Secure Transmission for Heterogeneous Cellular Networks with Wireless Information and Power Transfer

Bin Li, Zesong Fei, Senior Member, IEEE, Zheng Chu, and Yan Zhang, Senior Member, IEEE

Abstract—In this paper, we investigate an artificial-noise-aided secure beamforming design for simultaneous wireless information and power transfer in a two-tier downlink heterogeneous cellular network, in which each energy receiver in a femtocell is seen as a potential eavesdropper to wiretap the confidential message intended for the information receiver. Our design objective is to maximize the secrecy rate at the information receiver, while satisfying the signal-to-interference-plus-noise ratio requirement of each macrouser and the energy harvesting and transmit power constraints. Both the scenarios of perfect and imperfect channel state information (CSI) are considered. With perfect CSI, the formulated optimization problem constitutes a difference of a convex function programming problem, which is hard to directly solve. To tackle this challenge, we transform it into a series of semidefinite programs by using successive convex approximation, and an iterative algorithm is proposed to arrive at a provably convergent solution. With imperfect CSI, we address robust secure beamforming relying on the worst-case design philosophy. To circumvent this predicament, we resort to the S-procedure to reformulate the robust quadratic matrix inequality (QMI) constraints and then obtain the linear matrix inequality representations for these QMIs. Numerical results are finally presented to demonstrate the performance of our proposed schemes in improving the secrecy rate of heterogeneous cellular networks.

Index Terms—Beamforming, heterogeneous cellular networks (HCNs), quadratic matrix inequality (QMI), secrecy, simultaneous wireless information and power transfer (SWIPT), successive convex approximation (SCA).

I. INTRODUCTION

SINCE the tremendous popularity of Internet-enabled smart devices (e.g., smart phones and electronic tablets) has spurred the explosive growth of high-rate multimedia wireless services, it becomes urgent for mobile operators to achieve higher capacity and coverage for next-generation 5G wireless communications. One viable solution to do so is to increase cell density for higher spatial spectrum reuse [1], [2]. Recently, a heterogeneous cellular network (HCN) has emerged to be a promising network densification architecture and has attracted substantial interests due to achieving seamless coverage and higher data rate. In HCNs, small cells (e.g., picocells, femtocells, or Wi-Fi hotspots) are deployed within the coverage of an existing macrocell and share the same spectrum resource, but the main challenge is the resulting increased cross-tier interference as the spectral efficiency increases [3].

As the HCN creates a multitier topology where multiple terminals are deployed with dissimilar characteristics and the broadcasting nature of wireless channels, the wireless information of HCNs is particularly vulnerable to eavesdropping. As a result, how to secure wireless data transmission is of much concern facing HCNs. Responding to this, physical layer security (PLS) has been identified as a prominent technique to carry out secure communications by utilizing the random characteristics of physical channels such as noises and interferences [4]–[7], and it has been shown to be capable of substantially improving wireless security performance in HCNs [8], [9]. The idea of using PLS to achieve secure information transmission in HCNs was first investigated in [8], where the authors introduced PLS into a two-tier downlink HCN, and three transmit beamforming schemes were proposed to maximize the achieved secrecy rate. Wang et al. [9] analyzed the connection probability and the secrecy probability of the randomly located user in a K-tier HCN and derived the tractable expressions for the two metrics, respectively. In [10], the authors showed the closed-form expressions of the secrecy outage probability in a K-tier HCN, in which a base station (BS) association constraint was imposed. The authors of [11] further addressed the problem of secured coverage for a K-tier HCN operating with coordinated multipoint transmission, where the performance analysis of the secured coverage probability was conducted. In addition, Wang et al. [12] studied the secrecy and energy efficiency performance of a heterogeneous cloud radio access network assisted by massive multiple-input multiple-output.

With the intention of satisfying the high energy consumption due to the ever-increasing traffic needs in 5G, simultaneous wireless information and power transfer (SWIPT) has envisioned as a promising energy source for powering the energy-constrained wireless systems [13], in which wireless devices can harvest...
energy from man-made radio frequency (RF) signals instead of natural sources such as wind and solar in a self-supplied fashion [14]. SWIPT can apply into the emerging market of HCNs, which avoids the frequent replacing and replacement of batteries of the low-power wireless devices, such as sensor nodes operating in extreme environments [15]. On the other hand, the deployment of small cells makes the mobile devices harvest energy more efficiently from its serving BS due to short-range communications. Most recently, Sheng et al. [16] considered the intrinsic relationship of information transmission efficiency and energy harvesting efficiency in a two-tier HCN. In the context of SWIPT-enabled HCNs, related works were also presented in [17]–[19].

For the SWIPT system, the energy receivers (ERs) may have better channel conditions than the information receivers (IRs) due to different power sensitivity levels for ERs and IRs (e.g., −10 dBm versus −60 dBm) [20], which gives rise to the fact that ERs may retrieve the information intended for IRs [21], [22]. Therefore, it is of paramount importance to study the security problem in SWIPT systems. To address it, PLS has been applied to SWIPT and a host of related efforts have been developed in [23]–[26]. It is worth noting that most of the existing works assumed that perfect channel state information (CSI) was available at the BS; however, this is very difficult to be obtained perfectly in practical systems due to the lack of cooperation with hostile eavesdroppers (Eves), as well as quantization and feedback errors [27]–[30]. To this end, the authors of [28] and [29] designed the robust secure beamforming for SWIPT systems, where the external helper and cooperative jamming were considered. Khandaker et al. [30] discussed the probabilistic secrecy beamformer design for a more general SWIPT system in the presence of multiple multiantenna Eves. The authors of [31] addressed the secure transmission problem for the SWIPT multicasting scenario with imperfect CSI, where a low-complexity intelligent algorithm was proposed. The multicasting scenario of robust secure SWIPT was also presented in [32], where Eves form multiple eavesdropping-collusion parties to collaboratively intercept the transmission signals.

A common of previous related works is to address the secure issue separately in HCNs and SWIPT systems. Nevertheless, there is still not a comprehensive solution for SWIPT-enabled HCNs. Motivated by this, in this paper, we focus on the secure beamforming design for SWIPT in a two-tier HCN, in which one macrocell consisting of multiple macrocell users (MUs) and one femtocell consisting of one IR with multiple ERs. Meanwhile, each ER is also seen as a potential Eve to wiretap confidential messages intended for IR. Our objective is to maximize the secrecy rate at IR while guaranteeing the signal-to-interference-plus-noise ratio (SINR) requirement recorded at each MU, concerning the energy harvesting constraint recorded at each ER and the transmit power constraint. For the sake of clarification, the main contributions of this paper are summarized as follows.

1) We propose an SWIPT system model for a two-tier HCN. In particular, the femtocell base station (FBS) broadcasts wireless information to IR and transfers energy to ERs simultaneously. Then, we investigate the secure transmission issue for the proposed system model; such work has not been reported so far. To enhance secure transmission, the artificial noise (AN) is embedded at the intended signal to deteriorate the reception of ERs.

2) For perfect CSI, the secrecy rate maximization problem is nonconvex due to the coupling between optimization variables, and thus, it is hard to optimally solve. To tackle this challenge, we transform it into a series of semidefinite programs (SDPs) by employing successive convex approximation (SCA) and semidefinite relaxation (SDR) techniques. Then, an iterative algorithm is proposed to arrive at provably convergent solution. Furthermore, the convergence and computational complexity of the proposed algorithm are analyzed.

3) We further extend our work to the imperfect CSI case. Considering the deterministic channel estimation uncertainty model and following the worst-case robustness philosophy, we propose a robust secure beamforming design. Particularly, we reformulate the worst-case secrecy rate maximization problem into a quadratic matrix inequality (QMI) problem in light of the Schur complement framework, and then rely on the linear matrix inequality (LMI) reformulation for the semi-infinite QMI constraints to construct solvable SDPs.

The remaining part of this paper is organized as follows. In Section II, we introduce the system model and formulate the optimization problem. In Section III, we investigate the secure beamforming design with perfect CSI. In Section IV, we investigate the robust secure beamforming design for the imperfect CSI case. Finally, in Section V, we present simulation results to validate the effectiveness of the proposed schemes, followed by our conclusions in Section VI.

Notations: Boldface lowercase and uppercase letters denote vectors and matrices, respectively. The transpose, conjugate transpose, rank, and trace of the matrix \( A \) are denoted as \( A^T \), \( A^H \), \( \text{rank}(A) \), and \( \text{Tr}(A) \), respectively. \( A \succeq 0 \) means \( A \) is a positive-semidefinite (PSD) matrix. \( E[.] \) represents the expectation of a random variable, and \( \| . \| \) denotes the vector Euclidean norm. Random vector \( x \sim \mathcal{CN}(\mu, \Phi) \) with a mean vector \( \mu \) and covariance matrix \( \Phi \) follows a complex circularly symmetric Gaussian distribution.

II. SYSTEM MODEL AND PROBLEM FORMULATION

We consider a wireless-powered two-tier HCN, where an FBS can be deployed with a macrocell base station (MBS), as depicted in Fig. 1. The FBS serves \( K + 1 \) femtocell users (FUs) and shares certain spectral resources as MBS serving \( M > 1 \) MUs to improve the spectrum efficiency. The MBS and FBS are equipped with \( N_M \geq M \) and \( N_F \geq K + 1 \) transmit antennas, respectively, whereas each MU and FU are equipped with a single receive antenna. We assume that the FBS is capable of performing wireless power transfer, and two types of FUs exist in the femtocell, i.e., one IR and \( K > 1 \) ERs. It is assumed that ERs are also active users of the network and can only harvest energy from the ambient RF signals to extend their battery life. Note that ERs may be malicious for intercepting the information signal transmitted by the FBS to IR without

\footnote{In this paper, we assume that only one IR exists in the femtocell; the extension to multiple IRs network as in [31] and [32] is straightforward.}
any attacks. Thus, ERs are seen as potential Eves, which should be considered for providing secure transmission, which was commonly assumed [23]. Let \( M = \{1, \ldots, M\} \) denote the set of MUs and \( K = \{1, \ldots, K\} \) denote the set of ERs. For the sake of notational simplicity, we assume that the \( m \)th MU in the macrocell and the \( k \)th ER in the femtocell are denoted by \( \mu_m \) and \( E_k \), respectively.

The channel coefficients from the MBS to \( \mu_m \), from the MBS to IR, and from the MBS to ERs are denoted by \( h_m \in \mathbb{C}^{N_{m} \times 1} \), \( h_{0,0} \in \mathbb{C}^{N_{m} \times 1} \), and \( g_{k,0} \in \mathbb{C}^{N_{m} \times 1} \), respectively. Likewise, the channel coefficients from the FBS to IR, from the FBS to ERs, and from the FBS to \( \mu_m \) are denoted by \( h_{1} \in \mathbb{C}^{N_{F} \times 1} \), \( g_{k} \in \mathbb{C}^{N_{F} \times 1} \), and \( I_{m} \in \mathbb{C}^{N_{F} \times 1} \), respectively. These channel coefficients are independent, and the elements are independent and identically distributed (i.i.d.) complex Gaussian random variables.

To support secure communication and facilitate energy harvesting at ERs, the AN-aided beamforming scheme is performed at the FBS to prevent ERs from eavesdropping. Therefore, the transmitted signal vector is denoted by

\[
x = w_1 s_1 + v_E
\]

where \( s_1 \) and \( w_1 \) denote the data symbol and beamforming vector, respectively. Hence, \( w_1 s_1 \) carries the confidential information intended for IR. Without loss of generality, we assume that \( E[s_1 s_1^H] = 1 \). \( v_E \sim \mathcal{CN}(0, V_E) \) denotes the energy-carrying AN vector invoked by the FBS, which is independent of the information-carrying signal \( s_1 \), where \( V_E \) represents the transmit covariance matrix of \( v_E \). The AN vector \( v_E \) interferes IR and ERs simultaneously since \( v_E \) is unknown to both types of receivers. Hence, AN transmission has to be carefully designed to deteriorate the reception of ERs while having a minimal impact on IR.

Suppose \( s_m \sim \mathcal{CN}(0, 1) \) is the data symbol transmitted by MBS intended for \( \mu_m \) in the macrocell and \( w_m \) is the corresponding beamforming vector; the signal received at \( \mu_m \) by considering the cochannel interference can be expressed as

\[
y_m = h_m^H w_m s_m + \sum_{i=1, i \neq m}^M h_i^H w_i s_i + n_m
\]

where \( n_m \) is the additive white Gaussian noise (AWGN) at \( \mu_m \). Note that the first term is the intended signal for \( \mu_m \), the second term is the interference from other MUs in the macrocell, and the last two terms are the intertier interference and background noise.

To facilitate analysis, the single-user detection is employed at each MU, which means the interference from intertier and intratier is simply treated as a part of the background noise. Therefore, the SINR at \( \mu_m \) can be represented as

\[
\text{SINR}_m = \frac{|h_m^H w_m|^2}{\sum_{i=1, i \neq m}^M |h_i^H w_i|^2 + |l_m^H w_1|^2 + l_m^H V_E l_m + \sigma_m^2}.
\]

Since the FBS desires to send the confidential signal \( x \) to IR while ERs overhears, the signals received by IR and \( E_k \) can be expressed as

\[
y_t = h_1^H x + \sum_{m=1}^M h_m^H w_m s_m + n_t
\]

\[
y_{E,k} = g_k^H x + \sum_{m=1}^M g_{k,0}^H w_m s_m + n_{E,k}
\]

respectively, where \( \sigma_t^2 \) and \( \sigma_{E,k}^2 \) denote the variances of AWGN at IR and \( E_k \), respectively. As seen from (4) and (5), the IR and ERs suffer from the MUs’ interference in addition to the background noise.

Then, the total transmit power of the whole system is given by

\[
P_{\text{tot}} = \sum_{m=1}^M \|w_m\|^2 + \|w_1\|^2 + \text{Tr}(V_E).
\]

On the other hand, the harvested energy at \( E_k \) is written as

\[
E_k = \varepsilon \left( |g_k^H w_1|^2 + |g_k^H V_E g_k + \sum_{m=1}^M |g_{k,0}^H w_m|^2 \right)
\]

where \( \varepsilon \in (0, 1] \) is the energy conversion efficiency that accounts for the loss converting the harvested energy to the electrical energy. The harvested energy is preserved to extend the battery life of \( E_k \). Note that the contribution of the noise power to the total harvested energy is neglected in (7), since it is negligibly small compared to the received signals. In the following, we assume \( \varepsilon = 1 \) for convenience.

According to the received signal in (4) and (5), given \( \{w_m\} \), \( w_1 \), and \( V_E \), the achievable instantaneous secrecy rate is formulated as [33]

\[
R_s = C_I(\{w_m\}, w_1, V_E) - \max_k C_{E,k}(\{w_m\}, w_1, V_E)
\]

where the notation \( |x|^+ = \max\{x, 0\} \) is used, since the secrecy rate is defined as a nonnegative quantity. \( C_I(\{w_m\}, w_1, V_E) \)

\[\text{In this paper, we mainly focus on the secrecy rate optimization. The energy harvesting performance of ERs is exploited, whereas how to use the harvested power is outside the scope of this paper.}\]
and $C_{E,k}(\{w_m\}, w_I, V_E)$ are the achievable rates of the IR and ER$_k$, respectively, i.e.,

$$
C_l(\{w_m\}, w_I, V_E) = \log_2 (1 + \text{SINR}_I)
$$

$$
= \log_2 \left( 1 + \frac{|h_I^H w_I|^2}{\sum_{m=1}^M |h_{m,0}^H w_m|^2 + h_I^H V_E h_I + \sigma^2_{l}} \right)
$$

(9)

$$
C_{E,k}(\{w_m\}, w_I, V_E) = \log_2 (1 + \text{SINR}_{E,k})
$$

$$
= \log_2 \left( 1 + \frac{|g_{E,k}^H w_I|^2}{\sum_{m=1}^M |g_{E,k,0}^H w_m|^2 + g_{E,k}^H V_E g_{E,k} + \sigma^2_{E,k}} \right).
$$

(10)

From (9) and (10), we can see that the interference from the MBS invokes a negative impact on the quality of wireless transmission of both IR and ERs; meanwhile, it is beneficial for energy harvesting at ERs. As a result, it is not trivial to design secure beamforming for degrading ERs’ channels while having a minimal effect on IR. Under such a scenario, we focus on the joint design of beamforming vectors $w_m$, $w_I$, and AN covariance matrix $V_E$ to maximize the secrecy rate at IR, while satisfying the SINR requirement for each MU, the transmit power constraint, and the energy harvesting constraint. Hence, the optimization problem is formulated as

$$
\max_{\{w_m\}, w_I, V_E} \left\{ C_l(\{w_m\}, w_I, V_E) \right. \\
- \max_k C_{E,k}(\{w_m\}, w_I, V_E) \right\}
$$

(11a)

subject to

$$
\text{SINR}_m \geq \Gamma_m \ \forall m \in \mathcal{M}
$$

(11b)

$$
P_{\text{tot}} \leq P_{\text{th}}
$$

(11c)

$$
E_k \geq Q_k \ \forall k \in \mathcal{K}
$$

(11d)

$$
V_E \geq 0
$$

(11e)

where $\Gamma_m$ is the prescribed SINR requirement of MU$m$, $P_{\text{th}}$ denotes the maximum transmit power threshold, and $Q_k$ denotes the prescribed energy harvesting threshold at ER$_k$, respectively. It is clear that Problem (11) is nonconvex, since the objective function constitutes a difference of convex functions programming (DCP), which is, in general, hard to optimally solve due to prohibitively high computational complexity. To simplify the notations, we assume $\sigma^2_{l} = \sigma^2_{E,k} = \sigma^2_m = 1$ in the following.

### III. Secure Beamforming Design With Perfect CSI

In this section, we assumed that the CSI of all receivers is perfectly known at the MBS and the FBS such that the secure transmission is designed, which is a common assumption broadly used in the open literature. To tackle Problem (11), we apply first-order Taylor expansion and SCA techniques to approximate and then transform the original problem into a convex form. Furthermore, an SCA-based iterative algorithm is developed to obtain a provably convergent solution.

#### A. Optimal Beamforming With Perfect CSI

To proceed, we first define new matrices $W_m = w_m w_m^H$ and $W_I = w_I w_I^H$ with rank($W_m$) = 1 and rank($W_I$) = 1. Then, we introduce real-valued slack variables $\gamma_1$ and $\gamma_E$; Problem (11) can be equivalently rewritten as

$$
\max_{\gamma_1, \gamma_E, \{w_m\}, w_I, V_E} \gamma_1 - \gamma_E
$$

(12a)

subject to

$$
\begin{align*}
\sum_{m=1}^M |h_{m,0}^H w_m|^2 + h_I^H V_E h_I + 1 &\leq \frac{\gamma_1}{2} - 1 \hfill (12b) \\
\sum_{m=1}^M |g_{E,k,0}^H w_m|^2 + g_{E,k}^H V_E g_{E,k} + 1 &\leq \frac{\gamma_E}{2} - 1 \hfill (12c) \\
h_I^H W_I h_I &\geq \Gamma_m \hfill (12d) \\
g_{E,k}^H W_I g_{E,k} &\geq \sum_{m=1}^M |g_{E,k,0}^H w_m|^2 \geq Q_k \hfill (12e) \\
\text{Tr}(W_I) + \text{Tr}(V_E) + \sum_{m=1}^M \text{Tr}(W_m) &\leq P_{\text{th}} \hfill (12f) \\
W_m &\succeq 0, \ W_I \succeq 0, \ V_E \succeq 0 \hfill (12g) \\
\text{rank}(W_m) = 1 &\text{, rank}(W_I) = 1 \forall m \in \mathcal{M} ; k \in \mathcal{K}. \hfill (12h)
\end{align*}
$$

The equivalence between Problems (11) and (12) follows from the fact that the constraints in (12b) and (12c) hold with equality at optimality. It can be observed that Problem (12) is nonconvex, since the constraints in (12b) and (12c) involve the coupled optimization variables $\{w_m\}$, $2^\gamma_1$, $2^\gamma_E$, and the rank-1 constraint (12h), which are intractable.

To make the problem tractable, we introduce the auxiliary variables $v_1, v_2, u_1, u_2$ and define new matrices $H_m = h_m h_m^H$, $H_I = h_I h_I^H$, $H_{I,0} = h_{I,0} h_{I,0}^H$, $G_k = g_k g_k^H$, $G_{E,k} = g_{E,k} g_{E,k}^H$, and $L_m = l_m l_m^H$. By applying the SDR technique [33], [34] to drop the rank-1 constraint (12h), Problem (12) can be relaxed as

$$
\max_{\gamma_1, \gamma_E, \{w_m\}, w_I, V_E} \gamma_1 - \gamma_E
$$

(13a)

subject to

$$
\begin{align*}
\frac{1}{\Gamma_m} \text{Tr}(H_m W_m) - \sum_{i=1, i \neq m}^M \text{Tr}(H_m W_i) &\geq 1 \hfill (13b)
\end{align*}
$$

The equivalence between Problems (11) and (12) follows from the fact that the constraints in (12b) and (12c) hold with equality at optimality. It can be observed that Problem (12) is nonconvex, since the constraints in (12b) and (12c) involve the coupled optimization variables $\{w_m\}$, $2^\gamma_1$, $2^\gamma_E$, and the rank-1 constraint (12h), which are intractable.
\[ \text{Tr}(H_1 W_1) \geq v_1 \quad (13c) \]
\[ \sum_{m=1}^{M} \text{Tr}(H_{1,0} W_m) + \text{Tr}(H_1 V_E) + 1 \leq v_2 \quad (13d) \]
\[ \frac{v_1}{v_2} \geq 2^{\gamma_1} - 1 \quad (13e) \]
\[ \text{Tr}(G_k W_1) \leq u_{1k} \quad (13f) \]
\[ \sum_{m=1}^{M} \text{Tr}(G_{k,0} W_m) + \text{Tr}(G_k V_E) + 1 \geq u_{2k} \quad (13g) \]
\[ \frac{u_{1k}}{u_{2k}} \leq 2^{\gamma_k} - 1 \quad (13h) \]
\[ \text{Tr}(G_k W_1) + \text{Tr}(G_k V_E) + \sum_{m=1}^{M} \text{Tr}(G_{k,0} W_m) \geq Q_k \quad (13i) \]
\[ \text{Tr}(W_i) + \text{Tr}(V_E) + \sum_{m=1}^{M} \text{Tr}(W_m) \leq P_{th} \quad (13j) \]
\[ W_m \succeq 0, \quad W_1 \succeq 0, \quad V_E \succeq 0 \quad \forall m \in \mathcal{M}; \quad k \in \mathcal{K}. \quad (13k) \]

While Problem (13) is still nonconvex in its current form due to the nonconvex constraints in (13e) and (13h), no algorithm can be directly applied to it. In what follows, we will develop an iterative algorithm to find the optimal solution based on the spirit of the SCA technique [21, 35].

**B. Successive Convex Approximation**

To obtain a tractable convex formulation and design an efficient solution of Problem (13), following the idea of [21] and [35], we employ the SCA technique to deal with Problem (13) in this section.

1) Transformation of Constraint (13e): To begin with, introducing slack variables \( x_1, x_2, \) and \( x_3 \), (13e) can be reformulated as
\[
\begin{align*}
  v_1 &\geq e^{\gamma_1} x_1 - x_2 \geq x_3 \quad (14a) \\
v_2 &\leq e^{\gamma_2} 2^{\gamma_1} - 1 \leq e^{\gamma_3} \quad (14b)
\end{align*}
\]

It is easily seen that the constraints in (14a) are convex now. However, the constraints in (14b) are still nonconvex due to the fact that if a constraint is such that a convex function is smaller than or equal to a concave function, then the constraint is a convex constraint [36]. Fortunately, the functions \( e^{\gamma_2} \) and \( e^{\gamma_3} \) on the right-hand sides of (14b) are convex, which makes (14b) easier to handle than (13e). To this end, let us define \( x_2^n \) and \( x_3^n \) as the variables \( x_2 \) and \( x_3 \) at the \( [n-1] \)th iteration for an iterative algorithm given below. By applying first-order Taylor series expansions on \( e^{\gamma_2} \) and \( e^{\gamma_3} \), i.e., \( e^{\gamma_2} (x_2 - x_2^n) + 1 \leq e^{\gamma_2} \) and \( e^{\gamma_3} (x_3 - x_3^n) + 1 \leq e^{\gamma_3} \), the linearization of nonconvex constraints in (14b) are given by
\[
\begin{align*}
v_2 &\leq e^{\gamma_2} (x_2 - x_2^n) + 1 \quad (15) \\
2^{\gamma_1} - 1 &\leq e^{\gamma_3} (x_3 - x_3^n) + 1 \quad (16)
\end{align*}
\]

**Algorithm 1:** Proposed Iterative Algorithm for Solving Problem (20).

**Input:** Initialize \( \bar{x}_2^n, \bar{x}_3^n, x_4^n, \gamma_E^n \) as the values which are feasible to the problem (20), set \( n = 0 \).

**Step 1:** Solve the convex Problem (20) with \( x_2^n, x_3^n, x_4^n, \gamma_E^n \) and obtain the optimal values \( x_2^*, x_3^*, x_4^*, \gamma_E^* \).

**Step 2:** Update \( \bar{x}_2^n = x_2^*, x_3^n = x_3^*, x_4^n = x_4^*, \gamma_E^n = \gamma_E^* \).

**Output:** Until \( \left| \frac{(\gamma_1^n - \bar{\gamma}_1^{n+1}) - (\gamma_1 - \gamma_1^n)}{(\gamma_1^n - \bar{\gamma}_1^{n+1})} \right| \leq \epsilon \) is met, where \( \epsilon \) represents the convergence tolerance.

2) Transformation of Constraint (13h): Similar to constraint (13e), introducing slack variables \( x_{4k} \), \( x_{5k} \), and \( x_{6k} \), (13h) can be reformulated as
\[
\begin{align*}
u_{1k} &\leq e^{\gamma_{4k}} 2^{\gamma_k} - 1 \geq e^{\gamma_{5k}} \quad (17a) \\
u_{2k} &\geq e^{\gamma_{4k}} x_{4k} - x_{5k} \leq x_{6k} \quad (17b)
\end{align*}
\]

Note that constraint (17a) is still nonconvex; we then apply the first-order Taylor series expansions on \( e^{\gamma_{4k}} \) and \( 2^{\gamma_k} \), i.e., \( e^{\gamma_{4k}} (x_{4k} - x_{4k}^*) + 1 \leq e^{\gamma_{4k}} \) and \( 2^{\gamma_k} [(\gamma_E - \gamma_E^*) \ln 2 + 1] \leq 2^{\gamma_k} \); then, the linearization of nonconvex constraints in (17a) is given by
\[
\begin{align*}
u_{1k} &\leq e^{\gamma_{4k}} (x_{4k} - x_{4k}^*) + 1 \quad (18) \\
2^{\gamma_k} [(\gamma_E - \gamma_E^*) \ln 2 + 1] &\geq e^{\gamma_{5k}} \quad (19)
\end{align*}
\]

Up till now, replacing (13e) and (13h) by (14a), (15), (16), (17b), (18), and (19), the original Problem (13) can be recast as
\[
\begin{align*}
\max_{W_m, W_1, V_E, \gamma_E} & \quad \gamma_1 - \gamma_E \\
\text{s.t.} & \quad (13b), (13c), (13d), (13f), (13g), (13i), (13j), (13k), (14a), (15), (16), (17b), (18), (19). \quad (20)
\end{align*}
\]

It can be observed that Problem (20) is a convex SDP problem, which can be efficiently solved by using interior-point-based solvers, e.g., CVX [36]. The detailed procedure of the proposed SCA-based algorithm is listed in Algorithm 1.\(^3\) If the optimal solutions \( \{W_m^* \} \) and \( W_1^* \) for Problem (20) satisfy rank-1 constraints, then the optimal beamforming vectors for Problem (11) can be obtained via employing the eigenvalue decomposition. Alternatively, the Gaussian randomization technique [8, 37] can be applied to generate the approximate solutions.

To obtain further insight into Problem (20), we find from the simulations that the optimal solution \( W_1^* \) of Problem (20) is always rank-1, which implies that the rank relaxation about \( W_1 \) is tight.

\(^3\)The initial values of the variables in Algorithm 1 are generated randomly by extensive experiments until the feasible conditions are all met.
TABLE I

<table>
<thead>
<tr>
<th>Variables</th>
<th>PSD constraints</th>
<th>Slack constraints</th>
</tr>
</thead>
<tbody>
<tr>
<td>design variables (size, number)</td>
<td>slack variables (size, number)</td>
<td>(size, number)</td>
</tr>
<tr>
<td>$(N_M \times N_M, M)$</td>
<td>$(1 \times 1, 5K + 3M + 2)M + 2K + 5K M$</td>
<td>$(N_F \times N_F, 2)$</td>
</tr>
</tbody>
</table>

3) Convergence Analysis: From Algorithm 1, the approximation with the current optimal solution can be updated iteratively until constraints (15), (16), (18), and (19) hold with equality, which implies that Problem (13) is optimally solved. We can observe from (15), (16), (18), and (19) that the nth iteration admits a larger feasible region than the $[n-1]$th iteration, since the nth iterative solutions can at least achieve the $[n-1]$th iterative solutions. Furthermore, the transmit power constraint is a finite value; we conclude that Algorithm 1 will converge, which is later shown by the numerical results.

Remark 1: The computational complexity for solving Problem (20) based on Algorithm 1 is briefly discussed here. Since the proposed Algorithm 1 is based on SDP, the computational complexity is determined significantly by the number and size of variables (i.e., design variables and slack variables) and constraints (i.e., PSD constraints and slack constraints). Especially, the major computational complexity for Problem (20) is summarized in Table I.

IV. SECURE ROBUST BEAMFORMING DESIGN WITH IMPERFECT CSI

In the previous section, we have investigated the secrecy rate maximization problem when all the CSI is known at the MBS and the FBS, but in practical communication systems, perfect CSI is very difficult to be obtained at the MBS and the FBS due to imperfect channel estimation, quantization, and feedback errors. It is more reasonable to study the robust secure beamforming scheme under imperfect CSI. In this section, the deterministic uncertainty model is adopted to develop the robust algorithm, which is widely used in the published works [5], [27], [31] and is very useful in practical applications.

A. Channel Estimation Uncertainty Model

We characterize the imperfect CSI associated with the receivers using the worst-case constrained model\(^4\) [5], [27], [31]. Assuming that the channel estimation uncertainty is bounded, the regions of the exact wireless channels $h_m, h_1, h_{1,0}, g_k$, respectively, where $h_m, h_1, h_{1,0}, g_k, g_{k,0}$, and $l_m$ are the estimated channel vectors, which are available to the MBS and the FBS. $h_m, h_1, h_{1,0}, g_k, g_{k,0}$, and $l_m$ denote the corresponding channel-error vectors. And $\epsilon_m, \epsilon_1, \epsilon_{1,0}, \varpi_k, \varpi_1, \varpi_m$ denote the nonnegative channel error bounds, respectively.

To enhance the robustness against the CSI errors, the original optimization problem is modified to maximize the worst-case secrecy rate based on the spherical uncertainty model in (21) under predefined constraints. As a result, the robust version of Problem (11) is formulated as

\[
\max_{\{W_m\}, W_E} \left\{ C_1(\{W_m\}, W_1, V_E) \right\}
\]

\[
\text{s.t.} \quad \min_{\{W_m\}, W_1, V_E} \frac{h_m^H W_m h_m}{\sum_{i \neq m} h_i^H W_i h_i + l_m^H (W_1 + V_E) l_m + 1} \geq \Gamma_m
\]

\[
\min_{\{W_m\}, W_1, V_E} \frac{g_k^H W_k g_k + g_{k,0}^H V_E g_{k,0} + \sum_{m=1}^M g_m^H W_m g_{m,0}}{Q_k} \geq 0
\]

\[
\text{Tr}(W_1) + \text{Tr}(V_E) + \sum_{m=1}^M \text{Tr}(W_m) \leq P_{th}
\]

\[
W_1 \succeq 0, V_E \succeq 0, W_m \succeq 0
\]

\[
\text{rank}(W_m) = 1, \text{rank}(W_1) = 1 \forall m \in M; k \in K.
\]

It is worth highlighting that Problem (22) is costly to solve globally than Problem (11) owing to the nonconvex secrecy rate expression and the infinite number of constraints caused by the norm-bounded CSI errors. Instead of directly solving Problem (22), we resort to obtaining a tractable form and reformulating it into a semidefinite optimization problem in the following.

B. Optimal Beamforming With Imperfect CSI

In general, the objective function in the form of DCP is nonconvex. It has been shown in [38] that maximizing such an objective function of Problem (22) is equivalent to maximizing $C_1(\{W_m\}, W_1, V_E)$ subject to an abstract upper bound on

\[\text{rank}(W_m) = 1, \text{rank}(W_1) = 1 \forall m \in M; k \in K.\]
\( C_{E,k}(\{W_m\}, W_1, V_E) \). By properly adjusting the upper bound on \( C_{E,k}(\{W_m\}, W_1, V_E) \), it is possible to attain the optimal solutions of the original robust Problem (22). To tackle the robust security problem, we first introduce a slack variable \( \tau \) and drop the rank-1 constraint (22f) by means of the SDR technique \([33], [34]\); then, Problem (22) can be calculated as \( \text{max} \frac{1+\log(1+\tau)}{1-\tau} \) (23a) of interest can be solved through the above-mentioned two solutions of the original robust Problem (22). To tackle the robust security problem, we first introduce a slack variable \( \tau \) and then equivalently rewrite Problem (26) as

\[
\begin{align*}
\text{max} & \quad \gamma = \left( \frac{1}{1-\tau} \right) \log_2 \left( \frac{1}{1+\tau} \right) \\
\text{s.t.} & \quad 0 \leq \tau \leq \tau_{\text{max}} \tag{24a}
\end{align*}
\]

where the function \( f(\tau) \) is defined by the second-stage optimization problem as described below. The lower bound of \( \tau \) is recognized by noting that the constraint in (23b) \( C_{E,k}(\{W_m\}, W_1, V_E) \geq 0 \). And the upper bound \( \tau_{\text{max}} \) follows the fact that

\[
\begin{align*}
\tau \leq \frac{h^H W_1 h_1}{\sum_{m=1}^M h^H \sigma_m h_1 + h^H V_E h_1 + 1} & \leq \text{Tr}(H_1) \leq \frac{1}{P_h \text{Tr}(H_1)} \triangleq \tau_{\text{max}}. \tag{25}
\end{align*}
\]

For a fixed \( \tau \), it can be easily seen that \( \frac{1+\log(1+\tau)}{1-\tau} \) is maximized when \( f(\tau) \) is maximized. Therefore, we cast the second-stage optimization problem as follows:

\[
\begin{align*}
f(\tau) & \triangleq \max_{W_m, W_1, V_E} \frac{h^H W_1 h_1}{\sum_{m=1}^M h^H \sigma_m h_1 + h^H V_E h_1 + 1} \tag{26a} \\
\text{s.t.} & \quad \sum_{m=1}^M h^H \sigma_m h_1 + h^H V_E h_1 + 1 \leq \tau \tag{26b} \\
\end{align*}
\]

As can be observed from (24) and (26), the original Problem (23) of interest can be solved through the above-mentioned two stages. First, for given \( \tau \), we solve to obtain \( f(\tau) \); then, we solve to obtain the optimal \( \tau^* \). The upshot of the reformulation (24) is that it is a single-variable optimization problem, which can be solved via performing a 1-D line search over the interval \([0, P_h \text{Tr}(H_1)]\). In the subsequent, we will focus on solving Problem (26) and discuss how to handle it for the case of channel uncertainties.

We note that the objective function of (26) is a linear fractional function; thus, it is quasi-convex. To further proceed, we introduce a slack variable \( \gamma \) and then equivalently rewrite Problem (26) as

\[
\begin{align*}
\text{max} & \quad \gamma = \left( \frac{1}{1-\tau} \right) \log_2 \left( \frac{1}{1+\tau} \right) \tag{27a} \\
\text{s.t.} & \quad 0 \leq \tau \leq \tau_{\text{max}} \tag{24b} \\
\end{align*}
\]

where the function \( f(\tau) \) is defined by the second-stage optimization problem as described below. The lower bound of \( \tau \) is recognized by noting that the constraint in (23b) \( C_{E,k}(\{W_m\}, W_1, V_E) \geq 0 \). And the upper bound \( \tau_{\text{max}} \) follows the fact that

\[
\begin{align*}
\tau \leq \frac{h^H W_1 h_1}{\sum_{m=1}^M h^H \sigma_m h_1 + h^H V_E h_1 + 1} & \leq \text{Tr}(H_1) \leq \frac{1}{P_h \text{Tr}(H_1)} \triangleq \tau_{\text{max}}. \tag{25}
\end{align*}
\]

For a fixed \( \tau \), it can be easily seen that \( \frac{1+\log(1+\tau)}{1-\tau} \) is maximized when \( f(\tau) \) is maximized. Therefore, we cast the second-stage optimization problem as follows:

\[
\begin{align*}
f(\tau) & \triangleq \max_{W_m, W_1, V_E} \frac{h^H W_1 h_1}{\sum_{m=1}^M h^H \sigma_m h_1 + h^H V_E h_1 + 1} \tag{26a} \\
\text{s.t.} & \quad \sum_{m=1}^M h^H \sigma_m h_1 + h^H V_E h_1 + 1 \leq \tau \tag{26b} \\
\end{align*}
\]

As can be observed from (24) and (26), the original Problem (23) of interest can be solved through the above-mentioned two stages. First, for given \( \tau \), we solve to obtain \( f(\tau) \); then, we solve to obtain the optimal \( \tau^* \). The upshot of the reformulation (24) is that it is a single-variable optimization problem, which can be solved via performing a 1-D line search over the interval \([0, P_h \text{Tr}(H_1)]\). In the subsequent, we will focus on solving Problem (26) and discuss how to handle it for the case of channel uncertainties.

We note that the objective function of (26) is a linear fractional function; thus, it is quasi-convex. To further proceed, we introduce a slack variable \( \gamma \) and then equivalently rewrite Problem (26) as

\[
\begin{align*}
\text{max} & \quad \gamma = \left( \frac{1}{1-\tau} \right) \log_2 \left( \frac{1}{1+\tau} \right) \tag{27a} \\
\text{s.t.} & \quad 0 \leq \tau \leq \tau_{\text{max}} \tag{24b} \\
\end{align*}
\]

where the function \( f(\tau) \) is defined by the second-stage optimization problem as described below. The lower bound of \( \tau \) is recognized by noting that the constraint in (23b) \( C_{E,k}(\{W_m\}, W_1, V_E) \geq 0 \). And the upper bound \( \tau_{\text{max}} \) follows the fact that

\[
\begin{align*}
\tau \leq \frac{h^H W_1 h_1}{\sum_{m=1}^M h^H \sigma_m h_1 + h^H V_E h_1 + 1} & \leq \text{Tr}(H_1) \leq \frac{1}{P_h \text{Tr}(H_1)} \triangleq \tau_{\text{max}}. \tag{25}
\end{align*}
\]
Although Problem (30) is still nonconvex due to nonconvex constraints in (30b)–(30f), Problem (30) has a more tractable form than Problem (27).

Remark 2: It is worth pointing out that the constraint in (30c) can be replaced by \( \max_{\Delta h_1 \in \mathcal{H}_{1,0}} \Delta h_1, \Delta h_{1,0} \in \mathcal{H}_{1,0} \) \( \sum_{m=1}^{M} h_m W_{m} h_{1,0} + h_1^T \bar{V}_E h_1 + \kappa_1 \leq 1 \). When Problem (30) obtains its optimum value, the inequality is active. The interested readers can refer to [28] and the references therein for more details.

In what follows, we convert the worst-case constraints in (30b)–(30f) into LMIs by using the S-Procedure and the generalized S-Procedure given in the following lemmas, respectively.

**Lemma 1:** (S-Procedure [36]): Let

\[
f_k(x) = x^T A_k x + 2Re \{ b_k^T x \} + c_k, \quad k = 1, 2 \tag{31}
\]

where \( A_k \in \mathbb{C}^{n \times n}, b_k \in \mathbb{C}^{n \times 1}, x \in \mathbb{C}^{n \times 1}, \) and \( c_k \in \mathbb{R} \). Then, the implication \( f_1(x) \leq 0 \implies f_2(x) \leq 0 \) holds if and only if there exists a \( \mu \geq 0 \) such that

\[
\mu \begin{bmatrix} A_1 & b_1^T \\ b_1 & c_1 \end{bmatrix} - \begin{bmatrix} A_2 & b_2 \\ b_2 & c_2 \end{bmatrix} \succeq 0 \tag{32}
\]

provided that there exists a point \( \bar{x} \) such that \( f_1(\bar{x}) < 0 \).

Since the channel uncertainty with respect to \( h_t \) is constrained, we commence rewrite the constraint in (30b) as follows:

\[
\begin{align*}
\{ (\hat{h}_t + \Delta h_t)^T \hat{W}_t (\hat{h}_t + \Delta h_t) - \gamma & \geq 0 \\
\forall \Delta h_t : \| \Delta h_t \|_2 & \leq \epsilon_t 
\} \tag{33}
\end{align*}
\]

Applying Lemma 1 and introducing a slack variable \( \lambda_t \geq 0 \), we convert (30b) into an LMI given by

\[
\begin{bmatrix}
\begin{bmatrix} \lambda_t I + \hat{W}_t - \hat{h}_t^T \hat{h}_t \\
\hat{h}_t^T \hat{W}_t - \lambda_t \epsilon_t - \gamma
\end{bmatrix} \succeq 0 
\end{bmatrix} \tag{34}
\]

Since the channel uncertainties with respect to \( h_t \) and \( h_{1,0} \) are constrained separately, we then rewrite the constraint in (30c) as follows:

\[
\begin{align*}
\{ (\hat{h}_t + \Delta h_t)^T B_1 (\hat{h}_t + \Delta h_t) \\
+ (h_1,0 + \delta h_{1,0})^T C_1 (h_1,0 + \delta h_{1,0}) + d_1 & \geq 0 \\
\forall \Delta h_t, \delta h_{1,0} : \| \Delta h_t \|_2 & \leq \epsilon_t, \| \delta h_{1,0} \|_2 \leq \epsilon_{1,0}
\} \tag{35}
\end{align*}
\]

where \( B_1 = -\bar{V}_E, C_1 = -\sum_{m=1}^{M} \hat{W}_m \), and \( d_1 = 1 - \kappa \).

Then, (35) is equivalent to the following form:

\[
\begin{align*}
\{ (\hat{h}_t + \Delta h_t)^T & B_1 (\hat{h}_t + \Delta h_t) \\
+ (h_1,0 + \delta h_{1,0})^T C_1 (h_1,0 + \delta h_{1,0}) + d_1 & \geq 0 \\
\forall \Delta h_t, \delta h_{1,0} : \| \Delta h_t \|_2 & \leq \epsilon_t, \| \delta h_{1,0} \|_2 \leq \epsilon_{1,0}
\} \tag{36}
\end{align*}
\]

By performing the Lemma 1 with respect to the uncertainty sets \( \mathcal{H}_{1,0}, \mathcal{H}_t \) (36) can be equivalently transformed into the following QMI by the Schur complement [28]:

\[
\begin{bmatrix}
\lambda_t I + B_1 \\
\hat{h}_t^T B_1 Y_1 + (h_1,0 + \delta h_{1,0})^T C_1 (h_1,0 + \delta h_{1,0})
\end{bmatrix} \succeq 0 \tag{37}
\]

where \( \lambda_t \geq 0 \) is the introduced slack variable, \( Y_1 = \hat{h}_t^T B_1 \hat{h}_t - \lambda_t \epsilon_t^2 + d_1 \).

To further solve the semidefiniteness of \( \mathcal{H}_{1,0} \), we have the following lemma.

**Lemma 2** (see [39, Th. 4.2]): If \( D \succeq 0 \), the data matrices \( h_j, j \in \{1, \ldots, 0\} \), satisfy

\[
\begin{bmatrix}
H_1 & H_2 & H_3 & X \\
(H_2 + X H_3) & H_4 & H_5 & X + H_6 X \\
X + H_7 X & H_8 & H_9 & X \\
\end{bmatrix} \succeq 0
\]

\( \forall X : I - X X^H D X \succeq 0 \) \tag{38}

is equivalent to the LMI system

\[
\begin{bmatrix}
H_1 & H_2 & H_3 \\
H_4 & H_5 & H_6 \\
H_7 & H_8 & H_9
\end{bmatrix} - \begin{bmatrix}
0 & 0 & 0 \\
0 & I & 0 \\
0 & 0 & -D
\end{bmatrix} \succeq 0 \tag{39}
\]

where \( \lambda \geq 0 \), \( \lambda \geq 0 \).

Following similar arguments, let us define \( B_2 = \tau \bar{V}_E - W_1, C_2 = \sum_{m=1}^{M} \bar{W}_m, d_2 = \tau, B_3 = W_m - \sum_{m=1, m \neq m}^{M} \bar{W}_m, C_3 = \Gamma_m (W_1 + V_E), d_3 = \Gamma_m, B_4 = W_1 + V_E, C_4 = \sum_{m=1}^{M} \bar{W}_m, \) and \( d_4 = Q_k \). Similar to the constraint in (30c), the constraints in (30d)–(30f) can also be converted into the following LMIs:

\[
\begin{bmatrix}
\lambda_k I + B_2 \\
g_k^T B_2 Y_2 + g_k^T C_2 g_k - \lambda_k C_2 \\
0 \\
C_2 + \frac{1}{\lambda_k} I
\end{bmatrix} \succeq 0 \tag{41}
\]

\[
\begin{bmatrix}
\lambda_m I + B_3 \\
\hat{h}_m^T B_3 Y_3 - \hat{h}_m^T C_3 \hat{h}_m - \mu_m Y_3 - \hat{h}_m^T C_3 \hat{h}_m \\
0 \\
C_3 + \frac{1}{\lambda_m} I
\end{bmatrix} \succeq 0 \tag{42}
\]

\[
\begin{bmatrix}
\mu_k I + B_4 \\
g_k^T B_4 Y_4 + g_k^T C_4 g_k - \mu_k C_4 \\
0 \\
C_4 + \frac{1}{\mu_k} I
\end{bmatrix} \succeq 0 \tag{43}
\]

respectively, where \( \{ \lambda_k \geq 0 \}, \{ \lambda_k \geq 0 \}, \{ \lambda_m \geq 0 \}, \{ \lambda_k \geq 0 \}, \{ \mu_k \geq 0 \}, \{ \mu_k \geq 0 \}, \) and \( \{ \mu_m \geq 0 \} \) are the introduced slack variables.
Algorithm 2: Proposed Two-Stage Algorithm for Solving Problem (23).

Input: Initialize \( \{ \Gamma_m \}, \{ Q_k \}, P_b \) and \( \tau_{\text{max}} = P_b \text{Tr}(H_1) \).

Repeat: For \( \tau = [0, \tau_{\text{max}}] \), performing 1-D search.

Step 1: Solve the convex Problem (44) and obtain \( f(\tau) \).

Set: \( \tau^* = \arg \max \frac{1 + f(\tau)}{1 + \tau} \).

Step 2: For a given \( \tau^* \), solve Problem (44) to obtain 
\( (W^*_m, W^*_1, V^*_E, \kappa^*) \).

Step 3: Let \( W^*_m = \frac{w^*_m}{\|w^*_m\|}, W^*_1 = \frac{w^*_1}{\|w^*_1\|} \).

Output: If rank\( (W^*_m) = 1 \) and rank\( (W^*_1) = 1 \), we can obtain \( w^*_m \) and \( w^*_1 \) by applying eigenvalue decomposition; Otherwise, we resort to Gaussian randomization method to find the rank-1 approximate solutions.

be expressed as

\[
\begin{align}
\max \quad & \{ w_m, w_1, v_E, \gamma, \kappa, \lambda_1, \lambda_k \} \\
\text{s.t.} \quad & (22d), (22e), (34), (40), (41), (42), \text{and } (43).
\end{align}
\]

It is worth mentioning that Problem (44) is a convex SDP problem, which can be efficiently solved by using interior-point-based solvers, e.g., CVX [36]. In this setup, however, the rank-1 solutions of \( \{ w_m^* \} \) and \( w_1^* \) are difficult to prove directly. Toward this end, if the optimal solutions of Problem (44) satisfy rank-1 constraints, then the optimal beamforming vectors \( \{ w_m^* \} \) and \( w_1^* \) can be obtained by utilizing the eigenvalue decomposition. Alternatively, the rank-1 approximation technique, e.g., Gaussian randomization method [37] can be applied to generate the approximate solutions. In general, the eigenvalue decomposition method performs worse than the Gaussian randomization method, provided that the number of randomizations is sufficiently large.

Based on the above analysis, a two-stage optimization algorithm is proposed to solve the original Problem (23) of interest. In each outer iteration, we aim to update \( \tau \) via 1-D search such as uniform sampling method. While in each inner iteration, we focus on solving Problem (44) with a fixed \( \tau \). A very brief outline of the proposed algorithm is summarized in Algorithm 2.

Remark 3: It is to be noted that the original Problem (23) is a two-stage optimization problem; the computational complexity for solving Problem (23) is dominated by a 1-D search from the first-stage \( L_1 \) times the second-stage SDP. In particular, the major computational complexity for the second-stage SDP is summarized in Table II.

Remark 4: It is easy to extend the proposed schemes to the scenario where the legitimate users in the femtocell are supported by the FBS as well as the MBS, which demonstrates that the MBS is more capable than the FBS [40]. The only difference is that heterogeneous cell association is considered. For this scenario, the process of solving secrecy rate maximization is similar to the proposed algorithms.

### V. Numerical Results

In this section, we present simulation results to show the performance of the proposed secure beamforming design in a two-tier SWIPT-enabled HCN for both perfect and imperfect CSI cases. Without loss of generality, we assume that the number of antennas equipped at the MBS and the FBS are \( N_M = N_F = 4 \); the number of MUUs and ERs are \( M = 2 \) and \( K = 2 \), respectively, unless otherwise specified. For the sake of simplicity, we assume that the noise powers are identical as \( \sigma_m^2 = \sigma_1^2 = \sigma_k^2 = 1 \) dBm, the EH threshold is set to be \( Q_k = Q = 20 \) dBm, the target SINR of each MU is set to be \( \xi = 1 \). As in [21] and [28], we assume the channel models including the large-scale fading and the small-scale channel fading. Especially, the simplified large-scale fading model can be expressed as

\[
D = A_0 \left( \frac{d}{d_0} \right)^{-\alpha}
\]

where \( A_0 \) is a constant set to be 1, \( d \) denotes the propagation distance from the transmitter to receiver, \( d_0 \) is a reference distance set to be 100, and \( \alpha \) is the path loss exponent set to be 3. We assume that the propagation distances in intertier and intratier are set as 500 m and 200 m, respectively. On the other hand, the small-scale fading channel coefficients are assumed to be i.i.d. obeying \( CN(0, 1) \). All simulation results are averaged over 1000 randomly generated channel realizations.

#### A. Perfect CSI Case

In this section, we evaluate the performance of our proposed secure beamforming in the case of perfect CSI. For comparison, three benchmark schemes are considered, i.e., orthogonal spectrum allocation scheme [8] (denoted as “OSA scheme”), without AN scheme (denoted as “w/o AN scheme”), and nonsecrecy-oriented beamforming scheme (denoted as “Non-secrecy scheme”), respectively. When the “OSA scheme” is considered, different spectrum resources are allocated to the MBS and the FBS; thus, no cross-tier interference exists in this scheme. The “Non-secrecy scheme” has been considered in the literature [8], [41].

In Fig. 2, we show the convergent behavior of our proposed Algorithm 1 over a few random channel realizations under...
Fig. 2. Convergence of the proposed Algorithm 1 with $P_{th} = 40$ dBm.

Fig. 3. Secrecy rate performance comparison of various schemes for the transmit power threshold $P_{th}$.

$P_{th} = 40$ dBm. It can be observed that the proposed Algorithm 1 can efficiently converge to a stable point after only four steps, which illustrates that the proposed Algorithm 1 has a fast convergence behavior and hence has a low computational complexity.

Fig. 3 compares the achieved secrecy rate performance of our proposed Algorithm 1 scheme, “OSA scheme,” “w/o AN scheme,” and “Non-secrecy scheme.” As expected, the proposed Algorithm 1 always outperforms the three benchmark schemes under perfect CSI. This is because the introduced interference is capable of improving the secrecy rate performance of IR. At the same time, this demonstrated that AN-aided is an effective approach in enhancing security for wiretap channels. From Fig. 3, we can also observe that the achieved secrecy rate increases as the transmit power threshold $P_{th}$ increases.

To further observe the superior performance of the proposed scheme in the case of perfect CSI, we examine the relationship between the secrecy rate achieved by different schemes and the number of FBS transmit antennas $N_F$ when fixing transmit power threshold $P_{th} = 40$ dBm. As can be seen from Fig. 4, a higher secrecy rate can be obtained with more transmit antennas $N_F$, with the increased spatial degrees of freedom. Furthermore, it can be found that the proposed Algorithm 1 scheme significantly outperforms the counterparts in terms of the achieved secrecy rate, especially when the number of transmit antennas $N_F$ is set relatively large.

B. Imperfect CSI Case

In this section, we evaluate the performance of our proposed robust secure beamforming design and the nonrobust design under the imperfect CSI case. The nonrobust design scheme is obtained for solving Problem (22), where channel-error vectors $\Delta h_m = 0$, $\Delta h_I = 0$, $\Delta h_{I,0} = 0$, $\Delta g_k = 0$, $\Delta g_{k,0} = 0$, and $\Delta l_m = 0$.

Fig. 5 compares the achieved secrecy rate versus transmit power threshold $P_{th}$ for different channel error $\epsilon$. As shown in Fig. 5, the proposed robust algorithm 2 scheme performs better than the nonrobust scheme in the whole transmit power threshold $P_{th}$ region. Therefore, the proposed robust design scheme has a good anti-Eve ability than the nonrobust design scheme. In addition, we can observe that the performance loss becomes larger as the channel error $\epsilon$ increases, even with a slight channel error. This implies that the robust design scheme is very sensitive to the CSI accuracy.

Fig. 6 illustrates the secure performance of the proposed robust design scheme in comparison with the nonrobust design scheme for different number of Eves $K$ by fixing $P_{th} = 40$ dBm. Intuitively, the secrecy rate of the robust design scheme decreases with the increase of the channel error $\epsilon$, which validates the motivation of the worst-case robust optimization. Furthermore, it is clearly seen that the proposed robust design scheme performs considerably better than the nonrobust design scheme in the whole channel-error region. In addition, it can be observed
Then, an SCA-based iterative algorithm was proposed to obtain the optimal beamforming solution. For the imperfect CSI case, we investigated the robust beamforming design relying on the worst-case design philosophy. To facilitate the solution, we converted the infinitely many robust constraints into LMIs by using the S-Procedure and the Schur complement, respectively. Numerical results have showed that the proposed beamforming schemes can achieve good system performance in improving the secrecy rate.

VI. CONCLUSION

In this paper, we have studied the secure beamforming design in a two-tier HCN supporting SWIPT, where the ERs were powered by RF signals. Both the scenarios of perfect and imperfect CSI were, respectively, considered. We aimed at maximizing the secrecy rate at IR while satisfying the required constraints. For the perfect CSI case, the formulated nonconvex secrecy rate maximization problem was relaxed and reformulated into a series of convex forms by using both SDR and SCA techniques.

from Fig. 6 that the proposed robust design scheme suffers from a serious secrecy rate degradation as the number of Eves $K$ increases. This is because there may have a stronger intercept ability when the number of Eves $K$ becomes large. The curves reveal that the advantage of the proposed robust design scheme holds and shows the superiority in resisting more Eves than the “Non-robust” scheme.

Fig. 5. Secrecy rate versus transmit power threshold $P_{th}$ with different channel error $\epsilon$.

Fig. 6. Secrecy rate versus channel error $\epsilon$ for different number of Eves $K$ under $P_{th}$ = 40 dBm.

REFERENCES


