Hybrid Analog-Digital Precoder Design for Securing Cognitive Millimeter Wave Networks

Zhengmin Kong, Jing Song, Chao Wang, *Member, IEEE*, Hongyang Chen, *Senior Member, IEEE*, and Lajos Hanzo, *Fellow Member, IEEE*

***Abstract*—Millimeter wave (mmWave) communications and cognitive radio technologies constitute key technologies of improving the spectral efficiency of communications. Hence, we conceive a hybrid secure precoder for enhancing the physical layer security of a cognitive mmWave wiretap channel, where a secondary transmitter broadcasts confidential information signals to multiple secondary users under the interference temperature constraint of the primary user (PU). The optimization problem is formulated as jointly optimizing the analog and digital precoder for maximizing the minimum secrecy rate of all the secondary users under practical constraints. In particular, our design satisfies the constraint on the maximum interference power received by multiple PUs, as well as the secondary users' minimum quality-of-service (Qos), and the unit-modulus constraint on the analog precoder. Due to the non-convexity of the resultant objective function and owing to the coupling between the analog and digital precoder, the optimization problem formulated is nonconvex and nonlinear, hence it is very challenging to solve directly. Hence, we first transform it into a tractable form, and develop a penalty dual decomposition (PDD) based iterative algorithm to locate its Karush-Kuhn-Tucker (KKT) solution. Finally, we generalize the proposed PDD algorithm to a secure hybrid precoder design relying on practical finite-resolution phase shifters and show that the proposed PDD algorithm can be straightforwardly adapted to handle the scenario, where each PU is equipped with multiple antennas and the CSI of multiple eavesdroppers (Eves) is imperfectly known. Our simulation results validate the efficiency of the proposed iterative algorithm.**

***Index Terms*—Millimeter wave, cognitive radio, physical layer security, hybrid precoder, penalty dual decomposition.**

The work of C. Wang was supported in part by the National Natural Science Foundation of China under Grant No. 61801518, in part by the Fundamental Research Funds for the Central Universities under Grant No. XJS200113, in part by the China Postdoctoral Science Foundation under Grant No. 2020M683428, and in part by the open research fund of National Mobile Communications Research LaboratorySoutheast University under Grant No. 2021D06. The work of L. Hanzo was supported by the Engineering and Physical Sciences Research Council projects EP/N004558/1, EP/P034284/1, EP/P034284/1, EP/P003990/1 (COALESCE), of the Royal Society's Global Challenges Research Fund Grant as well as of the European Research Council's Advanced Fellow Grant QuantCom. (*Corresponding author: Chao Wang.*).

Z. Kong and J. Song are with the Automation Department, School of Electrical Engineering and Automation, Wuhan University, Wuhan 430072, China (e-mail: zmkong@whu.edu.cn, jsong@whu.edu.cn)

C. Wang is with the Integrated Service Networks Lab, Xidian University, Xi'an 710071, China, also with National Mobile Communications Research Laboratory, Southeast University, Nan Jing 210096, China. (e-mail: drchaowang@126.com).

H. Chen is with ZhejiangLab, Hangzhou 311121, China (e-mail:dr.h.chen@ieee.org;hongyang@zhejianglab.com).

L. Hanzo is with the School of Electronics and Computer Science, University of Southampton, Southampton SO17 1BJ, U.K. (e-mail: l-h@ecs.soton.ac.uk).

I. Introduction

With the increasing proliferation of intelligent devices, including smartphones and Internet-of-Things (IoT) devices, the data traffic of mobile communications has increased exponentially for decades [1], which leads to an impending spectrum scarcity. Both millimeter wave (mmWave) and cognitive communications play a key role in mitigating this problem [2]-[3].

Due to the broadcast nature, wireless communication is prone to security value abilities. As IoT is pervading both industry and our daily life, more and more confidential information will be transmitted over wireless channels, hence communication security is vitally important [4], [5]. Physical layer security (PLS) exploits the randomness of the wireless media in an innovative way for securing the confidential information transmission [4], [26]. The study of cognitive radio networks relying on PLS is a particularly active research field [15]–[20]. Despite the above-mentioned feverish research activities, there is a paucity of literature on the PLS of mmWave cognitive networks.

A. Related Works

Wang et al. [21] have investigated the potential extra security gains offered by mmWave communications. Soon afterwards, Wang and Wang [22] have studied the PLS of cellular networks. By considering a single-user mmWave network, the authors of [23]–[27] have studied the various hybrid secure precoders conceived for maximizing the achievable secrecy rate. Explicitly, Eltayeb et al. [23] investigated both analog beamforming and hybrid precoding designed for maximizing the secrecy rate of vehicular networks. Ramadan et al. [24] have proposed hybrid precoders for securing mmWave multiple-input-single-output (MISO) orthogonal frequency division multiplexing (OFDM) systems. As a further development, Ramadan and Minn [25] have imposed the artificial noise on the eavesdropper for enhancing the PLS of mmWave communications. By considering a mmWave MISO network and assuming low-resolution digital-to-analog converters as well as quantized phase shifters, Xu et al. [26] have designed a hybrid secure precoder for maximizing the achievable secrecy rate. Zi et al. [27] have studied the hybrid precoder design for improving the secure energy efficiency of IoT networks. In a nutshell, all the above contributions concentrating on the secure transmission strategy design of a single-user network without considering mmWave cognitive networks, even though cognitive systems are potentially more vulnerable than

their conventional counterparts. More importantly, all of the algorithms mentioned above are heuristic and cannot give any guarantee concerning the secrecy performance.

Nonetheless, the PLS of cognitive mmWave wiretap networks has been studied by Song et al. [19] and Zhao et al. [20]. Specially, Song et al. [19] analyzed the reliability and security performance of a secondary network under a specific interference temperature constraint, while the secrecy outage probability of a secondary network has been analyzed by Zhao et al. [20]. However, these contributions have investigated the PLS of mmWave cognitive networks from a general performance analysis perspective, rather than by considering a hybrid secure precoder design. The challenges in designing a hybrid precoder for maximizing the secrecy rate of a cognitive mmWave wiretap network can be summarized as follows.

Firstly, the non-convexity of the secrecy rate makes the joint optimization of the analog and digital precoder nonconvex, hence finding the optimal solution is very difficult. Secondly, the effect of the coupling between the analog and digital precoder often results in the alternating optimization (AO) algorithm getting trapped in sub-optimal solutions, which degrades the achievable secrecy performance [28], [29]. Thirdly, since there is no well-established optimization framework for jointly designing the analog and digital precoder, the quality-of-service (Qos) of each served user and their interference temperature constraint are hard to handle. Recently, an optimization framework has been proposed by Shi et al. [28] for handling nonconvex problems in the face of coupled optimization variables, relying on penalty dual decomposition (PDD).

B. Motivation

As mentioned above, there is a paucity of literature on the PLS of cognitive mmWave networks and there are no efficient algorithms to design secure hybrid precoders for maximizing the secrecy rate due to the non-convexity of the objective function and coupling constraints. Most of the existing contributions resort to heuristic algorithms, which rely on separately designing analog and digital precoders or approximating the secrecy rate maximization problem as a more tractable one. For example, Eltayeb *et al.* [23] first designed a fully digital precoder to maximize the achievable secrecy rate, and then, designed a hybrid precoder to approximate the fully digital one. The authors of [24], [25], [27] proposed several heuristic algorithms, which resort to separate design approaches for independently optimizing the analog precoder and digital precoder or adopt an approximate secrecy performance metric instead of the secrecy rate as the objective function. Xu *et al.* [26] proposed a gradient ascent algorithm to alternatively design the analog and digital precoder. However, none of the contributions mentioned above address the secrecy rate maximization problem from a mathematical optimization perspective. Furthermore, they have no provable convergence guarantees for finding a stationary solution of the original problem. More importantly, the heuristic algorithms proposed in [23]–[27] cannot be extended to the PLS of cognitive mmWave networks with the QoS constraint and interference-temperature constraints, since heuristic algorithms cannot guarantee the feasibility of the constrained problems during the iterations. Against this background, we conceive a secure hybrid precoder design for a secondary multi-user network, where a secondary mmWave transmitter serves multiple secondary users in the presence of multiple eavesdroppers (Eves) and multiple primary users (PUs). The main challenge lies in how to handle the nonconvex coupling constraints. We resort to the PDD algorithm for overcoming this obstacle [28]. In particular, we first move the coupling terms in the constraints into equality constraints by introducing auxiliary variables. Then, we dualize the equality constraints into the objective function with an appropriate penalty, and then handle the non-convexity of the augmented Lagrangian problem by jointly employing the block coordinate descent (BCD) algorithm and successive convex approximation (SCA) method [30]. The core idea of the PDD algorithm can be summarized as relaxing the coupling constraints to build an appropriate problem that is suitable for implementing the BCD algorithm, and then gradually increasing the penalty parameter to enforce the coupling constraints [31]. The PDD algorithm makes it possible to jointly optimize the variables appearing in a common constraint jointly, which prevents the BCD algorithm from getting trapped in any inefficient solution. Therefore, our proposed hybrid secure precoder design has guaranteed convergence to the Karush-Kuhn-Tucker (KKT) solution set of the original nonconvex problem, which has significant performance advantages over existing heuristic algorithms.

C. Our Contributions

The main contributions of this paper can be summarized as follows.

1) It is quite challenging to solve the original joint optimization problem directly. Hence, we introduce some auxiliary variables and reformulate the original problem as a more tractable form. In particular, the coupled optimization variables are moved into equality constraints and the nonconvex constraints are all approximated as a sequence of convex ones by employing the SCA method.

2) We adopt the PDD algorithm of [28] for tackling the coupling effect introduced by the product of the analog and digital precoder as well as by the unit modulus constraint of the analog precoder. Superficially, upon employing the augmented Lagrangian method, the equality constraints are moved into the objective functions (OFs) by penalizing and dualizing the equality constraints. With the advent of these manipulations, the original non-convex optimization problem is transformed into a sequence of augmented Lagrangian problems, which can be solved in a double-loop-based iterative fashion. The inner iteration solves the augmented Lagrangian problem, while the outer iteration updates both the dual variables and penalty parameters.

3) For the augmented Lagrangian problem, we employ the BCD method for partitioning the optimization variables into four blocks, where the optimization variables in each block can be solved in parallel by employing the classic Lagrange multiplier method and the optimization variables in different

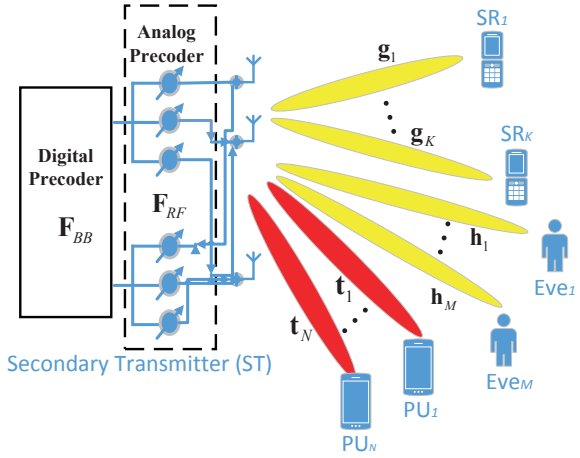

Fig. 1. Illustration of the Cognitive MmWave Secrecy Transmission Model.

blocks are optimized sequentially. These manipulations reduce the computational complexity significantly.

4) We generalize the proposed joint optimization algorithm to the hybrid precoder design relying on realistic finite-resolution phase-shifters and show that our proposed PDD algorithm can be straightforwardly adapted to handle the scenario, where each PU is equipped with multiple antennas and only the imperfect CSI of multiple Eves is available.

Notation: $(\cdot)^T$, $(\cdot)^*$, and $(\cdot)^H$ denote the transpose, conjugate, and conjugate transpose of a matrix, respectively; $\arg(\cdot)$ denotes the phase angle (in radians); $\mathrm{Tr}(\cdot)$, $\mathrm{vec}(\cdot)$, $(\cdot)^\dagger$ and $(\cdot)^{-1}$ denotes the trace, the vectorization, pseudo-inverse and the inverse of a matrix, respectively; $\otimes$, $||\cdot||_1$ and $||\cdot||_F$ denotes the Kronecker product, L_1 norm and Frobenius norm of a matrix, respectively; $\mathcal{R}(\cdot)$ denotes the real part of a variable; $\mathbb{C}^{n\times n}$ stands for a $n\times n$ complex matrix; $\mathbf{I}_K$ denotes the $K\times K$ identity matrix, $\mathbf{e}_k$ denotes the kth column of $\mathbf{I}_K$, and $\mathbb{H}_+^N$ denotes the set of $N\times N$ Hermitian positive semi-definite matrix. $\mathbf{x}\sim\mathcal{CN}(\mathbf{\Lambda},\mathbf{\Delta})$ denotes the circularly symmetric complex Gaussian vector having a mean vector of $\mathbf{\Lambda}$ and covariance matrix of $\mathbf{\Delta}$. $I(x;y)$ stands for mutual information.

II. System Model and Problem Statement

A. System Model

Let us consider a cognitive mmWave network, where a secondary transmitter (ST) broadcasts confidential information to K single-antenna-aided secondary receivers (SR) in the presence of N single-antenna primary users (PU) and M single-antenna Eves, who may wiretap the confidential information. The extension to the scenario where each PU is equipped with multiple antennas, can be found in Section IV. Assuming that the mmWave ST is equipped with N_t transmit antennas (TA) and N_{RF} radio frequency (RF) chains, the received signals at the kth SR and mth Eve, denoted as y_k and $y_{e,m}$, are respectively given by

$$y_k=\mathbf{g}_k^H\mathbf{F}_{\mathrm{RF}}\sum_{k\in\mathcal{K}}\mathbf{f}_{\mathrm{BB},k}s_k+n_k, \tag{1}$$

$$y_{e,m}=\mathbf{h}_m^H\mathbf{F}_{\mathrm{RF}}\sum_{k\in\mathcal{K}}\mathbf{f}_{\mathrm{BB},k}s_k+n_{e,m}, \tag{2}$$

where s_k denotes the confidential information signal destined for the kth SR from the ST, $\mathbf{g}_k$ represents the channel vector spanning from the ST to the kth SR, and $\mathbf{h}_m$ is the channel vector spanning from the ST to the mth Eve. In addition, $n_k\sim\mathcal{CN}(0,1)$ and $n_{e,m}\sim\mathcal{CN}(0,1)$ respectively denote the noise contaminating the kth SR and mth Eve. Furthermore, $\mathbf{F}_{\mathrm{RF}}$ and $\mathbf{F}_{\mathrm{BB}}\triangleq[\mathbf{f}_{\mathrm{BB},1},\ldots,\mathbf{f}_{\mathrm{BB},K}]$, respectively, denote the RF analog precoder and digital precoder of the ST. The total transmit power at the ST is $||\mathbf{F}_{\mathrm{RF}}\mathbf{F}_{\mathrm{BB}}||_F^2$, which is limited to P_{tot}. Assuming that the maximum tolerable interference power at each PUs is Γ and denoting the channel from the ST to the nth PU as $\mathbf{t}_n$, the interference power received at the nth PU is $||\mathbf{t}_n^H\mathbf{F}_{\mathrm{RF}}\mathbf{F}_{\mathrm{BB}}||_F^2$, which is limited to Γ.

We adopt the widely used clustered channel model of [36, Ch. 7.3.2] for the mmWave channel $\mathbf{h}_m$, $\mathbf{g}_k$ and $\mathbf{t}_n$, which are given by

$$\mathbf{h}_m=\sqrt{\frac{N_t}{L_{\mathbf{h}_m}}}\sum_{l=1}^{L_{\mathbf{h}_m}}w_{\mathbf{h}_m}^l\mathbf{a}\left(\theta_{\mathbf{h}_m}^l\right), \tag{3}$$

$$\mathbf{g}_k=\sqrt{\frac{N_t}{L_{\mathbf{g}_k}}}\sum_{l=1}^{L_{\mathbf{g}_k}}w_{\mathbf{g}_k}^l\mathbf{a}\left(\theta_{\mathbf{g}_k}^l\right), \tag{4}$$

$$\mathbf{t}_n=\sqrt{\frac{N_t}{L_{\mathbf{t}_n}}}\sum_{l=1}^{L_{\mathbf{t}_n}}w_{\mathbf{t}_n}^l\mathbf{a}\left(\theta_{\mathbf{t}_n}^l\right), \tag{5}$$

where L_x denotes the number of distinguishable paths, $w_x^l\sim\mathcal{CN}(0,1)$ and θ_l^x respectively denote the coefficient and azimuth angle of the distinguishable paths. The array response vector of the lth path in the clustered channel model is formulated as

$$\mathbf{a}\left(\theta_l^x\right)=\frac{1}{\sqrt{N_t}}\left[e^{j2\pi i\frac{d}{\zeta}\sin(\theta_l^x)}\right]_{i\in\mathcal{N}_t},\mathcal{N}_t\triangleq\{0,1,\ldots,N_t-1\}, \tag{6}$$

where d is the antenna spacing and ζ is the signal wavelength. For simplicity, we set $d=\frac{\zeta}{2}$ [24].

In this paper, we adopt the widely used secrecy performance metric: secrecy rate, which defines the rate at which the confidential information is decodable at Bob while keeping it undecodable at Eve [32]. As shown in [33], employing the Gaussian inputs and stochastic encoders, and introducing auxiliary variable v_k, the secrecy capacity (Bits/s/Hz) of the kth user is characterized by

$$C_{s,k}=\max_{v_k\to s_k\to y_k,y_{e,m}}I\left(v_k;y_k\right)-I\left(v_k;y_{e,m}\right), \tag{7}$$

where the maximum is calculated over variables $v_k,s_k,y_k,y_{e,m}$ on the condition that the Markov chain $v_k\to s_k\to y_k,y_{e,m}$ holds. The kth user's achievable secrecy rate $R_{s,k}$ (Bits/s/Hz) can be obtained by setting $v_k=s_k$ [34], yielding:

$$R_{s,k}=I\left(s_k;y_k\right)-I\left(s_k;y_{e,m}\right), \tag{8}$$

where the information rate (Bits/s/Hz) of the kth user and the

information rate (Bits/s/Hz) leaked to Eve are, respectively,

$$R_k \triangleq I\left(s_k; y_k\right) = \log_2\left(1 + \frac{|\mathbf{g}_k^H \mathbf{F}_{\mathrm{RF}} \mathbf{F}_{\mathrm{BB}} \mathbf{e}_k|^2}{\sum_{j \neq k} |\mathbf{g}_k^H \mathbf{F}_{\mathrm{RF}} \mathbf{F}_{\mathrm{BB}} \mathbf{e}_j|^2 + \sigma^2}\right), \tag{9}$$

$$R_{e_{k,m}} \triangleq I\left(s_k; y_{e,m}\right) = \log_2\left(1 + \frac{|\mathbf{h}_m^H \mathbf{F}_{\mathrm{RF}} \mathbf{F}_{\mathrm{BB}} \mathbf{e}_k|^2}{\sum_{j \neq k} |\mathbf{h}_m^H \mathbf{F}_{\mathrm{RF}} \mathbf{F}_{\mathrm{BB}} \mathbf{e}_j|^2 + \sigma^2}\right). \tag{10}$$

In this paper, similar to [35], we aim to maximize the worst-case secrecy rate of multiple users for guaranteeing user fairness in terms of the achievable secrecy performance. In particular, the minimum secrecy rate (Bits/s/Hz) of the K users is

$$R_s \triangleq \min_{k \in \mathcal{K}} \min_{m \in \mathcal{M}} \left[R_k - R_{e_{k,m}}\right]. \tag{11}$$

We first consider the perfect CSI of multiple Eves to design the hybrid precoder, and then in Section IV, we will show that our proposed algorithm can be straightforwardly adapted to handle the scenario, where only the imperfect CSI of multiple Eves is available.

B. Problem Statement

The joint design of the analog and digital secure precoder is formulated as maximizing the minimum secrecy rate R_s under the constraint of the maximum interference power received by multiple PUs and the rate constraints of multiple secondary users, which is given by

$$\underset{\mathbf{F}_{\mathrm{RF}}, \mathbf{F}_{\mathrm{BB}}}{\text{maximize}} R_s, \tag{12a}$$

$$\text{s.t.} R_k \geq \gamma_k, k \in \mathcal{K}, \tag{12b}$$

$$||\mathbf{t}_n^H \mathbf{F}_{\mathrm{RF}} \mathbf{F}_{\mathrm{BB}}||_F^2 \leq \Gamma, n \in \mathcal{N}, \tag{12c}$$

$$||\mathbf{F}_{\mathrm{RF}} \mathbf{F}_{\mathrm{BB}}||_F^2 \leq P_{\mathrm{tot}}, \tag{12d}$$

$$|\mathbf{F}_{\mathrm{RF}}(i,j)| = 1, \forall i, j, \tag{12e}$$

where the OF is the minimum secrecy rate of multiple users defined in (11). Constraint (12b) is the Qos constraint of each served secondary user and γ_k is the system's requirement for the kth user's information rate. Constraint (12c) is the interference-temperature constraint imposed by each PU and Γ is the maximal allowable interference power received at each PU. Constraint (12d) represents the total power constraint at the ST. Constraint (12e) is the unit-modulus requirement of the analog precoder.

The difficulties in solving problem (12) lie in the following two aspects: the non-convexity of the OF and constraints, as well as the effect of the coupling between $\mathbf{F}_{\mathrm{RF}}$ and $\mathbf{F}_{\mathrm{BB}}$. The non-convexity of the OF and constraints makes the problem non-convex, which makes its globally optimal solution difficult to obtain. The coupling effect introduced by the product of the analog and digital precoder may result in the existing block decomposition methods, such as the BCD, the block successive upper-bound minimization (BSUM) and the inexact flexible parallel algorithm (FLEXA) becoming trapped in sub-optimal solutions and failing to achieve a satisfactory secrecy performance [28]. For handling the obstacles mentioned above, we employ the PDD algorithm proposed in [28] to locate its KKT solution.

III. Iterative Hybrid Precoder Design Algorithm

The PDD algorithm is a double-loop iterative solution, where the outer loop updates the dual variables or penalty parameters in terms of constraint violations, while the inner loop solves the augmented Lagrangian problems. Shi et al. [28] has proved that the PDD algorithm guarantees to converge to a set of KKT solutions of our non-convex problem even for coupled variables. For further details on the PDD algorithm, please refer to [28].

A. Problem Reformulation

In the following, setting $\hat{\mathbf{X}} = \mathbf{F}_{\mathrm{RF}} \mathbf{F}_{\mathrm{BB}}$ and introducing auxiliary variables $\hat{\mathbf{X}}, R_s, \hat{\alpha}_1, \hat{\beta}_1, \tau_1$, we reformulate the objective function of problem (12) as

$$R_s = \log_2\left(1 + \hat{\alpha}_1\right) - \log_2\left(1 + \hat{\beta}_1\right), \tag{13}$$

where

$$\frac{|\mathbf{e}_k^H \hat{\mathbf{X}} \mathbf{g}_k|^2}{\hat{\alpha}_1} = \sum_{j \neq k} |\mathbf{g}_k^H \hat{\mathbf{X}} \mathbf{e}_j|^2 + \sigma^2, k \in \mathcal{K}, \tag{14}$$

$$|\mathbf{h}_m^H \hat{\mathbf{X}} \mathbf{e}_k|^2 = \hat{\beta}_1 \tau_1, k \in \mathcal{K}, m \in \mathcal{M}, \tag{15}$$

$$\sum_{j \neq k} \left(|\mathbf{h}_m^H \hat{\mathbf{X}} \mathbf{e}_j|^2\right) + \sigma^2 = \tau_1, m \in \mathcal{M}, k \in \mathcal{K}. \tag{16}$$

With (13)-(16), problem (12) can be equivalently reformulated as follows:

$$\max_{\hat{\mathbf{X}}, \mathbf{F}_{\mathrm{RF}}, \mathbf{F}_{\mathrm{BB}}, \hat{\alpha}_1, \hat{\beta}_1, \tau_1} R_s,$$

$$\text{s.t.} \log_2\left(1 + \hat{\alpha}_1\right) - \log_2\left(1 + \hat{\beta}_1\right) \geq R_s, \tag{17a}$$

$$\frac{|\mathbf{e}_k^H \hat{\mathbf{X}} \mathbf{g}_k|^2}{\hat{\alpha}_1} \geq \sum_{j \neq k} |\mathbf{g}_k^H \hat{\mathbf{X}} \mathbf{e}_j|^2 + \sigma^2, k \in \mathcal{K}, \tag{17b}$$

$$|\mathbf{h}_m^H \hat{\mathbf{X}} \mathbf{e}_k|^2 \leq \hat{\beta}_1 \tau_1, k \in \mathcal{K}, m \in \mathcal{M}, \tag{17c}$$

$$\sum_{j \neq k} \left(|\mathbf{h}_m^H \hat{\mathbf{X}} \mathbf{e}_j|^2\right) + \sigma^2 \geq \tau_1, m \in \mathcal{M}, k \in \mathcal{K}, \tag{17d}$$

$$|\mathbf{g}_k^H \hat{\mathbf{X}} \mathbf{e}_k|^2 \geq (2^{\gamma_k} - 1)\left(\sum_{n \neq k} |\mathbf{g}_k^H \hat{\mathbf{X}} \mathbf{e}_n|^2 + \sigma^2\right), k \in \mathcal{K}, \tag{17e}$$

$$||\mathbf{t}_n^H \hat{\mathbf{X}}||_F^2 \leq \Gamma, n \in \mathcal{N}, \tag{17f}$$

$$||\hat{\mathbf{X}}||_F^2 \leq P_{\mathrm{tot}}, \tag{17g}$$

$$\hat{\mathbf{X}} = \mathbf{F}_{\mathrm{RF}} \mathbf{F}_{\mathrm{BB}}, |\mathbf{F}_{\mathrm{RF}}(i,j)| = 1, \forall i, j. \tag{17h}$$

When the inequality constraints (17a)-(17d) are active at the optimal solutions, the equivalence between problem (12) and problem (17) holds. First, if the inequality constraint (17a) is not active at the optimal solutions, we can increase R_s further to improve the OF value which runs against the optimality. Similarly, when inequality constraints (17b)-(17d) are not active at the optimal solutions, we can also increase $\hat{\alpha}_1$, decrease $\hat{\beta}_1$, or increase τ_1 to obtain a better OF value. Therefore, we can conclude that constraints (17a)-(17d)

should be active at the optimal solutions, and problem (17) is equivalent to problem (12). Since the function $\frac{|\mathbf{e}_k^H\hat{\mathbf{X}}\mathbf{g}_k|^2}{\hat{\alpha}_1}$ at the left of the inequality constraint (17b) is the perspective of the convex function $|\mathbf{e}_k^H\hat{\mathbf{X}}\mathbf{g}_k|^2$, it is also convex [37]. Therefore, constraint (17b) is nonconvex. Accordingly, it may be readily seen that constraints (17a), (17c), (17d) and (17e) are all nonconvex.

Secondly, for handling these nonconvex constraints, we first adopt the SCA method for approximating the nonconvex constraints (17a), (17b), (17d) and (17e) as a sequence of inner convex constraints, where the nonconvex terms are approximated as their inner convex ones satisfying the conditions in [30, Property A]. As it has been widely exploited, the first-order Taylor expansion of the convex function satisfies the conditions in [30, Property A]. Therefore, the convex terms at the left-hand side of the inequality constraint are approximated as

$$\log_2\left(1+\hat{\alpha}_1\right)-\log_2\left(1+\hat{\beta}_1(l-1)\right)-\frac{\hat{\beta}_1-\hat{\beta}_1(l-1)}{\ln(2)\left(1+\hat{\beta}_1(l-1)\right)} \geq R_s, \tag{18}$$

$$\frac{2\mathcal{R}\left(\mathbf{e}_k^H\hat{\mathbf{X}}^H(l-1)\mathbf{g}_k\mathbf{g}_k^H\hat{\mathbf{X}}\mathbf{e}_k\right)}{\hat{\alpha}_1(l-1)}-\frac{|\mathbf{g}_k^H\hat{\mathbf{X}}\left(l-1\right)\mathbf{e}_k|^2}{\left(\hat{\alpha}_1(l-1)\right)^2}\hat{\alpha}_1 \geq \sum_{j\neq k}\left|\mathbf{g}_k^H\hat{\mathbf{X}}\mathbf{e}_j\right|^2+\sigma^2, \tag{19}$$

$$\sum_{j\neq k}\left(2\mathcal{R}\left(\mathrm{Tr}\left(\mathbf{h}_m^H\hat{\mathbf{X}}\mathbf{e}_j\mathbf{e}_j^H\hat{\mathbf{X}}^H(l-1)\mathbf{h}_m\right)\right)\right) \geq \tau_1-\sigma^2 +\sum_{j\neq k}\left(|\mathbf{h}_m^H\hat{\mathbf{X}}(l-1)\mathbf{e}_j|^2\right), \tag{20}$$

$$-|\mathbf{g}_k^H\hat{\mathbf{X}}(l-1)\mathbf{e}_k|^2+2\mathcal{R}\left(\mathrm{Tr}\left(\mathbf{g}_k^H\hat{\mathbf{X}}\mathbf{e}_k\mathbf{e}_k^H\hat{\mathbf{X}}^H(l-1)\mathbf{g}_k\right)\right) \geq(2^{\gamma_k}-1)\left(\sum_{n\neq k}\left|\mathbf{g}_k^H\hat{\mathbf{X}}\mathbf{e}_n\right|^2+\sigma^2\right), \tag{21}$$

where $\hat{\alpha}_1(l-1)$, $\hat{\beta}_1(l-1)$, and $\hat{\mathbf{X}}(l-1)$ are the optimal solutions at the $(l-1)$th iteration. Upon replacing the nonconvex constraints (17a), (17b), (17d), and (17e) by the convex ones (18)-(21), we may approximate the nonconvex optimization problem (17) as the following one:

$$\begin{aligned}&\max_{\hat{\mathbf{X}},\mathbf{F}_{\mathrm{RF}},\mathbf{F}_{\mathrm{BB}},\hat{\alpha}_1,\hat{\beta}_1,\tau_1} R_s,\\ &\text{s.t}\quad (18)-(21),(17c),(17f),(17g),(17h),\\ &\qquad \hat{\mathbf{X}}=\mathbf{F}_{\mathrm{RF}}\mathbf{F}_{\mathrm{BB}}.\end{aligned} \tag{22}$$

However, problem (22) is still nonconvex due to the coupling of the variables $\hat{\beta}_1$ and τ_1 in constraint (17c) and the variables $\mathbf{F}_{\mathrm{RF}}$ and $\mathbf{F}_{\mathrm{BB}}$ in the last equality constraint.

Thirdly, following the PDD algorithm, we introduce some auxiliary variables to handle the coupled optimization variables in problem (22). However, there are many ways of introducing auxiliary variables. In the following, we briefly summarize a pair of rules to facilitate solving our problem:

1 Each optimization variable is involved in no more than one inequality constraint.

2 The optimization variables in a common inequality constraint should be optimized jointly at each iteration.

Bearing this in mind, we introduce a set of auxiliary variables, denoted as $\mathbf{\Xi}=\left\{\hat{\mathbf{X}},\ \mathbf{Z}_n,\ \mathbf{X}_{k,m},\ \mathbf{V}_k,\ \alpha_k,\ \hat{\alpha}_{k,m},\ \beta_{k,m},\ \hat{\beta}_{k,m},\ \tau_{k,m},\ \mathbf{Y}_k,\ \mathbf{W}_{k,m},\text{ and }\ \hat{R}_{s,k,m}\right\}$, and then reformulate problem (22) as problem (23), given at the top of next page.

Until now, the coupled variables have all been moved into equality constraints. For handling these equality constraints, we introduce a set of Lagrange multipliers $\mathbf{\Lambda}\triangleq\{\boldsymbol{\lambda}_1,\boldsymbol{\lambda}_{2,m},\ \boldsymbol{\lambda}_{3,k,m},\boldsymbol{\lambda}_{4,k},\lambda_{5,k,m},\lambda_{6,k,m},\boldsymbol{\lambda}_{7,k},\ \boldsymbol{\lambda}_{8,k},\lambda_{9,k,m},\ k\in\mathcal{K}\}$. Following the PDD algorithm, we move equality constraint (23g) into the OF to construct the augmented Lagrange problem (24) given at the top of next page, where ρ is the penalty parameter introduced for penalizing equality constraint.

B. The Iterative Algorithm Proposed for Solving Problem (24)

In the following, we employ the BCD algorithm to solve problem (24). In particular, we split the optimization variables into four blocks, for ensuring that for each block, the optimization variables can be solved with the Lagrange multiplier method in parallel, and the blocks are optimized serially. These operations have significantly reduced the computational complexity, which facilitates the practical implementation of the proposed iterative algorithm. The corresponding developments are given in the following four steps.

Step 1. By fixing the other variables, we optimize the set of variables $\{\hat{\alpha}_{k,m},\hat{\beta}_{k,m},\hat{R}_{s,k,m}\}$, $\{\mathbf{Y}_k\}$ and $\{\mathbf{Z}_n\}$ in parallel. Then, problem (24) is partitioned into three independent problems, given by (A.1)-(A.3) at Appendix A-A. We solve them by applying the Lagrange multiplier method and the detailed derivation has been given in Appendix A-A.

Step 2. Upon fixing the other variables, we optimize the set of variables $\{\alpha_k,\mathbf{V}_k\}$, $\{\mathbf{X}_{k,m},\beta_k\}$, $\mathbf{F}_{\mathrm{BB}}$ and R_s in parallel. Then, problem (24) is partitioned into the following four independent problems.

$$\min_{\mathbf{V}_k,\alpha_k}\sum_{\substack{k\in\mathcal{K}\\ m\in\mathcal{M}}}\left(||\hat{\mathbf{X}}-\mathbf{V}_k+\rho\boldsymbol{\lambda}_{4,k}||_F^2+|\hat{\alpha}_{k,m}-\alpha_k+\rho\lambda_{5,k,m}|^2\right), \quad \text{s.t.}\quad (23b), \tag{25}$$

$$\min_{\mathbf{X}_{k,m},\beta_{k,m}}\sum_{k\in\mathcal{K},m\in\mathcal{M}}\left(||\hat{\mathbf{X}}-\mathbf{X}_{k,m}+\rho\boldsymbol{\lambda}_{3,k,m}||_F^2 +|\beta_{k,m}-\hat{\beta}_{k,m}\tau_k+\rho\lambda_{6,k,m}|^2\right), \quad \text{s.t.}\quad (23c), \tag{26}$$

$$\min_{\mathbf{F}_{\mathrm{BB}}}||\hat{\mathbf{X}}-\mathbf{F}_{\mathrm{RF}}\mathbf{F}_{\mathrm{BB}}+\rho\boldsymbol{\lambda}_1||_F^2, \tag{27}$$

$$\min_{R_s}R_s-\frac{1}{2\rho}\sum_{k\in\mathcal{K},m\in\mathcal{M}}\left(|R_s-\hat{R}_{s,k,m}+\rho\lambda_{9,k,m}|^2\right). \tag{28}$$

Problems (25) and (26) can also be solved by applying the Lagrange multiplier method. The detailed derivation has been given in Appendix A-B.

The optimal solutions of problems (27)-(28) can be obtained

$$\max_{\mathbf{F}_{\mathrm{RF}},\mathbf{F}_{\mathrm{BB}},\boldsymbol{\Xi}} R_s$$

$$\log_2\left(1+\hat{\alpha}_{k,m}\right)-\log_2\left(1+\hat{\beta}_{k,m}(l-1)\right)-\frac{\hat{\beta}_{k,m}-\hat{\beta}_{k,m}(l-1)}{\ln(2)\left(1+\hat{\beta}_{k,m}(l-1)\right)}\geq \hat{R}_{s,k,m}, k\in\mathcal{K}, m\in\mathcal{M}, \tag{23a}$$

$$\frac{2\mathcal{R}\left(\mathbf{e}_k^H\mathbf{V}_k^H(l-1)\mathbf{g}_k\mathbf{g}_k^H\mathbf{V}_k\mathbf{e}_k\right)}{\alpha_k(l-1)}-\frac{|\mathbf{g}_k^H\mathbf{V}_k\left(l-1\right)\mathbf{e}_k|^2}{\left(\alpha_k(l-1)\right)^2}\alpha_k\geq\sum_{j\neq k}\left|\mathbf{g}_k^H\mathbf{V}_k\mathbf{e}_j\right|^2+\sigma^2, k\in\mathcal{K}, \tag{23b}$$

$$|\mathbf{h}_m^H\mathbf{X}_{k,m}\mathbf{e}_k|^2\leq\beta_{k,m}, k\in\mathcal{K}, m\in\mathcal{M}, \tag{23c}$$

$$\sum_{j\neq k}\left(2\mathcal{R}\left(\mathrm{Tr}\left(\mathbf{h}^H\mathbf{W}_{k,m}\mathbf{e}_j\mathbf{e}_j^H\mathbf{W}_{k,m}^H(l-1)\mathbf{h}\right)\right)\right)\geq\tau_{k,m}-\sigma^2+\sum_{j\neq k}\left(|\mathbf{h}^H\mathbf{W}_{k,m}(l-1)\mathbf{e}_j|^2\right), k\in\mathcal{K}, m\in\mathcal{M}, \tag{23d}$$

$$-|\mathbf{g}_k^H\mathbf{Y}_k(l-1)\mathbf{e}_k|^2+2\mathcal{R}\left(\mathrm{Tr}\left(\mathbf{g}_k^H\mathbf{Y}_k\mathbf{e}_k\mathbf{e}_k^H\mathbf{Y}_k^H(l-1)\mathbf{g}_k\right)\right)\geq\left(2^{\gamma_k}-1\right)\left(\sum_{n\neq k}\left|\mathbf{g}_k^H\mathbf{Y}_k\mathbf{e}_n\right|^2+\sigma^2\right), k\in\mathcal{K}, \tag{23e}$$

$$||\mathbf{t}_n^H\mathbf{Z}_n||_F^2\leq\Gamma, ||\hat{\mathbf{X}}||_F^2\leq P_{\mathrm{tot}}, |\mathbf{F}_{\mathrm{RF}}(i,j)|=1, \forall i,j, \tag{23f}$$

$$\hat{\mathbf{X}}=\mathbf{F}_{\mathrm{RF}}\mathbf{F}_{\mathrm{BB}}, \hat{\mathbf{X}}=\mathbf{Z}_n, \hat{\mathbf{X}}=\mathbf{X}_{k,m}, \hat{\mathbf{X}}=\mathbf{Y}_k, \hat{\mathbf{X}}=\mathbf{W}_{k,m}, \hat{\mathbf{X}}=\mathbf{V}_k, \hat{\alpha}_{k,m}=\alpha_k, \beta_{k,m}=\hat{\beta}_{k,m}\tau_{k,m},$$
$$R_s=\hat{R}_{s,k,m}, k\in\mathcal{K}, m\in\mathcal{M}, n\in\mathcal{N}. \tag{23g}$$

$$\max_{\mathbf{F}_{\mathrm{RF}},\mathbf{F}_{\mathrm{BB}},\boldsymbol{\Xi}} R_s-\frac{1}{2\rho}||\hat{\mathbf{X}}-\mathbf{F}_{\mathrm{RF}}\mathbf{F}_{\mathrm{BB}}+\rho\boldsymbol{\lambda}_1||_F^2-\frac{1}{2\rho}\sum_{n\in\mathcal{N}}||\hat{\mathbf{X}}-\mathbf{Z}_n+\rho\boldsymbol{\lambda}_{2,n}||_F-\frac{1}{2\rho}\sum_{k\in\mathcal{K},m\in\mathcal{M}}\Big(||\hat{\mathbf{X}}-\mathbf{X}_{k,m}+\rho\boldsymbol{\lambda}_{3,k,m}||_F^2$$
$$+||\hat{\mathbf{X}}-\mathbf{V}_k+\rho\boldsymbol{\lambda}_{4,k}||_F^2+|\hat{\alpha}_{k,m}-\alpha_k+\rho\lambda_{5,k,m}|^2+|\beta_{k,m}-\hat{\beta}_{k,m}\tau_{k,m}+\rho\lambda_{6,k,m}|^2+||\hat{\mathbf{X}}-\mathbf{Y}_k+\rho\boldsymbol{\lambda}_{7,k}||_F^2$$
$$+||\hat{\mathbf{X}}-\mathbf{W}_{k,m}+\rho\boldsymbol{\lambda}_{8,k,m}||_F^2+|R_s-\hat{R}_{s,k,m}+\rho\lambda_{9,k,m}|^2\Big), \tag{24a}$$

$$\text{s.t.}\quad (23a)-(23f). \tag{24b}$$

---

from their first-order optimality conditions, given by

$$\mathbf{F}_{\mathrm{BB}}=\mathbf{F}_{\mathrm{RF}}^{\dagger}\left(\hat{\mathbf{X}}+\rho\boldsymbol{\lambda}_1\right), \tag{29}$$

$$R_s=\frac{\sum_{k\in\mathcal{K},m\in\mathcal{M}}\left(\hat{R}_{s,k,m}-\rho\lambda_{9,k,m}\right)+\rho}{KM}. \tag{30}$$

Step 3. Upon fixing the other variables, we optimize the set of variables $\{\tau_k,\mathbf{W}_k\}$ and $\{\mathbf{F}_{\mathrm{RF}}\}$ in parallel. Then, problem (24) is partitioned into the following two independent problems:

$$\min_{\tau_k,\mathbf{W}_{k,m}}\sum_{k\in\mathcal{K},m\in\mathcal{M}}\Big(|\hat{\beta}_{k,m}\tau_{k,m}-\beta_{k,m}+\rho\lambda_{6,k,m}|^2$$
$$+||\hat{\mathbf{X}}-\mathbf{W}_{k,m}+\rho\boldsymbol{\lambda}_{8,k,m}||_F^2\Big),$$
$$\text{s.t.}\quad (23d), \tag{31}$$

$$\min_{||\mathbf{F}_{\mathrm{RF}}(i,j)||_F=1,\forall i,j}||\hat{\mathbf{X}}-\mathbf{F}_{\mathrm{RF}}\mathbf{F}_{\mathrm{BB}}+\rho\boldsymbol{\lambda}_1||_F^2. \tag{32}$$

Again, we can use the Lagrange multiplier method to solve problem (31), whose details have been given in Appendix A-C.

For deriving the optimal solution of problem (32), we first reformulate it as

$$\min_{|\mathbf{F}_{\mathrm{RF}}(i,j)|=1,\forall i,j}\mathrm{Tr}\left(\mathbf{F}_{\mathrm{RF}}\mathbf{F}_{\mathrm{BB}}\mathbf{F}_{\mathrm{BB}}^H\mathbf{F}_{\mathrm{RF}}^H\right)$$
$$-2\mathcal{R}\left(\mathrm{Tr}\left(\mathbf{F}_{\mathrm{RF}}\mathbf{F}_{\mathrm{BB}}\left(\hat{\mathbf{X}}^H+\rho\boldsymbol{\lambda}_1^H\right)\right)\right). \tag{33}$$

Upon introducing $\boldsymbol{\mu}=[\mathrm{vec}\left(\mathbf{F}_{\mathrm{RF}}\right);1]$, $\boldsymbol{\Pi}=\mathbf{F}_{\mathrm{BB}}\mathbf{F}_{\mathrm{BB}}^H$ and $\boldsymbol{\Theta}=\mathbf{F}_{\mathrm{BB}}\left(\hat{\mathbf{X}}^H+\rho\boldsymbol{\lambda}_1^H\right)$, and following some matrix manipulations, problem (33) can equivalently be reformulated as

$$\max_{|\boldsymbol{\mu}(i)|=1,\forall i}\boldsymbol{\mu}^H\left(-\boldsymbol{\Psi}+\nu_{\max}\mathbf{I}_{N_t\times K}\right)\boldsymbol{\mu}, \tag{34}$$

where $\boldsymbol{\Psi}\triangleq\begin{bmatrix}\boldsymbol{\Pi}^T\otimes\mathbf{I}_{N_t}, & \mathrm{vec}\left(\boldsymbol{\Theta}\right)\\ \mathrm{vec}^H\left(\boldsymbol{\Theta}\right), & ,0\end{bmatrix}$ and $\nu_{\max}$ is the maximal eigen-value of $\boldsymbol{\Psi}$.

The following theorem gives a fixed point iteration method for locating a stationary point of problem (34).

Theorem 1: Upon introducing $\boldsymbol{\Upsilon}\triangleq-\boldsymbol{\Psi}+\nu_{\max}\mathbf{I}_{N_t\times K}$ and assuming that the limiting point obtained by the following fixed point iteration

$$\boldsymbol{\mu}(l+1)=e^{j\mathrm{arg}[\boldsymbol{\Upsilon}\boldsymbol{\mu}(l)]}, \tag{35}$$

is $\boldsymbol{\mu}^*$, $e^{-j\mathrm{arg}[\boldsymbol{\mu}^*(M+1)]}\boldsymbol{\mu}^*$ is a stationary point of problem (34).

Proof: The proof is given in Appendix B. ■

Step 4. Upon fixing the other variables, we optimize the

Algorithm 1 BCD Algorithm for Solving problem (24)

1: Define the accuracy tolerance ϵ_1 and the maximum number $N_{\max}$ of iterations.
2: **Repeat**
3: Fixing other variables, update $\{\hat{\alpha}_{k,m}, \hat{\beta}_{k,m}, \hat{R}_{s,k,m}\}$, $\{\mathbf{Y}_k\}$, and $\{\mathbf{Z}_m\}$ in parallel.
4: Fixing other variables, update $\{\alpha_k, \mathbf{V}_k\}$, $\{\mathbf{X}_{k,m}, \beta_{k,m}\}$, $\mathbf{F}_{\rm BB}$ and R_s in parallel.
5: Fixing other variables, update $\{\tau_{k,m}, \mathbf{W}_{k,m}\}$ and $\{\mathbf{F}_{\rm RF}\}$.
6: Fixing other variables, update $\hat{\mathbf{X}}$.
7: **Until** The difference of the OF values at two successive iterations is less than ϵ_1, or the number of iterations is higher than $N_{\max}$.

variable $\hat{\mathbf{X}}$. Then, problem (24) can be rewritten as

$$\begin{aligned}&\min_{\hat{\mathbf{X}}} ||\hat{\mathbf{X}} - \mathbf{F}_{\rm RF}\mathbf{F}_{\rm BB} + \rho\boldsymbol{\lambda}_1||_F^2 + \sum_{n\in\mathcal{N}} ||\hat{\mathbf{X}} - \mathbf{Z}_n + \rho\boldsymbol{\lambda}_{2,n}||_F^2 \\ &+ \sum_{\substack{k\in\mathcal{K}\\ m\in\mathcal{M}}} \Big(||\hat{\mathbf{X}} - \mathbf{X}_{k,m} + \rho\boldsymbol{\lambda}_{3,k,m}||_F^2 + ||\hat{\mathbf{X}} - \mathbf{V}_k + \rho\boldsymbol{\lambda}_{4,k}||_F^2 \\ &+ ||\hat{\mathbf{X}} - \mathbf{Y}_k + \rho\boldsymbol{\lambda}_{7,k}||_F^2 + ||\hat{\mathbf{X}} - \mathbf{W}_{k,m} + \rho\boldsymbol{\lambda}_{8,k,m}||_F^2\Big), \\ &\text{s.t.} ||\hat{\mathbf{X}}||_F^2 \le P_{\rm tot}. \end{aligned} \tag{36}$$

The detailed derivation of the solution of problem (36) has been given in Appendix A-D.

Algorithm 1 summarizes the procedures of solving problem (24), where ϵ_1 is the accuracy tolerance. When the difference of the OF values of two successive iterations in Algorithm 1 becomes less than ϵ_1 or the number of iterations is higher than $N_{\max}$, Algorithm 1 terminates.

C. Summary of the Proposed Hybrid Secure Precoder Design

Algorithm 2 summarizes the proposed PDD method conceived for handling the hybrid secure precoder design, i.e., optimization problem (12), where $\mathbf{\Sigma}^k$ and $\mathbf{\Lambda}^k$ respectively denote the set of optimization variables $\{\mathbf{F}_{\rm RF}, \mathbf{F}_{\rm BB}, \mathbf{\Xi}\}$, and the set of dual variables $\{\boldsymbol{\lambda}_1, \boldsymbol{\lambda}_{2,m}, \boldsymbol{\lambda}_{3,k,m}, \ldots, \lambda_{9,k,m}\}$ at the kth iteration, while $||h\left(\mathbf{\Sigma}^k, \mathbf{\Lambda}^k\right)||_\infty$ represents the constraint violation at the kth iteration, given by (37) at the top of the next page.

Upon introducing $\eta^k \triangleq 0.9||h\left(\mathbf{\Sigma}^{k-1}, \mathbf{\Lambda}^{k-1}\right)||_\infty$, when $||h\left(\mathbf{\Sigma}^k, \mathbf{\Lambda}^k\right)||_\infty > \eta_k$, we decrease the penalty parameter ρ according to $\rho = c\rho$. Otherwise, the dual variables are updated by

Algorithm 2 The Proposed PDD Method for Solving problem (17)

1: Initialize $\mathbf{\Sigma}^0$, $\mathbf{\Lambda}^0$, $\rho^0 > 0$, $0 < c < 1$, ϵ_2, and $m = 1$.
2: **while** $||h\left(\mathbf{\Sigma}^k, \mathbf{\Lambda}^k\right)||_\infty \ge \epsilon_2$ **do**
3: Applying Algorithm 1 to obtain the optimization variables $\mathbf{\Sigma}^k$
4: **if** $||h\left(\mathbf{\Sigma}^k, \mathbf{\Lambda}^k\right)||_\infty > \eta^k$ **then**
5: Update $\mathbf{\Lambda}^k$ by applying (38)-(46), and $\rho^{k+1} = \rho^k$
6: **else**
7: $\mathbf{\Lambda}^{k+1} = \mathbf{\Lambda}^k, \quad \rho^{k+1} = c\rho^k$
8: **end if**
9: $k = k + 1$
10: **end while**

$$\boldsymbol{\lambda}_1 = \boldsymbol{\lambda}_1 + \frac{\hat{\mathbf{X}} - \mathbf{F}_{\rm RF}\mathbf{F}_{\rm BB}}{\rho}, \tag{38}$$

$$\boldsymbol{\lambda}_{2,m} = \boldsymbol{\lambda}_{2,m} + \frac{\hat{\mathbf{X}} - \mathbf{Z}_m}{\rho}, \tag{39}$$

$$\boldsymbol{\lambda}_{3,k,m} = \boldsymbol{\lambda}_{3,k,m} + \frac{\hat{\mathbf{X}} - \mathbf{X}_{k,m}}{\rho}, \tag{40}$$

$$\boldsymbol{\lambda}_{4,k} = \boldsymbol{\lambda}_{4,k} + \frac{\hat{\mathbf{X}} - \mathbf{V}_k}{\rho}, \tag{41}$$

$$\lambda_{5,k,m} = \lambda_{5,k,m} + \frac{\hat{\alpha}_{k,m} - \alpha_k}{\rho} \tag{42}$$

$$\lambda_{6,k,m} = \lambda_{6,k,m} + \frac{\beta_{k,m} - \hat{\beta}_{k,m}\tau_{k,m}}{\rho}, \tag{43}$$

$$\boldsymbol{\lambda}_{7,k} = \boldsymbol{\lambda}_{7,k} + \frac{\hat{\mathbf{X}} - \mathbf{Y}_k}{\rho} \tag{44}$$

$$\boldsymbol{\lambda}_{8,k,m} = \boldsymbol{\lambda}_{8,k,m} + \frac{\hat{\mathbf{X}} - \mathbf{W}_{k,m}}{\rho}, \tag{45}$$

$$\lambda_{9,k,m} = \lambda_{9,k,m} + \frac{R_s - \hat{R}_{s,k,m}}{\rho}. \tag{46}$$

Algorithm 2 terminates, when $||h\left(\mathbf{\Sigma}^k, \mathbf{\Lambda}^k\right)||_\infty \le \epsilon_2$.

The convergence of the proposed Algorithm 2 is analyzed as follows. From [28, Theorem 4.1], we know that when Robinson's condition of problem (12) is satisfied, Algorithm 2 will converge to a KKT solution of problem (12). Then, according to [28, Section V-A], we know that Slater's condition is sufficient for satisfying Robinson's condition. It is easy to prove that Slater's condition holds, and then Algorithm 2 can be proved to converge to a KKT solution of problem (12).

D. Hybrid Secure Precoder Design with Finite-Resolution Phase-Shifters

So far, the hybrid secure precoder has been optimized with infinite-resolution phase-shifters. However, maintaining accurate phase control is expensive [42]. Therefore, it is necessary to study the hybrid precoder design with finite-resolution phase-shifters.

Similar to [43], a uniform quantizer is assumed to be adopted in this work. Upon denoting the set of phase-shifters as $\mathcal{F} \triangleq \left\{0, e^{j\Delta}, e^{2j\Delta}, \ldots, e^{j\left(2^b-1\right)\Delta}\right\}$, where b is the number

$$||h\left(\mathbf{\Sigma}^k,\mathbf{\Lambda}^k\right)||_\infty \triangleq \max\Big(||\hat{\mathbf{X}}-\mathbf{F}_{\rm RF}\mathbf{F}_{\rm BB}+\rho\boldsymbol{\lambda}_1||_F^2, ||\hat{\mathbf{X}}-\mathbf{Z}_m+\rho\boldsymbol{\lambda}_{2,m}||_F^2, ||\hat{\mathbf{X}}-\mathbf{X}_{k,m}+\rho\boldsymbol{\lambda}_{3,k,m}||_F^2,\ ||\hat{\mathbf{X}}-\mathbf{V}_k+\rho\boldsymbol{\lambda}_{4,k}||_F^2,$$
$$|\hat{\alpha}_{k,m}-\alpha_k+\rho\lambda_{5,k,m}|^2, |\beta_{k,m}-\hat{\beta}_{k,m}\tau_{k,m}+\rho\lambda_{6,k,m}|^2, ||\hat{\mathbf{X}}-\mathbf{Y}_k+\rho\boldsymbol{\lambda}_{7,k}||_F^2, ||\hat{\mathbf{X}}-\mathbf{W}_{k,m}+\rho\boldsymbol{\lambda}_{8,k,m}||_F^2,$$
$$|R_s-\hat{R}_{s,k,m}+\rho\lambda_{9,k,m}|^2\Big). \tag{37}$$

of bits used for quantizing the phase and $\Delta \triangleq \frac{2\pi}{2^b}$ is the quantization step size. Therefore, the choices for the elements of $\mathbf{F}_{\rm RF}$ are limited, which is subject to the set $\mathcal{F}$. Then, the secrecy rate optimization problem using finite-resolution phase-shifters can be formulated as

$$\begin{aligned}&\max_{\mathbf{F}_{\rm RF},\mathbf{F}_{\rm BB}} R_s,\\ &{\rm s.t.} R_k\geq\gamma_k, k\in\mathcal{K},\\ &\quad ||\mathbf{t}_n^H\mathbf{F}_{\rm RF}\mathbf{F}_{\rm BB}||_F^2\leq\Gamma, n\in\mathcal{N},\\ &\quad ||\mathbf{F}_{\rm RF}\mathbf{F}_{\rm BB}||_F^2\leq P_{\rm tot}, |\mathbf{F}_{\rm RF}(i,j)|\in\mathcal{F},\forall i,j.\end{aligned} \tag{47}$$

Following the procedures in Section III-A, we can obtain the augmented Lagrange problem of problem (47) which is similar to problem (24), but replacing the unit-modulus constraint in constraint (23f) by $|\mathbf{F}_{\rm RF}(i,j)|\in\mathcal{F},\forall i,j$.

Following the procedures in Section III-B, Algorithm 1 can be adapted to handle problem (47). It can be found that the modification only lies in Step 5 of Algorithm 1, i.e., (33), which is reformulated as

$$\min_{|\mathbf{F}_{\rm RF}(i,j)|\in\mathcal{F},\forall i,j} {\rm Tr}\left(\mathbf{F}_{\rm RF}\mathbf{F}_{\rm BB}\mathbf{F}_{\rm BB}^H\mathbf{F}_{\rm RF}^H\right) - 2\mathcal{R}\left({\rm Tr}\left(\mathbf{F}_{\rm RF}\mathbf{F}_{\rm BB}\left(\hat{\mathbf{X}}^H+\rho\boldsymbol{\lambda}_1^H\right)\right)\right). \tag{48}$$

For handling problem (48), the iterative algorithm of [29, Algorithm 4] can be readily adapted to handle problem (48). Specifically, the modification lies only in Step 4 of [29, Algorithm 4], which is replaced by an one-dimensional exhaustive search over $\mathcal{F}$. Therefore, we can still apply Algorithm 1 to handle the finite-resolution phase-shifter case, but updating the optimization problem of $\mathbf{F}_{\rm RF}$ at Step 5 by solving problem (48). Furthermore, the iterative algorithm proposed in Section III-B can still be applied to handle other optimization variables in the augmented Lagrange problem of problem (47).

Algorithm 3 summarizes the proposed PDD algorithm for handling problem (47).

Algorithm 3 The Proposed PDD Method for Solving problem (47)

1: Define the accuracy tolerance ϵ_1 and the maximum number $N_{\max}$ of iterations. Initialize $\mathbf{\Sigma}^0$, $\mathbf{\Lambda}^0$, $\rho^0>0$, $0<c<1$, ϵ_2, and $m=1$.
2: **while** $||h\left(\mathbf{\Sigma}^k,\mathbf{\Lambda}^k\right)||_\infty\geq\epsilon_2$ **do**
3: **Repeat**
4: Fixing other variables, update $\{\hat{\alpha}_{k,m},\hat{\beta}_{k,m},\hat{R}_{s,k,m}\}$, $\{\mathbf{Y}_k\}$ and $\{\mathbf{Z}_m\}$ according to (A.12)-(A.16), in parallel.
5: Fixing other variables, update $\{\alpha_k,\mathbf{V}_k\}$, $\{\mathbf{X}_{k,m},\beta_{k,m}\}$, $\mathbf{F}_{\rm BB}$ and R_s according to (A.17)-(A.20) and (29)-(30), in parallel.
6: Fixing other variables, update $\{\tau_{k,m},\mathbf{W}_{k,m}\}$ according to (A.21)-(A.24), and update $\{\mathbf{F}_{\rm RF}\}$ by solving problem (48).
7: Fixing other variables, update $\hat{\mathbf{X}}$ according to (A.25).
8: **Until** The difference of the OF values at two successive iterations is less than ϵ_1, or the number of iterations is higher than $N_{\max}$.
9: **if** $||h\left(\mathbf{\Sigma}^k,\mathbf{\Lambda}^k\right)||_\infty>\eta^k$ **then**
10: Update $\mathbf{\Lambda}^k$ by applying (38)-(46), and $\rho^{k+1}=\rho^k$
11: **else**
12: $\mathbf{\Lambda}^{k+1}=\mathbf{\Lambda}^k,\quad \rho^{k+1}=c\rho^k$
13: **end if**
14: $k=k+1$
15: **end while**

E. Computational Complexity Analysis

This subsection gives the computational complexity analysis of the proposed hybrid precoder design. Firstly, considering a hybrid precoder design with infinite resolution phase shifters, from (A.15) and (A.16) in Appendix A, we can find that the computational complexity of updating $\{\mathbf{Y}_k\}$, and $\{\mathbf{Z}_n\}$ is dominated by the matrix inversion and the bisection search algorithm used for obtaining optimal Lagrange multipliers whose number of iteration is $\log_2\left(\frac{\upsilon_1}{\upsilon_2}\right)$, where υ_1 is the initial interval size and υ_2 is the tolerance. Since the complexity of the matrix inversion based on the Gauss-Jordan elimination is dominated by $\mathcal{O}\left((N_t\times K)^3\right)$, the computational complexity of updating $\{\mathbf{Y}_k\}$, and $\{\mathbf{Z}_n\}$ is dominated by $\mathcal{O}\left((N_t\times K)^3+\log_2\left(\frac{\upsilon_1}{\upsilon_2}\right)\right)$. Accordingly, from (A.17) and (A.19) in Appendix A, the computational complexity of updating $\mathbf{V}_k$ and $\mathbf{X}_{k,m}$ is also dominated by $\mathcal{O}\left((N_t\times K)^3+\log_2\left(\frac{\upsilon_1}{\upsilon_2}\right)\right)$. From (A.21), (A.23), and (A.25) in Appendix A, the computational complexity of updating $\mathbf{W}_{k,m}$ and $\hat{\mathbf{X}}$ is dominated by $\mathcal{O}\left((N_t)^3+\log_2\left(\frac{\upsilon_1}{\upsilon_2}\right)\right)$ and $\mathcal{O}\left(N_tN_{\rm RF}^2\right)$, respectively. The computational complexity of updating $\mathbf{F}_{\rm BB}$ and $\mathbf{F}_{\rm RF}$ is dominated by $\mathcal{O}\left((N_t)^3+N_{\rm RF}^2N_t\right)$ and $\mathcal{O}\left(I_3N_t^2K^2\right)$, respectively, where I_3 is the number of fixed-point iterations. Finally, since $N_t>N_{\rm RF}$, by retaining the dominant terms, the computational complexity of Algorithm 2 is dominated by $\mathcal{O}\left(N_1N_2\left((N_t\times K)^3+I_3N_t^2K^2+\log_2\left(\frac{\upsilon_1}{\upsilon_2}\right)\right)\right)$, where N_1 and N_2 are the number of iterations of the outer and inner loops, respectively.

Similarly, the computational complexity of the hybrid precoder design with finite-resolution phase shifters is $\mathcal{O}\left(N_1N_2\left((N_t\times K)^3+I_4N_tN_{\rm RF}\left(N_tN_{\rm RF}+2^b\right)+\log_2\left(\frac{\upsilon_1}{\upsilon_2}\right)\right)\right)$,

where I_4 is the number of iterations required for updating $\mathbf{F}_{\mathrm{RF}}$.

IV. Hybrid Precoder Design with Multiple-antenna PUs and Imperfect Eves' CSI

In the previous sections, we consider multiple single-antenna aided PUs and perfect Eves' CSI. By contrast, in this subsection, we will show that the proposed PDD algorithm can also be adapted to the scenario where each PU is equipped with N_p antennas and only the imperfect CSI of multiple Eves is available. Similar to [29], we adopt the widely used geometric channel model for characterizing the channels spanning from the ST to the nth PU, which is given by

$$\mathbf{T}_n = \sqrt{\frac{N_t N_p}{L_{\mathbf{T}_n}}} \sum_{l=1}^{L_{\mathbf{T}_n}} \omega_{\mathbf{T}_n}^l \mathbf{a}\left(\theta_{\mathbf{T}_n,r}^l\right) \mathbf{a}^H\left(\theta_{\mathbf{T}_n,t}^l\right), \tag{49}$$

where $L_{\mathbf{T}_n}$ and $\omega_{\mathbf{T}_n}^l$ are defined similarly as their counterparts in (5). Furthermore, $\mathbf{a}\left(\theta_{\mathbf{T}_n,r}^l\right)$ and $\mathbf{a}\left(\theta_{\mathbf{T}_n,t}^l\right)$ are the receive and transmit array response vectors at the angle of arrival (AOA) $\theta_{\mathbf{T}_n,r}^l \in [0, 2\pi]$ and the angle of departure (AOD) $\theta_{\mathbf{T}_n,t}^l \in [0, 2\pi]$, respectively.

Similar to [49]–[51], the channel uncertainty of multiple Eves is characterized by the widely-used Gaussian CSI error model. In particular, the channel between the ST and the mth Eve is given by

$$\mathbf{h}_m = \hat{\mathbf{h}}_m + \mathbf{\Delta}_{\mathbf{h}_m}, \tag{50}$$

where the Gaussian error vector $\mathbf{\Delta}_{\mathbf{h}_m} \sim \mathcal{CN}\left(\mathbf{0}, \mathbf{E}_m\right)$ having the covariance matrix of $\mathbf{E}_m \in \mathbb{H}_+^{N_t}$, represents the mth Eve's channel uncertainty, and $\hat{\mathbf{h}}_m$ denotes the estimated CSI. The uncertain model (50) is a more general model, which can capture the extreme case, i.e., the instantaneous CSI of multiple Eves is unavailable ($\hat{\mathbf{h}}_m = \mathbf{0}_{N_t \times 1}$).

We adopt the widely used stochastic approach [26], [46]–[48] for handling Eves' CSI uncertainty. In particular, we adopt the average secrecy rate as the objective function, which averages the achievable secrecy rate over Eves' uncertainty and converts the impact of Eves' CSI uncertainty into a more amenable formulation. The average secrecy rate of the kth user is given as follows

$$\bar{R}_{s,k} \triangleq \min_{m \in \mathcal{M}} \left(R_k - \mathbb{E}_{\mathbf{\Delta}_{\mathbf{h}_m}}\left(R_{e_{k,m}}\right)\right), \tag{51}$$

where $\bar{R}_{s,k}$ characterizes the achievable average secrecy rate of the kth user in the presence of Eves' CSI uncertainty.

Employing the stochastic approach, the optimization of the hybrid precoder can be formulated as

$$\max_{\mathbf{F}_{\mathrm{RF}},\mathbf{F}_{\mathrm{BB}}} \min_{k \in \mathcal{K}} \bar{R}_{s,k}, \tag{52a}$$

$$\text{s.t.} (12b), (12d), (12e), \tag{52b}$$

$$||\mathbf{T}_n^H \mathbf{F}_{\mathrm{RF}} \mathbf{F}_{\mathrm{BB}}||_F^2 \leq \Gamma, n \in \mathcal{N}. \tag{52c}$$

However, since it is an open challenge to derive a tractable analytical formula for the average secrecy rate, similar to [46]–[48], we adopt the widely-used lower-bound technique to optimize the hybrid precoder. In particular, we first employ Jensen's inequality to find a lower bound of the achievable average secrecy rate and optimize the hybrid precoder to maximize the lower bound. An upper bound of the average rate of the mth Eve is given by (53) at the top of the next page, where step (a) is due to Jensen's inequality and step (b) is derived based on [45, Lemma 1]. As commented by Zhang *et al.* [45], such an approximation becomes accurate upon increasing the number of antennas, hence it is quite accurate in the massive MIMO setting. Furthermore, this approximation has been widely adopted by authoritative contributions on PLS [26], [46]–[48]. Therefore, employing the lower bound technique, problem (52) can be approximated as follows:

$$\max_{\mathbf{F}_{\mathrm{RF}},\mathbf{F}_{\mathrm{BB}}} \min_{k \in \mathcal{K}} \min_{m \in \mathcal{M}} \left(R_k - \bar{R}_{e_{k,m}}^U\right) \tag{54a}$$

$$\text{s.t.} (52b), (52c). \tag{54b}$$

It is worth pointing out that the impact of Eves' CSI uncertainty on the achievable secrecy performance is determined by the terms $||\mathbf{E}_m^{\frac{1}{2}} \mathbf{F}_{\mathrm{RF}} \mathbf{F}_{\mathrm{BB}} \mathbf{e}_k||_F^2$ and $||\mathbf{E}_m^{\frac{1}{2}} \mathbf{F}_{\mathrm{RF}} \mathbf{F}_{\mathrm{BB}} \mathbf{e}_j||_F^2$ in (53). For reformulating $\bar{R}_{e_{k,m}}^U$ as a more tractable formulation, we introduce a composite channel $\mathbf{G}_{e,m} \triangleq \left[\hat{\mathbf{h}}_m, \mathbf{E}_m^{\frac{1}{2}}\right]$, which consists of both the estimated CSI of the mth Eve, as well as of $\hat{\mathbf{h}}_m$ and the covariance matrix of uncertainty, $\mathbf{E}_m$. Then, a more concise formulation of $\bar{R}_{e_{k,m}}^U$ can be built as

$$\bar{R}_{e_{k,m}}^U = \log_2\left(1 + \frac{||\mathbf{G}_{e,m} \mathbf{F}_{\mathrm{RF}} \mathbf{F}_{\mathrm{BB}} \mathbf{e}_k||_F^2}{\sum_{j \neq k} ||\mathbf{G}_{e,m} \mathbf{F}_{\mathrm{RF}} \mathbf{F}_{\mathrm{BB}} \mathbf{e}_j||_F^2 ||_F^2 + \sigma^2}\right).$$

Following the procedures in Section III-A, and introducing auxiliary variables $\mathbf{\Xi} = \left\{\hat{\mathbf{X}}, \mathbf{Z}_n, \mathbf{X}_{k,m}, \mathbf{V}_k, \alpha_k, \hat{\alpha}_{k,m}, \beta_{k,m}, \hat{\beta}_{k,m}, \tau_{k,m}, \mathbf{Y}_k, \mathbf{W}_{k,m}, \hat{R}_{s,k,m}, R_s^L\right\}$, and a set of Lagrange multipliers $\mathbf{\lambda} \triangleq \{\mathbf{\lambda}_1, \mathbf{\lambda}_{2,m}, \mathbf{\lambda}_{3,k,m}, \mathbf{\lambda}_{4,k}, \lambda_{5,k,m}, \lambda_{6,k,m}, \mathbf{\lambda}_{7,k}, \mathbf{\lambda}_{8,k}, \lambda_{9,k,m}, k \in \mathcal{K}\}$, the augmented Lagrange problem of the convex approximation of problem (54) at the lth iteration, can be formulated as problem (55) at the top of the next page.

The proposed hybrid secure precoder design algorithm introduced in Section III can also be adapted to handle problem (54) with some small modifications. The modifications lie in the optimization of $\mathbf{X}_{k,m}$, $\mathbf{W}_{k,m}$, and $\mathbf{Z}_n$, which are formulated as problems (C.1), (C.2), and (C.3) in Appendix C. They can be solved by applying the Lagrange multiplier method. See the details in Appendix C.

V. Simulation Results and Discussions

In this section, simulation results are provided for characterizing the average secrecy performance achieved by the proposed PDD algorithm. Similar to [30], the tolerance of Algorithm 1-3 is set to be some prescribed small constant, i.e., $\epsilon_1 = \epsilon_2 = 10^{-4}$, where ϵ_1 controls the accuracy of Algorithm 1 and ϵ_2 represents the minimum constraint violation. For balancing the achievable secrecy performance and convergence rate of the proposed PDD algorithm, we set the maximum number of iterations as $N_{\max} = 300$ for avoiding the possibly slow convergence of Algorithm 1 [30]. Furthermore, similar to [28], [30], we set the control parameter c in Algorithm 2 to be 0.7 for reducing ρ gradually to obtain an efficient solution. Similar to [29], the number of distinguishable paths

$$\mathbb{E}\left(R_{e_{k,m}}\left(\mathbf{F}_{\mathrm{RF}},\mathbf{F}_{\mathrm{BB}}\right)\right)\overset{(a)}{\leq}\log_2\left(1+\mathbb{E}\left(\frac{|\mathbf{h}_m^H\mathbf{F}_{\mathrm{RF}}\mathbf{F}_{\mathrm{BB}}\mathbf{e}_k|^2}{\sum_{j\neq k}|\mathbf{h}_m^H\mathbf{F}_{\mathrm{RF}}\mathbf{F}_{\mathrm{BB}}\mathbf{e}_j|^2+\sigma^2}\right)\right)\overset{(b)}{\approx}\log_2\left(1+\frac{\mathbb{E}\left(|\mathbf{h}_m^H\mathbf{F}_{\mathrm{RF}}\mathbf{F}_{\mathrm{BB}}\mathbf{e}_k|^2\right)}{\mathbb{E}\left(\sum_{j\neq k}|\mathbf{h}_m^H\mathbf{F}_{\mathrm{RF}}\mathbf{F}_{\mathrm{BB}}\mathbf{e}_j|^2\right)+\sigma^2}\right)$$
$$=\bar{R}^U_{e_{k,m}}\triangleq\log_2\left(1+\frac{|\hat{\mathbf{h}}_m^H\mathbf{F}_{\mathrm{RF}}\mathbf{F}_{\mathrm{BB}}\mathbf{e}_k|^2+||\mathbf{E}_m^{\frac{1}{2}}\mathbf{F}_{\mathrm{RF}}\mathbf{F}_{\mathrm{BB}}\mathbf{e}_k||_F^2}{\sum_{j\neq k}\left(|\hat{\mathbf{h}}_m^H\mathbf{F}_{\mathrm{RF}}\mathbf{F}_{\mathrm{BB}}\mathbf{e}_j|^2+||\mathbf{E}_m^{\frac{1}{2}}\mathbf{F}_{\mathrm{RF}}\mathbf{F}_{\mathrm{BB}}\mathbf{e}_j||_F^2\right)+\sigma^2}\right), \tag{53}$$

$$\max_{\mathbf{F}_{\mathrm{RF}},\mathbf{F}_{\mathrm{BB}},\boldsymbol{\Xi}} R_s^L-\frac{1}{2\rho}||\hat{\mathbf{X}}-\mathbf{F}_{\mathrm{RF}}\mathbf{F}_{\mathrm{BB}}+\rho\boldsymbol{\lambda}_1||_F^2-\frac{1}{2\rho}\sum_{n\in\mathcal{N}}||\hat{\mathbf{X}}-\mathbf{Z}_n+\rho\boldsymbol{\lambda}_{2,n}||_F^2-\frac{1}{2\rho}\sum_{k\in\mathcal{K},m\in\mathcal{M}}\Big(||\hat{\mathbf{X}}-\mathbf{X}_{k,m}+\rho\boldsymbol{\lambda}_{3,k,m}||_F^2$$
$$+||\hat{\mathbf{X}}-\mathbf{V}_k+\rho\boldsymbol{\lambda}_{4,k}||_F^2+|\hat{\alpha}_{k,m}-\alpha_k+\rho\lambda_{5,k,m}|^2+|\beta_{k,m}-\hat{\beta}_{k,m}\tau_{k,m}+\rho\lambda_{6,k,m}|^2+||\hat{\mathbf{X}}-\mathbf{Y}_k+\rho\boldsymbol{\lambda}_{7,k}||_F^2$$
$$+||\hat{\mathbf{X}}-\mathbf{W}_{k,m}+\rho\boldsymbol{\lambda}_{8,k,m}||_F^2+|R_s^L-\hat{R}^L_{s,k,m}+\rho\lambda_{9,k,m}|^2\Big), \tag{55a}$$

$$\text{s.t.}\log_2\left(1+\hat{\alpha}_{k,m}\right)-\log_2\left(1+\hat{\beta}_{k,m}(l-1)\right)-\frac{\hat{\beta}_{k,m}-\hat{\beta}_{k,m}(l-1)}{\ln(2)\left(1+\hat{\beta}_{k,m}(l-1)\right)}\geq\hat{R}^L_{s,k,m},k\in\mathcal{K},m\in\mathcal{M}, \tag{55b}$$

$$\frac{2\mathcal{R}\left(\mathbf{e}_k^H\mathbf{V}_k^H(l-1)\mathbf{g}_k\mathbf{g}_k^H\mathbf{V}_k\mathbf{e}_k\right)}{\alpha_k(l-1)}-\frac{|\mathbf{g}_k^H\mathbf{V}_k\left(l-1\right)\mathbf{e}_k|^2}{\left(\alpha_k(l-1)\right)^2}\alpha_k\geq\sum_{j\neq k}\left|\mathbf{g}_k^H\mathbf{V}_k\mathbf{e}_j\right|^2+\sigma^2,k\in\mathcal{K}, \tag{55c}$$

$$\left|\left|\mathbf{G}_{e,m}^H\mathbf{X}_{k,m}\mathbf{e}_k\right|\right|_F^2\leq\beta_{k,m},k\in\mathcal{K},m\in\mathcal{M}, \tag{55d}$$

$$\sum_{j\neq k}\left(2\mathcal{R}\left(\mathrm{Tr}\left(\mathbf{G}_{e,m}^H\mathbf{W}_{k,m}\mathbf{e}_j\mathbf{e}_j^H\mathbf{W}_{k,m}^H(l-1)\mathbf{G}_{e,m}\right)\right)\right)\geq\tau_{k,m}-\sigma^2+\sum_{j\neq k}\left(|\mathbf{G}_{e,m}^H\mathbf{W}_{k,m}(l-1)\mathbf{e}_j|^2\right),k\in\mathcal{K},m\in\mathcal{M}, \tag{55e}$$

$$-|\mathbf{g}_k^H\mathbf{Y}_k(l-1)\mathbf{e}_k|^2+2\mathcal{R}\left(\mathrm{Tr}\left(\mathbf{g}_k^H\mathbf{Y}_k\mathbf{e}_k\mathbf{e}_k^H\mathbf{Y}_k^H(l-1)\mathbf{g}_k\right)\right)\geq\left(2^{\gamma_k}-1\right)\left(\sum_{n\neq k}\left|\mathbf{g}_k^H\mathbf{Y}_k\mathbf{e}_n\right|^2+\sigma^2\right),k\in\mathcal{K}, \tag{55f}$$

$$||\mathbf{T}_n\mathbf{Z}_n||_F^2\leq\Gamma,||\hat{\mathbf{X}}||_F^2\leq P_{\mathrm{tot}},|\mathbf{F}_{\mathrm{RF}}(i,j)|=1,\forall i,j, \tag{55g}$$

in the channel model (3), (4), (5), and (49) is set as 15. In the following simulation results, the secrecy performance achieved by the proposed PDD method is denoted as "PDD". The performance achieved by a fully-digital zero-forcing precoder using $N_t=N_{\mathrm{RF}}$ is adopted as the benchmark, where the ST transmits confidential information in the null-space of the channels of PUs and Eves. Specifically, the fully-digital zero-forcing precoder $\mathbf{F}_{ZF}$ is formulated as:

$$\mathbf{F}_{ZF}=\mathbf{U}_{ZF}\left(\mathbf{G}^H\mathbf{U}_{ZF}\right)^H\left(\mathbf{G}^H\mathbf{U}_{ZF}\left(\mathbf{G}^H\mathbf{U}_{ZF}\right)^H\right)^{-1}, \tag{56}$$

where, $\mathbf{U}_{ZF}$ is the null-space of the channels from ST to PUs and Eves. For simplicity, the secrecy performance achieved by the zero-forcing precoder is marked by "Zero-Forcing".

A. Convergence Rate of the Proposed PDD Algorithm

The convergence rates of the proposed PDD algorithm for the infinite and finite resolution phase-shifter case are portrayed in Fig. 2 and Fig. 3, respectively. Fig. 2(a) and Fig. 3(a) plot the secrecy rate versus the number of iterations. From Fig. 2(a), we can find that the secrecy rate converges to a constant value within about 20 iterations for the infinite-resolution phase-shifter case. Furthermore, simulation results in Fig. 3(a) show that the secrecy rate converges to a constant value within about 60 iterations for the finite-resolution phase-shifter case. Fig. 2(b) and Fig. 3(b) show that the constraint violations will reduce to at least 10^{-4} after 120 iterations.

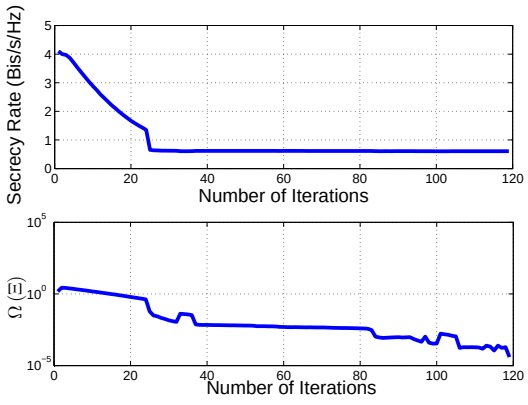

Fig. 2. (a): The minimum secrecy rate of the served SU, (b): the constraint violation $\Omega\left(\Xi\right)$ versus the number of iterations for the infinite-resolution phase-shifter case with $N_t=10$, $N_{\mathrm{RF}}=4$,, $K=3$, $P_t=0$ dBW, $\gamma_k=0.3$bits/s/Hz, and $\Gamma=0$ dB.

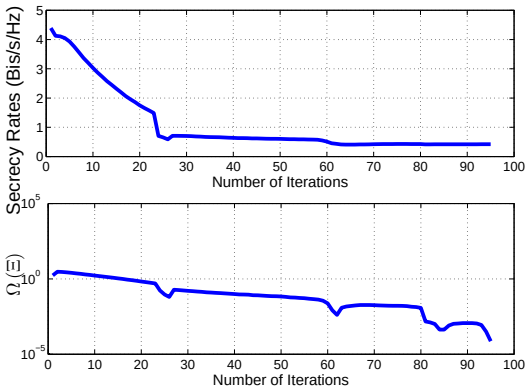

Fig. 3. (a): The minimum secrecy rate of the served SU, (b): the constraint violation Ω (Ξ) versus the number of iterations for the finite-resolution phase-shifter case with $N_t = 20$, $N_{\mathrm{RF}} = 4$,, $K = 3$, $P_t = 0$ dBW, $\gamma_k = 0.3$bits/s/Hz, and $\Gamma = 0$dB.

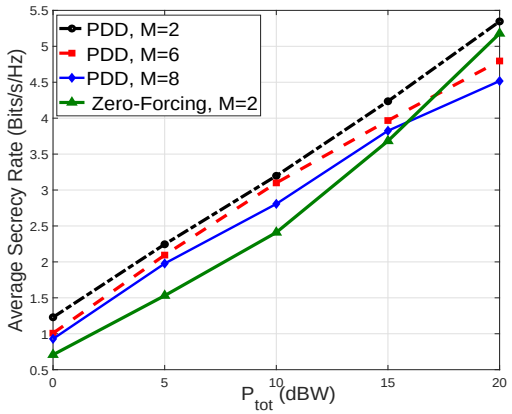

Fig. 5. Average secrecy rate versus P_{tot} for $R_t = 0.3$, $\Gamma = 0$dB $N_t = 10$, $N = 3$, $K = 2$, $N_{\mathrm{RF}} = 3$, and different M.

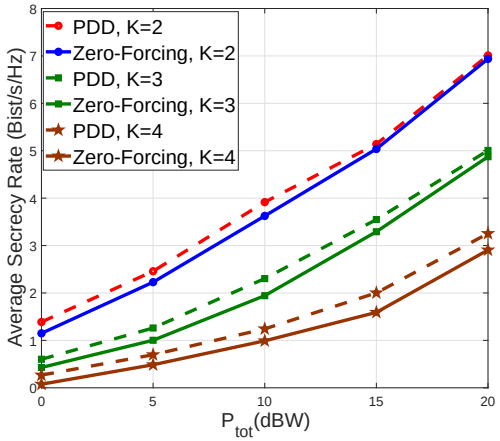

Fig. 4. Average secrecy rate versus P_{tot} for $N_{\mathrm{RF}} = 4$, $R_t = 0.3$, $\Gamma = 10$dB $N_t = 10$, $M = 1$, $N = 1$, different K.

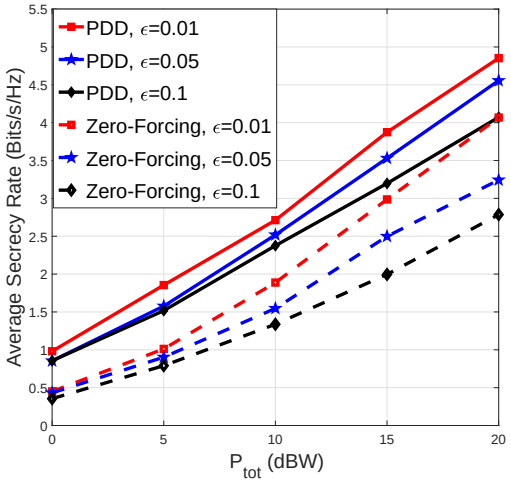

Fig. 6. Average secrecy rate of the infinite-resolution phase-shifter case versus P_{tot}, for the imperfect Eves' CSI and a multi-antenna PUs, with $N_p = 6$, $K = 2$, $N_{\mathrm{RF}} = 4$, $N_t = 10$, $R_t = 0.3$, $\Gamma = 10$dB, $M = 1$, $N = 1$, and different ϵ.

B. Secrecy Performance of the Hybrid Precoder with Infinite-Resolution Phase-Shifters

We first investigate the secrecy performance of the proposed PDD method for a single Eve and PU. Fig. 4 shows the average minimum secrecy rate of multiple SUs achieved by the proposed PDD solution versus P_{tot} for different K values. Simulation results in Fig. 4 show that the proposed PDD method outperforms the fully digital zero-forcing precoder. In particular, the secrecy performance gain is reduced upon increasing P_{tot}. It is worth mentioning that similar performance trends have been shown in [44, Fig. 3]. This phenomenon is not unexpected, since upon increasing P_{tot}, the zero-forcing approach tends to become optimal. Therefore, such a result validates the efficiency of the proposed PDD method from another perspective.

Fig. 5 shows the secrecy performance achieved by the proposed PDD algorithm versus P_{tot} for different M. Since the security threat increases with the increasing M, it is anticipated that the average secrecy rate will decrease with the increasing M. Simulation results in Fig. 5 validate this speculation. Moreover, the secrecy performance degradation brought by increasing M is very little, e.g., increasing M from 2 to 8, the secrecy performance degradation is about 0.4 Bits/s/Hz for $P_{\mathrm{tot}} = 15$ dBW. Such result has shown the robustness of the proposed PDD method for resisting the increasing security threat brought by the increasing number of Eves.

Fig. 6 has shown the average secrecy rate of the proposed PDD algorithm when multiple PUs are equipped with N_p antennas and only the imperfect Eves' CSI is available, where $\mathbf{E}_m = \epsilon \mathbf{I}_{N_t}$, $\forall m \in \mathcal{M}$. For the zero-forcing precoder, we design the precoder based on the estimated Eves' CSI $\hat{\mathbf{h}}_m$. The imperfect Eves' CSI makes the information leakage unavoidable, even for the zero-forcing precoder. Simulation results in Fig. 6 show that the secrecy performance degrades upon increasing ϵ. This is because a larger ϵ will result in increasing information leakage. Additionally, we also find that in contrast to the perfect Eves' CSI case, the secrecy performance of the zero-forcing precoder does not converge

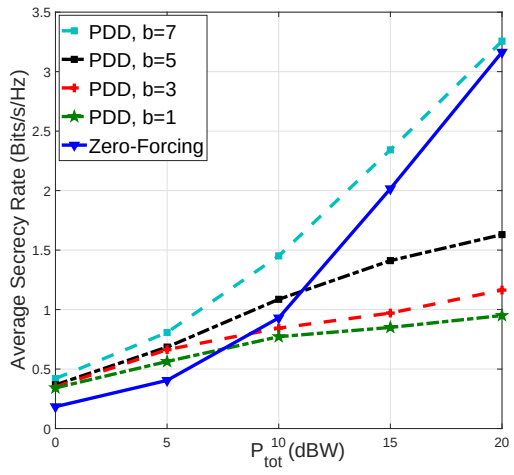

Fig. 7. Average secrecy rate of the finite-resolution phase-shifter case versus $P_{\rm tot}$ for $N_{\rm RF}=4$, $R_t=0.3$, $\Gamma=0$dB, $N_t=10$, $K=3$, $M=2$, $N=3$, and different b.

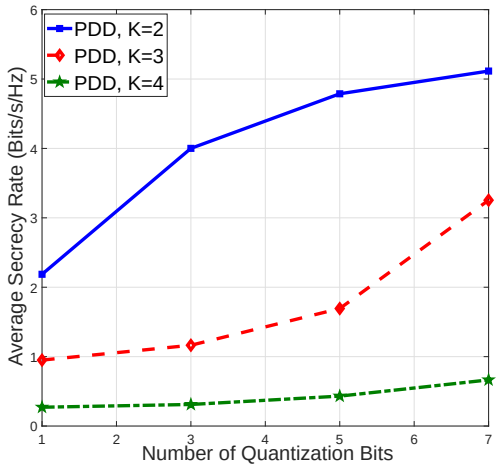

Fig. 8. Average secrecy rate of the finite-resolution phase-shifter case versus the number of quantization bits, b for $P_{\rm tot}=20$ dBW, $N_{\rm RF}=4$, $R_t=0.3$, $\Gamma=0$dB $N_t=10$, $M=2$, $N=3$, different K.

to that of the proposed PDD method upon increasing $P_{\rm tot}$. This is because the zero-forcing precoder is designed based on the estimated Eves' CSI, and the uncertainty inevitably results in information leakage, which degrades the achievable secrecy performance. This result validates the superiority of our proposed PDD method, once again.

C. Secrecy Performance of the Hybrid Precoder with Finite-Resolution Phase-Shifters

Fig. 7 shows the average secrecy rate with the finite-resolution phase-shifters versus $P_{\rm tot}$. The average secrecy rate achieved by the fully-digital zero-forcing precoder is given for reference. From simulation results in Fig. 7, we can find that the proposed PDD algorithm can achieve a better secrecy performance than the zero-forcing precoder when $P_{\rm tot}<5$ dBW for all numbers of quantization bits, even if $b=1$. Moreover, when $b=7$, our proposed PDD algorithm outperforms the zero-forcing precoder over the whole region of $P_{\rm tot}$. Such results validate the superiority of our proposed PDD algorithm. On the other hand, the performance degradation at high $P_{\rm tot}$ is serious when b decreases from 7 bits to 5 bits, which is due to the increasing confidential signal leakage to Eves with the decreasing b.

Fig. 8 shows the impact of the number of the quantization bits on the achievable secrecy rate for different K. With the increasing b, the resolution of the phase-shifters increases, leading to an increase in the achievable secrecy rate. Moreover, from Fig. 8, we can find that the increment in the secrecy rate decreases with the increasing K, which may be due to the limited number of RF chains.

The above simulation results not only validate the superiority of the proposed PDD algorithm but also reveal some insights on the hybrid precoder design. First, the secrecy performance degrades seriously with the increasing number of served users, especially for high $P_{\rm tot}$, due to the reducing number of degrees-of-freedom (DoF). Such a phenomenon tells that for broadcast communications, allowing the number of served users equal to the maximal available DoF may not be an optimal choice, from the perspective of the communication security. Second, the resolution of the phase-shifters plays a dominant role in determining the achievable secrecy performance. Although increasing the resolution can improve the achievable secrecy performance, the corresponding system complexity also increases. Furthermore, simulation results in Fig. 8 also show that the performance gains brought by increasing the resolution decrease. Therefore, there is an optimal balance between the secrecy performance and system complexity, which needs to be investigated in the future work. Third, simulation results show that the secrecy performance of the zero-forcing precoder approaches the proposed PDD algorithm for high $P_{\rm tot}$, which implies that the optimal structure of the hybrid precoder approaches the zero-forcing precoder, when $P_{\rm tot}$ is very large.

VI. Conclusions and Future Works

In this paper, we have investigated the hybrid secure precoder design for the confidential information transmission in cognitive mmWave networks by maximizing the minimum secrecy rate of multiple served SUs under the interference temperature constraint of multiple PUs. The studied problem was formulated as a nonlinear and nonconvex optimization problem with coupling constraints. For handling this challenging problem, we employed the PDD algorithm to handle the nonconvexity of the joint design problem and the coupling constraint. In particular, the proposed PDD algorithm first converts the coupling variables into equality constraints, which are then augmented to the OF by applying the augmented Lagrange method. Then, we combined the SCA and BCD algorithm for transforming the nonconvex joint design problem into a sequence of convex problems, which are solved by using the Lagrange multiplier method. The proposed PDD algorithm has provable convergence to a KKT solution of

the original nonconvex joint design problem, which is computationally efficient, due to the parallel optimization of the optimization variables in each block. Finally, we showed that the proposed PDD algorithm can be adapted both to the finite resolution shifter case and to the scenario, where multiple PUs are equipped with multiple antennas and only the imperfect CSI of multiple Eves is available. Our simulation results have verified the efficiency of our proposed hybrid secure precoder design explicitly. In particular, we show that our proposed algorithm outperforms the fully-digital zero-forcing precoder, demonstrating its near-optimal secrecy performance in cognitive mmWave networks. Furthermore, our simulation results show that compared to the zero-forcing precoder, the proposed joint design algorithm relying on finite-resolution phase-shifters achieves a satisfactory secrecy performance by using 7 bits for phase quantization, striking a compelling secrecy performance vs. system complexity trade-off.

Some future research directions for improving the system model considered in this work are outlined as follows. Firstly, this treatise does not consider the quantization noise of the finite resolution digital to analog converters (DACs). Since conventional high-resolution DACs are power hungry, it is interesting to consider the joint optimization of the DAC resolution and hybrid precoder for maximizing the secrecy energy efficiency of mmWave cognitive networks. Secondly, this work has adopted a fully-connected hybrid beamforming structure, where each RF chain is connected to all antennas. It is meaningful to extend the work to consider an adaptively-connected structure, where a switch-controlled connection is employed between each antenna and each RF, and to consider the joint optimization of switch-controlled connections as well as a hybrid precoder for maximizing the secrecy energy efficiency.

APPENDIX A

A. Optimization Problems and Solutions at Step 1

The optimization of $\{\hat{\alpha}_{k,m}, \hat{\beta}_{k,m}, \hat{R}_{s,k,m}\}$, $\{\mathbf{Y}_k\}$ and $\{\mathbf{Z}_n\}$ can built as problem (A.1) at the top of next page, problems (A.2) and (A.3) given as follows.

$$\min_{\mathbf{Y}_k} \sum_{k\in\mathcal{K}} \left(||\hat{\mathbf{X}} - \mathbf{Y}_k + \rho\boldsymbol{\lambda}_{7,k}||_F^2\right), \quad \text{s.t.}(23e), \tag{A.2}$$

$$\min_{\mathbf{Z}_n} \sum_{n\in\mathcal{N}} ||\hat{\mathbf{X}} - \mathbf{Z}_n + \rho\boldsymbol{\lambda}_{2,n}||_F^2,$$
$$\text{s.t.} \quad ||\mathbf{t}_n^H\mathbf{Z}_n||_F^2 \leq \Gamma, n \in \mathcal{N}. \tag{A.3}$$

Upon introducing the nonnegative Lagrange multipliers $\nu_{1,1,k,m}, \nu_{1,2,k}, \nu_{1,3,n}$, $k \in \mathcal{K}, n \in \mathcal{N}$ for these problems, their KKT conditions can be obtained by applying the vectorization operator of [38, Section 1.11.2] and the complex-valued matrix derivatives of [39], which are given by

$$2\hat{\alpha}_{k,m} - 2\left(\alpha_k - \rho\lambda_{5,k,m}\right) - \frac{\nu_{1,1,k,m}}{\ln 2\left(1+\hat{\alpha}_{k,m}\right)} = 0, \tag{A.4}$$

$$2\hat{\beta}_{k,m} - 2\left(\beta_{k,m} - \rho\lambda_{6,k,m}\right) + \frac{\nu_{1,1,k,m}}{\ln 2\left(1+\hat{\beta}_{k,m}(l-1)\right)} = 0, \tag{A.5}$$

$$2\hat{R}_{s,k,m} - 2\left(R_s + \rho\lambda_{9,k,m}\right) + \nu_{1,1,k,m} = 0, \tag{A.6}$$

$$\nu_{1,1,k,m}\left(\log_2\left(1+\hat{\alpha}_{k,m}\right) - \log_2\left(1+\hat{\beta}_{k,m}(l-1)\right)\right.$$
$$\left. - \frac{\hat{\beta}_{k,m} - \hat{\beta}_{k,m}(l-1)}{\ln(2)\left(1+\hat{\beta}_{k,m}(l-1)\right)} - \hat{R}_{s,k,m}\right) = 0, \tag{A.7}$$

$$-\hat{\mathbf{X}} + \mathbf{Y}_k - \rho\boldsymbol{\lambda}_{7,k} + \nu_{1,2,k}\left(\left(2^{\gamma_k}-1\right)\mathbf{g}_k\mathbf{g}_k^H\mathbf{Y}_k\mathbf{e}_n\mathbf{e}_n^H\right.$$
$$\left. -\mathbf{g}_k\mathbf{g}_k^H\mathbf{Y}_k\left(l-1\right)\mathbf{e}_k\mathbf{e}_k^H\right) = \mathbf{0}, \tag{A.8}$$

$$\nu_{1,2,k}\left(2\mathcal{R}\left(\text{Tr}\left(\mathbf{g}_k^H\mathbf{Y}_k\mathbf{e}_k\mathbf{e}_k^H\mathbf{Y}_k^H(l-1)\mathbf{g}_k\right)\right) -\right.$$
$$\left. |\mathbf{g}_k^H\mathbf{Y}_k(l-1)\mathbf{e}_k|^2 - (2^{\gamma_k}-1)\left(\sum_{n\neq k}\left|\mathbf{g}_k^H\mathbf{Y}_k\mathbf{e}_n\right|^2 + \sigma^2\right)\right) = 0, \tag{A.9}$$

$$-\hat{\mathbf{X}} + \mathbf{Z}_n - \rho\boldsymbol{\lambda}_{2,n} + \nu_{1,3,n}\mathbf{t}_n\mathbf{t}_n^H\mathbf{Z}_n = \mathbf{0}, \tag{A.10}$$

$$\nu_{1,3,n}\left(||\mathbf{Z}_n||_F^2 - \Gamma\right) = 0. \tag{A.11}$$

The condition sets (A.4)-(A.7), (A.8)-(A.9), and (A.10)-(A.11) are respectively the KKT conditions of Problems (A.1)-(A.3). Conditions (A.7), (A.9) and (A.11) represent respectively the complementary slackness in the KKT conditions of Problems (A.1)-(A.3).

From the KKT conditions above, the optimal solutions of problems (A.1)-(A.3) can be obtained as functions of the Lagrange multipliers, given by

$$\hat{R}_{s,k,m} = R_s + \rho\lambda_{9,k,m} - \frac{\nu_{1,1,k,m}\ln(2)}{2}, \tag{A.12}$$

$$\hat{\beta}_{k,m} = \frac{\beta_{k,m} + \rho\lambda_{6,k,m}}{\tau_{k,m}} - \frac{\nu_{1,1,k,m}}{2\ln 2\left(1+\hat{\beta}_{k,m}\left(l-1\right)\right)\left(\tau_{k,m}\right)^2}, \tag{A.13}$$

$$\hat{\alpha}_{k,m} = \frac{-b_{k,m} + \sqrt{b_{k,m}^2 - 4a_{k,m}c_{k,m}}}{2a_{k,m}}, \tag{A.14}$$

$$\mathbf{Z}_n = \left(\mathbf{I}_{N_t} + \nu_{1,3,n}\mathbf{t}_n\mathbf{t}_n^H\right)^{-1}\left(\hat{\mathbf{X}} + \rho\boldsymbol{\lambda}_{2,n}\right), \tag{A.15}$$

$$\text{vec}\left(\mathbf{Y}_k\right) = \left(\boldsymbol{\Phi}_k + \mathbf{I}_{N_t\times K}\right)^{-1}\boldsymbol{\Theta}_k, \tag{A.16}$$

where $a_{k,m} = 1$, $b_{k,m} = 1 + \rho\lambda_{5,k,m} - \alpha_{k,m}$, $c_{k,m} = \rho\lambda_{5,k,m} - \alpha_{k,m} - \frac{\nu_{1,1,k,m}}{2\ln 2}$, $\boldsymbol{\Phi}_k \triangleq \nu_{1,2,k}\left(2^{\gamma_k}-1\right)\left(\left(\sum_{n\neq k}\mathbf{e}_n\mathbf{e}_n^H\right)^T \otimes \mathbf{g}_k\mathbf{g}_k^H\right)$ and $\boldsymbol{\Theta}_k = \hat{\mathbf{X}} + \rho\lambda_{7,k} + \nu_{1,2,k}\mathbf{g}_k\mathbf{g}_k^H\mathbf{Y}_k\left(l-1\right)\mathbf{e}_k\mathbf{e}_k^H$.

Therefore, once the Lagrange multipliers $\nu_{1,1,k,m}, \nu_{1,2,k}$ and $\nu_{1,3,m}$ have been determined, the optimal solutions can be obtained with the aid of (A.12)-(A.16). Based on the complementary slackness (A.7), (A.9) and (A.11), we can conclude that either the introduced Lagrange multiplier is zero, or the corresponding constraint is active. Therefore, we first set the introduced Lagrange multipliers as zero, i.e.,

$$\min_{\hat{\alpha}_{k,m},\hat{\beta}_{k,m},\hat{R}_{s,k,m}} \sum_{k\in\mathcal{K},m\in\mathcal{M}} \left(|\hat{\alpha}_{k,m}-\alpha_k+\rho\lambda_{5,k,m}|^2 + |\hat{\beta}_{k,m}\hat{\tau}_{k,m}-\beta_{k,m}+\rho\lambda_{6,k,m}|^2 + |R_s-\hat{R}_{s,k,m}+\rho\lambda_{9,k,m}|^2\right),$$
$$\text{s.t.} \quad (23a), \tag{A.1}$$

$\nu_{1,1,k,m}=0, \nu_{1,2,k}=0$, $k\in\mathcal{K}$, and $\nu_{1,3,m}=0$, $m\in\mathcal{M}$, and check whether the inequality constraints of problems (A.1)-(A.3) hold, or not. If the inequality constraints do hold, the optimal solutions can be obtained by setting the Lagrange multipliers as zero. Otherwise, employing the bisection search of [40], we first search the Lagrange multipliers to make the inequality constraints of problems (A.1)-(A.3) active, and then, substitute them back into (A.12)-(A.16) for obtaining the optimal solutions.

B. Solutions of Problems (25)-(26) at Step 2

Following the procedures in Appendix A-A, we first introduce the nonnegative Lagrange multipliers $\nu_{2,1,k}$ and $\nu_{2,2,k,m}$ for problems (25)-(26), and then derive the optimal solutions from their KKT conditions, which are functions of the introduced Lagrange multipliers, given by

$$\text{vec}\left(\mathbf{V}_k\right)=\left(\nu_{2,1,k}\left(\sum_{j\neq k}\mathbf{e}_j\mathbf{e}_j\right)^T\otimes\left(\mathbf{g}_k\mathbf{g}_k^H\right)+\mathbf{I}_{N_t\times K}\right)^{-1}\boldsymbol{\Delta}_k, \tag{A.17}$$

$$\alpha_k=\frac{\sum_{m\in\mathcal{M}}\left(\hat{\alpha}_{k,m}+\rho\lambda_{5,k,m}\right)}{M}-\frac{\nu_{2,1,k}\left|\mathbf{g}_k^H\mathbf{V}_k(l-1)\mathbf{e}_k\right|^2}{2M\left(\alpha_k(l-1)\right)^2}, \tag{A.18}$$

$$\text{vec}\left(\mathbf{X}_{k,m}\right)=\left(\mathbf{I}_{N_t\times K}+\nu_{2,2,k,m}\left(\left(\mathbf{e}_k\mathbf{e}_k^H\right)^T\otimes\mathbf{h}\mathbf{h}^H\right)\right)^{-1}\boldsymbol{\Omega}_{k,m}, \tag{A.19}$$

$$\beta_{k,m}=\max\left(\hat{\beta}_{k,m}\tau_{k,m}-\rho\lambda_{6,k,m}+\frac{\nu_{2,2,k,m}}{2},0\right), \tag{A.20}$$

where $\boldsymbol{\Delta}_k\triangleq\text{vec}\left(\hat{\mathbf{X}}+\rho\boldsymbol{\lambda}_{4,k}+\nu_{2,1,k}\frac{\mathbf{g}_k\mathbf{g}_k^H\mathbf{V}_k(l-1)\mathbf{e}_k\mathbf{e}_k^H}{\alpha_k(l-1)}\right)$ and $\boldsymbol{\Omega}_{k,m}\triangleq\text{vec}\left(\hat{\mathbf{X}}\right)+\rho\text{vec}\left(\boldsymbol{\lambda}_{3,k,m}\right)$. Finally, the optimal solutions can be obtained from their complementary slackness in the KKT condition.

C. Solution of Problem (31) at Step 3

Following the procedures at Step 1, we introduce the nonnegative Lagrange multipliers $\nu_{3,1,k,m}$ for problem (31), and derive its optimal solutions as functions of the Lagrange multipliers introduced.

When $\hat{\beta}_{k,m}\neq 0$, we have

$$\mathbf{W}_{k,m}=\hat{\mathbf{X}}+\rho\boldsymbol{\lambda}_{8,k,m}+\nu_{3,1,k,m}\mathbf{h}\mathbf{h}^H\mathbf{W}_{k,m}(l-1)\sum_{j\neq k}\left(\mathbf{e}_j\mathbf{e}_j^H\right), \tag{A.21}$$

$$\tau_{k,m}=\frac{\beta_{k,m}+\rho\lambda_{8,k,m}}{\hat{\beta}_{k,m}}-\frac{\nu_{3,1,k,m}}{2\left(\hat{\beta}_{k,m}\right)^2}. \tag{A.22}$$

Then, the optimal solutions can be obtained from their complementary slackness in the KKT condition of problem (31).

On the other hand, when $\hat{\beta}_{k,m}=0$, we have $\nu_{3,1,k,m}=0$ and the optimal solutions are given by

$$\mathbf{W}_{k,m}=\hat{\mathbf{X}}+\rho\boldsymbol{\lambda}_{8,k,m}, \tag{A.23}$$

$$\tau_{k,m}=\sum_{j\neq k}\left(2\mathcal{R}\left(\text{Tr}\left(\mathbf{h}^H\mathbf{W}_{k,m}\mathbf{e}_j\mathbf{e}_j^H\mathbf{W}_{k,m}^H(l-1)\mathbf{h}\right)\right)\right)+\sigma^2 - \sum_{j\neq k}\left(|\mathbf{h}^H\mathbf{W}_{k,m}(l-1)\mathbf{e}_j|^2\right). \tag{A.24}$$

D. Solution of Problem (36) at Step 4

After introducing a nonnegative Lagrange multiplier $\nu_{4,1}$ for problem (36), its optimal solutions can be derived as a function of $\nu_{4,1}$, given by (A.25) at the top of next page.

Then, we adopt the classic bisection search to obtain $\nu_{4,1}$ that satisfies the complementary slackness in the KKT condition of problem (36) and then substitute it back into (A.25) to get its optimal solution.

APPENDIX B
PROOF OF THEOREM 1

We first prove the convergence of fixed point iteration (35). For proving the convergence of fixed point iteration (35), we should show that the OF value is increasing throughout the iterative process, i.e.,

$$\boldsymbol{\mu}^H(l+1)\boldsymbol{\Upsilon}\boldsymbol{\mu}(l)\geq\boldsymbol{\mu}^H(l)\boldsymbol{\Upsilon}\boldsymbol{\mu}(l-1). \tag{B.1}$$

This is because we have:

$$\boldsymbol{\mu}^H(l+1)\boldsymbol{\Upsilon}\boldsymbol{\mu}(l)\geq\mathcal{R}\left(\boldsymbol{\mu}^H(l-1)\boldsymbol{\Upsilon}\boldsymbol{\mu}(l)\right) =\mathcal{R}\left(\left(\boldsymbol{\mu}(l)^H\boldsymbol{\Upsilon}^H\boldsymbol{\mu}(l-1)\right)^H\right)\overset{(a)}{=}\boldsymbol{\mu}(l)^H\boldsymbol{\Upsilon}\boldsymbol{\mu}(l-1) \tag{B.2}$$

The equality (a) is valid, because $\boldsymbol{\Upsilon}$ is positive-semidefinite and $\boldsymbol{\mu}(l)^H\boldsymbol{\Upsilon}\boldsymbol{\mu}(l-1)$ is real. Additionally, $|\boldsymbol{\Upsilon}\boldsymbol{\mu}|_1\leq|\boldsymbol{\Upsilon}|_1$ due to the property of the norm of the product of two matrices [38], which represents an upper bound of the value obtained by the fixed-point iteration (35).

In conclusion, the function value is increasing throughout the fixed point iteration (35) and it has an upper bound. Therefore, the fixed point iteration (35) is bound to converge.

As shown in [41], the limit point obtained by the fixed point iteration (35) can be characterized by the following equation

$$\boldsymbol{\Upsilon}\boldsymbol{\mu}=\boldsymbol{\varrho}\odot\boldsymbol{\mu}, \tag{B.3}$$

where the vector $\boldsymbol{\varrho}$ is real-valued and non-negative. Then, following the proof in [41, Appendix B], we can prove that the fixed point iteration (35) will converge to a stationary point of problem (34). Further details are omitted for brevity.

$$\hat{\mathbf{X}}=\frac{\mathbf{F}_{\mathrm{RF}}\mathbf{F}_{\mathrm{BB}}-\rho\boldsymbol{\lambda}_1+\sum_{k\in\mathcal{K},m\in\mathcal{M},n\in\mathcal{N}}\left(\mathbf{Z}_n-\rho\boldsymbol{\lambda}_{2,n}+\mathbf{X}_{k,m}-\rho\boldsymbol{\lambda}_{3,k,m}+\mathbf{V}_k-\rho\boldsymbol{\lambda}_{4,k}+\mathbf{Y}_k-\rho\boldsymbol{\lambda}_{7,k}+\mathbf{W}_{k,m}-\rho\boldsymbol{\lambda}_{8,k,m}\right)}{2KM+2K+N+1+\nu_{4,1}}. \quad \text{(A.25)}$$

Finally, since $e^{-j\arg[\boldsymbol{\mu}^*(M+1)]}\boldsymbol{\mu}^*$ achieves the same OF value as $\boldsymbol{\mu}^*$, we can keep the last term in the solution vector as 1. Then, the proof is completed.

APPENDIX C

Similar to Appendix A, the optimal solutions of problems (C.1), (C.2) and (C.3) can also be obtained by employing the Lagrange multiplier method, whose detailed derivations are omitted for brevity. In particular, the optimal solutions of problem (C.1) are given as (C.4), where $\boldsymbol{\Omega}_{k,m}\triangleq\mathrm{vec}\left(\hat{\mathbf{X}}\right)+\rho\mathrm{vec}\left(\boldsymbol{\lambda}_{3,k,m}\right)$ and $\nu_{2,2,k,m}$ is the Lagrange multiplier of problem (C.1).

The optimal solutions of problem (C.2) can be derived by considering the following two cases. When $\hat{\beta}_{k,m}\neq 0$, the optimal $\mathbf{W}_{k,m}$ and $\tau_{k,m}$ are given by (C.5), where $\nu_{3,1,k,m}$ is the Lagrange multiplier of problem (C.2). When $\hat{\beta}_{k,m}=0$, the optimal solution is given by $\mathbf{W}_{k,m}$ in (C.6).

The optimal solution of problem (C.3) is $\mathbf{Z}=\left(\mathbf{I}_{N_t}+\nu_{1,3,n}\mathbf{T}_n\mathbf{T}_n^H\right)^{-1}\left(\hat{\mathbf{X}}+\rho\boldsymbol{\lambda}_{2,n}\right)$, where $\nu_{1,3,n}$ is the Lagrange multiplier of problem (C.3).

Although the solutions obtained above are all functions of the introduced Lagrange multipliers, following similar procedures in Appendix A, the optimal Lagrange multipliers can be obtained from their complementary slackness in the KKT condition and the corresponding optimal solutions can be obtained. Detailed derivations are omitted for brevity.

REFERENCES

[1] M. Agiwal, A. Roy and N. Saxena, "Next generation 5G wireless networks: A comprehensive survey," *IEEE Communications Surveys & Tutorials*, vol. 18, no. 3, pp. 1617-1653, Third Quarter 2016.

[2] S. A. Busari, K. M. S. Huq, S. Mumtaz, L. L. Dai and J. Rodriguez, "Millimeter-wave massive MIMO communication for future wireless systems: A survey," *IEEE Communications Surveys & Tutorials*, vol. 20, no. 2, pp. 836-869, Second Quarter 2018.

[3] X. Xu, B. He, W. Yang, X. Zhou and Y. Cai, "Secure transmission design for cognitive radio networks with Poisson distributed eavesdroppers" *IEEE Transactions on Information Forensics and Security*, vol. 11, no. 2, pp. 373-387, Feb. 2016.

[4] N. Wang, P. Wang, A. Alipour-Fanid, L. Jiao and K. Zeng, "Physical-layer security of 5G wireless networks for IoT: Challenges and opportunities," *IEEE Internet of Things Journal*, vol. 6, no. 5, pp.8169-8181, Oct. 2019

[5] R. Zhang and Q. Zhu, "`FlipIn`: A game-theoretic cyber insurance framework for incentive-compatible cyber risk management of Internet of Things," *IEEE Transactions on Information Forensics and Security*, vol. 15, pp. 2026-2041, 2020.

[6] A. D. Wyner, "The wire-tap channel," *Bell System Technical Journal*, vol. 54, no. 8, pp. 1355-1387, 1975.

[7] I. Csiszar and J. Korner, "Broadcast channels with confidential messages," *IEEE Transactions on Information Theory*, vol. IT-24, no. 3, pp. 339-348, May 1978.

[8] S. Leung-Yan-Cheong and M. Hellman, "The Gaussian wire-tap channel," *IEEE Transactions on Information Theory*, vol. 26, no. 4, pp. 451-456, Jul. 1978.

[9] Y. Liang, H. V. Poor and S. Shamai (Shitz), "Secure communication over fading channels," *IEEE Transactions on Information Theory*, vol. 54, no. 6, pp. 2470-2492, Jun. 2008

[10] F. Oggier and B. Hassibi, "The secrecy capacity of the MIMO wiretap channel," *IEEE Transactions on Information Theory*, vol. 57, no. 8, pp. 4961-4972, Aug. 2011.

[11] Y. Liang, H. V. Poor and S. Shamai, "Information theoretic security," *Foundations and Trends® in Communications and Information Theory*, vol. 5, no. 4-5, pp. 355-580, 2008.

[12] C. Wang and H.-M. Wang, "Robust joint beamforming and jamming for secure AF networks: Low-complexity design," *IEEE Transactions on Vehicular Technology*, vol. 64, no. 5, pp. 2192-2198, May 2014.

[13] Y.-W. P. Hong, P.-C. Lan and C.-C. J. Kuo, "Enhancing physical layer secrecy in multiantenna wireless systems: An overview of signal processing approaches," *IEEE Signal Processing Magazine*, vol. 30, no. 5, pp. 29-40, Sep. 2013.

[14] N. Yang, L. Wang, G. Geraci, M. Elkashlan, J. Yuan and M. Di Renzo, "Safeguarding 5G wireless communication networks using physical layer security," *IEEE Communications Magazine*, vol. 53, no. 4, pp. 20-27, Apr. 2015.

[15] C. Wang and H.-M. Wang, "On the secrecy throughput maximization for MISO cognitive radio network in slow fading channels," *IEEE Transactions on Information Forensics and Security*, vol. 9, no. 11, pp. 1814-1827, Nov. 2014

[16] Z. Xiang, W. Yang, G. Pan, Y. Cai and Y. Song, "Physical layer security in cognitive radio inspired NOMA network," *IEEE Journal of Selected Topics in Signal Processing*, vol. 13, no. 3, pp. 700-714, Jun. 2019.

[17] M. Li, H. Yin, Y. Huang, Y. Wang and R. Yu, "Physical layer security in overlay cognitive radio networks with energy harvesting," *IEEE Transactions on Vehicular Technology*, vol. 67, no. 11, pp. 11274-11279, Nov. 2018.

[18] X. Ding, Y. Zou, G. Zhang, X. Chen, X. Wang and L. Hanzo, "The security-reliability tradeoff of multiuser scheduling-aided energy harvesting cognitive radio networks," *IEEE Transactions on Communications*, vol. 67, no. 6, pp. 3890-3904, Jun. 2019

[19] Y. Song, W. Yang, X. Yang, Z. Xiang and B. Wang, "Physical layer security in cognitive millimeter wave networks," *IEEE Access*, vol. 7, pp. 109162-109180, Aug. 2019.

[20] H. Zhao, J. Zhang, L. Yang, G. Pan and M.-S. Alouini, "Secure mmWave communications in cognitive radio networks," *IEEE Wireless Communications Letters*, vol. 8, no. 4, pp. 1171-1174, Aug. 2019.

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

[22] C. Wang and H. Wang, "Physical layer security in millimeter wave cellular networks," *IEEE Transactions on Wireless Communications*, vol. 15, no. 8, pp. 5569-5585, Aug. 2016.

[23] M. E. Eltayeb, J. Choi, T. Y. Al-Naffouri and R. W. Heath, Jr., "Enhancing secrecy with multiantenna transmission in millimeter wave vehicular communication systems," *IEEE Transactions on Vehicular Technology*, vol. 66, no. 9, pp. 8139-8151, Sep. 2017

[24] Y. R. Ramadan, H. Minn and A. S. Ibrahim, "Hybrid analog-digital precoding design for secrecy mmwave MISO-OFDM systems," *IEEE Transactions on Communications*, vol. 65, no. 12, pp. 5009-5026, Nov. 2017.

[25] Y. R. Ramadan and H. Minn, "Artificial noise aided hybrid precoding design for secure mmwave MISO systems with partial channel knowledge," *IEEE Signal Processing Letters*, vol. 24, no. 11, pp. 1729-1733, May 2017

[26] L. Xu, L. Sun, G. Xia, T. Liu, F. Shu, Y. Zhang and J. Wang, "Secure hybrid digital and analog precoder for mmWave systems with low-resolution DACs and finite-quantized phase shifters," *IEEE Access*, vol. 7, pp. 109763-109775, Aug. 2019.

[27] R. Zi, J. Liu, L. Gu and X. Ge, "Enabling security and high energy efficiency in the Internet of Things with massive MIMO hybrid precoding," *IEEE Internet of Things Journal*, vol. 6, no. 5, pp. 8615-8625, Oct. 2019.

[28] Q. Shi and M. Hong, "Penalty dual decomposition method for non-smooth nonconvex optimization—Part I: Algorithms and convergence

$$\min_{\mathbf{x}_{k,m},\beta_{k,m}} \sum_{k\in\mathcal{K},m\in\mathcal{M}} \left(||\hat{\mathbf{X}}-\mathbf{X}_{k,m}+\rho\boldsymbol{\lambda}_{3,k,m}||_F^2+|\beta_{k,m}-\hat{\beta}_{k,m}\tau_{k,m}+\rho\lambda_{6,k,m}|^2\right). \text{ s.t.} \quad (55d). \tag{C.1}$$

$$\min_{\tau_k,\mathbf{W}_{k,m}} \sum_{k\in\mathcal{K},m\in\mathcal{M}} \left(|\beta_{k,m}-\hat{\beta}_{k,m}\tau_{k,m}+\rho\lambda_{6,k,m}|^2+||\hat{\mathbf{X}}-\mathbf{W}_{k,m}+\rho\boldsymbol{\lambda}_{8,k,m}||_F^2\right), \text{ s.t.} \quad (55e). \tag{C.2}$$

$$\min_{\mathbf{Z}_n} \sum_{n\in\mathcal{N}} ||\hat{\mathbf{X}}-\mathbf{Z}_n+\rho\boldsymbol{\lambda}_{2,n}||_F^2, \quad \text{s.t.}||\mathbf{T}_n^H\mathbf{Z}_n||_F^2\leq\Gamma, n\in\mathcal{N}. \tag{C.3}$$

$$\text{vec}\left(\mathbf{X}_{k,m}\right)=\left(\mathbf{I}_{N_t\times K}+\nu_{2,2,k,m}\left(\left(\mathbf{e}_k\mathbf{e}_k^H\right)^T\otimes\left(\mathbf{G}_{\text{e,m}}\mathbf{G}_{\text{e,m}}^H\right)\right)\right)^{-1}\boldsymbol{\Omega}_{k,m}, \beta_{k,m}=\max\left(\hat{\beta}_{k,m}\tau_{k,m}-\rho\lambda_{6,k,m}+\frac{\nu_{2,2,k,m}}{2},0\right). \tag{C.4}$$

$$\mathbf{W}_{k,m}=\hat{\mathbf{X}}+\rho\boldsymbol{\lambda}_{8,k,m}+\nu_{3,1,k,m}\mathbf{G}_{\text{e,m}}\mathbf{G}_{\text{e,m}}^H\mathbf{W}_{k,m}(l-1)\sum_{j\neq k}\left(\mathbf{e}_j\mathbf{e}_j^H\right), \ \tau_{k,m}=\frac{\beta_{k,m}+\rho\lambda_{8,k,m}}{\hat{\beta}_{k,m}}-\frac{\nu_{3,1,k,m}}{2\left(\hat{\beta}_{k,m}\right)^2}. \tag{C.5}$$

$$\mathbf{W}_{k,m}=\hat{\mathbf{X}}+\rho\boldsymbol{\lambda}_{8,k,m}, \tau_{k,m}=\sum_{j\neq k}\left(2\mathcal{R}\left(\text{Tr}\left(\mathbf{G}_{\text{e,m}}^H\mathbf{W}_{k,m}\mathbf{e}_j\mathbf{e}_j^H\mathbf{W}_{k,m}^H(l-1)\mathbf{G}_{\text{e,m}}\right)\right)\right)+\sigma^2-\sum_{j\neq k}\left(|\mathbf{G}_{\text{e,m}}^H\mathbf{W}_{k,m}(l-1)\mathbf{e}_j|^2\right). \tag{C.6}$$

analysis," *IEEE Transactions on Signal Processing*, vol. 68, pp. 4108-4122, Jun. 2020.

[29] Q. Shi and M. Hong, "Spectral efficiency optimization for millimeter wave multiuser MIMO systems," *IEEE Journal on Selected Areas in Signal Processing*, vol. 12, no. 3, pp. 455-468, Jun. 2018

[30] A. Beck, A. Ben-Tal, L. Tetruashvili, "A sequential parametric convex approximation method with applications to nonconvex truss topology design problems," *Journal of Global Optimization*, vol. 47, no. 1, pp: 29-51, May 2010.

[31] D. Bertsekas, *Nonlinear Programming*, 2nd ed. Belmont, MA: Athena Scientific, 1999.

[32] J. M. Hamamreh, H. M. Furqan and H. Arslan, "Classifications and applications of physical layer security techniques for confidentiality: A comprehensive survey," *IEEE Communications Surveys & Tutorials*, vol. 21, no. 2, pp. 1773-1828.

[33] I. Csiszar and J. Komer, "Broadcast channels with confidential messages," *IEEE Transactions on Information Theory*, vol. 24, no. 3, pp. 339-348, May 1978.

[34] S. Shafiee and S. Ulukus, "Achievable rates in Gaussian MISO channels with secrecy constraints," *2007 IEEE International Symposium on Information Theory*, Nice, 2007, pp. 2466-2470.

[35] M. Mirzaee and S. Akhlaghi, "Maximizing the minimum achievable secrecy rate for a two-user Gaussian weak interference channel," *IEEE Transactions on Information Forensics and Security*, vol. 14, no. 8, pp. 2190-2202, Aug. 2019.

[36] D. Tse and P. Viswanath, *Fundamentals of Wireless Communication. Cambridge*, U.K.: Cambridge Univ. Press, 2005.

[37] S. Boyd and L. Vandenberghe, *Convex Optimization*. Cambridge, U.K.: Cambridge University Press, 2004.

[38] X. Zhang, *Matrix Analysis and Applications*, Second Edition. Beijing, China: Tsinghua University Press, 2013.

[39] A. Hjϕrungnes and D. Gesbert, "Complex-valued matrix differentiation: Techniques and key results," *IEEE Transactions on Signal Processing*, vol. 55, no. 6, pp. 2740-2746, Jun. 2007.

[40] S. Intep, "A review of bracketing methods for finding zeros of nonlinear functions," *Applied Mathematical Sciences*, vol. 12, no. 3, pp. 137-146, 2018.

[41] M. Soltanalian and P. Stoica, "Designing unimodular codes via quadratic optimization," *IEEE Transactions on Signal Processing*, vol. 62, no. 5, pp. 1221-1234, Mar. 2014.

[42] J. D. Krieger, C.-P. Yeang and G. W. Wornell, "Dense delta-sigma phased arrays," *IEEE Transactions on Antennas and Propagation*, vol. 61, no. 4, pp. 1825-1837, Jan. 2013.

[43] J. Chen, "Hybrid beamforming with discrete phase shifters for millimeter-wave massive MIMO systems," *IEEE Transactions on Vehicular Technology*, vol. 66, no. 8, pp. 7604-7608, Aug. 2017.

[44] Q. Li and W.-K. Ma, "Optimal and robust transmit designs for MISO channel secrecy by semidefinite programming," *IEEE Transactions on Signal Processing*, vol. 59, no. 8, pp. 3799-3812, Aug. 2011.

[45] Q. Zhang, S. Jin, K.-K. Wong, H. Zhu and M. Matthaiou "Power scaling of uplink massive MIMO systems with arbitrary-rank channel means," *IEEE Journal of Selected Topics in Signal Processing*, vol. 8, no. 5, pp. 966-981, Oct. 2014.

[46] P.-H. Lin, S.-H. Lai, S.-C. Lin and H.-J. Su, "On secrecy rate of the generalized artificial-noise assisted secure beamforming for wiretap channels," *IEEE Journal Selected Areas on Communications*, vol. 31, no. 9, pp. 1728-1740, Sep. 2013.

[47] W.-C. Liao, T.-H. Chang, W.-K. Ma and C.-Y. Chi, "QoS-based transmit beamforming in the presence of eavesdroppers: An optimized artificialnoise-aided approach," *IEEE Transactions on Signal Processing*, vol. 59, no. 3, pp. 1202-1216, Mar. 2011.

[48] X. Zhou, J. Li, F. Shu, Q. Wu, Y. Wu, W. Chen and L. Hanzo, "Secure SWIPT for directional modulation-aided AF relaying networks," *IEEE Journal Selected Areas on Communications*, vol. 37, no. 2, pp. 253-268, Feb. 2019

[49] G. Xia, Y. Lin, F. Shu, Y. Wu and J. Wang, "An anti-eavesdropping strategy for precoding-aided spatial modulation with rough CSI of Eve," *IEEE Transactions on Vehicular Technology*, vol. 69, no. 2, pp. 2343-2347, Feb. 2020.

[50] Z. Zhu, Z. Chu, Z. Wang and I. Lee, "Outage constrained robust beamforming for secure broadcasting systems with energy harvesting," *IEEE Transactions on Wireless Communications*, vol. 15, no. 11, pp. 7610-7620, Sep. 2016.

[51] B. Wang and P. Mu, "Artificial noise-aided secure multicasting design under secrecy outage constraint," *IEEE Transactions on Communications*, vol. 65, no. 12, pp. 5401-5414, Dec. 2017.