$, $\mathbf{A}(i,j)$ denotes the $(i,j)^{\mathrm{th}}$ element of $\mathbf{A}$, $\mathbf{A}(i:j,m)$ consists of the i^{th} to the j^{th} elements of the m^{th} column of $\mathbf{A}$, $\mathbf{A}(i,:)$ consists of the i^{th} row of $\mathbf{A}$, and $\mathbf{A}(i:j,:)$ and

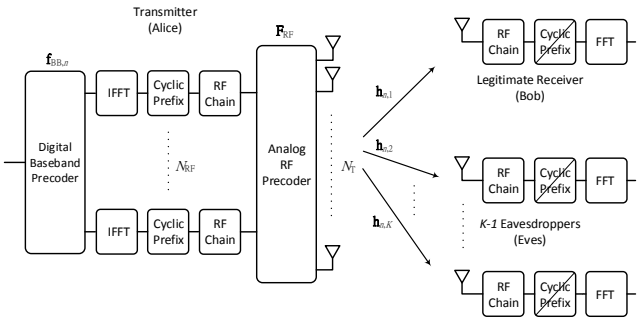


Fig. 1. Secrecy mmWave massive MISO-OFDM system with $K-1$ Eves.

$\mathbf{A}(:, i:j)$ consist of the i^{th} to the j^{th} rows and columns of $\mathbf{A}$ respectively. $\Gamma(m) = \int_0^\infty t^{m-1}e^{-t}dt$ is the Gamma function, $\Gamma(m,x) = \int_x^\infty t^{m-1}\exp(-t)\,dt$ is the upper incomplete Gamma function, and $\Upsilon(m,x) = \int_0^x t^{m-1}\exp(-t)\,dt$ is the lower incomplete Gamma function.

The rest of this paper is organized as follows. In section II, we describe the system and the channel models. In section III, with full channel knowledge at Alice, the hybrid precoder is designed to maximize the secrecy rate. In section IV, with partial channel knowledge at Alice, the hybrid precoder is designed for secrecy throughput maximization. In section V, we present the numerical results. Finally, section VI concludes the paper.

II. System and Channel Models

A. System Model

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

Due to the large transmission bandwidth of mmWave communications, mmWave channels are likely to be frequency-selective. Hence, OFDM is one of the most appropriate modulation techniques as it can convert the frequency-selective fading channel into a number of parallel flat fading subchannels. The received signal $y_{n,k}$ at the n^{th} subcarrier and k^{th} receiver is given by

$$y_{n,k} = \mathbf{h}_{n,k}\mathbf{F}_{\text{RF}}\mathbf{f}_{\text{BB},n}s_n + z_{n,k}, \tag{1}$$

where $\mathbf{h}_{n,k} \in \mathbb{C}^{1\times N_{\text{T}}}$ is the mmWave frequency domain channel at the n^{th} subcarrier to the k^{th} receiver, $\mathbf{F}_{\text{RF}} \in \mathbb{C}^{N_{\text{T}}\times N_{\text{RF}}}$ is the analog RF precoder, $\mathbf{f}_{\text{BB},n} \in \mathbb{C}^{N_{\text{RF}}\times 1}$ and s_n are the digital baseband precoder and the transmitted coded confidential symbol with $\mathbb{E}\left[|s_n|^2\right] = P_{\text{T}}$ at the n^{th} subcarrier respectively, and $z_{n,k}$ is the zero-mean additive white complex Gaussian noise with variance σ^2 at the n^{th} subcarrier and the k^{th} receiver. Since the analog RF precoder $\mathbf{F}_{\text{RF}}$ is applied in time-domain, it is fixed across the subcarriers of OFDM symbol. On the other hand, the digital baseband precoder $\mathbf{f}_{\text{BB},n}$ is designed per subcarrier since it is applied in frequency-domain. The RF precoder $\mathbf{F}_{\text{RF}}$ and baseband precoder $\mathbf{f}_{\text{BB},n}$ have to be designed jointly due to the coupled power constraint, $\sum_{n=1}^{N_{\text{C}}}\|\mathbf{F}_{\text{RF}}\mathbf{f}_{\text{BB},n}\|^2 = N_{\text{C}}$, where N_{C} is the number of subcarriers.

B. Channel Model

Millimeter-wave channels are expected to have limited scattering [22], [23]. We adopt a sparse geometric multipath channel model. The discrete-time channel vector $\tilde{\mathbf{h}}_{t,k} \in \mathbb{C}^{1\times N_{\text{T}}}$ at time instant t to the k^{th} receiver is given by

$$\tilde{\mathbf{h}}_{t,k} = \sum_{l=1}^{L}\alpha_{l,k}\mathbf{a}_{l,k}^H\delta(t-\tau_{l,k}), \tag{2}$$

where L is the number of paths, $\alpha_{l,k}$ and $\tau_{l,k}$ are the complex channel gain and delay (in samples) of the the l^{th} path to the k^{th} receiver, similar to [24]–[28] $\{\alpha_{l,k}\}$ are independent complex random variables representing a multipath Nakagami-m fading channel [29] with shape parameter of m and scale parameters of $\left\{\frac{\rho_l}{m}\right\}$ where $\{\rho_1,\rho_2,\ldots,\rho_L\}$ is the power delay profile, $\mathbf{a}_{l,k}$ is transmit steering vectors of the l^{th} path to the k^{th} receiver with angle of departure (AoD) of $\varphi_{l,k}$,

$$\mathbf{a}_{l,k} = \left[1, e^{-j\frac{2\pi d}{\lambda_{\text{c}}}\cos(\varphi_{l,k})}, \ldots, e^{-j\frac{2\pi d}{\lambda_{\text{c}}}(N_{\text{T}}-1)\cos(\varphi_{l,k})}\right]^T, \tag{3}$$

where $d = \frac{\lambda_{\text{c}}}{2}$ is the spacing between antennas and λ_{c} is the wavelength, and $\delta(t)$ is the Dirac delta function. Assuming perfect synchronization, the frequency domain channel vector $\mathbf{h}_{n,k}$ at the n^{th} subcarrier to the k^{th} receiver is given by

$$\mathbf{h}_{n,k} = \sum_{l=1}^{L}\alpha_{l,k}\mathbf{a}_{l,k}^H\omega_{n,l,k}, \tag{4}$$

where $\omega_{n,l,k}$ is defined as $\omega_{n,l,k} = \exp\left(\frac{-j2\pi(n-1)\tau_{l,k}}{N_{\text{c}}}\right)$. We can write $\mathbf{h}_{n,k}$ in a compact form as

$$\mathbf{h}_{n,k} = \mathbf{w}_{n,k}\mathbf{D}_k\mathbf{A}_{\text{T},k}^H, \tag{5}$$

where $\mathbf{w}_{n,k} = [\omega_{n,1,k}, \omega_{n,2,k}, \ldots, \omega_{n,L,k}] \in \mathbb{C}^{1\times L}$, $\mathbf{D}_k = \text{diag}(\alpha_{1,k}, \alpha_{2,k}, \ldots, \alpha_{L,k}) \in \mathbb{C}^{L\times L}$, and $\mathbf{A}_{\text{T},k} \in \mathbb{C}^{N_{\text{T}}\times L}$ is transmit array response matrix to the k^{th} receiver given by

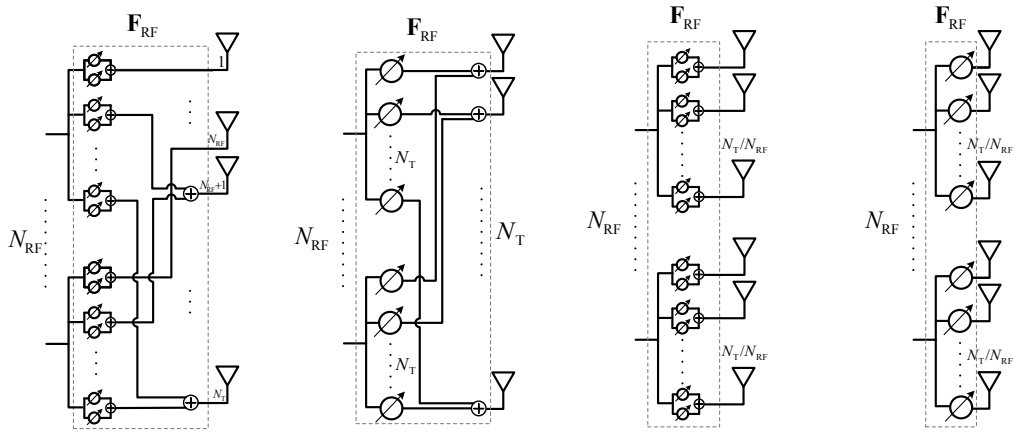
$$\mathbf{A}_{\text{T},k} = [\mathbf{a}_{1,k}, \mathbf{a}_{2,k}, \ldots, \mathbf{a}_{L,k}]. \tag{6}$$

C. Analog RF Precoder Structures

The analog RF preocder $\mathbf{F}_{\text{RF}}$ is usually implemented using analog phase shifters and analog combiners. Four structures for the analog RF precoder are shown in Fig. 2. The fully-connected structure F1 requires $2N_{\text{RF}}(N_{\text{T}}-N_{\text{RF}}+1)$ analog phase shifters and $N_{\text{RF}}(N_{\text{T}}-N_{\text{RF}})+N_{\text{T}}$ analog combiners [30], while the fully-connected structure F2 requires $N_{\text{T}}N_{\text{RF}}$ analog phase shifters and N_{T} analog combiners. The subarray structure S1 requires $2N_{\text{T}}$ analog phase shifters and N_{T} analog combiners, while the subarray structure S2 requires only N_{T} analog phase shifters.

In [30], it was shown that the fully-connected structure F1 has no constraints on the entries of $\mathbf{F}_{\text{RF}}$. Each non-zero entry of $\mathbf{F}_{\text{RF}}$ can be expressed as a sum of two analog phase shifters. The other three structures have constraints on the entries of $\mathbf{F}_{\text{RF}}$. For the fully-connected structure F2, we have $|\mathbf{F}_{\text{RF}}(l,m)| = 1/\sqrt{N_{\text{T}}}\ \forall l,m$. For the subarray structure S1, $\mathbf{F}_{\text{RF}}$ has to be expressed as $\mathbf{F}_{\text{RF}} =$

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TCOMM.2017.2734666, IEEE Transactions on Communications



(a) Fully-connected structure F1 (b) Fully-connected structure F2 (c) Subarray structure S1 (d) Subarray structure S2

Fig. 2. Analog RF precoding structures.

$\mathrm{blkdiag}\left(\mathbf{f}_{\mathrm{RF},1}, \mathbf{f}_{\mathrm{RF},2}, \ldots, \mathbf{f}_{\mathrm{RF},N_{\mathrm{RF}}}\right)$ where $\mathbf{f}_{\mathrm{RF},r} \in \mathbb{C}^{\frac{N_{\mathrm{T}}}{N_{\mathrm{RF}}} \times 1}$ $\forall r \in \{1, 2, \ldots, N_{\mathrm{RF}}\}$. Similarly, each entry of $\mathbf{f}_{\mathrm{RF},r}$ can be expressed as a sum of two analog phase shifters. The subarray structure S2 has the same constraint of subarray structure S1 and an additional constraint that $|\mathbf{f}_{\mathrm{RF},r}(l)| = 1/\sqrt{N_{\mathrm{T}}/N_{\mathrm{RF}}}$ $\forall l$. Let us denote by $\mathcal{F}_{\mathrm{RF}}^{\mathrm{F1}}$ the set of all $N_{\mathrm{T}} \times N_{\mathrm{RF}}$ complex matrices and by $\mathcal{F}_{\mathrm{RF}}^{\mathrm{F2}}$ the set of analog RF precoders satisfying the constraint of fully-connected structure F2, while by $\mathcal{F}_{\mathrm{RF}}^{\mathrm{S1}}$ and $\mathcal{F}_{\mathrm{RF}}^{\mathrm{S2}}$ the sets of analog RF precoders satisfying the constraints of subarray structure S1 and S2 respectively. Note that $\mathcal{F}_{\mathrm{RF}}^{\mathrm{S2}} \subset \mathcal{F}_{\mathrm{RF}}^{\mathrm{S1}} \subset \mathcal{F}_{\mathrm{RF}}^{\mathrm{F1}}$ and $\mathcal{F}_{\mathrm{RF}}^{\mathrm{S2}} \subset \mathcal{F}_{\mathrm{RF}}^{\mathrm{F2}} \subset \mathcal{F}_{\mathrm{RF}}^{\mathrm{F1}}$.

D. Hybrid Precoding Design Problems

The achievable rate R_k of the k^{th} receiver is given by

$$R_k = \frac{1}{N_{\mathrm{C}}} \sum_{n=1}^{N_{\mathrm{C}}} \log_2 \left(1 + \gamma \left|\mathbf{h}_{n,k} \mathbf{F}_{\mathrm{RF}} \mathbf{f}_{\mathrm{BB},n}\right|^2\right), \quad (7)$$

where $\gamma = P_{\mathrm{T}}/\sigma^2$ is the transmit SNR per subcarrier. Throughout the paper, we assume that the secure coding is applied jointly across all subchannels (coding across sub-messages [31]). With full knowledge of all channels at the transmitter, maximizing the secrecy rate R_{sec} given by [4]

$$R_{\mathrm{sec}} = \min_k \{R_1 - R_k\}_{k=2}^{K} \quad (8)$$

is preferred. With full knowledge of the channel to Bob and partial knowledge of the channels to Eves at the transmitter, maximizing the secrecy throughput η_{sec} given by [32], [33]

$$\eta_{\mathrm{sec}} = R_{\mathrm{sec}} \left(1 - \epsilon_{\mathrm{sec}}\right) \quad (9)$$

is preferred, where ϵ_{sec} is the secrecy outage probability.

The subsequent parts of the paper focus on designing the secure hybrid precoder for the the aforementioned two types of channel knowledge at the transmitter:

1) With full knowledge of all channels at the transmitter, section III focuses on designing the hybrid precoder to maximize the secrecy rate R_{sec},

$$\underset{\mathbf{F}_{\mathrm{RF}}, \{\mathbf{f}_{\mathrm{BB},n}\}}{\arg\max} \; R_{\mathrm{sec}},$$

$$\text{s.t. } \mathbf{F}_{\mathrm{RF}} \in \mathcal{F}_{\mathrm{RF}}, \; \sum_{n=1}^{N_{\mathrm{C}}} \left\|\mathbf{F}_{\mathrm{RF}} \mathbf{f}_{\mathrm{BB},n}\right\|^2 = N_{\mathrm{C}}. \quad (10)$$

2) With full knowledge of the channel to Bob and partial knowledge of the channels to Eves at the transmitter, section IV focuses on designing the hybrid precoder to maximize the secrecy throughput η_{sec},

$$\underset{\mathbf{F}_{\mathrm{RF}}, \{\mathbf{f}_{\mathrm{BB},n}\}, R_{\mathrm{sec}}}{\arg\max} \; \eta_{\mathrm{sec}},$$

$$\text{s.t. } \mathbf{F}_{\mathrm{RF}} \in \mathcal{F}_{\mathrm{RF}}, \; \sum_{n=1}^{N_{\mathrm{C}}} \left\|\mathbf{F}_{\mathrm{RF}} \mathbf{f}_{\mathrm{BB},n}\right\|^2 = N_{\mathrm{C}}. \quad (11)$$

Note that for the two hybrid precoder design problems in (10) and (11), $\mathcal{F}_{\mathrm{RF}}$ can be $\mathcal{F}_{\mathrm{RF}}^{\mathrm{F1}}$, $\mathcal{F}_{\mathrm{RF}}^{\mathrm{F2}}$, $\mathcal{F}_{\mathrm{RF}}^{\mathrm{S1}}$, or $\mathcal{F}_{\mathrm{RF}}^{\mathrm{S2}}$ according to the used structure. We consider all the four structures.

III. Hybrid Precoder Design for Secrecy Rate Maximization with Full Channel Knowledge

We design the hybrid precoder to maximize the secrecy rate R_{sec} for a given transmit SNR per subcarrier γ. We assume that Alice has perfect full knowledge of the channels to Bob and to Eves. Bob and Eves have full knowledge of their channels to Alice. Furthermore, we assume that Eves do not cooperate. These assumptions become realistic if Eves are active nodes which have communicated with Alice [34].

To decouple the hybrid precoder design and the power allocation, we sub-optimally divide the problem into two sub-problems. In the first sub-problem, we relax the power constraint to $\left\|\mathbf{F}_{\mathrm{RF}} \mathbf{f}_{\mathrm{BB},n}\right\|^2 = 1 \; \forall n$ (which satisfies $\sum_{n=1}^{N_{\mathrm{C}}} \left\|\mathbf{F}_{\mathrm{RF}} \mathbf{f}_{\mathrm{BB},n}\right\|^2 = N_{\mathrm{C}}$) and then design the hybrid precoder (as will be presented in this section). In the second sub-problem, based on the equivalent single-input-single-output (SISO) channels $\{\mathbf{h}_{n,k} \mathbf{F}_{\mathrm{RF}} \mathbf{f}_{\mathrm{BB},n}\}$ and the constraint $\sum_{n=1}^{N_{\mathrm{C}}} \left\|\mathbf{F}_{\mathrm{RF}} \mathbf{f}_{\mathrm{BB},n}\right\|^2 = N_{\mathrm{C}}$, the power allocation across subcarriers is obtained in a closed-form solution as in [35].

A. Fully Digital Precoding Design and The Minimum Number of RF Chains to Realize It

When $N_{\mathrm{RF}} = N_{\mathrm{T}}$, Alice applies fully digital precoding to maximize the secrecy rate R_{sec}. The optimal baseband precoder can be obtained by solving the optimization problem in (10) using semidefinite programming (SDP) as in [6]. To obtain a closed-form solution, we apply an approximation by treating the $K-1$ Eves as one Eve with $K-1$ antennas. This approximation gives a secrecy rate lower bound $\tilde{R}_{\mathrm{sec}}$ for the

system with $K-1$ Eves, which can be written as

$$\tilde{R}_{\text{sec}} = \frac{1}{N_{\text{C}}} \sum_{n=1}^{N_{\text{C}}} \log_2 \left(\frac{1+\gamma \left| \mathbf{h}_{n,1} \mathbf{f}_{\text{opt},n} \right|^2}{1+\gamma \left\| \mathbf{H}_n \mathbf{f}_{\text{opt},n} \right\|^2} \right), \quad (12)$$

where $\mathbf{H}_n = \left[\mathbf{h}_{n,2}^T, \mathbf{h}_{n,3}^T, \ldots, \mathbf{h}_{n,K}^T \right]^T \in \mathbb{C}^{(K-1)\times N_{\text{T}}}$ and $\mathbf{f}_{\text{opt},n} \in \mathbb{C}^{N_{\text{T}}\times 1}$ is the fully digital precoder. Satisfying the power constraint $\left\| \mathbf{f}_{\text{opt},n} \right\|^2 = 1$, $\mathbf{f}_{\text{opt},n}$ maximizing (12) is obtained using the generalized eigenvector decomposition as

$$\mathbf{f}_{\text{opt},n} = \boldsymbol{\mathcal{E}}_{\max} \left[\left(\mathbf{I}_{N_{\text{T}}} + \gamma \mathbf{H}_n^H \mathbf{H}_n \right)^{-1} \left(\mathbf{I}_{N_{\text{T}}} + \gamma \mathbf{h}_{n,1}^H \mathbf{h}_{n,1} \right) \right], \quad (13)$$

and the corresponding $\tilde{R}_{\text{sec}}$ is given by

$$\tilde{R}_{\text{sec}} = \frac{1}{N_{\text{c}}} \sum_{n=1}^{N_{\text{c}}} \log_2 \left(\lambda_{\max} \left[\left(\mathbf{I}_{N_{\text{T}}} + \gamma \mathbf{H}_n^H \mathbf{H}_n \right)^{-1} \left(\mathbf{I}_{N_{\text{T}}} + \gamma \mathbf{h}_{n,1}^H \mathbf{h}_{n,1} \right) \right] \right). \quad (14)$$

Let us define $\mathbf{F}_{\text{opt}} = [\mathbf{f}_{\text{opt},1}, \mathbf{f}_{\text{opt},2}, \ldots, \mathbf{f}_{\text{opt},N_{\text{C}}}] \in \mathbb{C}^{N_{\text{T}}\times N_{\text{C}}}$. Next, we provide sufficient conditions on the number of RF chains needed for the hybrid precoder to realize the performance of fully digital precoding (i.e., expressing $\mathbf{F}_{\text{opt}}$ as $\mathbf{F}_{\text{opt}} = \mathbf{F}_{\text{RF}} [\mathbf{f}_{\text{BB},1}, \mathbf{f}_{\text{BB},2}, \ldots, \mathbf{f}_{\text{BB},N_{\text{C}}}]$).

Proposition 1. To realize the performance of fully digital precoding, it is sufficient for the hybrid precoding utilizing the fully-connected structure F1 that $N_{\text{RF}} \geq KL$. For the hybrid precoding utilizing the fully-connected structure F2, the sufficient condition becomes $N_{\text{RF}} \geq 2KL$, and it reduces to $N_{\text{RF}} \geq KL$ only if all the channels follow the mmWave channel model in (2).

Proof: See Appendix A. ∎

Proposition 2. For the subarray structures, there is no sufficient condition depending only on the number of RF chains to realize the performance of fully digital precoding.

Proof: See Appendix B. ∎

For practical system parameters, the above sufficient conditions are not likely to be satisfied. Next, we provide different hybrid precoder designs to maximize the secrecy rate.

B. Low-Complexity Secrecy Hybrid Precoding Desgins

1) Approximating The Fully Digital Precoding (App-FD): Traditionally, the hybrid precoder is designed to approximate the fully digital precoder by minimizing the average Euclidean distance between the fully digital precoder and the hybrid precoder [21], [36], [37]. Different from the average Euclidean distance criterion, we design the hybrid precoder to approximate the fully digital precoder by maximizing the average projection between the fully digital precoder and the hybrid precoder. Interestingly, the two criteria are related to each other, and they have similarity in the design of baseband precoder (see Appendix C).

In the following, we obtain closed-form solutions for the hybrid precoder maximizing the average projection between the fully digital precoder and the hybrid precoder. In other words, the hybrid precoder is designed as

$$\begin{aligned} &\underset{\mathbf{F}_{\text{RF}}, \{\mathbf{f}_{\text{BB},n}\}}{\arg\max} \sum_{n=1}^{N_{\text{C}}} \left\| \mathbf{f}_{\text{opt},n}^H \mathbf{F}_{\text{RF}} \mathbf{f}_{\text{BB},n} \right\|^2, \\ &\text{s.t. } \mathbf{F}_{\text{RF}} \in \mathcal{F}_{\text{RF}}, \ \left\| \mathbf{F}_{\text{RF}} \mathbf{f}_{\text{BB},n} \right\|^2 = 1 \, \forall n. \end{aligned} \quad (15)$$

After applying the power constraint $\left\| \mathbf{F}_{\text{RF}} \mathbf{f}_{\text{BB},n} \right\|^2 = 1$ into the objective function and dropping the constraint on the entries of the RF precoder, we have

$$\underset{\mathbf{F}_{\text{RF}}, \{\mathbf{f}_{\text{BB},n}\}}{\arg\max} \sum_{n=1}^{N_{\text{C}}} \frac{\mathbf{f}_{\text{BB},n}^H \left(\mathbf{F}_{\text{RF}}^H \mathbf{f}_{\text{opt},n} \mathbf{f}_{\text{opt},n}^H \mathbf{F}_{\text{RF}} \right) \mathbf{f}_{\text{BB},n}}{\mathbf{f}_{\text{BB},n}^H \left(\mathbf{F}_{\text{RF}}^H \mathbf{F}_{\text{RF}} \right) \mathbf{f}_{\text{BB},n}}. \quad (16)$$

Using the generalized eigenvector decomposition, $\mathbf{f}_{\text{BB},n}$ maximizing (16) is given by

$$\begin{aligned} \mathbf{f}_{\text{BB},n} &= \kappa_n \boldsymbol{\mathcal{E}}_{\max} \left[\left(\mathbf{F}_{\text{RF}}^H \mathbf{F}_{\text{RF}} \right)^{-1} \mathbf{F}_{\text{RF}}^H \mathbf{f}_{\text{opt},n} \mathbf{f}_{\text{opt},n}^H \mathbf{F}_{\text{RF}} \right] \\ &= \frac{\left(\mathbf{F}_{\text{RF}}^H \mathbf{F}_{\text{RF}} \right)^{-1} \mathbf{F}_{\text{RF}}^H \mathbf{f}_{\text{opt},n}}{\left\| \left(\mathbf{F}_{\text{RF}}^H \mathbf{F}_{\text{RF}} \right)^{-\frac{1}{2}} \mathbf{F}_{\text{RF}}^H \mathbf{f}_{\text{opt},n} \right\|}, \end{aligned} \quad (17)$$

where κ_n is a scaling factor to have $\left\| \mathbf{F}_{\text{RF}} \mathbf{f}_{\text{BB},n} \right\|^2 = 1$, and the second equality holds since $\left(\mathbf{F}_{\text{RF}}^H \mathbf{F}_{\text{RF}} \right)^{-1} \mathbf{F}_{\text{RF}}^H \mathbf{f}_{\text{opt},n}$ $\mathbf{f}_{\text{opt},n}^H \mathbf{F}_{\text{RF}}$ is a rank-one matrix. Substituting (17) into (16), we get

$$\begin{aligned} &\underset{\mathbf{F}_{\text{RF}}}{\arg\max} \sum_{n=1}^{N_{\text{C}}} \lambda_{\max} \left[\left(\mathbf{F}_{\text{RF}}^H \mathbf{F}_{\text{RF}} \right)^{-1} \mathbf{F}_{\text{RF}}^H \mathbf{f}_{\text{opt},n} \mathbf{f}_{\text{opt},n}^H \mathbf{F}_{\text{RF}} \right] \\ &= \underset{\mathbf{F}_{\text{RF}}}{\arg\max} \operatorname{Tr} \left[\left(\mathbf{F}_{\text{RF}}^H \mathbf{F}_{\text{RF}} \right)^{-\frac{1}{2}} \mathbf{F}_{\text{RF}}^H \left(\sum_{n=1}^{N_{\text{C}}} \mathbf{f}_{\text{opt},n} \mathbf{f}_{\text{opt},n}^H \right) \right. \\ &\quad \left. \times \mathbf{F}_{\text{RF}} \left(\mathbf{F}_{\text{RF}}^H \mathbf{F}_{\text{RF}} \right)^{-\frac{1}{2}} \right] \\ &= \boldsymbol{\mathcal{E}}_{1:\text{N}_{\text{RF}}} \left[\sum_{n=1}^{N_{\text{C}}} \mathbf{f}_{\text{opt},n} \mathbf{f}_{\text{opt},n}^H \right]. \end{aligned} \quad (18)$$

For the fully-connected structure F1, as there are no constraints on the entries of $\mathbf{F}_{\text{RF}}$, the RF precoder is simply given by (18). Since $\mathbf{F}_{\text{RF}}^H \mathbf{F}_{\text{RF}} = \mathbf{I}_{N_{\text{RF}}}$ due to (18), $\mathbf{f}_{\text{BB},n}$ in (17) is simplified to

$$\mathbf{f}_{\text{BB},n} = \frac{\mathbf{F}_{\text{RF}}^H \mathbf{f}_{\text{opt},n}}{\left\| \mathbf{F}_{\text{RF}}^H \mathbf{f}_{\text{opt},n} \right\|}. \quad (19)$$

For the fully-connected structure F2, we obtain $\mathbf{F}_{\text{RF}}$ as

$$\mathbf{F}_{\text{RF}} = \frac{1}{\sqrt{N_{\text{T}}}} \exp \left(j \angle \boldsymbol{\mathcal{E}}_{1:\text{N}_{\text{RF}}} \left[\sum_{n=1}^{N_{\text{C}}} \mathbf{f}_{\text{opt},n} \mathbf{f}_{\text{opt},n}^H \right] \right), \quad (20)$$

which satisfies the modulus constraint and is a good approximation to (18). Then, we obtain $\mathbf{f}_{\text{BB},n}$ as in (17) since $\mathbf{F}_{\text{RF}}^H \mathbf{F}_{\text{RF}} \neq \mathbf{I}_{N_{\text{RF}}}$.

For the subarray structures, $\mathbf{F}_{\text{RF}}^H \mathbf{F}_{\text{RF}} = \text{diag} \left(\left\| \mathbf{f}_{\text{RF},1} \right\|^2, \ldots, \left\| \mathbf{f}_{\text{RF},N_{\text{RF}}} \right\|^2 \right)$, and hence, (18) can be solved for each $\mathbf{f}_{\text{RF},r}$ as

$$\mathbf{f}_{\text{RF},r} = \underset{\mathbf{f}_{\text{RF},r}}{\arg\max} \frac{\mathbf{f}_{\text{RF},r}^H \left(\sum_{n=1}^{N_{\text{C}}} \mathbf{f}_{\text{opt},n,r} \mathbf{f}_{\text{opt},n,r}^H \right) \mathbf{f}_{\text{RF},r}}{\mathbf{f}_{\text{RF},r}^H \mathbf{f}_{\text{RF},r}}, \quad (21)$$

where $\mathbf{f}_{\text{opt},n,r} = \mathbf{f}_{\text{opt},n} \left((r-1) \frac{N_{\text{T}}}{N_{\text{RF}}} + 1 : r \frac{N_{\text{T}}}{N_{\text{RF}}} \right) \in \mathbb{C}^{\frac{N_{\text{T}}}{N_{\text{RF}}} \times 1}$ $\forall r \in \{1, 2, \ldots, N_{\text{RF}}\}$. Therefore, $\mathbf{f}_{\text{RF},r}$ is obtained in a closed-form for the subarray structure S1 as

$$\mathbf{f}_{\text{RF},r} = \boldsymbol{\mathcal{E}}_{\max} \left[\sum_{n=1}^{N_{\text{C}}} \mathbf{f}_{\text{opt},n,r} \mathbf{f}_{\text{opt},n,r}^H \right], \quad (22)$$

while $\mathbf{f}_{\text{RF},r}$ for the subarray structure S2 is obtained as

$$\mathbf{f}_{\text{RF},r} = \frac{1}{\sqrt{N_{\text{T}}/N_{\text{RF}}}} \exp \left(j \angle \boldsymbol{\mathcal{E}}_{\max} \left[\sum_{n=1}^{N_{\text{C}}} \mathbf{f}_{\text{opt},n,r} \mathbf{f}_{\text{opt},n,r}^H \right] \right). \quad (23)$$

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TCOMM.2017.2734666, IEEE Transactions on Communications

Since $\mathbf{F}_{\mathrm{RF}}^H\mathbf{F}_{\mathrm{RF}}=\mathbf{I}_{N_{\mathrm{RF}}}$ for the subarray structures due to (22) and (23), $\mathbf{f}_{\mathrm{BB},n}$ in (17) is simplified to

$$\mathbf{f}_{\mathrm{BB},n}=\frac{\left[\mathbf{f}_{\mathrm{RF},1}^H\mathbf{f}_{\mathrm{opt},n,1},\ldots,\mathbf{f}_{\mathrm{RF},N_{\mathrm{RF}}}^H\mathbf{f}_{\mathrm{opt},n,N_{\mathrm{RF}}}\right]^T}{\sqrt{\sum_{r=1}^{N_{\mathrm{RF}}}\left|\mathbf{f}_{\mathrm{RF},r}^H\mathbf{f}_{\mathrm{opt},n,r}\right|^2}}. \quad (24)$$

Although the average projection criterion and the average Euclidean distance criterion are slightly different (as shown in Appendix C), we observe in our numerical results that our closed-form hybrid precoder in this subsection achieves exactly the same performance of the hybrid precoder obtained in [21] which applies two nested iterative algorithms to design the hybrid precoder. The computational complexity of App-FD is $\mathcal{O}\left(N_{\mathrm{T}}^3N_{\mathrm{C}}+N_{\mathrm{T}}^2N_{\mathrm{C}}K\right)$.

2) Projected Maximum Ratio Transmission (P-MRT): The main idea of P-MRT is to maximize the average SNR of Bob $\left(\overline{\mathrm{SNR}}_{\mathrm{B}}\right)$ in the null space of channels to Eves [6]. Generally, P-MRT is suboptimal at low and moderate SNRs but optimal at high SNRs. We will show how to design P-MRT using the hybrid precoder. Nulling the channels to Eves can be done using the analog RF precoder (at time domain TD-P-MRT) or using the digital baseband precoder (at frequency domain FD-P-MRT). The two schemes TD-P-MRT and FD-P-MRT have different regions of feasibility (as will be shown). As a result, our P-MRT adaptively selects the better scheme from TD-P-MRT and FD-P-MRT depending on the system parameters and channel realizations. This will yield higher secrecy rate.

a) TD-P-MRT: First, we consider the fully-connected structures F1 and F2. For both structures, it is necessary that $N_{\mathrm{T}}>(K-1)L$ to apply TD-P-MRT. We express $\mathbf{F}_{\mathrm{RF}}$ as

$$\mathbf{F}_{\mathrm{RF}}=\mathbf{U}_{\mathrm{RF}}\tilde{\mathbf{F}}_{\mathrm{RF}}, \quad (25)$$

where $\mathbf{U}_{\mathrm{RF}}=\mathcal{N}\left[\mathbf{A}_{\mathrm{T,Eves}}\right]\in\mathbb{C}^{N_{\mathrm{T}}\times(N_{\mathrm{T}}-(K-1)L)}$ is a semi-unitary matrix in the null space of the channels to Eves, where $\mathbf{A}_{\mathrm{T,Eves}}\in\mathbb{C}^{N_{\mathrm{T}}\times(K-1)L}$ is given by

$$\mathbf{A}_{\mathrm{T,Eves}}=\left[\mathbf{A}_{\mathrm{T},2},\mathbf{A}_{\mathrm{T},3},\ldots,\mathbf{A}_{\mathrm{T},K}\right]. \quad (26)$$

We design $\tilde{\mathbf{F}}_{\mathrm{RF}}$ and $\mathbf{f}_{\mathrm{BB},n}$ to maximize $\overline{\mathrm{SNR}}_{\mathrm{B}}$ given by

$$\begin{aligned}\overline{\mathrm{SNR}}_{\mathrm{B}}&=\frac{\gamma}{N_{\mathrm{C}}}\sum_{n=1}^{N_{\mathrm{C}}}\frac{\left|\mathbf{h}_{n,1}\mathbf{U}_{\mathrm{RF}}\tilde{\mathbf{F}}_{\mathrm{RF}}\mathbf{f}_{\mathrm{BB},n}\right|^2}{\left\|\mathbf{U}_{\mathrm{RF}}\tilde{\mathbf{F}}_{\mathrm{RF}}\mathbf{f}_{\mathrm{BB},n}\right\|^2}\\&=\frac{\gamma}{N_{\mathrm{C}}}\sum_{n=1}^{N_{\mathrm{C}}}\frac{\mathbf{f}_{\mathrm{BB},n}^H(\tilde{\mathbf{F}}_{\mathrm{RF}}^H\mathbf{U}_{\mathrm{RF}}^H\mathbf{h}_{n,1}^H\mathbf{h}_{n,1}\mathbf{U}_{\mathrm{RF}}\tilde{\mathbf{F}}_{\mathrm{RF}})\mathbf{f}_{\mathrm{BB},n}}{\mathbf{f}_{\mathrm{BB},n}^H(\tilde{\mathbf{F}}_{\mathrm{RF}}^H\tilde{\mathbf{F}}_{\mathrm{RF}})\mathbf{f}_{\mathrm{BB},n}},\end{aligned} \quad (27)$$

where $\mathbf{U}_{\mathrm{RF}}^H\mathbf{U}_{\mathrm{RF}}=\mathbf{I}_{N_{\mathrm{T}}-(K-1)L}$. Using the generalized eigenvector decomposition, $\mathbf{f}_{\mathrm{BB},n}$ maximizing (27) is given by

$$\begin{aligned}\mathbf{f}_{\mathrm{BB},n}&=\kappa_n\boldsymbol{\mathcal{E}}_{\max}\left[\left(\tilde{\mathbf{F}}_{\mathrm{RF}}^H\tilde{\mathbf{F}}_{\mathrm{RF}}\right)^{-1}\tilde{\mathbf{F}}_{\mathrm{RF}}^H\mathbf{U}_{\mathrm{RF}}^H\mathbf{h}_{n,1}^H\mathbf{h}_{n,1}\mathbf{U}_{\mathrm{RF}}\tilde{\mathbf{F}}_{\mathrm{RF}}\right]\\&=\frac{\left(\tilde{\mathbf{F}}_{\mathrm{RF}}^H\tilde{\mathbf{F}}_{\mathrm{RF}}\right)^{-1}\tilde{\mathbf{F}}_{\mathrm{RF}}^H\mathbf{U}_{\mathrm{RF}}^H\mathbf{h}_{n,1}^H}{\left\|\left(\tilde{\mathbf{F}}_{\mathrm{RF}}^H\tilde{\mathbf{F}}_{\mathrm{RF}}\right)^{-\frac{1}{2}}\tilde{\mathbf{F}}_{\mathrm{RF}}^H\mathbf{U}_{\mathrm{RF}}^H\mathbf{h}_{n,1}^H\right\|},\end{aligned} \quad (28)$$

where κ_n is a scaling factor to have $\|\mathbf{F}_{\mathrm{RF}}\mathbf{f}_{\mathrm{BB},n}\|^2=1$, the second equality holds since $\left(\tilde{\mathbf{F}}_{\mathrm{RF}}^H\tilde{\mathbf{F}}_{\mathrm{RF}}\right)^{-1}\tilde{\mathbf{F}}_{\mathrm{RF}}^H\mathbf{U}_{\mathrm{RF}}^H\mathbf{h}_{n,1}^H\mathbf{h}_{n,1}\mathbf{U}_{\mathrm{RF}}\tilde{\mathbf{F}}_{\mathrm{RF}}$ is a rank-one matrix, and the corresponding $\overline{\mathrm{SNR}}_{\mathrm{B}}$ is expressed as

$$\begin{aligned}\overline{\mathrm{SNR}}_{\mathrm{B}}=&\frac{\gamma}{N_{\mathrm{C}}}\sum_{n=1}^{N_{\mathrm{C}}}\lambda_{\max}\left[\left(\tilde{\mathbf{F}}_{\mathrm{RF}}^H\tilde{\mathbf{F}}_{\mathrm{RF}}\right)^{-1}\tilde{\mathbf{F}}_{\mathrm{RF}}^H\mathbf{U}_{\mathrm{RF}}^H\mathbf{h}_{n,1}^H\right.\\&\left.\times\mathbf{h}_{n,1}\mathbf{U}_{\mathrm{RF}}\tilde{\mathbf{F}}_{\mathrm{RF}}\right]\\=&\frac{\gamma}{N_{\mathrm{C}}}\mathrm{Tr}\left[\left(\mathbf{F}_{\mathrm{RF}}^H\mathbf{F}_{\mathrm{RF}}\right)^{-\frac{1}{2}}\tilde{\mathbf{F}}_{\mathrm{RF}}^H\left(\sum_{n=1}^{N_{\mathrm{C}}}\mathbf{U}_{\mathrm{RF}}^H\mathbf{h}_{n,1}^H\mathbf{h}_{n,1}\mathbf{U}_{\mathrm{RF}}\right)\right.\\&\left.\times\tilde{\mathbf{F}}_{\mathrm{RF}}\left(\mathbf{F}_{\mathrm{RF}}^H\mathbf{F}_{\mathrm{RF}}\right)^{-\frac{1}{2}}\right].\end{aligned} \quad (29)$$

For the fully-connected structure F1, $\tilde{\mathbf{F}}_{\mathrm{RF}}$ maximizing (29) is obtained as

$$\tilde{\mathbf{F}}_{\mathrm{RF}}=\boldsymbol{\mathcal{E}}_{1:\mathrm{N_{RF}}}\left[\sum_{n=1}^{N_{\mathrm{C}}}\mathbf{U}_{\mathrm{RF}}^H\mathbf{h}_{n,1}^H\mathbf{h}_{n,1}\mathbf{U}_{\mathrm{RF}}\right]. \quad (30)$$

Since $\tilde{\mathbf{F}}_{\mathrm{RF}}^H\tilde{\mathbf{F}}_{\mathrm{RF}}=\mathbf{I}_{N_{\mathrm{RF}}}$ due to (30), $\mathbf{f}_{\mathrm{BB},n}$ in (28) is simplified to

$$\mathbf{f}_{\mathrm{BB},n}=\frac{\tilde{\mathbf{F}}_{\mathrm{RF}}^H\mathbf{U}_{\mathrm{RF}}^H\mathbf{h}_{n,1}^H}{\left\|\mathbf{h}_{n,1}\mathbf{U}_{\mathrm{RF}}\tilde{\mathbf{F}}_{\mathrm{RF}}\right\|}, \quad (31)$$

which is the well-known MRT precoder for the equivalent channel $\mathbf{h}_{n,1}\mathbf{U}_{\mathrm{RF}}\tilde{\mathbf{F}}_{\mathrm{RF}}$. For the fully-connected structure F2, we need $\mathbf{U}_{\mathrm{RF}}\tilde{\mathbf{F}}_{\mathrm{RF}}$ to satisfy the modulus constraint. Consequently, we obtain $\tilde{\mathbf{F}}_{\mathrm{RF}}$ using only half of the number of RF chains as

$$\tilde{\mathbf{F}}_{\mathrm{RF}}=\boldsymbol{\mathcal{E}}_{1:\frac{\mathrm{N_{RF}}}{2}}\left[\sum_{n=1}^{N_{\mathrm{C}}}\mathbf{U}_{\mathrm{RF}}^H\mathbf{h}_{n,1}^H\mathbf{h}_{n,1}\mathbf{U}_{\mathrm{RF}}\right], \quad (32)$$

and $\tilde{\mathbf{f}}_{\mathrm{BB},n}=\frac{\tilde{\mathbf{F}}_{\mathrm{RF}}^H\mathbf{U}_{\mathrm{RF}}^H\mathbf{h}_{n,1}^H}{\left\|\mathbf{h}_{n,1}\mathbf{U}_{\mathrm{RF}}\tilde{\mathbf{F}}_{\mathrm{RF}}\right\|}\in\mathbb{C}^{\frac{N_{\mathrm{RF}}}{2}\times1}$. Then, $\mathbf{U}_{\mathrm{RF}}\tilde{\mathbf{F}}_{\mathrm{RF}}$ is decomposed (as described in proof of Proposition 1) as $\mathbf{U}_{\mathrm{RF}}\tilde{\mathbf{F}}_{\mathrm{RF}}=\mathbf{Q}_{\mathrm{RF}}\mathbf{R}_{\mathrm{BB}}$ where $\mathbf{Q}_{\mathrm{RF}}\in\mathbb{C}^{N_{\mathrm{T}}\times N_{\mathrm{RF}}}$ is with unit modulus entries and $\mathbf{R}_{\mathrm{BB}}\in\mathbb{R}^{N_{\mathrm{RF}}\times\frac{N_{\mathrm{RF}}}{2}}$. Finally, we set $\mathbf{F}_{\mathrm{RF}}=\frac{1}{\sqrt{N_{\mathrm{T}}}}\mathbf{Q}_{\mathrm{RF}}$ and $\mathbf{f}_{\mathrm{BB},n}=\sqrt{N_{\mathrm{T}}}\mathbf{R}_{\mathrm{BB}}\tilde{\mathbf{f}}_{\mathrm{BB},n}\in\mathbb{C}^{N_{\mathrm{RF}}\times1}$.

For the subarray structure S1, each $\mathbf{f}_{\mathrm{RF},r}$ has to null the channels to Eves. As a result, we need $N_{\mathrm{T}}>N_{\mathrm{RF}}(K-1)L$. However, we may have $N_{\mathrm{T}}>(K-1)L$ but $N_{\mathrm{T}}\leq N_{\mathrm{RF}}(K-1)L$. Therefore, we divide the RF chains into $\tilde{N}_{\mathrm{RF}}$ distinct groups, each group has $\frac{N_{\mathrm{RF}}}{\tilde{N}_{\mathrm{RF}}}$ RF chains which process the same digitally-preocded symbols, where $\tilde{N}_{\mathrm{RF}}=\gcd\left(\min\left(\left\lfloor\frac{N_{\mathrm{T}}-1}{(K-1)L}\right\rfloor,N_{\mathrm{RF}}\right),N_{\mathrm{RF}}\right)$. Therefore, we should have $N_{\mathrm{T}}>\tilde{N}_{\mathrm{RF}}(K-1)L$ provided that $N_{\mathrm{T}}>(K-1)L$. Equivalently, we proceed assuming that we have $\tilde{N}_{\mathrm{RF}}$ chains, each is connected to $\frac{N_{\mathrm{T}}}{\tilde{N}_{\mathrm{RF}}}$ antennas such that $N_{\mathrm{T}}>\tilde{N}_{\mathrm{RF}}(K-1)L$. We express $\mathbf{f}_{\mathrm{RF},r}$ as

$$\mathbf{f}_{\mathrm{RF},r}=\mathbf{U}_{\mathrm{RF},r}\tilde{\mathbf{f}}_{\mathrm{RF},r}, \quad (33)$$

where $\mathbf{U}_{\mathrm{RF},r}=\mathcal{N}\left[\mathbf{A}_{\mathrm{T,Eves},r}\right]\in\mathbb{C}^{\frac{N_{\mathrm{T}}}{\tilde{N}_{\mathrm{RF}}}\times\left(\frac{N_{\mathrm{T}}}{\tilde{N}_{\mathrm{RF}}}-(K-1)L\right)}$ is a semi-unitary matrix in the null space of the channels to Eves seen by the r^{th} RF chain group, $\mathbf{A}_{\mathrm{T,Eves},r}=\mathbf{A}_{\mathrm{T,Eves}}\left((r-1)\frac{N_{\mathrm{T}}}{\tilde{N}_{\mathrm{RF}}}+1:r\frac{N_{\mathrm{T}}}{\tilde{N}_{\mathrm{RF}}},:\right)$, and $\tilde{\mathbf{f}}_{\mathrm{RF},r}\in\mathbb{C}^{\left(\frac{N_{\mathrm{T}}}{\tilde{N}_{\mathrm{RF}}}-(K-1)L\right)\times1}$. Let $\mathbf{U}_{\mathrm{RF}}=\mathrm{blkdiag}\left(\mathbf{U}_{\mathrm{RF},1},\ldots,\mathbf{U}_{\mathrm{RF},\tilde{N}_{\mathrm{RF}}}\right)\in\mathbb{C}^{N_{\mathrm{T}}\times\left(N_{\mathrm{T}}-\tilde{N}_{\mathrm{RF}}(K-1)L\right)}$ and $\tilde{\mathbf{F}}_{\mathrm{RF}}=\mathrm{blkdiag}\left(\tilde{\mathbf{f}}_{\mathrm{RF},1},\ldots,\tilde{\mathbf{f}}_{\mathrm{RF},N_{\mathrm{RF}}}\right)\in\mathbb{C}^{\left(N_{\mathrm{T}}-\tilde{N}_{\mathrm{RF}}(K-1)L\right)\times N_{\mathrm{RF}}}$, then we have $\mathbf{F}_{\mathrm{RF}}=\mathbf{U}_{\mathrm{RF}}\tilde{\mathbf{F}}_{\mathrm{RF}}$, and $\mathbf{U}_{\mathrm{RF}}^H\mathbf{U}_{\mathrm{RF}}=\mathbf{I}_{N_{\mathrm{T}}-\tilde{N}_{\mathrm{RF}}(K-1)L}$.

Therefore, $\overline{\mathrm{SNR}}_{\mathrm{B}}$ and $\mathbf{f}_{\mathrm{BB},n}$ can also be given by (27) and (28) respectively. Furthermore, $\overline{\mathrm{SNR}}_{\mathrm{B}}$ can be simplified to

$$\overline{\mathrm{SNR}}_{\mathrm{B}} = \frac{\gamma}{N_{\mathrm{C}}} \sum_{r=1}^{\tilde{N}_{\mathrm{RF}}} \frac{\tilde{\mathbf{f}}_{\mathrm{RF},r}^H \left(\sum_{n=1}^{N_{\mathrm{C}}} \mathbf{U}_{\mathrm{RF},r}^H \mathbf{h}_{n,1,r}^H \mathbf{h}_{n,1,r} \mathbf{U}_{\mathrm{RF},r} \right) \tilde{\mathbf{f}}_{\mathrm{RF},r}}{\tilde{\mathbf{f}}_{\mathrm{RF},r}^H \tilde{\mathbf{f}}_{\mathrm{RF},r}}, \tag{34}$$

where $\mathbf{h}_{n,1,r} = \mathbf{h}_{n,1} \left((r-1) \frac{N_{\mathrm{T}}}{\tilde{N}_{\mathrm{RF}}} + 1 : r \frac{N_{\mathrm{T}}}{\tilde{N}_{\mathrm{RF}}} \right) \ \forall r$. Therefore, we obtain $\tilde{\mathbf{f}}_{\mathrm{RF},r}$ which maximizes (34) as

$$\tilde{\mathbf{f}}_{\mathrm{RF},r} = \boldsymbol{\mathcal{E}}_{\max} \Big[\sum_{n=1}^{N_{\mathrm{C}}} \mathbf{U}_{\mathrm{RF},r}^H \mathbf{h}_{n,1,r}^H \mathbf{h}_{n,1,r} \mathbf{U}_{\mathrm{RF},r} \Big]. \tag{35}$$

Since $\tilde{\mathbf{F}}_{\mathrm{RF}}^H \tilde{\mathbf{F}}_{\mathrm{RF}} = \mathbf{I}_{\tilde{N}_{\mathrm{RF}}}$ due to (35), $\mathbf{f}_{\mathrm{BB},n}$ is simplified to

$$\mathbf{f}_{\mathrm{BB},n} = \frac{\left[\tilde{\mathbf{f}}_{\mathrm{RF},1}^H \mathbf{U}_{\mathrm{RF},1}^H \mathbf{h}_{n,1,1}^H, \ldots, \tilde{\mathbf{f}}_{\mathrm{RF},N_{\mathrm{RF}}}^H \mathbf{U}_{\mathrm{RF},N_{\mathrm{RF}}}^H \mathbf{h}_{n,1,N_{\mathrm{RF}}}^H \right]^T}{\sqrt{\sum_{r=1}^{N_{\mathrm{RF}}} \left| \mathbf{h}_{n,1,r} \mathbf{U}_{\mathrm{RF},r} \tilde{\mathbf{f}}_{\mathrm{RF},r} \right|^2}}, \tag{36}$$

which is the well-known MRT precoder for the equivalent channel $\mathbf{h}_{n,1} \mathbf{U}_{\mathrm{RF}} \tilde{\mathbf{F}}_{\mathrm{RF}}$. Note that entries of $\mathbf{U}_{\mathrm{RF},r} \tilde{\mathbf{f}}_{\mathrm{RF},r}$ are not likely to satisfy the modulus constraint. Moreover, approximating $\mathbf{U}_{\mathrm{RF},r} \tilde{\mathbf{f}}_{\mathrm{RF},r}$ by $\exp\left(j \angle \left(\mathbf{U}_{\mathrm{RF},r} \tilde{\mathbf{f}}_{\mathrm{RF},r} \right) \right) / \sqrt{N_{\mathrm{T}}/N_{\mathrm{RF}}}$ results in losing the null space property. Therefore, TD-P-MRT is not applicable for the subarray structure S2. The computational complexity of TD-P-MRT is $\mathcal{O}\left(N_{\mathrm{T}}^3 + N_{\mathrm{T}} N_{\mathrm{RF}} N_{\mathrm{C}} \right)$.

b) FD-P-MRT: For the four structures, it is necessary that $N_{\mathrm{RF}} \geq K$ to apply FD-P-MRT. We express the baseband precoder $\mathbf{f}_{\mathrm{BB},n}$ as

$$\mathbf{f}_{\mathrm{BB},n} = \mathbf{U}_{\mathrm{BB},n} \tilde{\mathbf{f}}_{\mathrm{BB},n}, \tag{37}$$

where $\mathbf{U}_{\mathrm{BB},n} = \mathcal{N}\left[\mathbf{H}_n \mathbf{F}_{\mathrm{RF}} \right] \in \mathbb{C}^{N_{\mathrm{RF}} \times (N_{\mathrm{RF}} - (K-1))}$ is a semi-unitary matrix in the null space of the equivalent frequency domain channels to Eves $\mathbf{H}_n \mathbf{F}_{\mathrm{RF}}$. We design $\mathbf{F}_{\mathrm{RF}}$ and $\tilde{\mathbf{f}}_{\mathrm{BB},n}$ to maximize $\overline{\mathrm{SNR}}_{\mathrm{B}}$ given by

$$\begin{aligned} \overline{\mathrm{SNR}}_{\mathrm{B}} &= \frac{\gamma}{N_{\mathrm{C}}} \sum_{n=1}^{N_{\mathrm{C}}} \frac{\left| \mathbf{h}_{n,1} \mathbf{F}_{\mathrm{RF}} \mathbf{U}_{\mathrm{BB},n} \tilde{\mathbf{f}}_{\mathrm{BB},n} \right|^2}{\left\| \mathbf{F}_{\mathrm{RF}} \mathbf{U}_{\mathrm{BB},n} \tilde{\mathbf{f}}_{\mathrm{BB},n} \right\|^2} \\ &= \frac{\gamma}{N_{\mathrm{C}}} \sum_{n=1}^{N_{\mathrm{C}}} \frac{\tilde{\mathbf{f}}_{\mathrm{BB},n}^H (\mathbf{U}_{\mathrm{BB},n}^H \mathbf{F}_{\mathrm{RF}}^H \mathbf{h}_{n,1}^H \mathbf{h}_{n,1} \mathbf{F}_{\mathrm{RF}} \mathbf{U}_{\mathrm{BB},n}) \tilde{\mathbf{f}}_{\mathrm{BB},n}}{\tilde{\mathbf{f}}_{\mathrm{BB},n}^H (\mathbf{U}_{\mathrm{BB},n}^H \mathbf{F}_{\mathrm{RF}}^H \mathbf{F}_{\mathrm{RF}} \mathbf{U}_{\mathrm{BB},n}) \tilde{\mathbf{f}}_{\mathrm{BB},n}}. \end{aligned} \tag{38}$$

Using the generalized eigenvector decomposition, $\tilde{\mathbf{f}}_{\mathrm{BB},n}$ maximizing (38) is given by

$$\begin{aligned} \tilde{\mathbf{f}}_{\mathrm{BB},n} &= \kappa_n \boldsymbol{\mathcal{E}}_{\max} \Big[\left(\mathbf{U}_{\mathrm{BB},n}^H \mathbf{F}_{\mathrm{RF}}^H \mathbf{F}_{\mathrm{RF}} \mathbf{U}_{\mathrm{BB},n} \right)^{-1} \\ &\quad \times \mathbf{U}_{\mathrm{BB},n}^H \mathbf{F}_{\mathrm{RF}}^H \mathbf{h}_{n,1}^H \mathbf{h}_{n,1} \mathbf{F}_{\mathrm{RF}} \mathbf{U}_{\mathrm{BB},n} \Big] \\ &= \frac{\left(\mathbf{U}_{\mathrm{BB},n}^H \mathbf{F}_{\mathrm{RF}}^H \mathbf{F}_{\mathrm{RF}} \mathbf{U}_{\mathrm{BB},n} \right)^{-1} \mathbf{U}_{\mathrm{BB},n}^H \mathbf{F}_{\mathrm{RF}}^H \mathbf{h}_{n,1}^H}{\left\| \left(\mathbf{U}_{\mathrm{BB},n}^H \mathbf{F}_{\mathrm{RF}}^H \mathbf{F}_{\mathrm{RF}} \mathbf{U}_{\mathrm{BB},n} \right)^{-\frac{1}{2}} \mathbf{U}_{\mathrm{BB},n}^H \mathbf{F}_{\mathrm{RF}}^H \mathbf{h}_{n,1}^H \right\|}, \end{aligned} \tag{39}$$

where κ_n is a scaling factor to have $\left\| \mathbf{F}_{\mathrm{RF}} \mathbf{f}_{\mathrm{BB},n} \right\|^2 = 1$, the second equality holds since $(\mathbf{U}_{\mathrm{BB},n}^H \mathbf{F}_{\mathrm{RF}}^H \mathbf{F}_{\mathrm{RF}} \mathbf{U}_{\mathrm{BB},n})^{-1} \mathbf{U}_{\mathrm{BB},n}^H \mathbf{F}_{\mathrm{RF}}^H \mathbf{h}_{n,1}^H \mathbf{h}_{n,1} \mathbf{F}_{\mathrm{RF}} \mathbf{U}_{\mathrm{BB},n}$ is a rank-one matrix, and the corresponding $\overline{\mathrm{SNR}}_{\mathrm{B}}$ is expressed as

$$\begin{aligned} \overline{\mathrm{SNR}}_{\mathrm{B}} &= \frac{\gamma}{N_{\mathrm{C}}} \sum_{n=1}^{N_{\mathrm{C}}} \mathbf{h}_{n,1} \mathbf{F}_{\mathrm{RF}} \mathbf{U}_{\mathrm{BB},n} \left(\mathbf{U}_{\mathrm{BB},n}^H \mathbf{F}_{\mathrm{RF}}^H \mathbf{F}_{\mathrm{RF}} \mathbf{U}_{\mathrm{BB},n} \right)^{-1} \\ &\quad \times \mathbf{U}_{\mathrm{BB},n}^H \mathbf{F}_{\mathrm{RF}}^H \mathbf{h}_{n,1}^H. \end{aligned} \tag{40}$$

Note that $\mathbf{U}_{\mathrm{BB},n}$ is a function of $\mathbf{F}_{\mathrm{RF}}$, and $\mathbf{F}_{\mathrm{RF}}$ is fixed across subcarriers while $\mathbf{U}_{\mathrm{BB},n}$ is not. Even if we fix $\mathbf{U}_{\mathrm{BB},n}$, we cannot get $\mathbf{F}_{\mathrm{RF}}$ in a closed-form. Consequently, we cannot get $\mathbf{F}_{\mathrm{RF}}$ in a closed-form or by an alternately optimizing algorithm. As suboptimal solutions, we obtain $\mathbf{F}_{\mathrm{RF}}$ for the fully-connected structures F1 and F2 as in (18) and (20) respectively, and for the subarray structures S1 and S2 as in (22) and (23) respectively. Then, $\mathbf{f}_{\mathrm{BB},n}$ is obtained as in (37). The computational complexity of FD-P-MRT is $\mathcal{O}\left(N_{\mathrm{T}}^3 N_{\mathrm{C}} + N_{\mathrm{RF}}^3 N_{\mathrm{C}} \right)$.

C. Iterative Secrecy Hybrid Precoding Design

The drawback of the aforementioned solutions is that they do not directly consider the original problem in (10). In this subsection, we propose an iterative hybrid precoding design to maximize the secrecy rate lower bound $\tilde{R}_{\mathrm{sec}}$, which gives a good solution to the problem in (10) (as will be shown). The reason why we choose $\tilde{R}_{\mathrm{sec}}$ to maximize is that we can write $\tilde{R}_{\mathrm{sec}}$ as a function of $\mathbf{F}_{\mathrm{RF}}$ only.

Similar to (12), $\tilde{R}_{\mathrm{sec}}$ can be written as a function of $\mathbf{F}_{\mathrm{RF}}$ and $\mathbf{f}_{\mathrm{BB},n}$ as

$$\tilde{R}_{\mathrm{sec}} = \frac{1}{N_{\mathrm{C}}} \sum_{n=1}^{N_{\mathrm{C}}} \log_2 \left(\frac{1 + \gamma \left| \mathbf{h}_{n,1} \mathbf{F}_{\mathrm{RF}} \mathbf{f}_{\mathrm{BB},n} \right|^2}{1 + \gamma \left\| \mathbf{H}_n \mathbf{F}_{\mathrm{RF}} \mathbf{f}_{\mathrm{BB},n} \right\|^2} \right). \tag{41}$$

Applying the power constraint $\left\| \mathbf{F}_{\mathrm{RF}} \mathbf{f}_{\mathrm{BB},n} \right\|^2 = 1$ into (41), we get

$$\tilde{R}_{\mathrm{sec}} = \frac{1}{N_{\mathrm{C}}} \sum_{n=1}^{N_{\mathrm{C}}} \log_2 \left(\frac{\mathbf{f}_{\mathrm{BB},n}^H (\mathbf{F}_{\mathrm{RF}}^H \mathbf{F}_{\mathrm{RF}} + \gamma \mathbf{F}_{\mathrm{RF}}^H \mathbf{h}_{n,1}^H \mathbf{h}_{n,1} \mathbf{F}_{\mathrm{RF}}) \mathbf{f}_{\mathrm{BB},n}}{\mathbf{f}_{\mathrm{BB},n}^H (\mathbf{F}_{\mathrm{RF}}^H \mathbf{F}_{\mathrm{RF}} + \gamma \mathbf{F}_{\mathrm{RF}}^H \mathbf{H}_n^H \mathbf{H}_n \mathbf{F}_{\mathrm{RF}}) \mathbf{f}_{\mathrm{BB},n}} \right). \tag{42}$$

Using the generalized eigenvector decomposition, $\mathbf{f}_{\mathrm{BB},n}$ maximizing (42) is given by

$$\begin{aligned} \mathbf{f}_{\mathrm{BB},n} &= \kappa_n \boldsymbol{\mathcal{E}}_{\max} \Big[(\mathbf{F}_{\mathrm{RF}}^H \mathbf{F}_{\mathrm{RF}} + \gamma \mathbf{F}_{\mathrm{RF}}^H \mathbf{H}_n^H \mathbf{H}_n \mathbf{F}_{\mathrm{RF}})^{-1} \\ &\quad \times (\mathbf{F}_{\mathrm{RF}}^H \mathbf{F}_{\mathrm{RF}} + \gamma \mathbf{F}_{\mathrm{RF}}^H \mathbf{h}_{n,1}^H \mathbf{h}_{n,1} \mathbf{F}_{\mathrm{RF}}) \Big] \end{aligned} \tag{43}$$

where κ_n is a scaling factor to have $\left\| \mathbf{F}_{\mathrm{RF}} \mathbf{f}_{\mathrm{BB},n} \right\|^2 = 1$, and the corresponding $\tilde{R}_{\mathrm{sec}}$ is expressed as

$$\begin{aligned} \tilde{R}_{\mathrm{sec}} &= \frac{1}{N_{\mathrm{C}}} \sum_{n=1}^{N_{\mathrm{C}}} \log_2 \Big(\lambda_{\max} \Big[(\mathbf{F}_{\mathrm{RF}}^H \mathbf{F}_{\mathrm{RF}} + \gamma \mathbf{F}_{\mathrm{RF}}^H \mathbf{H}_n^H \mathbf{H}_n \mathbf{F}_{\mathrm{RF}})^{-1} \\ &\quad \times (\mathbf{F}_{\mathrm{RF}}^H \mathbf{F}_{\mathrm{RF}} + \gamma \mathbf{F}_{\mathrm{RF}}^H \mathbf{h}_{n,1}^H \mathbf{h}_{n,1} \mathbf{F}_{\mathrm{RF}}) \Big] \Big). \end{aligned} \tag{44}$$

Now, we can write the hybrid precoding design problem as a function of $\mathbf{F}_{\mathrm{RF}}$ only as

$$\begin{aligned} &\arg\max_{\mathbf{F}_{\mathrm{RF}}} \frac{1}{N_{\mathrm{C}}} \sum_{n=1}^{N_{\mathrm{C}}} \log_2 \Big(\lambda_{\max} \Big[(\mathbf{F}_{\mathrm{RF}}^H \mathbf{F}_{\mathrm{RF}} + \gamma \mathbf{F}_{\mathrm{RF}}^H \mathbf{H}_n^H \mathbf{H}_n \mathbf{F}_{\mathrm{RF}})^{-1} \\ &\quad \times (\mathbf{F}_{\mathrm{RF}}^H \mathbf{F}_{\mathrm{RF}} + \gamma \mathbf{F}_{\mathrm{RF}}^H \mathbf{h}_{n,1}^H \mathbf{h}_{n,1} \mathbf{F}_{\mathrm{RF}}) \Big] \Big), \\ &\quad \text{s.t. } \mathbf{F}_{\mathrm{RF}} \in \mathcal{F}_{\mathrm{RF}}. \end{aligned} \tag{45}$$

We know that $\tilde{R}_{\mathrm{sec}}$ is a non-convex function of $\mathbf{F}_{\mathrm{RF}}$. Moreover, the constraint is non-convex (except for $\mathcal{F}_{\mathrm{RF}} = \mathcal{F}_{\mathrm{RF}}^{\mathrm{F1}}$).

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TCOMM.2017.2734666, IEEE Transactions on Communications

Algorithm 1 Hybrid precoder design for secrecy rate maximization

Initialization: Obtain $\mathbf{F}_{\mathrm{RF}}^{(0)}$ as in App-FD or P-MRT (choose the scheme that achieves higher secrecy rate), $p=0$.
while $p \leq P$ (or any other appropriate stopping criterion)
Calculate the gradient $\nabla_{\mathbf{F}_{\mathrm{RF}}}^{(p)}$ using (46).
Updating rule:
For fully-connected structure F1,
$\left[\mathbf{F}_{\mathrm{RF}}^{(p+1)}, \alpha\right] = \underset{\mathbf{F}_{\mathrm{RF}}, \alpha}{\arg\max}\, \tilde{R}_{\mathrm{sec}}\left(\mathbf{F}_{\mathrm{RF}}\right)$,
s.t. $\mathbf{F}_{\mathrm{RF}} = \mathbf{F}_{\mathrm{RF}}^{(p)} + \alpha \nabla_{\mathbf{F}_{\mathrm{RF}}}^{(p)}$.
For fully-connected structure F2,
$\left[\mathbf{F}_{\mathrm{RF}}^{(p+1)}, \alpha\right] = \underset{\mathbf{F}_{\mathrm{RF}}, \alpha}{\arg\max}\, \tilde{R}_{\mathrm{sec}}\left(\mathbf{F}_{\mathrm{RF}}\right)$,
s.t. $\mathbf{F}_{\mathrm{RF}} = \exp\left(j\angle\left(\mathbf{F}_{\mathrm{RF}}^{(p)} + \alpha \nabla_{\mathbf{F}_{\mathrm{RF}}}^{(p)}\right)\right)/\sqrt{N_{\mathrm{T}}}$.
For subarray structure S1,
$\left[\mathbf{F}_{\mathrm{RF}}^{(p+1)}, \alpha\right] = \underset{\mathbf{F}_{\mathrm{RF}}, \alpha}{\arg\max}\, \tilde{R}_{\mathrm{sec}}\left(\mathbf{F}_{\mathrm{RF}}\right)$,
s.t. $\mathbf{F}_{\mathrm{RF}} = \boldsymbol{\mathcal{M}}\left(\mathbf{F}_{\mathrm{RF}}^{(p)} + \alpha \nabla_{\mathbf{F}_{\mathrm{RF}}}^{(p)}\right)$.
For subarray structure S2,
$\left[\mathbf{F}_{\mathrm{RF}}^{(p+1)}, \alpha\right] = \underset{\mathbf{F}_{\mathrm{RF}}, \alpha}{\arg\max}\, \tilde{R}_{\mathrm{sec}}\left(\mathbf{F}_{\mathrm{RF}}\right)$,
s.t. $\mathbf{F}_{\mathrm{RF}} = \boldsymbol{\mathcal{M}}\left(\exp\left(j\angle\left(\mathbf{F}_{\mathrm{RF}}^{(p)} + \alpha \nabla_{\mathbf{F}_{\mathrm{RF}}}^{(p)}\right)\right)\right)/\sqrt{\frac{N_{\mathrm{T}}}{N_{\mathrm{RF}}}}$.
$p = p+1$.
end while
Obtain the baseband precoders $\left\{\mathbf{f}_{\mathrm{BB},n}\right\}$ using (43).

We propose a suboptimal gradient ascent algorithm to design $\mathbf{F}_{\mathrm{RF}}$. However, the maximum eigenvalue function $\lambda_{\max}[\mathbf{X}]$ is non-differentiable. Applying the inequality $\lambda_{\max}[\mathbf{X}] \geq \frac{1}{\mathrm{rank}[\mathbf{X}]}\mathrm{Tr}[\mathbf{X}]$ into (44), we obtain a differentiable lower bound with gradient $\nabla_{\mathbf{F}_{\mathrm{RF}}}$ given by [38]

$$\nabla_{\mathbf{F}_{\mathrm{RF}}} = \sum_{n=1}^{N_{\mathrm{C}}} \frac{\left(\mathbf{I}_{N_{\mathrm{T}}} - \mathbf{C}_n \mathbf{F}_{\mathrm{RF}} (\mathbf{F}_{\mathrm{RF}}^H \mathbf{C}_n \mathbf{F}_{\mathrm{RF}})^{-1} \mathbf{F}_{\mathrm{RF}}^H\right) \mathbf{B}_n \mathbf{F}_{\mathrm{RF}} (\mathbf{F}_{\mathrm{RF}}^H \mathbf{C}_n \mathbf{F}_{\mathrm{RF}})^{-1}}{N_{\mathrm{RF}} N_{\mathrm{C}} \ln 2 \log_2\left(\frac{1}{N_{\mathrm{RF}}}\mathrm{Tr}\left[(\mathbf{F}_{\mathrm{RF}}^H \mathbf{C}_n \mathbf{F}_{\mathrm{RF}})^{-1} \mathbf{F}_{\mathrm{RF}}^H \mathbf{B}_n \mathbf{F}_{\mathrm{RF}}\right]\right)}, \tag{46}$$

where $\mathbf{C}_n = \mathbf{I}_{N_{\mathrm{T}}} + \gamma \mathbf{H}_n^H \mathbf{H}_n$ and $\mathbf{B}_n = \mathbf{I}_{N_{\mathrm{T}}} + \gamma \mathbf{h}_{n,1}^H \mathbf{h}_{n,1}$. Using the gradient $\nabla_{\mathbf{F}_{\mathrm{RF}}}$ in (46), we obtain the RF precoder $\mathbf{F}_{\mathrm{RF}}$ by Algorithm 1, where P is the number of iterations, $\boldsymbol{\mathcal{M}}(\mathbf{X}) = \mathrm{blkdiag}(\mathbf{x}_1, \mathbf{x}_2, \ldots, \mathbf{x}_{N_{\mathrm{RF}}}) \in \mathbb{C}^{N_{\mathrm{T}} \times N_{\mathrm{RF}}}$ and $\mathbf{x}_r = \mathbf{X}\left((r-1)\frac{N_{\mathrm{T}}}{N_{\mathrm{RF}}} + 1 : r\frac{N_{\mathrm{T}}}{N_{\mathrm{RF}}}, r\right) \in \mathbb{C}^{\frac{N_{\mathrm{T}}}{N_{\mathrm{RF}}} \times 1}$ $\forall r \in \{1, 2, \ldots, N_{\mathrm{RF}}\}$. The step size α is obtained by a backtracking line search [39].

It is well-known that gradient ascent algorithm is highly affected by the initial solution since it is a local solver. As an initialization, we propose to use the hybrid precoder of App-FD or P-MRT, where we choose the scheme that achieves higher secrecy rate. The computational complexity of Algorithm 1 is $\mathcal{O}\left(N_{\mathrm{T}}^3 N_{\mathrm{C}} + N_{\mathrm{T}} N_{\mathrm{RF}} N_{\mathrm{C}} + \left(N_{\mathrm{RF}}^3 + N_{\mathrm{T}} N_{\mathrm{RF}}^2\right) N_{\mathrm{C}} P\right)$.

IV. Hybrid Precoder Design for Secrecy Throughput Maximization with Partial Channel Knowledge

We design the hybrid precoder to maximize the secrecy throughput defined as $\eta_{\mathrm{sec}} = R_{\mathrm{sec}}(1 - \epsilon_{\mathrm{sec}})$ [32], [33], where ϵ_{sec} is the secrecy outage probability. We assume that Alice has perfect full knowledge of the channel to Bob but has partial knowledge of the channels to Eves. Similar to [15] and [16], Alice has knowledge only of the AoDs of the paths to Eves. Bob and Eves have full knowledge of their channels to Alice. Furthermore, we assume that Eves do not cooperate.

Due to the limited scattering nature of mmWave channels and the large number of antennas at the transmitter, the mmWave channel is typically estimated by estimating the channel gains and AoDs of the propagation paths based on compressed sensing (e.g., [40]–[42]). The assumption of partial knowledge of the channels to Eves can be viewed in two different scenarios as follows:

Scenario-1: The transmission is performed based on frequency-division-duplexing (FDD). The uplink and downlink channels are different. However, the AoDs are invariant with frequency [43]–[46], and hence without any feedback Alice has partial knowledge (knowledge of the AoDs only) of channels to Bob and Eves. Alice receives a channel feedback from Bob to complete the channel knowledge, but Alice does not receive any channel feedback from Eves. Therefore, Alice uses the AoDs of the paths to Eves as partial channel knowledge.

Scenario-2: The transmission is performed based on time-division-duplexing (TDD). The uplink and downlink channels are reciprocal. Since we assume that Eves are active nodes in the system (Bob and Eves play interchangeable roles), the channel knowledge of Bob and Eves may not be up-to-date. Alice re-estimates the channel to Bob. Since the coherence time of the AoDs is much longer than that of the channel gains [15], [16], [43]–[45], [47], Alice uses the estimates of the AoDs of the paths to Eves as partial channel knowledge (assuming that the AoDs remain almost unchanged), and does not re-estimate the channel gains to Eves.[1]

In the following, we derive a secrecy outage probability upper bound $\tilde{\epsilon}_{\mathrm{sec}}$, which results in a secrecy throughput lower bound $\tilde{\eta}_{\mathrm{sec}} = R_{\mathrm{sec}}(1 - \tilde{\epsilon}_{\mathrm{sec}})$. Then, we design the hybrid precoder to maximize the secrecy throughput lower bound $\tilde{\eta}_{\mathrm{sec}}$.

A. Secrecy Outage Probability

The secrecy outage probability ϵ_{sec} is defined as [31], [51]

$$\epsilon_{\mathrm{sec}} = \mathbb{P}\left(\min_k \{R_1 - R_k\}_{k=2}^K < R_{\mathrm{sec}}\right). \tag{47}$$

It can be rewritten as

$$\epsilon_{\mathrm{sec}} = 1 - \mathbb{P}\left(\max_k \{R_k\}_{k=2}^K < R_{\mathrm{o}}\right) = 1 - \prod_{k=2}^K \mathbb{P}\left(R_k < R_{\mathrm{o}}\right), \tag{48}$$

where $R_{\mathrm{o}} = R_1 - R_{\mathrm{sec}}$. We derive a secrecy outage probability upper bound $\tilde{\epsilon}_{\mathrm{sec}}$. Applying Jensen's inequality into (7), we get

$$\begin{aligned} R_k &\leq \log_2\left(1 + \gamma \frac{1}{N_{\mathrm{C}}} \sum_{n=1}^{N_{\mathrm{C}}} \left|\mathbf{h}_{n,k} \mathbf{F}_{\mathrm{RF}} \mathbf{f}_{\mathrm{BB},n}\right|^2\right) \\ &= \log_2\left(1 + \gamma \frac{1}{N_{\mathrm{C}}} \sum_{n=1}^{N_{\mathrm{C}}} \left|\sum_{l=1}^{L} \alpha_{l,k} \mathbf{a}_{l,k}^H \omega_{n,l,k} \mathbf{F}_{\mathrm{RF}} \mathbf{f}_{\mathrm{BB},n}\right|^2\right). \end{aligned} \tag{49}$$

[1]For link adaptation or channel knowledge exploitation, the key parameter is the coherence time of the relevant channel parameters divided by transmission time interval (TTI). For mmWave systems, although the channel coherence time can become much shorter than that of current systems (e.g., 10 times shorter if 30 GHz versus 3 GHz with the same mobile speed), TTI for mmWave systems are also much shorter than that of current systems due to much smaller latency requirement (e.g., 125 μs TTI for mmWave system [48] versus 1 ms TTI for long-term evolution (LTE) [49]). The relevant channel parameter for our case is AoD, which has coherence time much longer (tens or hundreds times as reported in [50]) than that of the channel gains [15], [16], [43]–[45], [47]. Thus, this justifies our assumptions.

Using the triangle inequality and the arithmetic-quadratic mean inequality, we have

$$\left|\frac{1}{L}\sum_{l=1}^{L}\alpha_{l,k}\mathbf{a}_{l,k}^{H}\omega_{n,l,k}\mathbf{F}_{\mathrm{RF}}\mathbf{f}_{\mathrm{BB},n}\right|^{2}\leq\frac{1}{L}\sum_{l=1}^{L}\left|\alpha_{l,k}\right|^{2}\left|\mathbf{a}_{l,k}^{H}\mathbf{F}_{\mathrm{RF}}\mathbf{f}_{\mathrm{BB},n}\right|^{2}. \tag{50}$$

Applying (49) and (50) into (48), we get

$$\begin{aligned}\epsilon_{\mathrm{sec}}&\leq 1-\prod_{k=2}^{K}\mathbb{P}\left(\sum_{l=1}^{L}\left|\alpha_{l,k}\right|^{2}\sum_{n=1}^{N_{\mathrm{C}}}\left|\mathbf{a}_{l,k}^{H}\mathbf{F}_{\mathrm{RF}}\mathbf{f}_{\mathrm{BB},n}\right|^{2}<\delta\right)\\&\triangleq\tilde{\epsilon}_{\mathrm{sec}},\end{aligned} \tag{51}$$

where $\delta=\frac{\left(2^{R_{\mathrm{o}}}-1\right)N_{\mathrm{C}}}{\gamma L}$. The term $\sum_{l=1}^{L}\left|\alpha_{l,k}\right|^{2}\sum_{n=1}^{N_{\mathrm{C}}}\left|\mathbf{a}_{l,k}^{H}\mathbf{F}_{\mathrm{RF}}\mathbf{f}_{\mathrm{BB},n}\right|^{2}$ represents a sum of independent Gamma-distributed random variables with shape parameter of m and scale parameters of $\left\{\frac{r_{l,k}}{m}\right\}$, where $r_{l,k}=\rho_{l}\sum_{n=1}^{N_{\mathrm{C}}}\left|\mathbf{a}_{l,k}^{H}\mathbf{F}_{\mathrm{RF}}\mathbf{f}_{\mathrm{BB},n}\right|^{2}$. Using [52, Eq. 15], we can write the secrecy outage probability upper bound $\tilde{\epsilon}_{\mathrm{sec}}$ in (51) as

$$\tilde{\epsilon}_{\mathrm{sec}}=1-\prod_{k=2}^{K}\left[\prod_{l=1}^{L}\left(\frac{r_{\min,k}}{r_{l,k}}\right)^{m}\right]\sum_{t=0}^{\infty}v_{t}\frac{\Upsilon\left(mL+t,\frac{m\delta}{r_{\min,k}}\right)}{\Gamma\left(mL+t\right)}, \tag{52}$$

where $r_{\min,k}=\min_{l}\{r_{l,k}\}$, and the coefficients $\{v_t\}$ can be obtained recursively as

$$v_{t}=\frac{m}{t}\sum_{i=1}^{t}\left[\sum_{j=1}^{L}\left(1-\frac{r_{\min,k}}{r_{j,k}}\right)^{i}\right]v_{t-i},\ \forall t\geq 1, \tag{53}$$

where $v_0=1$. For integer values of m, $\tilde{\epsilon}_{\mathrm{sec}}$ in (52) is simplified (with the help of [53, Sec. II]) to

$$\tilde{\epsilon}_{\mathrm{sec}}=1-\prod_{k=2}^{K}\Big[\prod_{l=1}^{L}\left(\frac{-r_{l,k}}{m}\right)^{m}\Big]\sum_{l=1}^{L}\sum_{t=1}^{m}\left(-1\right)^{t}v_{l,t,k}\frac{\Upsilon\left(t,\frac{m\delta}{r_{l,k}}\right)}{\Gamma\left(t\right)}, \tag{54}$$

where the coefficients $\{v_{l,t,k}\}$ can be obtained as

$$v_{l,t,k}=\lim_{s\to\frac{m}{r_{l,k}}}\frac{1}{(m-t)!}\frac{\partial^{m-t}}{\partial^{m-t}s}\Big[\prod_{i=1,\,i\neq l}^{L}\left(s-\frac{m}{r_{i,k}}\right)^{-m}\Big]. \tag{55}$$

For the special case $m=1$, $\tilde{\epsilon}_{\mathrm{sec}}$ in (54) can be simplified to

$$\tilde{\epsilon}_{\mathrm{sec}}=1-\prod_{k=2}^{K}\Big(1-\sum_{l=1}^{L}e^{-\frac{\delta}{r_{l,k}}}\prod_{n\neq l}\frac{r_{l,k}}{r_{l,k}-r_{n,k}}\Big). \tag{56}$$

Now, we obtain the secrecy throughput lower bound $\tilde{\eta}_{\mathrm{sec}}$ as $\tilde{\eta}_{\mathrm{sec}}=R_{\mathrm{sec}}\left(1-\tilde{\epsilon}_{\mathrm{sec}}\right)$.

B. Low-Complexity Secrecy Hybrid Precoding Designs

In this subsection, we investigate if the low-complexity secrecy hybrid precoding strategies in subsection III-B are applicable in case of partial channel knowledge. Examining the secrecy outage probability upper bound $\tilde{\epsilon}_{\mathrm{sec}}$ in (59) with $N_{\mathrm{RF}}=N_{\mathrm{T}}$ ($\mathbf{F}_{\mathrm{RF}}=\mathbf{I}_{N_{\mathrm{T}}}$), we know that the fully digital precoders $\{\mathbf{f}_{\mathrm{BB},n}\}$ have to be designed jointly and do not have closed-form expressions, in contrast to maximizing the secrecy rate in subsection III-A where the fully digital precoders are designed separately and have closed-form expressions. As a result, we cannot have sufficient conditions on the number of RF chains needed to realize the performance of the fully digital precoding in case of partial channel knowledge. Furthermore, it is not tractable to design the hybrid precoder by approximating the fully digital precoders in case of partial channel knowledge.

Since TD-P-MRT described in subsection III-B2 requires only the knowledge of the AoDs to Eves which is available at Alice in case of partial channel knowledge, TD-P-MRT can be applied also in case of partial channel knowledge with the same constraints on N_{RF}. On the contrary, FD-P-MRT cannot be applied since it requires the knowledge of frequency domain channels to Eves which is not available at Alice in case of partial channel knowledge.

C. Iterative Secrecy Hybrid Precoding Design

Following the derived secrecy outage probability upper bound $\tilde{\epsilon}_{\mathrm{sec}}$ in (59), the hybrid precoder is designed to maximize the secrecy throughput lower bound $\tilde{\eta}_{\mathrm{sec}}$ as

$$\begin{aligned}\underset{\mathbf{F}_{\mathrm{RF}},\{\mathbf{f}_{\mathrm{BB},n}\},R_{\mathrm{sec}}}{\arg\max}\quad & R_{\mathrm{sec}}\left(1-\tilde{\epsilon}_{\mathrm{sec}}\left(\mathbf{F}_{\mathrm{RF}},\{\mathbf{f}_{\mathrm{BB},n}\},R_{\mathrm{sec}}\right)\right),\\ \text{s.t. } & 0\leq R_{\mathrm{sec}}\leq R_{\mathrm{MRT}},\ \mathbf{F}_{\mathrm{RF}}\in\mathcal{F}_{\mathrm{RF}},\\ & \sum_{n=1}^{N_{\mathrm{C}}}\left\|\mathbf{F}_{\mathrm{RF}}\mathbf{f}_{\mathrm{BB},n}\right\|^{2}=N_{\mathrm{C}},\end{aligned} \tag{57}$$

where R_{MRT} is the maximum achievable rate of Bob by the maximum ratio transmission (MRT) scheme in [54] where the hybrid precoder is designed to maximize the rate of Bob while ignoring Eves. The optimization problem in (57) is non-convex, and cannot be solved directly. In the following, we will focus on the secrecy outage probability minimization problem written as

$$\begin{aligned}\underset{\mathbf{F}_{\mathrm{RF}},\{\mathbf{f}_{\mathrm{BB},n}\}}{\arg\min}\quad & \tilde{\epsilon}_{\mathrm{sec}}\left(\mathbf{F}_{\mathrm{RF}},\{\mathbf{f}_{\mathrm{BB},n}\},R_{\mathrm{sec}}\right),\\ \text{s.t. } & \mathbf{F}_{\mathrm{RF}}\in\mathcal{F}_{\mathrm{RF}},\ \sum_{n=1}^{N_{\mathrm{C}}}\left\|\mathbf{F}_{\mathrm{RF}}\mathbf{f}_{\mathrm{BB},n}\right\|^{2}=N_{\mathrm{C}}.\end{aligned} \tag{58}$$

Then, we will show how to use the secrecy outage probability minimization problem to maximize the secrecy throughput.

We know that $\tilde{\epsilon}_{\mathrm{sec}}$ in (52) is a non-convex and non-differentiable function of the hybrid precoder. Applying the average-max inequality onto (51), we have

$$\begin{aligned}\tilde{\epsilon}_{\mathrm{sec}}&\leq 1-\prod_{k=2}^{K}\mathbb{P}\Big(\max_{l}\Big\{\left|\alpha_{l,k}\right|^{2}\sum_{n=1}^{N_{\mathrm{C}}}\left|\mathbf{a}_{l,k}^{H}\mathbf{F}_{\mathrm{RF}}\mathbf{f}_{\mathrm{BB},n}\right|^{2}\Big\}<\frac{\delta}{L}\Big),\\&=1-\prod_{k=2}^{K}\prod_{l=1}^{L}\mathbb{P}\Big(\left|\alpha_{l,k}\right|^{2}\sum_{n=1}^{N_{\mathrm{C}}}\left|\mathbf{a}_{l,k}^{H}\mathbf{F}_{\mathrm{RF}}\mathbf{f}_{\mathrm{BB},n}\right|^{2}<\frac{\delta}{L}\Big)\\&=1-\prod_{k=2}^{K}\prod_{l=1}^{L}\frac{1}{\Gamma\left(m\right)}\Upsilon(m,\frac{m\delta}{Lr_{l,k}}),\end{aligned} \tag{59}$$

where the upper bound in (59) is a non-convex but differentiable function of the hybrid precoder. Next, we propose an alternating algorithm which designs the RF precoder and the baseband precoders alternately using the gradient of the upper bound in (59).

1) RF Precoding Design: First, we fix the baseband precoders $\{\mathbf{f}_{\mathrm{BB},n}\}$ and optimize over the RF precoder $\mathbf{F}_{\mathrm{RF}}$ to minimize the secrecy outage probability upper bound $\tilde{\epsilon}_{\mathrm{sec}}$. We propose a suboptimal gradient descent algorithm to design the RF precoder. The gradient $\nabla_{\mathbf{F}_{\mathrm{RF}}}$ of the the upper bound in (59) with respect to the RF precoder is obtained (with the help

Algorithm 2 RF precoding design for secrecy outage probability minimization

Input: $\mathbf{F}_{\mathrm{RF}}^{(0)}$, $\left\{\mathbf{f}_{\mathrm{BB},n}^{(0)}\right\}$, R_{sec}.
$p=0$.
while $p \le P_{\mathrm{RF}}$ (or any other appropriate stopping criterion)
Calculate the gradient $\nabla_{\mathbf{F}_{\mathrm{RF}}}^{(p)}$ using (60).
Updating rule:
For fully-connected structure F1,
$\left[\mathbf{F}_{\mathrm{RF}}^{(p+1)}, \left\{\mathbf{f}_{\mathrm{BB},n}^{(p+1)}\right\}, \alpha\right] = \underset{\mathbf{F}_{\mathrm{RF}}, \{\mathbf{f}_{\mathrm{BB},n}\}, \alpha}{\arg\min} \ \tilde{\epsilon}_{\mathrm{sec}}\left(\mathbf{F}_{\mathrm{RF}}, \{\mathbf{f}_{\mathrm{BB},n}\}, R_{\mathrm{sec}}\right)$,
s.t. $\mathbf{F}_{\mathrm{RF}} = \mathbf{F}_{\mathrm{RF}}^{(p)} + \alpha \nabla_{\mathbf{F}_{\mathrm{RF}}}^{(p)}$,
$\mathbf{f}_{\mathrm{BB},n} = \mathbf{f}_{\mathrm{BB},n}^{(p)} / \sqrt{\sum_{n=1}^{N_{\mathrm{C}}} \left\| \mathbf{F}_{\mathrm{RF}} \mathbf{f}_{\mathrm{BB},n}^{(p)} \right\|^2} \ \forall n$.
For fully-connected structure F2,
$\left[\mathbf{F}_{\mathrm{RF}}^{(p+1)}, \left\{\mathbf{f}_{\mathrm{BB},n}^{(p+1)}\right\}, \alpha\right] = \underset{\mathbf{F}_{\mathrm{RF}}, \{\mathbf{f}_{\mathrm{BB},n}\}, \alpha}{\arg\min} \ \tilde{\epsilon}_{\mathrm{sec}}\left(\mathbf{F}_{\mathrm{RF}}, \{\mathbf{f}_{\mathrm{BB},n}\}, R_{\mathrm{sec}}\right)$,
s.t. $\mathbf{F}_{\mathrm{RF}} = \exp\left(j \angle \left(\mathbf{F}_{\mathrm{RF}}^{(p)} + \alpha \nabla_{\mathbf{F}_{\mathrm{RF}}}^{(p)}\right)\right) / \sqrt{N_{\mathrm{T}}}$,
$\mathbf{f}_{\mathrm{BB},n} = \mathbf{f}_{\mathrm{BB},n}^{(p)} / \sqrt{\sum_{n=1}^{N_{\mathrm{C}}} \left\| \mathbf{F}_{\mathrm{RF}} \mathbf{f}_{\mathrm{BB},n}^{(p)} \right\|^2} \ \forall n$.
For subarray structure S1,
$\left[\mathbf{F}_{\mathrm{RF}}^{(p+1)}, \left\{\mathbf{f}_{\mathrm{BB},n}^{(p+1)}\right\}, \alpha\right] = \underset{\mathbf{F}_{\mathrm{RF}}, \{\mathbf{f}_{\mathrm{BB},n}\}, \alpha}{\arg\min} \ \tilde{\epsilon}_{\mathrm{sec}}\left(\mathbf{F}_{\mathrm{RF}}, \{\mathbf{f}_{\mathrm{BB},n}\}, R_{\mathrm{sec}}\right)$,
s.t. $\mathbf{F}_{\mathrm{RF}} = \boldsymbol{\mathcal{M}}\left(\mathbf{F}_{\mathrm{RF}}^{(p)} + \alpha \nabla_{\mathbf{F}_{\mathrm{RF}}}^{(p)}\right)$,
$\mathbf{f}_{\mathrm{BB},n} = \mathbf{f}_{\mathrm{BB},n}^{(p)} / \sqrt{\sum_{n=1}^{N_{\mathrm{C}}} \left\| \mathbf{F}_{\mathrm{RF}} \mathbf{f}_{\mathrm{BB},n}^{(p)} \right\|^2} \ \forall n$.
For subarray structure S2,
$\left[\mathbf{F}_{\mathrm{RF}}^{(p+1)}, \left\{\mathbf{f}_{\mathrm{BB},n}^{(p+1)}\right\}, \alpha\right] = \underset{\mathbf{F}_{\mathrm{RF}}, \{\mathbf{f}_{\mathrm{BB},n}\}, \alpha}{\arg\min} \ \tilde{\epsilon}_{\mathrm{sec}}\left(\mathbf{F}_{\mathrm{RF}}, \{\mathbf{f}_{\mathrm{BB},n}\}, R_{\mathrm{sec}}\right)$,
s.t. $\mathbf{F}_{\mathrm{RF}} = \boldsymbol{\mathcal{M}}\left(\exp\left(j \angle \left(\mathbf{F}_{\mathrm{RF}}^{(p)} + \alpha \nabla_{\mathbf{F}_{\mathrm{RF}}}^{(p)}\right)\right)\right) / \sqrt{\frac{N_{\mathrm{T}}}{N_{\mathrm{RF}}}}$,
$\mathbf{f}_{\mathrm{BB},n} = \mathbf{f}_{\mathrm{BB},n}^{(p)} / \sqrt{\sum_{n=1}^{N_{\mathrm{C}}} \left\| \mathbf{F}_{\mathrm{RF}} \mathbf{f}_{\mathrm{BB},n}^{(p)} \right\|^2} \ \forall n$.
$p = p+1$.
end while
Output: $\mathbf{F}_{\mathrm{RF}}^{(P_{\mathrm{RF}}+1)}$, $\left\{\mathbf{f}_{\mathrm{BB},n}^{(P_{\mathrm{RF}}+1)}\right\}$.

of Leibniz integral rule [55, Eq. A.2-1]) as

$$\nabla_{\mathbf{F}_{\mathrm{RF}}} = \sum_{k=2}^{K} \sum_{l=1}^{L} \frac{m\left(\frac{m\delta}{Lr_{l,k}}\right)^{m-1} \exp\left(-\frac{m\delta}{Lr_{l,k}}\right)}{L\Upsilon\left(m, \frac{m\delta}{Lr_{l,k}}\right) r_{l,k}^2} \times \left(\delta \nabla_{\mathbf{F}_{\mathrm{RF}}}(r_{l,k}) - r_{l,k} \nabla_{\mathbf{F}_{\mathrm{RF}}}(\delta)\right), \quad (60)$$

where $\nabla_{\mathbf{F}_{\mathrm{RF}}}(r_{l,k}) = \rho_l \mathbf{a}_{l,k} \mathbf{a}_{l,k}^H \mathbf{F}_{\mathrm{RF}} \sum_{n=1}^{N_{\mathrm{C}}} \mathbf{f}_{\mathrm{BB},n} \mathbf{f}_{\mathrm{BB},n}^H$ and $\nabla_{\mathbf{F}_{\mathrm{RF}}}(\delta) = \sum_{n=1}^{N_{\mathrm{C}}} \frac{2^{R_{\mathrm{o}}} \mathbf{h}_{n,1}^H \mathbf{h}_{n,1} \mathbf{F}_{\mathrm{RF}} \mathbf{f}_{\mathrm{BB},n} \mathbf{f}_{\mathrm{BB},n}^H}{L\left(1+\gamma |\mathbf{h}_{n,1} \mathbf{F}_{\mathrm{RF}} \mathbf{f}_{\mathrm{BB},n}|^2\right)}$. Using the gradient $\nabla_{\mathbf{F}_{\mathrm{RF}}}$ in (60), we obtain the RF precoder $\mathbf{F}_{\mathrm{RF}}$ by Algorithm 2, where P_{RF} is the number of iterations, and the step size α is obtained by a backtracking line search.

2) Baseband Precoding Design: Now, we fix the RF precoder $\mathbf{F}_{\mathrm{RF}}$ and optimize over the baseband precoders $\{\mathbf{f}_{\mathrm{BB},n}\}$ to minimize the secrecy outage probability upper bound $\tilde{\epsilon}_{\mathrm{sec}}$. We propose a suboptimal gradient descent algorithm to design the baseband precoders. The gradient $\nabla_{\mathbf{f}_{\mathrm{BB},n}}$ of the the upper bound in (59) with respect to the baseband precoder is obtained (with the help of Leibniz integral rule [55, Eq. A.2-1]) as

$$\nabla_{\mathbf{f}_{\mathrm{BB},n}} = \sum_{k=2}^{K} \sum_{l=1}^{L} \frac{m\left(\frac{m\delta}{Lr_{l,k}}\right)^{m-1} \exp\left(-\frac{m\delta}{Lr_{l,k}}\right)}{L\Upsilon\left(m, \frac{m\delta}{Lr_{l,k}}\right) r_{l,k}^2} \times \left(\delta \nabla_{\mathbf{f}_{\mathrm{BB},n}}(r_{l,k}) - r_{l,k} \nabla_{\mathbf{f}_{\mathrm{BB},n}}(\delta)\right), \quad (61)$$

where $\nabla_{\mathbf{f}_{\mathrm{BB},n}}(r_{l,k}) = \rho_l \mathbf{F}_{\mathrm{RF}}^H \mathbf{a}_{l,k} \mathbf{a}_{l,k}^H \mathbf{F}_{\mathrm{RF}} \mathbf{f}_{\mathrm{BB},n}$ and $\nabla_{\mathbf{f}_{\mathrm{BB},n}}(\delta) = \frac{2^{R_{\mathrm{o}}} \mathbf{F}_{\mathrm{RF}}^H \mathbf{h}_{n,1}^H \mathbf{h}_{n,1} \mathbf{F}_{\mathrm{RF}} \mathbf{f}_{\mathrm{BB},n}}{L\left(1+\gamma |\mathbf{h}_{n,1} \mathbf{F}_{\mathrm{RF}} \mathbf{f}_{\mathrm{BB},n}|^2\right)}$. Using the gradient $\nabla_{\mathbf{f}_{\mathrm{BB},n}}$ in (61), we obtain the baseband precoders $\{\mathbf{f}_{\mathrm{BB},n}\}$ by Algorithm 3, where P_{BB} is the number of iterations, and the step size α is obtained by a backtracking line search.

Algorithm 3 Baseband precoding design for secrecy outage probability minimization

Input: $\mathbf{F}_{\mathrm{RF}}$, $\left\{\mathbf{f}_{\mathrm{BB},n}^{(0)}\right\}$, R_{sec}.
$p=0$.
while $p \le P_{\mathrm{BB}}$ (or any other appropriate stopping criterion)
Calculate the gradient $\left\{\nabla_{\mathbf{f}_{\mathrm{BB},n}}^{(p)}\right\}$ using (61).
Updating rule:
$\left[\left\{\mathbf{f}_{\mathrm{BB},n}^{(p+1)}\right\}, \alpha\right] = \underset{\{\mathbf{f}_{\mathrm{BB},n}\}, \alpha}{\arg\min} \ \tilde{\epsilon}_{\mathrm{sec}}\left(\mathbf{F}_{\mathrm{RF}}, \{\mathbf{f}_{\mathrm{BB},n}\}, R_{\mathrm{sec}}\right)$, s.t. $\mathbf{f}_{\mathrm{BB},n} = \left(\mathbf{f}_{\mathrm{BB},n}^{(p)} + \alpha \nabla_{\mathbf{f}_{\mathrm{BB},n}}^{(p)}\right) / \sqrt{\sum_{n=1}^{N_{\mathrm{C}}} \left\| \mathbf{F}_{\mathrm{RF}} \left(\mathbf{f}_{\mathrm{BB},n}^{(p)} + \alpha \nabla_{\mathbf{f}_{\mathrm{BB},n}}^{(p)}\right) \right\|^2} \ \forall n$.
$p = p+1$.
end while
Output: $\left\{\mathbf{f}_{\mathrm{BB},n}^{(P_{\mathrm{BB}}+1)}\right\}$

3) Initial Hybrid Precoder: Generally, the average SNR of Bob $\overline{\mathrm{SNR}}_{\mathrm{B}}$ is expressed as $\overline{\mathrm{SNR}}_{\mathrm{B}} = \frac{\gamma}{N_{\mathrm{C}}} \sum_{n=1}^{N_{\mathrm{C}}} \frac{|\mathbf{h}_{n,1} \mathbf{F}_{\mathrm{RF}} \mathbf{f}_{\mathrm{BB},n}|^2}{\|\mathbf{F}_{\mathrm{RF}} \mathbf{f}_{\mathrm{BB},n}\|^2}$. For any RF precoder $\mathbf{F}_{\mathrm{RF}}$, the baseband precoder $\mathbf{f}_{\mathrm{BB},n}$ which maximizes $\overline{\mathrm{SNR}}_{\mathrm{B}}$ is obtained as

$$\mathbf{f}_{\mathrm{BB},n} = \frac{\left(\mathbf{F}_{\mathrm{RF}}^H \mathbf{F}_{\mathrm{RF}}\right)^{-1} \mathbf{F}_{\mathrm{RF}}^H \mathbf{h}_{n,1}^H}{\left\| \left(\mathbf{F}_{\mathrm{RF}}^H \mathbf{F}_{\mathrm{RF}}\right)^{-\frac{1}{2}} \mathbf{F}_{\mathrm{RF}}^H \mathbf{h}_{n,1}^H \right\|}, \quad (62)$$

and the corresponding $\overline{\mathrm{SNR}}_{\mathrm{B}} = \frac{\gamma}{N_{\mathrm{C}}} \sum_{n=1}^{N_{\mathrm{C}}} \mathbf{h}_{n,1} \mathbf{F}_{\mathrm{RF}} (\mathbf{F}_{\mathrm{RF}}^H \mathbf{F}_{\mathrm{RF}})^{-1} \mathbf{F}_{\mathrm{RF}}^H \mathbf{h}_{n,1}^H$. As an initial solution, we design the RF precoder $\mathbf{F}_{\mathrm{RF}}$ to maximize the average received SNR of Bob in the null space of the $K-1$ expected strongest directions to Eves.

For the fully-connected structure F1, we express $\mathbf{F}_{\mathrm{RF}}$ as

$$\mathbf{F}_{\mathrm{RF}} = \mathbf{U}_{\mathrm{RF}} \tilde{\mathbf{F}}_{\mathrm{RF}}, \quad (63)$$

where $\mathbf{U}_{\mathrm{RF}} = \mathcal{N}\left[\boldsymbol{\mathcal{E}}_{\max}[\sum_{l=1}^{L} \rho_l \mathbf{a}_{l,2} \mathbf{a}_{l,2}^H], \ldots, \boldsymbol{\mathcal{E}}_{\max}[\sum_{l=1}^{L} \rho_l \mathbf{a}_{l,K} \mathbf{a}_{l,K}^H]\right] \in \mathbb{C}^{N_{\mathrm{T}} \times (N_{\mathrm{T}} - (K-1))}$ is a semi-unitary matrix in the null space of the $K-1$ expected strongest directions to Eves. Similar to (30), $\tilde{\mathbf{F}}_{\mathrm{RF}}$ which maximizes $\overline{\mathrm{SNR}}_{\mathrm{B}}$ is obtained as $\tilde{\mathbf{F}}_{\mathrm{RF}} = \boldsymbol{\mathcal{E}}_{1:\mathrm{N_{RF}}}\left[\sum_{n=1}^{N_{\mathrm{C}}} \mathbf{U}_{\mathrm{RF}}^H \mathbf{h}_{n,1}^H \ \mathbf{h}_{n,1} \mathbf{U}_{\mathrm{RF}}\right]$. For the fully-connected structure F2, we obtain $\mathbf{F}_{\mathrm{RF}}$ as

$$\mathbf{F}_{\mathrm{RF}} = \frac{1}{\sqrt{N_{\mathrm{T}}}} \exp\left(j \angle \mathbf{U}_{\mathrm{RF}} \tilde{\mathbf{F}}_{\mathrm{RF}}\right), \quad (64)$$

which satisfies the modulus constraint and is a good approximation to (63).

For the subarray structure S1, we express $\mathbf{f}_{\mathrm{RF},r}$ as

$$\mathbf{f}_{\mathrm{RF},r} = \mathbf{U}_{\mathrm{RF},r} \tilde{\mathbf{f}}_{\mathrm{RF},r}, \quad (65)$$

where $\mathbf{U}_{\mathrm{RF},r} = \mathcal{N}\left[\boldsymbol{\mathcal{E}}[\sum_{l=1}^{L} \rho_l \mathbf{a}_{l,2,r} \mathbf{a}_{l,2,r}^H], \ldots, \boldsymbol{\mathcal{E}}_{\max}[\sum_{l=1}^{L} \rho_l \mathbf{a}_{l,K,r} \mathbf{a}_{l,K,r}^H]\right] \in \mathbb{C}^{\frac{N_{\mathrm{T}}}{N_{\mathrm{RF}}} \times \left(\frac{N_{\mathrm{T}}}{N_{\mathrm{RF}}} - (K-1)\right)}$ is a semi-unitary matrix in the null space of the $K-1$ expected strongest directions to Eves seen by the r^{th} RF chain, and $\mathbf{a}_{l,k,r} = \mathbf{a}_{l,k}\left((r-1)\frac{N_{\mathrm{T}}}{N_{\mathrm{RF}}} + 1 : r\frac{N_{\mathrm{T}}}{N_{\mathrm{RF}}}\right)$. Similar to (35), $\tilde{\mathbf{f}}_{\mathrm{RF},r}$ which maximizes $\overline{\mathrm{SNR}}_{\mathrm{B}}$ is obtained as $\tilde{\mathbf{f}}_{\mathrm{RF},r} = \boldsymbol{\mathcal{E}}_{\max}\left[\sum_{n=1}^{N_{\mathrm{C}}} \mathbf{U}_{\mathrm{RF},r}^H \mathbf{h}_{n,1,r}^H \mathbf{h}_{n,1,r} \mathbf{U}_{\mathrm{RF},r}\right]$. For the subarray structure S2, we obtain $\mathbf{f}_{\mathrm{RF},r}$ as

$$\mathbf{f}_{\mathrm{RF},r} = \frac{1}{\sqrt{N_{\mathrm{T}}/N_{\mathrm{RF}}}} \exp\left(j \angle \mathbf{U}_{\mathrm{RF},r} \tilde{\mathbf{f}}_{\mathrm{RF},r}\right), \quad (66)$$

which satisfies the modulus constraint and is a good approximation to (65). The initial RF precoders in (63) and (64) require $N_{\mathrm{T}} \ge K$, while the ones in (65) and (66) require $N_{\mathrm{T}} \ge K N_{\mathrm{RF}}$. These two conditions are likely to be satisfied for large-scale mmWave systems.

To solve the secrecy throughput maximization problem in (57), we convert it into a sequence of secrecy outage probabil-

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TCOMM.2017.2734666, IEEE Transactions on Communications

TABLE I. Necessary conditions to apply P-MRT

Channel knwoledge	Fully Digital Precoding ($N_{\mathrm{RF}} = N_{\mathrm{T}}$)	Hybrid Analog-Digital Precoding ($N_{\mathrm{RF}} < N_{\mathrm{T}}$)	
		Structures F1, F2, and S1	Subarray structure S2
Full knowledge	$N_{\mathrm{T}} \geq K$ (FD-P-MRT)	$N_{\mathrm{T}} > (K-1)L$ (TD-P-MRT) or $N_{\mathrm{RF}} \geq K$ (FD-P-MRT)	$N_{\mathrm{RF}} \geq K$ (FD-P-MRT)
Partial knowledge	$N_{\mathrm{T}} > (K-1)L$ (TD-P-MRT)	$N_{\mathrm{T}} > (K-1)L$ (TD-P-MRT)	infeasible

Algorithm 4 Hybrid precoding design for secrecy throughput maximization

Initialization: Obtain $\mathbf{F}_{\mathrm{RF}}^{(0)}$ as in (63), (64), (65), or (66) according to the used structure, then $\left\{\mathbf{f}_{\mathrm{BB},n}^{(0)}\right\}$ as in (62), $p = 0$.

$R_{\mathrm{sec}}^{(0)} = \arg\max_{R_{\mathrm{sec}}} R_{\mathrm{sec}} \left(1 - \tilde{\epsilon}_{\mathrm{sec}} \left(\mathbf{F}_{\mathrm{RF}}^{(0)}, \left\{\mathbf{f}_{\mathrm{BB},n}^{(0)}\right\}, R_{\mathrm{sec}}\right)\right)$,

s.t. $0 \leq R_{\mathrm{sec}} \leq R_{\mathrm{MRT}}$

while $p \leq P$ (or any other appropriate stopping criterion)

$\left[\mathbf{F}_{\mathrm{RF}}^{(p+1)}, \{\mathbf{f}_{\mathrm{BB},n}\}\right] = \arg\min_{\mathbf{F}_{\mathrm{RF}}, \{\mathbf{f}_{\mathrm{BB},n}\}} \tilde{\epsilon}_{\mathrm{sec}} \left(\mathbf{F}_{\mathrm{RF}}, \{\mathbf{f}_{\mathrm{BB},n}\}, R_{\mathrm{sec}}^{(p)}\right)$,

using Algorithm 2 with $\mathbf{F}_{\mathrm{RF}}^{(p)}$ and $\left\{\mathbf{f}_{\mathrm{BB},n}^{(p)}\right\}$ as initial solutions.

$\left\{\mathbf{f}_{\mathrm{BB},n}^{(p+1)}\right\} = \arg\min_{\{\mathbf{f}_{\mathrm{BB},n}\}} \tilde{\epsilon}_{\mathrm{sec}} \left(\mathbf{F}_{\mathrm{RF}}^{(p+1)}, \{\mathbf{f}_{\mathrm{BB},n}\}, R_{\mathrm{sec}}^{(p)}\right)$,

using Algorithm 3 with $\{\mathbf{f}_{\mathrm{BB},n}\}$ as an initial solution.

$R_{\mathrm{sec}}^{(p+1)} = \arg\max_{R_{\mathrm{sec}}} R_{\mathrm{sec}} \left(1 - \tilde{\epsilon}_{\mathrm{sec}} \left(\mathbf{F}_{\mathrm{RF}}^{(p+1)}, \left\{\mathbf{f}_{\mathrm{BB},n}^{(p+1)}\right\}, R_{\mathrm{sec}}\right)\right)$,

s.t. $R_{\mathrm{sec}}^{(p)} \leq R_{\mathrm{sec}} \leq R_{\mathrm{MRT}}$.

$p = p + 1$.

end while

ity minimization problems, each one is solved (as illustrated above) for a fixed target secrecy rate R_{sec}. The secrecy rate R_{sec} which maximizes the secrecy throughput is obtained by one dimensional search. The detailed algorithm is shown in Algorithm 4, where P is the number of iterations. Note that for fully digital precoding, the throughput maximization problem can also be solved using Algorithm 4 after excluding the RF precoder design step. The computational complexity of Algorithm 4 is $\mathcal{O}\Big(N_{\mathrm{T}}^3 + N_{\mathrm{T}} N_{\mathrm{RF}} N_{\mathrm{C}} + \max\left(N_{\mathrm{C}}, KL\right)\left(N_{\mathrm{RF}} N_{\mathrm{T}} P_{\mathrm{BB}} + N_{\mathrm{T}}^2 P_{\mathrm{RF}}\right) P\Big)$.

V. Simulation Results

We evaluate the performances of the proposed hybrid precoders and compare them with the performances of the fully digital precoder and MRT hybrid precoder by means of Monte-Carlo simulations. Regarding the simulation setup, we assume that Alice has 64 antennas ($N_{\mathrm{T}} = 64$). The number of RF chains N_{RF} will be an adjustable parameter through the numerical results. All channels follow the mmWave channel model described in subsection II-B with 12 propagation paths ($L = 12$), where the channel gains $\{\alpha_{l,k}\}$ represents a multi-path Nakagami-m fading channel [29] with shape parameter of $m = 2$ as used in [24], [26], [28] and exponential power delay profile defined as $\left\{\rho_l = \frac{q^{l-1}(1-q)}{(1-q^L)}\right\}$ where $q = 0.36$, and the angles of departure (AoDs) $\{\varphi_{l,k}\}$ are uniformly-distributed within $[0\ 2\pi)$. The number of subcarriers N_{C} is 256.

Note that if the system parameters N_T, K, L, and N_{RF} (do not) satisfy the sufficient conditions of Proposition 1, the proposed hybrid precoders (would not) achieve the same performance as the fully digital precoder with full channel knowledge. In the following numerical results, the system parameters do not satisfy the the sufficient conditions of Proposition 1, thus the hybrid precoders can show some performance gap from the fully digital precoder. The performance of the fully digital precoder of [6] and the performance of the MRT hybrid precoder of [54] will be presented as performance upper and lower bounds respectively.

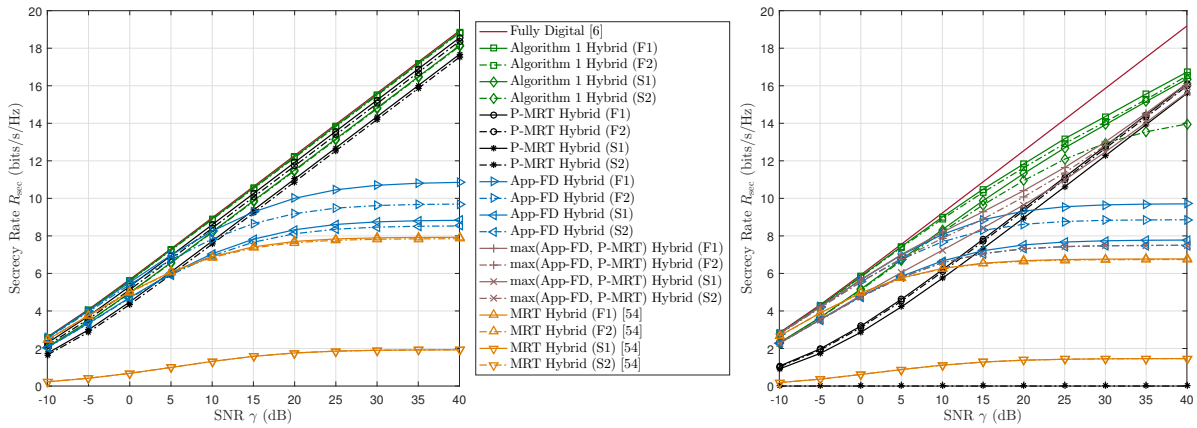
If P-MRT is feasible, the optimal precoding strategy at high SNRs is to maximize the rate of Bob in the null space of channels to Eves, and hence we have $\lim_{\gamma\to\infty} \frac{R_{\mathrm{sec}}(\gamma)}{\log_2(\gamma)} = \lim_{\gamma\to\infty} \frac{R_1(\gamma)}{\log_2(\gamma)} = 1$ since Bob has a single antenna [56]. This result means that the secrecy rate should have a unit slope at high SNRs if P-MRT is feasible. Similarly, the secrecy throughput should have a unit slope if P-MRT is feasible. Table 1 summarizes the necessary conditions (mentioned in subsections III-B2 and IV-B) to apply P-MRT for fully digital precoding and hybid precoding with full or partial channel knowledge. If P-MRT is infeasible, the secrecy rate and secrecy throughput will not have a unit slope at high SNRs.

A. Achievable Secrecy Rate with Full Channel Knowledge

Fig. 3 shows the achievable secrecy rate as a function of the transmit SNR with $N_{\mathrm{RF}} = 4$ and different numbers of Eves ($K - 1$). With two Eves (Fig. 3a), we observe that Algorithm 1 achieves a secrecy rate very close to that achieved by the fully digital precoding for the whole SNR range. The four RF precoder structures achieve slightly different secrecy rates due to the different hardware complexities. Algorithm1 approaches P-MRT at high SNRs since P-MRT is optimal at high SNRs. Note that FD-P-MRT is feasible for all structures since $N_{\mathrm{RF}} > K$. With four Eves (Fig. 3b), the secrecy rate gap between the fully digital precoding and Algorithm 1 increases as SNR increases. Algorithm 1 (F1, F2, and S1) approaches the corresponding P-MRT with unit secrecy slope at high SNRs since P-MRT is optimal at high SNRs, while Algorithm 1 (S2) does not achieve the unit secrecy slope. The reason is that FD-P-MRT is infeasible for all structures since $N_{\mathrm{RF}} < K$, while TD-P-MRT is feasible only for the structures F1, F2, and S1 since $N_{\mathrm{T}} > (K-1)L$.

For both Fig. 3a and Fig. 3b, we observe that App-FD achieve approximately the same secrecy rate as Algorithm 1 at low SNRs. However, App-FD does not achieve the unit secrecy slope at moderate and high SNRs, and the secrecy rate gap between Algorithm 1 and App-FD increases as SNR increases. The proposed adaptive hybrid precoder max(App-FD, P-MRT) in Fig. 4b combines the low/moderate SNR advantage of App-FD and the high SNR advantage of P-MRT, and yields better secrecy rate performance than App-FD and P-MRT with low computational complexity (both App-FD and P-MRT are obtained in closed forms as derived in Section III-B). Note that max(App-FD, P-MRT) reduces to App-FD if P-MRT is infeasible. On the contrary, MRT of [54] achieves the worst secrecy rate at moderate and high SNRs due to ignoring Eves.

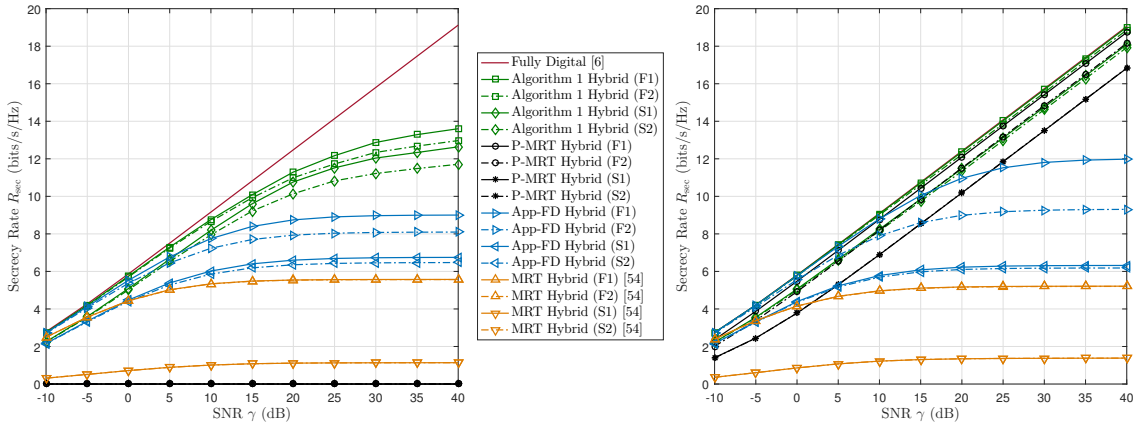
This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TCOMM.2017.2734666, IEEE Transactions on Communications



(a) Achievable secrecy rate with 2 Eves ($K = 3$)

(b) Achievable secrecy rate with 4 Eves ($K = 5$)

Fig. 3. Achievable secrecy rate as a function of transmit SNR γ with $N_{\mathrm{RF}} = 4$ and different numbers of Eves ($K - 1$).



(a) Achievable secrecy rate with $N_{\mathrm{RF}} = 4$

(b) Achievable secrecy rate with $N_{\mathrm{RF}} = 8$

Fig. 4. Achievable secrecy rate as a function of transmit SNR γ with 6 Eves ($K = 7$) and different numbers of RF chains N_{RF}.

With different number of RF chains N_{RF}, Fig. 4 shows the achievable secrecy rate as a function of the transmit SNR with six Eves ($K = 7$). As expected, Algorithm 1 achieves the highest secrecy rate among the hybrid precoding designs. With $N_{\mathrm{RF}} = 4$ (Fig. 4a), the secrecy rate gap between the fully digital precoding and all hybrid precoding schemes increases as SNR increases. Algorithm 1 does not achieve the unit secrecy slope at high SNRs since P-MRT is infeasible for all structures. On the other hand, with $N_{\mathrm{RF}} = 8$ (Fig. 4b), FD-P-MRT is feasible for all structures. As a result, Algorithm 1 achieves a secrecy rate very close to that achieved by the fully digital precoding. From Fig. 4a and Fig. 4b, we can observe the significant effect of the number of RF chains on the achievable secrecy rate.

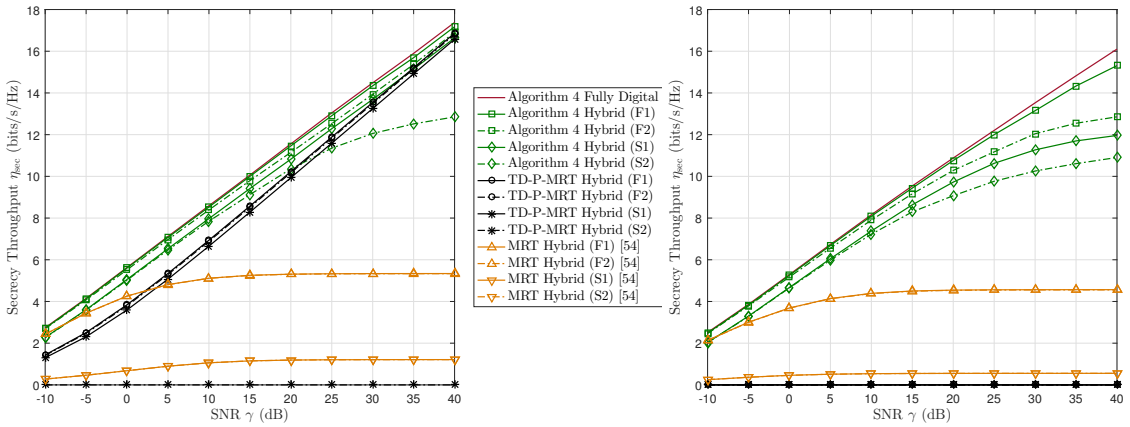
B. Achievable Secrecy Throughput with Partial Channel Knowledge

Fig. 5 shows the achievable secrecy throughput as a function of the transmit SNR with $N_{\mathrm{RF}} = 4$ and different numbers of Eves ($K - 1$). With four Eves (Fig. 5a), we observe that the hybrid precoding with Algorithm 4 (F1, F2, and S1) achieves a secrecy throughput very close to that of the fully digital precoding with Algorithm 4, and they have a unit secrecy slope at high SNRs since TD-PMRT is feasible for the fully digital precoding and the hybrid precoding structures F1, F2, and S1 due to $N_{\mathrm{T}} > (K-1)L$. On the contrary, Algorithm 4 (S2) does not achieve the unit secrecy slope since TD-P-MRT is not feasible for the subarray structure S2. With six Eves (Fig. 5b), the secrecy throughput gap between the fully digital precoding with Algorithm 4 and the hybrid precoding with Algorithm 4 increases as SNR increases. However, the hybrid precoding with Algorithm 4 achieves good performance at low and moderate SNRs. All precoding schemes (including the fully digital precoding) do not achieve the unit secrecy slope since TD-P-MRT is infeasible. Similarly, MRT of [54] achieves the worst secrecy throughput due to ignoring Eves. Note that increasing the number of RF chains (even if $N_{\mathrm{RF}} = N_T$) will not achieve the unit secrecy slope at high SNRs since FD-P-MRT is infeasible in case of partial channel knowledge, and TD-P-MRT is infeasible due to $N_{\mathrm{T}} < (K-1)L$.

C. Tightness of Secrecy Rate and Throughput Lower Bounds

Fig. 6 shows an example for the tightness of the secrecy rate lower bound $\tilde{R}_{\mathrm{sec}}$ and the secrecy throughput lower bound $\tilde{\eta}_{\mathrm{sec}}$ with $N_{\mathrm{RF}} = 4$ and 4 Eves ($K = 5$). The sold lines are for the exact values while the dotted lines are for the lower bound values. We observe from Fig. 6a that the secrecy rate lower bound is tight for the structures F1, F2, and S1, while the secrecy rate lower bound predicts the performance behavior of the structure S2 efficiently. From Fig. 6b, we observe that the proposed secrecy throughput lower bound is very tight for all structures. The difference between the exact values and the

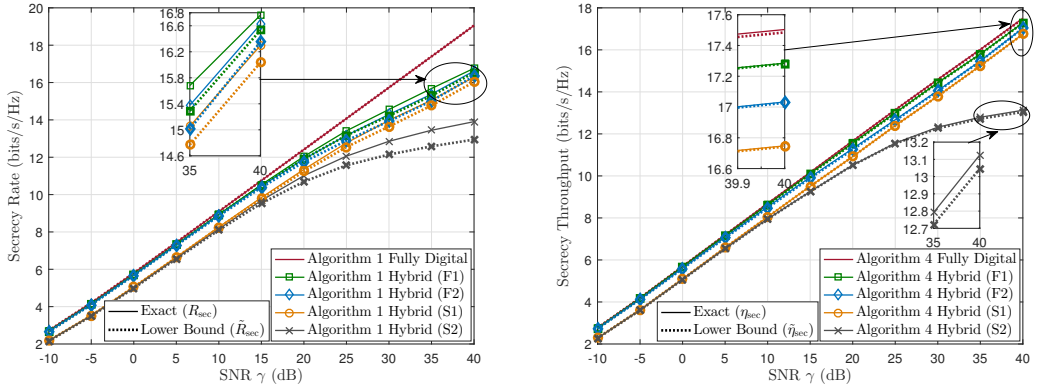
This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TCOMM.2017.2734666, IEEE Transactions on Communications



(a) Achievable secrecy throughput with 4 Eves ($K = 5$)

(b) Achievable secrecy throughput with 6 Eves ($K = 7$)

Fig. 5. Achievable secrecy throughput as a function of transmit SNR γ with $N_{\text{RF}} = 4$ and different numbers of Eves ($K - 1$).



(a) Tightness of secrecy rate lower bound $\tilde{R}_{\text{sec}}$

(b) Tightness of secrecy throughput lower bound $\tilde{\eta}_{\text{sec}}$

Fig. 6. Tightness of secrecy rate and throughput lower bounds with $N_{\text{RF}} = 4$, 4 Eves ($K = 5$), and transmit SNR $\gamma = 15$ dB.

lower bound values over the whole SNR range and all schemes is less than 0.0798 bits/s/Hz.

The reason of the tightness can be explained as follows. When the hybrid precoder is well designed (as the proposed schemes do) with $N_{\text{T}} \gg K$ (large-scale mmWave systems) and small L (limited scattering mmWave channels), the average receive SNR of Eves will be very small compared to the average receive SNR of Bob [3] (due to the capability of generating very sharp beams avoiding, as much as possible, the directions to Eves). Therefore, considering Eves as one Eve with $K - 1$ antennas (the approximation of Section III) will not decrease the secrecy rate significantly. Similarly, applying the inequalities of Section IV will not increase the rates of Eves significantly.

D. Convergence of Algorithms 1 and 4 and Effect of Finite Resolution Phase Shifters

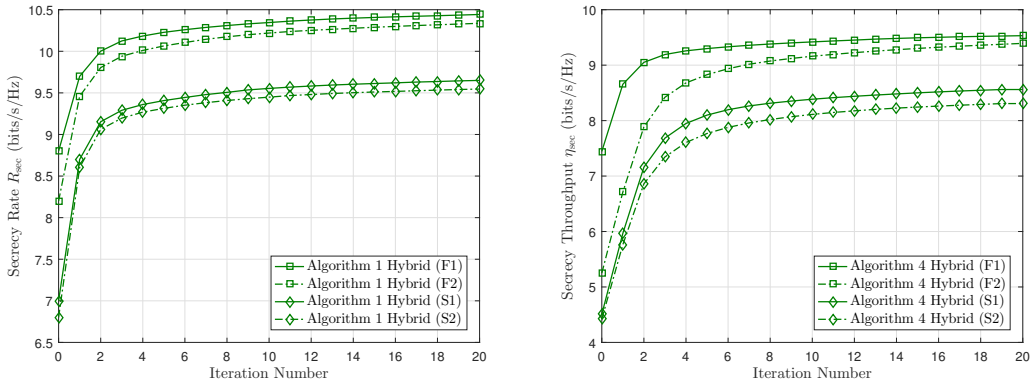
Fig. 7 shows an example for the convergence of Algorithm 1 and Algorithm 4 with $N_{\text{RF}} = 4$, 4 Eves ($K = 5$), and transmit SNR $\gamma = 15$ dB. The secrecy rate and throughput achieved by Algorithms 1 and 4 after each iteration are plotted in Fig. 7a and Fig. 7b respectively. We observe that both Algorithms 1 and 4 converge in a small number of iterations, where 10 iterations are sufficient for all RF precoder structures.

With finite resolution phase shifters, Fig. 8 shows the secrecy rate and throughput achieved by Algorithms 1 and 4 versus different numbers of quantization bits for the phase shifters with $N_{\text{RF}} = 4$, 4 Eves ($K = 5$), and transmit SNR $\gamma = 15$ dB. After designing the hybrid precoder using Algorithm 1 or Algorithm 4, the phases of the RF precoder are quantized into Q bits such that $\angle \mathbf{F}_{\text{RF}}(i,j) \in \left\{0, \frac{2\pi}{2^Q}, \ldots, \frac{2\pi 2^{Q-1}}{2^Q}\right\}$ $\forall\, \mathbf{F}_{\text{RF}}(i,j) \neq 0$. We observe that 6 quantization bits are sufficient for the RF precoder structures F2, S1, and S2 with secrecy rate/throughput loss less than 0.2 bits/s/Hz. On the other hand, the RF precoder structure F1 requires at least 10 quantization bits to outperform the structure F2. The reason is that the structure F1 uses approximately twice the number of phase shifters of the structure F2. As a result, the quantization error of the structure F1 is larger than that of the remaining structures.

VI. Conclusion

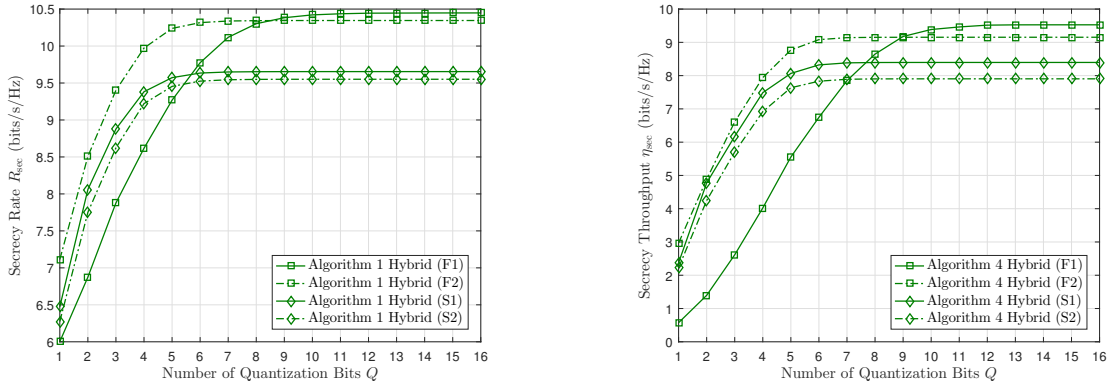
In this paper, we have designed the hybrid analog-digital precoder for physical layer security. With full channel knowledge at the transmitter, we provided sufficient conditions for the hybrid precoder to realize the performance of the fully digital precoding. If the sufficient conditions are not satisfied, we design the hybrid precoder to maximize the secrecy rate. By maximizing the average projection between the fully digital precoder and the hybrid precoder, we proposed a low-complexity closed-form hybrid precoder design. The conventional P-MRT scheme is extended to realize the hybrid

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TCOMM.2017.2734666, IEEE Transactions on Communications



(a) Convergence of Algorithm 1 (b) Convergence of Algorithm 4

Fig. 7. Convergence of Algorithm 1 and Algorithm 4 with $N_{\text{RF}} = 4$, 4 Eves ($K = 5$), and transmit SNR $\gamma = 15$ dB.



(a) Secrecy rate achieved by Algorithm 1 versus number of quantization bits

(b) Secrecy throughput achieved by Algorithm 4 versus number of quantization bits

Fig. 8. Effect of finite resolution phase shifters on the secrecy rate and throughput achieved by Algorithm 1 and Algorithm 4 with $N_{\text{RF}} = 4$, 4 Eves ($K = 5$), and transmit SNR $\gamma = 15$ dB.

precoder. Two P-MRT schemes were presented. TD-P-MRT nulls the channels to Eves at time domain, and FD-P-MRT nulls the channels to Eves at frequency domain. Moreover, we proposed an iterative hybrid precoder design, based on gradient ascent, which converges in a small number of iterations and achieves secrecy rate close to that achieved by the fully digital precoding.

With partial channel knowledge, we derived a secrecy outage probability upper bound. The secrecy throughput maximization problem is converted into a sequence of secrecy outage probability minimization problems. Then, the hybrid precoder is designed to minimize the secrecy outage probability by an iterative hybrid precoder design, based on gradient descent, which converges in a small number of iterations and achieves secrecy throughput close to that achieved by the fully digital precoding. With finite resolution phase shifters, we showed that 6 quantization bits are sufficient for the structures F2, S1, and S2. On the contrary, 10 quantization bits are needed for the structure F1 to outperform the structure F2.

Appendix A (Proof of Proposition 1)

As shown in (13), the optimal fully digital precoder $\mathbf{f}_{\text{opt},n}$ is the principal generalized eigenvector corresponding to the maximum eigenvalue of the pencil $\left(\mathbf{I}_{N_{\text{T}}} + \gamma \mathbf{H}_n^H \mathbf{H}_n,\ \mathbf{I}_{N_{\text{T}}} + \gamma \mathbf{h}_{n,1}^H \mathbf{h}_{n,1}\right)$. Among the N_{T} generalized eigenvalues, $(N_{\text{T}} - K)$ of them are equal to 1 and obtained using any vector that is orthogonal to the space spanned by $\left[\mathbf{h}_{n,1}^H, \mathbf{H}_n^H\right]$. The other K generalized eigenvectors corresponding to the other K eigenvalues (including the maximum eigenvalue) lie completely in the space spanned by $\left[\mathbf{h}_{n,1}^H, \mathbf{H}_n^H\right]$. Therefore, we can write $\mathbf{f}_{\text{opt},n}$ as

$$\mathbf{f}_{\text{opt},n} = \beta_n \frac{\mathbf{\Pi}_n \mathbf{h}_{n,1}^H}{\left\|\mathbf{\Pi}_n \mathbf{h}_{n,1}^H\right\|} + \sqrt{1-\beta_n^2}\, \frac{\mathbf{\Pi}_n^{\perp} \mathbf{h}_{n,1}^H}{\left\|\mathbf{\Pi}_n^{\perp} \mathbf{h}_{n,1}^H\right\|}, \tag{67}$$

where $\beta_n = \dfrac{\left|\mathbf{h}_{n,1} \mathbf{\Pi}_n \boldsymbol{\mathcal{E}}_{\max}\left[\left(\mathbf{I}_{N_{\text{T}}} + \gamma \mathbf{H}_n^H \mathbf{H}_n\right)^{-1}\left(\mathbf{I}_{N_{\text{T}}} + \gamma \mathbf{h}_{n,1}^H \mathbf{h}_{n,1}\right)\right]\right|}{\left\|\mathbf{\Pi}_n \mathbf{h}_{n,1}^H\right\|}$, $\mathbf{\Pi}_n = \mathbf{H}_n^H \left(\mathbf{H}_n \mathbf{H}_n^H\right)^{-1} \mathbf{H}_n \in \mathbb{C}^{N_{\text{T}} \times N_{\text{T}}}$ denotes the orthogonal projection onto the space spanned by $\mathbf{H}_n$, and $\mathbf{\Pi}_n^{\perp} = \mathbf{I}_{N_{\text{T}}} - \mathbf{\Pi}_n$ denotes the projection onto its orthogonal complement. Equation (67) can be rewritten as

$$\mathbf{f}_{\text{opt},n} = \mathbf{H}_{\text{TD}} \mathbf{W}_n \mathbf{p}_n, \tag{68}$$

where $\mathbf{H}_{\text{TD}} \in \mathbb{C}^{N_{\text{T}} \times KL}$ is the time domain channel matrix to the K receivers given by

$$\mathbf{H}_{\text{TD}} = \left[\tilde{\mathbf{h}}_{\tau_{1,1},1}^H, \ldots, \tilde{\mathbf{h}}_{\tau_{L,1},1}^H, \ldots, \tilde{\mathbf{h}}_{\tau_{1,K},K}^H, \ldots, \tilde{\mathbf{h}}_{\tau_{L,K},K}^H\right], \tag{69}$$

$\mathbf{W}_n = \text{blkdiag}\left(\mathbf{w}_{n,1}^H, \mathbf{w}_{n,2}^H, \ldots, \mathbf{w}_{n,K}^H\right) \in \mathbb{C}^{KL \times K}$, and $\mathbf{p}_n = \left[\mu_n, \nu_n \mathbf{h}_{n,1} \mathbf{H}_n^H \left(\mathbf{H}_n \mathbf{H}_n^H\right)^{-1}\right]^H \mathbb{C}^{K \times 1}$, where $\mu_n = \frac{\sqrt{1-\beta_n^2}}{\left\|\mathbf{\Pi}_n^{\perp} \mathbf{h}_{n,1}^H\right\|}$ and $\nu_n = \frac{\beta_n}{\left\|\mathbf{\Pi}_n \mathbf{h}_{n,1}^H\right\|} - \frac{\sqrt{1-\beta_n^2}}{\left\|\mathbf{\Pi}_n^{\perp} \mathbf{h}_{n,1}^H\right\|}$. The performance of fully digital precoding can be realized by setting $\mathbf{F}_{\text{RF}}(:, 1:KL) = \mathbf{H}_{\text{TD}}$ and $\mathbf{f}_{\text{BB},n}(1:KL) = \mathbf{W}_n \mathbf{p}_n$ if $N_{\text{RF}} \geq KL$. Thus, to realize the performance of fully digital precoding, it is sufficient for the hybrid precoding utilizing the

fully-connected structure F1 that $N_{\mathrm{RF}} \geq KL$. This completes the proof of the first statement.

For the fully-connected structure F2, we have to satisfy the modulus constraint. In [57], it was shown that any vector $\mathbf{x} \in \mathbb{C}^{N\times 1}$ can be expressed as $\mathbf{x} = \tilde{\mathbf{X}}\tilde{\mathbf{x}}$, where $\tilde{\mathbf{X}} \in \mathbb{C}^{N\times 2}$ is with unit modulus entries and $\tilde{\mathbf{x}} \in \mathbb{R}^{2\times 1}$. Following this decomposition, $\mathbf{H}_{\mathrm{TD}}$ can be expressed as $\mathbf{H}_{\mathrm{TD}} = \mathbf{Q}_{\mathrm{RF}}\mathbf{R}_{\mathrm{BB}}$, where $\mathbf{Q}_{\mathrm{RF}} \in \mathbb{C}^{N_{\mathrm{T}}\times 2KL}$ has unit modulus entries obtained as

$$\mathbf{Q}_{\mathrm{RF}}\left(l, 2m-1\right) = \exp\left(j\left(\angle \mathbf{H}_{\mathrm{TD}}\left(l,m\right) - \cos^{-1}\left(q_{+}\right)\right)\right), \tag{70}$$

$$\mathbf{Q}_{\mathrm{RF}}\left(l, 2m\right) = \exp\left(j\left(\angle \mathbf{H}_{\mathrm{TD}}\left(l,m\right) + \cos^{-1}\left(q_{-}\right)\right)\right), \tag{71}$$

$\forall l \in \{1,2,\ldots N_{\mathrm{T}}\}$ and $\forall m \in \{1,2,\ldots KL\}$ where $q_{+} = \frac{|\mathbf{H}_{\mathrm{TD}}(l,m)|^2 + b_{\max,m}b_{\min,m}}{|\mathbf{H}_{\mathrm{TD}}(l,m)|^2(b_{\max,m}+b_{\min,m})}$, $q_{-} = \frac{|\mathbf{H}_{\mathrm{TD}}(l,m)|^2 - b_{\max,m}b_{\min,m}}{|\mathbf{H}_{\mathrm{TD}}(l,m)|^2(b_{\max,m}-b_{\min,m})}$, $b_{\max,m} = \max\limits_{l} |\mathbf{H}_{\mathrm{TD}}\left(l,m\right)|$, $b_{\min,m} = \min\limits_{l} |\mathbf{H}_{\mathrm{TD}}\left(l,m\right)|$, and $\mathbf{R}_{\mathrm{BB}} \in \mathbb{R}^{2KL\times KL}$ is obtained as $\mathbf{R}_{\mathrm{BB}}\left(2m-1,m\right) = \left(b_{\max,m} + b_{\min,m}\right)/2$, $\mathbf{R}_{\mathrm{BB}}\left(2m,m\right) = \left(b_{\max,m} - b_{\min,m}\right)/2$ $\forall m \in \{1,2,\ldots KL\}$. Therefore, we can set $\mathbf{F}_{\mathrm{RF}}\left(:, 1:2KL\right) = \frac{1}{\sqrt{N_{\mathrm{T}}}}\mathbf{Q}_{\mathrm{RF}}$ and $\mathbf{f}_{\mathrm{BB},n}\left(1:2KL\right) = \sqrt{N_{\mathrm{T}}}\mathbf{R}_{\mathrm{BB}}\mathbf{W}_n\mathbf{p}_n$ if $N_{\mathrm{RF}} \geq 2KL$. As a result, it is sufficient that $N_{\mathrm{RF}} \geq 2KL$ for the hybrid precoding utilizing the fully-connected structure F2 to realize the performance of fully digital precoding. By assuming that all the channels follow the mmWave channel model in (2), equation (68) can be written as $\mathbf{f}_{\mathrm{opt},n} = \mathbf{A}_{\mathrm{T}}\mathbf{D}_{\mathrm{T}}\mathbf{W}_n\mathbf{p}_n$, where $\mathbf{A}_{\mathrm{T}} = \left[\mathbf{A}_{\mathrm{T},1}, \mathbf{A}_{\mathrm{T},2}, \ldots, \mathbf{A}_{\mathrm{T},K}\right] \in \mathbb{C}^{N_{\mathrm{T}}\times KL}$ and $\mathbf{D}_{\mathrm{T}} = \mathrm{blkdiag}\left(\mathbf{D}_1^H, \mathbf{D}_2^H, \ldots, \mathbf{D}_K^H\right) \in \mathbb{C}^{KL\times KL}$. Since $\mathbf{A}_{\mathrm{T}}$ is with unit modulus entries, the sufficient condition for the hybrid precoding utilizing the fully-connected structure F2 reduces to $N_{\mathrm{RF}} \geq KL$ by setting $\mathbf{F}_{\mathrm{RF}}\left(:, 1:KL\right) = \frac{1}{\sqrt{N_{\mathrm{T}}}}\mathbf{A}_{\mathrm{T}}$ and $\mathbf{f}_{\mathrm{BB},n}\left(1:KL\right) = \sqrt{N_{\mathrm{T}}}\mathbf{D}_{\mathrm{T}}\mathbf{W}_n\mathbf{p}_n$. This completes the proof of the second statement. The obtained sufficient conditions vanish if $N_{\mathrm{T}} \leq KL$ since $N_{RF} < N_{\mathrm{T}}$.

Appendix B (Proof of Proposition 2)

In Proposition 1, it was shown that if $N_{\mathrm{T}} \leq KL$, there is no sufficient condition depending only on the number of RF chains to realize the performance of fully digital precoding since $N_{RF} < N_{\mathrm{T}}$. Therefore, we consider the case that $KL \leq N_{\mathrm{RF}} < N_{\mathrm{T}}$. To realize the performance of the fully digital precoding, $\mathbf{f}_{\mathrm{BB},n}$ has to be expressed as $\mathbf{f}_{\mathrm{BB},n} = \mathbf{B}_{\mathrm{BB}}\mathbf{W}_n\mathbf{p}_n$, where $\mathbf{B}_{\mathrm{BB}} \in \mathbb{C}^{N_{\mathrm{RF}}\times KL}$ is a mapping matrix. We have to design $\mathbf{F}_{\mathrm{RF}}$ and $\mathbf{B}_{\mathrm{BB}}$ such that $\mathbf{H}_{\mathrm{TD}} = \mathbf{F}_{\mathrm{RF}}\mathbf{B}_{\mathrm{BB}}$. Let $N_{\mathrm{RF}} = N_{\mathrm{T}} - 1 \geq KL$ which means that each RF chain is connected to one antenna except only one RF chain that is connected to two antennas. Without loss of generality, let the first RF chain be the only RF chain that is connected to two antennas, we should have

$$\mathbf{H}_{\mathrm{TD}}\left(1,l\right) = \mathbf{f}_{\mathrm{RF},1}\left(1\right)\mathbf{B}_{\mathrm{BB}}\left(1,l\right), \tag{72}$$

$$\mathbf{H}_{\mathrm{TD}}\left(2,l\right) = \mathbf{f}_{\mathrm{RF},1}\left(2\right)\mathbf{B}_{\mathrm{BB}}\left(1,l\right), \tag{73}$$

where $l \in \{1,2,\ldots,KL\}$. To satisfy (72) and (73), it is necessary that $\mathbf{H}_{\mathrm{TD}}\left(2,:\right) = c\,\mathbf{H}_{\mathrm{TD}}\left(1,:\right)$ where c is a constant, which is not guaranteed and depends on the channel realizations. As a result, the hybrid precoding utilizing the subarray structure S1 cannot generally realize the fully digital precoding for any $N_{\mathrm{RF}} \leq N_{\mathrm{T}} - 1$. Since $\mathcal{F}_{\mathrm{RF}}^{\mathrm{S2}} \subset \mathcal{F}_{\mathrm{RF}}^{\mathrm{S1}}$, we arrive at the same conclusion for the subarray structure S2. This completes the proof of Proposition 2.

Appendix C (Approximating The Fully Digital Precoding)

For the average Euclidean distance criterion, the hybrid precoder is designed to approximate the fully digital precoding as [21], [36], [37]

$$\underset{\mathbf{F}_{\mathrm{RF}},\{\mathbf{f}_{\mathrm{BB},n}\}}{\arg\min} \sum_{n=1}^{N_{\mathrm{C}}} \left\| \mathbf{f}_{\mathrm{opt},n} - \frac{\mathbf{F}_{\mathrm{RF}}\mathbf{f}_{\mathrm{BB},n}}{\|\mathbf{F}_{\mathrm{RF}}\mathbf{f}_{\mathrm{BB},n}\|} \right\|^2. \tag{74}$$

It is straightforward to show that for any $\mathbf{F}_{\mathrm{RF}}$, $\mathbf{f}_{\mathrm{BB},n}$ is the least squares solution which can be expressed (after appropriate normalization) as

$$\mathbf{f}_{\mathrm{BB},n} = \frac{\left(\mathbf{F}_{\mathrm{RF}}^H\mathbf{F}_{\mathrm{RF}}\right)^{-1}\mathbf{F}_{\mathrm{RF}}^H\mathbf{f}_{\mathrm{opt},n}}{\left\|\left(\mathbf{F}_{\mathrm{RF}}^H\mathbf{F}_{\mathrm{RF}}\right)^{-\frac{1}{2}}\mathbf{F}_{\mathrm{RF}}^H\mathbf{f}_{\mathrm{opt},n}\right\|}, \tag{75}$$

which is exactly the same as (17), and the corresponding $\sum_{n=1}^{N_{\mathrm{C}}} \left\| \mathbf{f}_{\mathrm{opt},n} - \frac{\mathbf{F}_{\mathrm{RF}}\mathbf{f}_{\mathrm{BB},n}}{\|\mathbf{F}_{\mathrm{RF}}\mathbf{f}_{\mathrm{BB},n}\|} \right\|^2 = 2N_{\mathrm{C}} - 2\sum_{n=1}^{N_{\mathrm{C}}} \sqrt{\mathbf{f}_{\mathrm{opt},n}^H\mathbf{F}_{\mathrm{RF}}\left(\mathbf{F}_{\mathrm{RF}}^H\mathbf{F}_{\mathrm{RF}}\right)^{-1}\mathbf{F}_{\mathrm{RF}}^H\mathbf{f}_{\mathrm{opt},n}}$. Thus, (74) can be written as a function of $\mathbf{F}_{\mathrm{RF}}$ only as

$$\underset{\mathbf{F}_{\mathrm{RF}}}{\arg\max} \sum_{n=1}^{N_{\mathrm{C}}} \sqrt{\lambda_{\max}\left[\left(\mathbf{F}_{\mathrm{RF}}^H\mathbf{F}_{\mathrm{RF}}\right)^{-1}\mathbf{F}_{\mathrm{RF}}^H\mathbf{f}_{\mathrm{opt},n}\mathbf{f}_{\mathrm{opt},n}^H\mathbf{F}_{\mathrm{RF}}\right]}, \tag{76}$$

which is similar to the first equality of (18) except for the square root. For (18), we have a closed- form solution of $\mathbf{F}_{\mathrm{RF}} = \boldsymbol{\mathcal{E}}_{1:\mathrm{N_{RF}}}\left[\sum_{n=1}^{N_{\mathrm{C}}} \mathbf{f}_{\mathrm{opt},n}^H\mathbf{f}_{\mathrm{opt},n}\right]$, while there is no a closed-form solution for (76).

References

[1] T. Rappaport, S. Sun, R. Mayzus, H. Zhao, Y. Azar, K. Wang, G. Wong, J. Schulz, M. Samimi, and F. Gutierrez, "Millimeter wave mobile communications for 5G cellular: It will work!" *IEEE Access*, vol. 1, pp. 335–349, May 2013.

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

[3] 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.

[4] S. Shafiee and S. Ulukus, "Achievable rates in Gaussian MISO channels with secrecy constraints," in *Proc. IEEE ISIT 2007*, Jun. 2007, pp. 2466–2470.

[5] A. Khisti and G. W. Wornell, "Secure transmission with multiple antennas I: The MISOME wiretap channel," *IEEE Trans. Inf. Theory*, vol. 56, no. 7, pp. 3088–3104, Jul. 2010.

[6] Q. Li and W. K. Ma, "Optimal and robust transmit designs for MISO channel secrecy by semidefinite programming," *IEEE Trans. Signal Process.*, vol. 59, no. 8, pp. 3799–3812, Aug. 2011.

[7] R. Negi and S. Goel, "Secret communication using artificial noise," in *Proc. IEEE VTC 2005*, vol. 3, Sep. 2005, pp. 1906–1910.

[8] 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.

[9] 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.

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

[11] M. Daly, E. Daly, and J. Bernhard, "Demonstration of directional modulation using a phased array," *IEEE Trans. Antennas Propag.*, vol. 58, no. 5, pp. 1545–1550, May 2010.

[12] 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.

[13] 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. IEEE SPAWC 2014*, Jun. 2014, pp. 115–119.

[14] 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.

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

[16] 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.

[17] 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.

[18] S. Gong, C. Xing, Z. Fei, and S. Ma, "Millimeter-wave secrecy beamforming designs for two-way amplify-and-forward mimo relaying networks," *IEEE Trans. Veh. Technol.*, vol. 66, no. 3, pp. 2059–2071, Mar. 2017.

[19] J. Nsenga, A. Bourdoux, and F. Horlin, "Mixed analog/digital beamforming for 60 GHz MIMO frequency selective channels," in *Proc. IEEE ICC 2010*, May 2010, pp. 1–6.

[20] A. Alkhateeb and R. W. Heath, "Frequency selective hybrid precoding for limited feedback millimeter wave systems," *IEEE Trans. Commun.*, vol. 64, no. 5, pp. 1801–1818, May 2016.

[21] X. Yu, J. C. Shen, J. Zhang, and K. B. Letaief, "Alternating minimization algorithms for hybrid precoding in millimeter wave MIMO systems," *IEEE J. Sel. Topics Signal Process.*, vol. 10, no. 3, pp. 485–500, Apr. 2016.

[22] S.-K. Yong, P. Xia, and A. Valdes-Garcia, *60 GHz technology for Gbps WLAN and WPAN: From theory to practice*. Wiley, 2010.

[23] 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.

[24] T. Bai and R. W. Heath, "Coverage and rate analysis for millimeter-wave cellular networks," *IEEE Trans. Wireless Commun.*, vol. 14, no. 2, pp. 1100–1114, Feb. 2015.

[25] A. Thornburg, T. Bai, and R. W. Heath, "Performance analysis of outdoor mmwave Ad Hoc networks," *IEEE Trans. Signal Process.*, vol. 64, no. 15, pp. 4065–4079, Aug. 2016.

[26] 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.

[27] J. G. Andrews, T. Bai, M. N. Kulkarni, A. Alkhateeb, A. K. Gupta, and R. W. Heath, "Modeling and analyzing millimeter wave cellular systems," *IEEE Trans. Commun.*, vol. 65, no. 1, pp. 403–430, Jan. 2017.

[28] A. Alkhateeb, Y. H. Nam, M. S. Rahman, J. Zhang, and R. W. Heath, "Initial beam association in millimeter wave cellular systems: Analysis and design insights," *IEEE Trans. Wireless Commun.*, vol. 16, no. 5, pp. 2807–2821, May. 2017.

[29] M. D. Yacoub, G. Fraidenraich, and J. C. S. S. Filho, "Nakagami-m phase-envelope joint distribution," *IET Electron. Lett.*, vol. 41, no. 5, pp. 259–261, Mar. 2005.

[30] T. E. Bogale, L. B. Le, A. Haghighat, and L. Vandendorpe, "On the number of RF chains and phase shifters, and scheduling design with hybrid analog-digital beamforming," *IEEE Trans. Wireless Commun.*, vol. 15, no. 5, pp. 3311–3326, May 2016.

[31] M. Baldi, F. Chiaraluce, N. Laurenti, S. Tomasin, and F. Renna, "Secrecy transmission on parallel channels: Theoretical limits and performance of practical codes," *IEEE Trans. Inf. Forensics Security*, vol. 9, no. 11, pp. 1765–1779, Nov. 2014.

[32] S. Yan, G. Geraci, N. Yang, R. Malaney, and J. Yuan, "On the target secrecy rate for SISOME wiretap channels," in *Proc. IEEE ICC 2014*, Jun. 2014, pp. 987–992.

[33] W. Wang, K. C. Teh, and K. H. Li, "Secrecy throughput maximization for MISO multi-eavesdropper wiretap channels," *IEEE Trans. Inf. Forensics Security*, vol. 12, no. 3, pp. 505–515, Mar. 2017.

[34] X. Zhou, L. Song, and Y. Zhang, *Physical Layer Security in Wireless Communications*. CRC Press, 2013.

[35] E. A. Jorswieck and A. Wolf, "Resource allocation for the wire-tap multi-carrier broadcast channel," in *Proc. Int. Conf. Telecommun. 2008*, Jun. 2008, pp. 1–6.

[36] Z. Xu, S. Han, Z. Pan, and C. L. I, "Alternating beamforming methods for hybrid analog and digital MIMO transmission," in *Proc. IEEE ICC 2015*, Jun. 2015, pp. 1595–1600.

[37] W. Ni, X. Dong, and W. S. Lu, "Near-optimal hybrid processing for massive mimo systems via matrix decomposition," *IEEE Trans. Signal Process.*, vol. 65, no. 15, pp. 3922–3933, Aug. 2017.

[38] K. Petersen and M. Pedersen, *The Matrix Cookbook*, September 2007.

[39] S. Boyd and L. Vandenberghe, *Convex Optimization*. Cambridge, UK: Cambridge University Press, 2004.

[40] J. Lee, G. T. Gil, and Y. H. Lee, "Exploiting spatial sparsity for estimating channels of hybrid MIMO systems in millimeter wave communications," in *Proc. IEEE GLOBECOM 2014*, Dec. 2014, pp. 3326–3331.

[41] A. Alkhateeb, O. E. Ayach, G. Leus, and R. W. Heath, "Channel estimation and hybrid precoding for millimeter wave cellular systems," *IEEE J. Sel. Topics Signal Process.*, vol. 8, no. 5, pp. 831–846, Oct. 2014.

[42] K. Venugopal, A. Alkhateeb, N. G. Prelcic, and R. W. Heath, "Channel estimation for hybrid architecture based wideband millimeter wave systems," *IEEE J. Sel. Areas Commun.*, 2017, doi:10.1109/JSAC.2017.2720856.

[43] J. Wang, P. Ding, M. Zoltowski, and D. Love, "Space-time coding and beamforming with partial channel state information," in *Proc. IEEE GLOBECOM 2005*, vol. 5, Dec. 2005, pp. 3149–3153.

[44] A. Alkhateeb, O. El Ayach, G. Leus, and R. Heath, "Hybrid precoding for millimeter wave cellular systems with partial channel knowledge," in *Proc. ITA 2013, 2013*, Feb. 2013, pp. 1–5.

[45] Y. R. Ramadan, A. S. Ibrahim, and M. M. Khairy, "Minimum outage RF beamforming for millimeter wave MISO-OFDM systems," in *Proc. IEEE WCNC 2015*, Mar. 2015, pp. 557–561.

[46] M. F. Tang, S. Y. Wang, and B. Su, "Beamforming designs for multiuser transmissions in FDD massive MIMO systems using partial CSIT," in *Proc. IEEE SAM 2016)*, Jul. 2016, pp. 1–5.

[47] 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.

[48] S. Dutta, M. Mezzavilla, R. Ford, M. Zhang, S. Rangan, and M. Zorzi, "Frame structure design and analysis for millimeter wave cellular systems," *IEEE Trans. Wireless Commun.*, vol. 16, no. 3, pp. 1508–1522, Mar. 2017.

[49] C. Hoymann, D. Astely, M. Stattin, G. Wikstrom, J. F. Cheng, A. Hoglund, M. Frenne, R. Blasco, J. Huschke, and F. Gunnarsson, "LTE release 14 outlook," *IEEE Commun. Mag.*, vol. 54, no. 6, pp. 44–49, Jun. 2016.

[50] 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.

[51] J. Barros and M. Rodrigues, "Secrecy capacity of wireless channels," in *Proc. IEEE ISIT 2006*, Jul. 2006, pp. 356–360.

[52] M. S. Alouini, A. Abdi, and M. Kaveh, "Sum of gamma variates and performance of wireless communication systems over Nakagami-fading channels," *IEEE Trans. Veh. Technol.*, vol. 50, no. 6, pp. 1471–1480, Nov. 2001.

[53] A. M. Mathai, "Storage capacity of a dam with gamma type inputs," *Annals of the Institute of Statistical Mathematics*, vol. 34, no. 1, pp. 591–597, 1982.

[54] 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.

[55] H. Stark and J. Woods, *Probability, statistics, and random processes for engineers*. Prentice Hall, 2012.

[56] D. Tse and P. Viswanath, *Fundamentals of wireless communication*. Cambridge university press, 2005.

[57] X. Zhang, A. F. Molisch, and S.-Y. Kung, "Variable-phase-shift-based RF-baseband codesign for MIMO antenna selection," *IEEE Trans. Signal Process.*, vol. 53, no. 11, pp. 4091–4103, Nov. 2005.

Yahia R. Ramadan (S'14) received the B.S. (with highest honors) and M.S. degrees in Electronics and Communications Engineering from Cairo University, Cairo, Egypt, in 2011 and 2015, respectively. He is currently pursuing his Ph.D. degree in Electrical Engineering at the University of Texas at Dallas, Richarson, TX, USA. His research interests are in the areas of millimeter-wave communications, device-to-device communications, massive MIMO, physical layer security, cognitive radio networks, and spectrum access and sharing.

Hlaing Minn (S'99–M'01–SM'07–F'16) received B.E. degree in Electrical Engineering (Electronics) from the Yangon Institute of Technology, Yangon, Myanmar, in 1995; M.Eng. degree in Telecommunications from the Asian Institute of Technology, Pathumthani, Thailand, in 1997; and Ph.D. degree in Electrical Engineering from the University of Victoria, Victoria, BC, Canada, in 2001. During January–August 2002, he was a Postdoctoral Fellow with the University of Victoria. He has been with the University of Texas at Dallas since 2002 and is currently a Full Professor. His research interests include wireless communications, signal processing, signal design, dynamic spectrum access and sharing, and next-generation wireless technologies.

Dr. Minn serves as an Editor-at-Large since 2016 and served as an Editor from 2005 to 2016 for the IEEE Transactions on Communications. He served as a Technical Program Co-Chair for the Wireless Communications Symposium of the IEEE GLOBECOM 2014 and the Wireless Access Track of the IEEE VTC, Fall 2009, as well as a Technical Program Committee Member for several IEEE conferences.

Ahmed S. Ibrahim (M'09) is currently an Assistant Professor at the Electrical and Computer Engineering Department at Florida International University, Miami, FL, USA. He received the B.S. (with highest honors) and M.S. degrees in electronics and electrical communications engineering from Cairo University, Cairo, Egypt, in 2002 and 2004, respectively. He received the Ph.D. degree in electrical engineering from the University of Maryland, College Park, MD, USA, in 2009. In the past, Dr. Ibrahim was an Assistant Professor at Cairo University, Wireless Research Scientist at Intel Corporation, and Senior Engineer at Interdigital Communications Inc.

Dr. Ibrahim's research interests span various topics of next generation mobile networks and Internet of Things such as heterogeneous networks, vehicular networks, cooperative communications, Wi-Fi offloading, millimeter wave communications, and visible light communications. Dr. Ibrahim currently serves as an associate editor for the Elsevier Digital Communications and Networks (DCN) Journal. He served as a Technical Program Committee Member for several IEEE conferences.