Secrecy Transmit Beamforming for Heterogeneous Networks

Tiejun Lv, *Senior Member, IEEE*, Hui Gao, *Member, IEEE*, and Shaoshi Yang, *Member, IEEE*

Abstract—In this paper, we pioneer the study of physical-layer security in heterogeneous networks (HetNets). We investigate secure communications in a two-tier downlink HetNet, which comprises one macrocell and several femtocells. Each cell has multiple users and an eavesdropper attempts to wiretap the intended macrocell user. First, we consider an orthogonal spectrum allocation strategy to eliminate co-channel interference, and propose the secrecy transmit beamforming only operating in the macrocell (STB-OM) as a partial solution for secure communication in HetNet. Next, we consider a secrecy-oriented non-orthogonal spectrum allocation strategy and propose two cooperative STBs which rely on the collaboration amongst the macrocell base station (MBS) and the adjacent femtocell base stations (FBSs). Our first cooperative STB is the STB sequentially operating in the macrocell and femtocells (STB-SMF), where the cooperative FBSs individually design their STB matrices and then feed their performance metrics to the MBS for guiding the STB in the macrocell. Aiming to improve the performance of STB-SMF, we further propose the STB jointly designed in the macrocell and femtocells (STB-JMF), where all cooperative FBSs feed channel state information to the MBS for designing the joint STB. Unlike conventional STBs conceived for broadcasting or interference channels, the three proposed STB schemes all entail relatively sophisticated optimizations due to QoS constraints of the legitimate users. To efficiently use these STB schemes, the original optimization problems are reformulated and convex optimization techniques, such as second-order cone programming and semidefinite programming, are invoked to obtain the optimal solutions. Numerical results demonstrate that the proposed STB schemes are highly effective in improving the secrecy rate performance of HetNet.

Index Terms—Beamforming, femtocell, nonconvex optimization, heterogeneous network, physical-layer security, semidefinite programming (SDP).

I. Introduction

WITH the rapid proliferation of smart phones, tablets and machine-to-machine communications, there is an ever-increasing demand for seamless wireless coverage, extremely high mobile data rate and reliable secrecy performance [1].

Aiming to effectively enhance the spectral and/or energy efficiency of wireless networks, it has been suggested that the deployment density of various network-nodes should increase [2], [3], and smart access-point activation and resource management are essential to utilize the dense network-nodes [4]. Therefore, heterogeneous network (HetNet) [5], [6] has been attracting great research interests, and it is regarded as one of the most promising techniques for providing higher network capacity and wider coverage. HetNet is supported by various types of base stations with different transmit power budgets. Macrocell base stations (MBSs) provide public access and wide area coverage up to a few kilometers to all the marcocell users (MUs). Small cell base stations, such as femtocell base stations (FBSs), are typically overlaid on the existing macrocells and installed in the building or indoor environment close to femtocell users (FUs). It is noted that the network architecture of HetNet becomes more open and diverse compared to the conventional single-tier cellular networks, which makes the information exchange more susceptible to eavesdropping. Recently, physical-layer security (PLS) has been proposed as a family of viable techniques to secure wireless communications [7], [8], and it also has the potential to tackle the security problem encountered in HetNet.

Traditionally, the security problem in wireless networks was mainly studied at higher layers using key-based cryptographic methods [9]. This conventional wisdom relies on the assumption that the eavesdropper is not computationally powerful to break the secret key. However, as the computational capability of wireless devices develops rapidly, perfect security can be hardly guaranteed with the key-based solutions. It is reasonable to argue that security measures should be invoked at all layers where they can be implemented in a cost-effective manner. Notably, the physical layer has remained almost ignored for security in the past. The basic idea of PLS is to exploit the randomness of wireless channel for secure message transmission [10]. The authors in [8], [11], [12] investigated the PLS in single-antenna fading channels. Since then, the secure communication in multi-antenna channels has been extensively studied [13]–[19] and in particular, practical and robust multi-antenna secrecy beamforming schemes were investigated in [19] very recently. Secure broadcasting with more than two receivers were considered in [20]–[22]. Other related works in the contexts of the multiple-access channel with confidential messages [23], the Gaussian multiple-access wiretap channel [24], and the cognitive multiple-access channel with confidential messages [25] have also been reported. Recently, there are growing research interests in the secrecy communication over interference channels, where the interference may be

potentially exploited for improving the secrecy performance. More specifically, in [26], the authors studied the inner and outer bounds for the secrecy capacity regions of a two-user interference network where the receivers are potentially eavesdroppers. The secrecy rate of a two-user interference network with an external eavesdropper was investigated in [27]. The MIMO Gaussian interference channel with confidential messages was studied in [28] using game-theoretic approach. The authors of [29] addressed the problem of minimizing the transmit power with imperfect channel state information (CSI) in a K-user multiple-input single-output interference network, and the so-called "S-procedure" was applied. It should be noted that the existing works on PLS mainly focus on traditional network architectures, and the research on PLS for HetNet is still largely missing.

Because of the densely overlaid network architecture, there is ubiquitous interference of various types existing in HetNet [30]. From the viewpoint of PLS, deliberately introducing interference can be beneficial for the secrecy rate performance of the system [10]. Inspired by this insight, the interference should be utilized, rather than avoided, to improve the secrecy rate in HetNet using techniques such as proper spectrum allocation and cooperative beamforming. To elaborate a little further, motivated by the inter-cell interference coordination techniques [31]–[35], spectrum allocation can be rearranged dynamically in conjunction with various levels of cooperation between the network nodes, such as the MBS and FBSs, to generate the desired co-channel interference (CCI) to the eavesdropper. As a result, judicious cooperative beamforming schemes may be designed to cope with CCI for the sake of improving the secrecy rate performance in HetNet.

In this paper, a two-tier downlink HetNet system is considered, where MBS and FBSs serve the corresponding legitimate MUs and FUs, and an MU acts maliciously as an eavesdropper to wiretap another legitimate MU. For the considered scenario, we propose three secrecy transmit beamforming (STB) schemes in conjunction with two spectrum allocation schemes for secure communications in the HetNet, assuming different degrees of cooperation among the network nodes. As an initial study, we first consider the conventional orthogonal spectrum allocation (OSA) strategy [36], where orthogonal spectrum resources are allocated to the MBS and the adjacent FBSs to eliminate the cross-tier interference and the interference among adjacent femtocells. Employing OSA, the considered scenario can be simplified as the secure communication in a broadcasting channel, and we consider the STB only performed in macrocell (STB-OM) as a partial solution for the secure communication in HetNet. It is noted that STB-OM aims to maximize the secrecy rate of the intended MU subject to the quality of service (QoS) constraints of the other legitimate MUs, and no cooperation between the MBS and FBSs is necessary. Inspired by the fact that friendly interference can help secure communication [10], we deliberately introduce interference in the HetNet with the secrecy-oriented non-orthogonal spectrum allocation (SONOSA) strategy, which dynamically changes the local pattern of the underlay OSA. Specifically, some cooperative FBSs adjacent to the eavesdropper are assigned with the same frequency resource as MBS, while the OSA strategy

still applies to the non-cooperative FBSs. Consequently, CCI is deliberately introduced around the eavesdropper to enable more effective cooperative STB. Specifically, two STB schemes are proposed in conjunction with SONOSA, where MBS performs STB in collaboration with its cooperative co-channel FBSs. Firstly, a STB scheme is proposed to improve STB-OM with a little cross-tier cooperation, which is sequentially performed in macrocell and femtocells (STB-SMF). In this scheme, each cooperative FBS designs its STB to altruistically maximize the generated interference to the eavesdropper while serving its own FUs. Then each cooperative FBS calculates a performance metric and feeds it back to the MBS to facilitate the STB in macrocell, and the MBS can still use the STB-OM with minor modification. To improve the overall performance of STB-SMF, another STB is proposed with the limited cross-tier cooperation, which is jointly performed in macrocell and femtocells (STB-JMF). In this scheme, each cooperative FBS feeds its CSI back to the MBS for the joint STB, which aims to guarantee the QoS requirements of both MUs and FUs while enhancing the secrecy rate of the intended MU.

For the sake of clarity, the main contributions of this paper are summarized as follows:

1) Upon adopting the OSA strategy, an STB-OM scheme is proposed to secure the broadcast channel of the macrocell, where the confidential message and the common messages are simultaneously transmitted. In particular, an iterative algorithm is proposed to maximize the secrecy rate while satisfying the QoS of the common messages. To handle the complicated optimization problem, we transform the original nonconvex problem into a second-order cone program (SOCP) with the aid of a first-order Taylor approximation. The approximation can be improved with each iteration. Therefore, a local optimum of the original optimization problem can be obtained in several iterations. It is noted that the proposed STB-OM is different from the conventional STB schemes in the broadcasting channel [37], [38], where only the confidential message transmission is considered. Furthermore, the STB-OM is applicable to the general single cell scenarios and does not need cooperation between the MBS and FBSs, which also initiates our cooperative STB exploiting CCI.

2) Based on the SONOSA strategy, a STB-SMF scheme is proposed to improve the secrecy rate of STB-OM while guaranteeing the QoS requirements of legitimate MUs. Different from the traditional jamming sources [39], the cooperative FBSs still serve their FUs while helping the MBS. To enhance the secrecy rate performance of the intended MU, the cooperative FBSs selflessly increase the interference power towards the eavesdropper without considering the QoS of their FUs, and the optimization problem is efficiently solved by SOCP. It is worth pointing out that each cooperative FBS designs its STB with local CSI, and only a scalar is fed back to the MBS for its STB in macrocell, where the MBS can still adopt STB-OM. Therefore, the STB-SMF scheme imposes very little overhead for the cross-tier cooperation, and is compatible with STB-OM.

3) Employing SONOSA strategy, an STB-JMF scheme is proposed to strike a better balance between the secret-rate performance of the intended MUs and the QoS requirements of the legitimate MUs and FUs. It is noted that such complicated optimization is nonconvex, and we opt for reformulating it into a tractable two-stage problem. Specifically, we first fix the signal-to-interference-plus-noise ratio (SINR) of the eavesdropper to formulate the inner stage problem, which can be further transformed into a tractable semidefinite program (SDP) by applying the semidefinite relaxation technique. Then, we perform a one-dimensional search to solve the outer stage problem, which finds the most suitable SINR of the eavesdropper to optimize the original objective. It is noted that the MBS only needs to collect the CSI from its cooperative FBSs for this joint STB, and such cross-tier cooperation imposes acceptable overhead for the backhaul. Furthermore, unlike the altruistic STB of the cooperative FBSs in STB-SMF, the STB-JMF shceme guarantees the QoS of the FUs in the cooperative FBSs.

The rest of this paper is organized as follows. In Section II, the downlink HetNet system model and the corresponding spectrum allocation strategies are presented, and we derive SINR expressions of various network nodes for the following beamforming design. Based on the two spectrum allocation strategies, three STB schemes are proposed in Section III, where the related optimization problems are formulated and solved. In Section IV, simulation results show the effectiveness of the proposed algorithms. Finally, conclusions and future directions are provided in Section V.

Notations: Bold upper and lower case letters denote matrices and vectors, respectively. Transpose and conjugate transpose are denoted by $(\cdot)^T$ and $(\cdot)^H$, respectively, while $\mathrm{E}\{\cdot\}$ represents expectation. $\mathrm{Tr}(\cdot)$ is the trace operator, $\|\cdot\|$ represents the Euclidean norm, $|\cdot|$ denotes the mode of a complex number, and $\mathrm{rank}(\cdot)$ stands for the rank of a matrix. $\mathbf{X} \succeq 0$ indicates that $\mathbf{X}$ is Hermitian positive semidefinite. $\mathbb{C}$ represents the field of complex numbers. $\mathrm{Re}(\cdot)$ and $\mathrm{Im}(\cdot)$ denote the real part and the imaginary part of a complex number, respectively. Additionally, the integer set $\{1, 2, \ldots, K\}$ is abbreviated as $[1, K]$. $\mathcal{CN}(\mu, \sigma^2)$ denotes a complex Gaussian variable with mean μ and variance σ^2.

II. SYSTEM MODEL

We consider a downlink HetNet as shown in Fig. 1. There is one N_M-antenna MBS at the center, and M single-antenna MUs are randomly distributed throughout the macrocell coverage area, where we have $N_M > M$, while the single-antenna eavesdropper intends to wiretap the confidential message transmitted to a legitimate MU. Additionally, F N_F-antenna FBSs are spatially distributed according to a homogeneous Poisson point process and each FBS aims to serve K single-antenna FUs, where we have $N_F > K$. To simplify the analysis, we assume that the transmit power of each FBS is fixed and equal, denoted by P_F. Similar to that of the FBSs, the transmit power of the MBS is assumed to be P_M. Other relevant variables are defined in Table I.
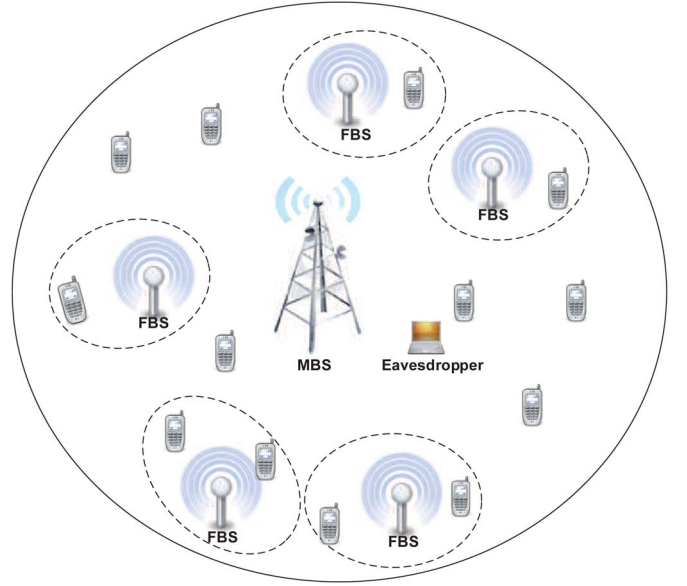

Fig. 1. Downlink HetNet system model, comprising a macrocell and N femtocells. The macrocell consists of a MBS, M legitimate MUs and an eavesdropper. Each FBS serves K FUs.

TABLE I
LIST OF THE MAJOR VARIABLES

Variable	Definition
MU_m, FBS_n FU_{nk}	the m-th MU, the n-th cooperative FBS of MBS and the k-th FU of the n-th cooperative FBS
s_m	the message signal intended for the MU_m, $m \in [1, M]$, satisfying $\mathrm{E}\{\|s_m\|\} = 1$
s_{nk}	the message signal intended for FU_{nk}, $n \in [1, N]$, $k \in [1, K]$, satisfying $\mathrm{E}\{\|s_{nk}\|\} = 1$
$\mathbf{h}_m$	the channel vector from the MBS to MU_m
$\mathbf{h}_{n,m}$	the channel vector from FBS_n to MU_m
$\mathbf{h}_E$	the channel vector from the MBS to the eavesdropper
$\mathbf{h}_{n,E}$	the channel vector from FBS_n to the eavesdropper
$\mathbf{h}_{nk}$	the channel vector from the MBS to FU_{nk}
$\mathbf{h}_{p,nk}$	the channel vector from FBS_p to FU_{nk}, $p \in [1, N]$
$\mathbf{w}_m$	the precoding vector for MU_m
$\mathbf{w}_{nk}$	the precoding vector for FU_{nk}

Two spectrum allocation strategies are developed in this paper, i.e., the OSA strategy and the SONOSA strategy. Serving as the underlay spectrum allocation strategy, OSA allocates orthogonal spectrum resources to the MBS and the adjacent FBSs to eliminate the cross-tier interference as well as the interference among adjacent femtocells [36]. Building upon OSA, SONOSA dynamically changes the local pattern of OSA to enable advanced cooperative STB schemes. Specifically, the SONOSA strategy assigns the same frequency resource occupied by the MBS to the FBSs which are adjacent to the eavesdropper, as shown in Fig. 2. Employing SONOSA, the co-channel FBSs can work in collaboration with the MBS to generate interference to the eavesdropper while serving their own FUs.

Fig. 2. An example for OSA and SONOSA, where the polygons with the same color denote the femtocells with the same frequency resource, the apple-green triangle is MBS, the cell phone is the eavesdropped MU and the ear denotes the eavesdropper. It is noted that OSA is the underlay strategy, and SONOSA dynamically changes the local pattern of OSA. Three apple-green femtocells are assigned with the same frequency resource as the macrocell to generate CCI against the eavesdropper.

Considering SONOSA, we assume that there are N ($1 \leq N < F$) cooperative FBSs employing CCI to improve the secrecy rate of the eavesdropped MU. Let us denote the n-th cooperative FBS of the MBS as FBS_n and the m-th MU as MU_m, then the received signal at MU_m is given by

$$
y_m = \mathbf{h}_m \mathbf{w}_m s_m + \sum_{q=1, q \neq m}^{M} \mathbf{h}_m \mathbf{w}_q s_q
$$
$$
+ \sum_{n=1}^{N} \sum_{k=1}^{K} \mathbf{h}_{n,m} \mathbf{w}_{nk} s_{nk} + n_m, \ m \in [1, M], \quad (1)
$$

where $\mathbf{h}_m \in \mathbb{C}^{1 \times N_M}$ and $\mathbf{h}_{n,m} \in \mathbb{C}^{1 \times N_F}$ denote the channel vector from the MBS to MU_m and the channel vector from the FBS_n to MU_m, respectively.[1] $\mathbf{w}_m \in \mathbb{C}^{N_M \times 1}$ and s_m represent the precoding vector and the message symbol intended for MU_m, respectively. Similarly, $\mathbf{w}_{nk} \in \mathbb{C}^{N_F \times 1}$ and s_{nk} are the precoding vector and the message signal intended for the k-th FU of the n-th cooperative FBS, denoted as FU_{nk}. n_m is the Gaussian noise following independent and identically distributed (i.i.d.) $\mathcal{CN}(0, \sigma_M^2)$ at MU_m. The precoding vectors for the MUs satisfy the power constraint of $\sum_{m=1}^{M} \|\mathbf{w}_m\|^2 = P_M$ and the precoding vectors for the FUs in a femtocell satisfy the power constraint of $\sum_{k=1}^{K} \|\mathbf{w}_{nk}\|^2 = P_F$. Without loss of generality, we assume

that there is an eavesdropper wiretapping MU_1,[2] therefore the received signal at the eavesdropper is given by

$$
y_E = \mathbf{h}_E \mathbf{w}_1 s_1 + \sum_{m=2}^{M} \mathbf{h}_E \mathbf{w}_m s_m
$$
$$
+ \sum_{n=1}^{N} \sum_{k=1}^{K} \mathbf{h}_{n,E} \mathbf{w}_{nk} s_{nk} + n_E, \quad (2)
$$

where $\mathbf{h}_E \in \mathbb{C}^{1 \times N_M}$ denotes the channel vector from the MBS to the eavesdropper, $\mathbf{h}_{n,E} \in \mathbb{C}^{1 \times N_F}$ is the channel vector from FBS_n to the eavesdropper, and n_E is the Gaussian noise obeying i.i.d. $\mathcal{CN}(0, \sigma_E^2)$ at the eavesdropper. Furthermore, the received signal at FU_{nk} can be formulated as

$$
y_{nk} = \mathbf{h}_{n,nk} \mathbf{w}_{nk} s_{nk} + \sum_{t=1, t \neq k}^{K} \mathbf{h}_{n,nk} \mathbf{w}_{nt} s_{nt}
$$
$$
+ \sum_{p=1, p \neq n}^{N} \sum_{t=1}^{K} \mathbf{h}_{p,nk} \mathbf{w}_{pt} s_{pt} + \sum_{m=1}^{M} \mathbf{h}_{nk} \mathbf{w}_m s_m + n_{nk}, \quad (3)
$$

where $\mathbf{h}_{n,nk} \in \mathbb{C}^{1 \times N_F}$ is the channel vector from FBS_n to FU_{nk}, $\mathbf{h}_{nk} \in \mathbb{C}^{1 \times N_M}$ is the channel vector form MBS_n to FU_k, and the Gaussian noise n_{nk} at FU_{nk} follows i.i.d. $\mathcal{CN}(0, \sigma_F^2)$.

To facilitate the analysis of secrecy rate performance, we define the SINR of MU_m as

$$
\text{SINR}_m = \frac{|\mathbf{h}_m \mathbf{w}_m|^2}{A_m}, \quad m \in [1, M], \quad (4)
$$

where

$$
A_m = \sum_{q=1, q \neq m}^{M} |\mathbf{h}_m \mathbf{w}_q|^2 + \sum_{n=1}^{N} \sum_{k=1}^{K} |\mathbf{h}_{n,m} \mathbf{w}_{nk}|^2 + \sigma_M^2.
$$

Similarly, the SINR of the eavesdropper is represented as

$$
\text{SINR}_E = \frac{|\mathbf{h}_E \mathbf{w}_1|^2}{B_E}, \quad (5)
$$

where

$$
B_E = \sum_{m=2}^{M} |\mathbf{h}_E \mathbf{w}_m|^2 + \underbrace{\sum_{n=1}^{N} \sum_{k=1}^{K} |\mathbf{h}_{n,E} \mathbf{w}_{nk}|^2}_{\text{IFT}_{sum}} + \sigma_E^2,
$$

and IFT_{sum} is the sum of the additional interference temperature from all the cooperative FBSs to the eavesdropper. Finally, the SINR of the FU_{nk} is written as

$$
\text{SINR}_{nk} = \frac{|\mathbf{h}_{n,nk} \mathbf{w}_{nk}|^2}{C_{nk}}, \ n \in [1, N], \ k \in [1, K], \quad (6)
$$

---

[1]In this paper, we just assume perfect CSI as our first step to get fundamental insights into the physical layer security problem in HetNet. We will consider a more practical model including imperfect CSI in our future work.

[2]Similar to [40], we focus on the beamforming design in this paper. The identification problem—how to identify which MU has been intercepted by the eavesdropper—is challenging and important, which will be investigated in detail in our future work. In principle, this problem can be solved by authentication: the MBS may broadcast some test messages to each MU in a round-robin manner, and ask each of them to feed back what has been listened. For the wiretapped MU, the MBS will receive feedback from two sources.

where

$$C_{nk} = \sum_{t=1,t\neq k}^{K} |\mathbf{h}_{n,nk}\mathbf{w}_{nt}|^2 + \sum_{p=1,p\neq n}^{N} \sum_{t=1}^{K} |\mathbf{h}_{p,nk}\mathbf{w}_{pt}|^2$$
$$+ \sum_{m=1}^{M} |\mathbf{h}_{nk}\mathbf{w}_m|^2 + \sigma_F^2.$$

After the above preliminary derivations, we will propose three STB schemes in the next section to maximize the secrecy rate of the intended MU_1.

III. SECURITY TRANSMIT BEAMFORMING SCHEMES FOR HetNet

In this section, we propose three secrecy communication schemes to improve the secrecy rate of HetNet by jointly considering the spectrum allocation strategy and the transmit beamforming. Firstly, based on the OSA strategy, we propose the STB-OM scheme as a partial solution for secure communication in HetNet. Then, we employ the SONOSA strategy to propose the STB-SMF scheme, which improves STB-OM with secrecy-oriented CCI generated by the altruistic cooperative FBSs. At last, aiming at a balanced system performance, we propose the STB-JMF scheme, which optimizes the security-rate of the intended MU while satisfying the QoS constraints of both legitimate MUs and FUs. In the remaining part of this section, we will discuss each STB scheme in detail. Note that in all the three proposed schemes, we assume that the local CSI of the MUs and of the eavesdropper is available at the MBS,[3] and each FBS knows the local CSI of its own femtocell.

A. Secrecy Transmit Beamforming Only Performed in Macrocell (STB-OM)

Let us first discuss the STB-OM scheme that relies on the OSA strategy. Because different frequency resources are allocated to the MBS and FBSs, no CCI exists in this scheme. As shown in Fig. 3, the MBS serves multiple legitimate MUs, and we assume that MU_1 is wiretapped by the eavesdropper. Our goal is to maximize the secrecy rate of MU_1 while guaranteeing the QoS, i.e., SINR, requirements of other legitimate MUs. The proposed STB-OM scheme is aiming at the secrecy rate maximization. Unfortunately, this optimization problem, formulated as (7a) to (7c), is non-convex and hence prohibitive computational complexity may be incurred for finding its optimum solution. As a compromise, we employ a low-complexity iterative algorithm [41] which conservatively approximates the original problem as several tractable SOCP subproblems. In the remaining part of this subsection, the details of the problem formulation and solution are provided.

Initially, the secrecy rate optimization problem of STB-OM can be formulated as
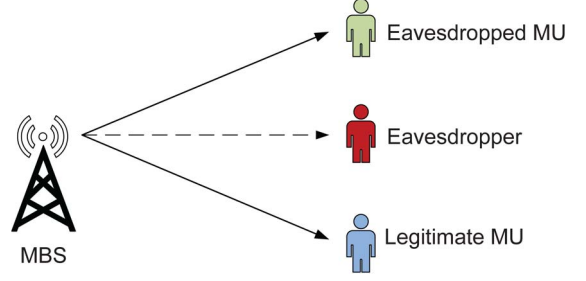

Fig. 3. An example channel model for the STB-OM scheme, consisting of one MBS, $M = 2$ MUs and one eavesdropper wiretaps the first MU. As the OSA is employed, the system is equivalent to a broadcast system. The solid lines indicate useful data streams, and the dash line indicates the interference stream.

$$\max_{\{\mathbf{w}_m\}_{m=1}^{M}} \quad \log(1 + \text{SINR}_1) - \log(1 + \text{SINR}_E) \quad (7a)$$

$$\text{s.t.} \quad \text{SINR}_m \geq \gamma_m, \ m \in [2, M], \quad (7b)$$

$$\sum_{m=1}^{M} \|\mathbf{w}_m\|^2 \leq P_M, \quad (7c)$$

where the received SINRs from (4) and (5), that are associated with MU_m and the eavesdropper, can be simplified as

$$\text{SINR}_m = \frac{|\mathbf{h}_m\mathbf{w}_m|^2}{\sigma_M^2 + \sum_{q=1,q\neq m}^{M} |\mathbf{h}_m\mathbf{w}_q|^2}, \quad (8)$$

and

$$\text{SINR}_E = \frac{|\mathbf{h}_E\mathbf{w}_1|^2}{\sigma_E^2 + \sum_{m=2}^{M} |\mathbf{h}_E\mathbf{w}_m|^2 + \text{IFT}_{sum}}, \quad (9)$$

respectively, when the OSA strategy is adopted. Note that the IFT_{sum} in this STB-OM is zero, because OSA does not introduce CCI. The constraint (7b) is the QoS requirements of the other legitimate MUs, i.e., $MU_m, m \in [2, M]$, and (7c) represents the total transmit power constraint at the MBS. To make the above problem more tractable, we introduce a pair of slack variables t_1 and t_2. Then, the original problem can be equivalently reformulated as

$$\max_{\{\mathbf{w}_m\}_{m=1}^{M}, t_1, t_2} \quad \log(t_1) + \log(t_2) \quad (10a)$$

$$\text{s.t.} \quad 1 + \text{SINR}_1 \geq t_1, \quad (10b)$$

$$1 + \text{SINR}_E \leq 1/t_2, \quad (10c)$$

$$\text{SINR}_m \geq \gamma_m, \ m \in [2, M], \quad (10d)$$

$$\sum_{m=1}^{M} \|\mathbf{w}_m\|^2 \leq P_M. \quad (10e)$$

Without loss of generality, in the following, we assume $\sigma_M^2 = \sigma_E^2 = \sigma_F^2 = \sigma^2 = 1$. Substituting (8) and (9) into the above

---

[3]Similar to [14], [15], [19], and [37], we assume that the CSI of the eavesdropper is also available at the MBS to make the STB more tractable.

problem, (10) can be transformed as follows

$$\max_{\{\mathbf{w}_m\}_{m=1}^M, t_1, t_2} \quad t_1 t_2 \tag{11a}$$

$$\text{s.t.} \quad 1 + \sum_{m=2}^M \mathbf{w}_m^H \mathbf{H}_1 \mathbf{w}_m \leq \frac{\mathbf{w}_1^H \mathbf{H}_1 \mathbf{w}_1}{t_1 - 1}, \tag{11b}$$

$$1 + \sum_{m=1}^M \mathbf{w}_m^H \mathbf{H}_E \mathbf{w}_m$$
$$\leq \frac{1 + \sum_{m=2}^M \mathbf{w}_m^H \mathbf{H}_E \mathbf{w}_m}{t_2}, \tag{11c}$$

$$\gamma_m \left(1 + \sum_{q=1, q \neq m}^M \mathbf{w}_q^H \mathbf{H}_m \mathbf{w}_q \right)$$
$$\leq \mathbf{w}_m^H \mathbf{H}_m \mathbf{w}_m, \ m \in [2, M], \tag{11d}$$

$$\sum_{m=1}^M \|\mathbf{w}_m\|^2 \leq P_M, \tag{11e}$$

where we introduce the matrices $\mathbf{H}_1 = \mathbf{h}_1^H \mathbf{h}_1$, $\mathbf{H}_m = \mathbf{h}_m^H \mathbf{h}_m$, $\mathbf{H}_E = \mathbf{h}_E^H \mathbf{h}_E$. It is noted the logarithm function is removed because of its monotonically increasing property. As we can see, the right-hand side of the constraints (11b) and (11c) are both quadratic-over-linear functions which are convex [42]. However, both constraints remain non-convex because they are expressed as the form of $f_1(x) \leq f_2(x)$, namely $f_1(x) - f_2(x) \leq 0$, where $f_1(x)$ and $f_2(x)$ are both convex functions. More specifically, it is well known that the sum of convex functions is convex. Then, $f_1(x) - f_2(x)$ is non-convex. Following the idea of the constrained convex procedure [41], we replace these quadratic-over-linear functions with their corresponding first-order expansions, and then the problem can be transformed into a convex one. Specifically, we define

$$F_{\mathbf{A}, a}(\mathbf{w}, x) = \frac{\mathbf{w}^H \mathbf{A} \mathbf{w}}{x - a}, \tag{12}$$

where $x \geq a$, $\mathbf{A} \succeq 0$. The first-order Taylor expansion of (12) at a certain point $(\tilde{\mathbf{w}}, \tilde{x})$ is given by

$$Q_{\mathbf{A}, a}(\mathbf{w}, x, \tilde{\mathbf{w}}, \tilde{x}) = \frac{2 \text{Re}\{\tilde{\mathbf{w}}^H \mathbf{A} \mathbf{w}\}}{\tilde{x} - a} - \frac{\tilde{\mathbf{w}}^H \mathbf{A} \tilde{\mathbf{w}}}{(\tilde{x} - a)^2}(x - a). \tag{13}$$

Furthermore, it is noted that $\max t_1 t_2$ can be transformed into a SOCP representation, e.g., $\max t_0$ with an additional constraint $\|[2t_0, (t_1 - t_2)]\| \leq t_1 + t_2$. This transformation is based on the fact that the constraint $t_1 t_2 \geq t_0^2$ is equivalent to $\|[2t_0, (t_1 - t_2)]\| \leq t_1 + t_2$, where we have $t_1 \geq 0$ and $t_2 \geq 0$. Based on the above preparations, for the point $(\tilde{\mathbf{w}}, \tilde{x})$, the problem (11) can then be transformed into a convex optimization

problem as follows

$$\max_{\{\mathbf{w}_m\}_{m=1}^M, t_0, t_1, t_2} \quad t_0 \tag{14a}$$

$$\text{s.t.} \quad 1 + \sum_{m=2}^M \mathbf{w}_m^H \mathbf{H}_1 \mathbf{w}_m$$
$$\leq Q_{\mathbf{H}_1, 1}(\mathbf{w}_1, t_1, \tilde{\mathbf{w}}_1, \tilde{t}_1), \tag{14b}$$

$$1 + \sum_{m=1}^M \mathbf{w}_m^H \mathbf{H}_E \mathbf{w}_m$$
$$\leq \frac{2}{\tilde{t}_2} - \frac{t_2}{\tilde{t}_2^2} + \sum_{m=2}^M Q_{\mathbf{H}_E, 0}(\mathbf{w}_m, t_2, \tilde{\mathbf{w}}_m, \tilde{t}_2), \tag{14c}$$

$$\gamma_m \left(1 + \sum_{q=1, q \neq m}^M \mathbf{w}_q^H \mathbf{H}_m \mathbf{w}_q \right)$$
$$\leq \mathbf{w}_m^H \mathbf{H}_m \mathbf{w}_m, m \in [2, M], \tag{14d}$$

$$\sum_{m=1}^M \|\mathbf{w}_m\|^2 \leq P_M, \tag{14e}$$

$$\|[2t_0, (t_1 - t_2)]\| \leq t_1 + t_2. \tag{14e}$$

Eventually, the problem can be converted to the following SOCP form (15), shown at the bottom of the next page, where the linear functions g_1, g_2, g_{3m} are respectively defined as

$$g_1 = Q_{\mathbf{H}_1, 1}(\mathbf{w}_1, t_1, \tilde{\mathbf{w}}_1, \tilde{t}_1) - 1, \tag{16}$$

$$g_2 = \sum_{m=2}^M Q_{\mathbf{H}_E, 0}(\mathbf{w}_m, t_2, \tilde{\mathbf{w}}_m, \tilde{t}_2) - t_2/\tilde{t}_2^2 - 1, \tag{17}$$

$$g_{3m} = \text{Re}\left(\mathbf{w}_m^H \mathbf{h}_m^H\right)/\sqrt{\gamma_m}, \ m \in [2, M]. \tag{18}$$

It is noted the SOCP (15) can be solved efficiently by using the available solvers such as `CVX` [43]. The proposed STB-OM scheme is summarized by Algorithm 1 as follows.

Algorithm 1 STB-OM

---

1) Initialization: Set $\tilde{\mathbf{w}}_m$, $\tilde{t}_1$ and $\tilde{t}_2$ as the values which are feasible to the problem (15).
2) Repeat:
   Solve the SOCP problem (15) with $(\tilde{\mathbf{w}}_m, \tilde{t}_1, \tilde{t}_2)$ and obtain the optimal values $(\mathbf{w}_m^*, t_1^*, t_2^*)$.
   Update $(\tilde{\mathbf{w}}_m, \tilde{t}_1, \tilde{t}_2) = (\mathbf{w}_m^*, t_1^*, t_2^*)$.
3) Until the convergence threshold is satisfied or the maximum number of iterations is reached.
4) Output $\mathbf{w}_m$.

The original optimization problem of STB-OM is nonconvex and NP-hard, thus its global optimum cannot be obtained with polynomial computational complexity using any known algorithm. By contrast, the proposed scheme, which is described by Algorithm 1, employs the first order Taylor approximations
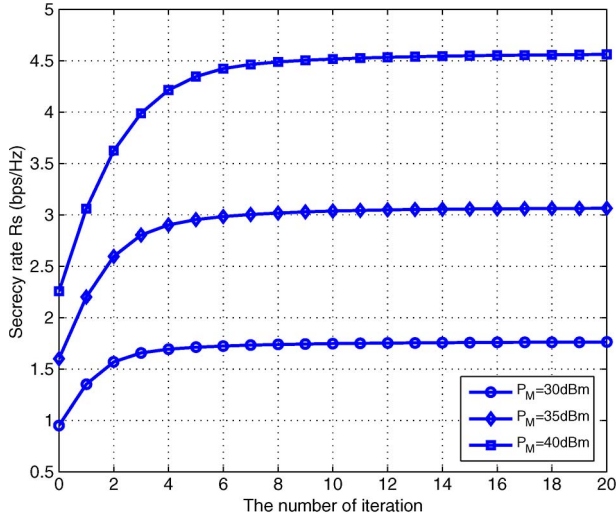
Fig. 4. The convergence property of Algorithm 1 under different values of the transmit power of the MBS.

to transform the original optimization problem into a convex optimization problem. The globally optimal solution of the resultant convex optimization problem can be obtained upon using Algorithm 1, which, according to [41], can be proved to converge to a local optimum of the original optimization problem in a few steps.[4]

Remark 1: Since the optimization problem defined in (15) is convex, the optimal solutions $\{\mathbf{w}_m^*\}_{m=1}^M, t_0^*, t_1^*, t_2^*$, are obtained by solving (15) for a given $(\tilde{\mathbf{w}}_m, \tilde{t}_1, \tilde{t}_2)$. At each iteration, $(\tilde{\mathbf{w}}_m, \tilde{t}_1, \tilde{t}_2)$ is updated based on the optimal solution $(\mathbf{w}_m^*, t_1^*, t_2^*)$ obtained in the previous iteration. Hence, $(\tilde{\mathbf{w}}_m, \tilde{t}_1, \tilde{t}_2)$ is always a feasible solution of the current iteration, and the value of t_0 obtained for the given $(\tilde{\mathbf{w}}_m, \tilde{t}_1, \tilde{t}_2)$ will be larger than or equal to the value of t_0 of the previous iteration. This observation reveals that the required secrecy rate

---

[4]The performance gap between Algorithm 1 and the optimal scheme cannot be provided at this stage due to the difficulty of obtaining the global optimum of the original optimization problem. Nevertheless, when proper initial values are given (although this is challenging as well), the local optimum achieved by Algorithm 1 may be equal to the global optimum of the original problem.

will be monotonically increasing (or at least nondecreasing) at each iteration, which is demonstrated by the numerical results in Fig. 4. Due to the power constraint, there is an upper bound for the achievable secrecy rate. Therefore, the convergence of the proposed Algorithm 1 can be guaranteed.

Remark 2: It is clear that for the STB-OM, only the local CSI is required at the MBS, including the CSI of MUs and the CSI of the eavesdropper.

Remark 3: If an FU in a femtocell is wiretapped by another FU in the same femtocell, the problem is mathematically identical to that we have solved in this subsection. In other words, the proposed approach is applicable to general single-cell interference-free scenarios.

B. Secrecy Transmit Beamforming Sequentially Performed in Macrocell and Femtocell (STB-SMF)

Compared to the conventional transmit beamforming without the consideration of secrecy, the secrecy rate performance of MU_1 can be improved by the STB-OM for its clear objective. In fact, we may further improve the secrecy rate performance by designing more sophisticated approaches. As shown in [44], it is potentially feasible to exploit interference for improving the secrecy rate performance. To achieve this goal, judicious interference management schemes could be developed. To justify these assumptions, a secrecy-oriented spectrum allocation strategy, i.e., the proposed SONOSA, is invoked to introduce deliberate CCI that is friendly with respect to the secrecy rate performance of MU_1. The SONOSA strategy dynamically changes the local pattern of the underlay OSA to improve the performance of STB-OM. Based on SONOSA, the cooperative co-channel FBSs can act independently as the sources of friendly CCI to degrade the performance of the eavesdropper. Specifically, the cooperative FBSs selflessly maximize the power of leakage interference imposed on the eavesdropper to improve the secrecy rate performance of MU_1. By exploiting the null space beamforming technique at the cooperative FBSs, the interference would only affect the eavesdropper's received signal.

$$\max_{\{\mathbf{w}_m\}_{m=1}^M, t_0, t_1, t_2} \quad t_0 \tag{15a}$$

$$\text{s.t.} \quad \left\| \left[2\mathbf{w}_2^H \mathbf{h}_1^H, \ldots, 2\mathbf{w}_M^H \mathbf{h}_1^H, g_1 - 1 \right]^T \right\| \le g_1 + 1, \tag{15b}$$

$$\left\| \left[2\mathbf{w}_1^H \mathbf{h}_E^H, \ldots, 2\mathbf{w}_M^H \mathbf{h}_E^H, g_2 - 1 \right]^T \right\| \le g_2 + 1, \tag{15c}$$

$$\left\| \left[2\mathbf{w}_1^H \mathbf{h}_m^H, \ldots, 2\mathbf{w}_{m-1}^H \mathbf{h}_m^H, 2\mathbf{w}_{m+1}^H \mathbf{h}_m^H, \ldots, 2\mathbf{w}_M^H \mathbf{h}_m^H, 2, g_{3m} - 1 \right]^T \right\| \le g_{3m} + 1, \tag{15d}$$

$$\text{Im} \left(\mathbf{w}_m^H \mathbf{h}_m^H \right) = 0, \ m \in [2, M], \tag{15e}$$

$$\left\| \left[\mathbf{w}_1^T, \ldots, \mathbf{w}_M^T \right]^T \right\| \le \sqrt{P_M}, \tag{15f}$$

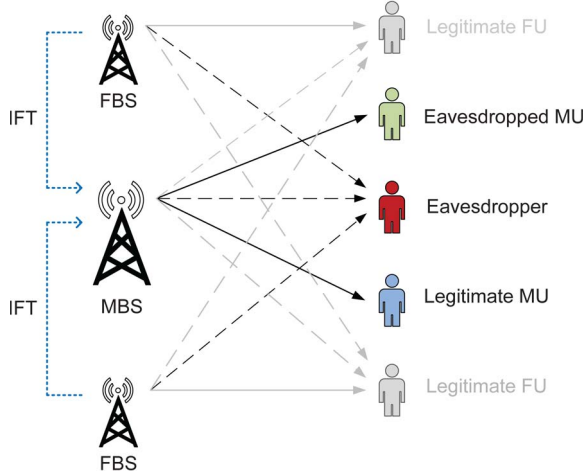$$\left\| [2t_0, (t_1 - t_2)] \right\| \le t_1 + t_2, \tag{15g}$$

Fig. 5. An example channel model for STB-SMF scheme, consisting of one MBS, $M = 2$ MUs, $N = 2$ cooperative FBSs, and $K = 1$ FU at each femtocell. An eavesdropper wiretaps the first MU in the macrocell. As the SONOSA is adopted, the channel model is equivalent to an interference channel model. The black solid lines indicate useful data streams, and the black dash lines indicate interference streams, which are optimized by STB-SMF. In particular, the blue dotted lines indicate the feedback of interference temperatures from FBSs to the MBS.

Here, as shown in Fig. 5, we develop a novel STB-SMF scheme to exploit the interference in HetNet with SONOSA. In what follows, we first discuss the STB design for the n-th cooperative FBS FBS_n, $n \in [1, N]$. We consider that FBS_n transmits data streams in the null space of $\mathbf{G}_n = [\mathbf{h}_{n,1}^T, \mathbf{h}_{n,2}^T, \ldots, \mathbf{h}_{n,M}^T]^T \in \mathbb{C}^{M \times N_F}$, which is the collective channels from FBS_n to all legitimate MUs. To guarantee the existence of the null space, $N_M > N_F > M$ has to be satisfied. As a consequence, the interference from FBS_n would only degrade the eavesdropper's channel. To improve the secrecy rate, we aim at maximizing the interference from FBS_n to the eavesdropper subject to the transmit power constraint. The problem can be then formulated as follows

$$\max_{\mathbf{W}_n} \quad \mathrm{Tr}\left[\mathbf{W}_n^H \mathbf{H}_{n,E} \mathbf{W}_n\right] \tag{19a}$$

$$\text{s.t.} \quad \mathrm{Tr}\left[\mathbf{W}_n^H \mathbf{W}_n\right] \leq P_F, \tag{19b}$$

$$\mathbf{G}_n \mathbf{W}_n = \mathbf{0}, \tag{19c}$$

where $\mathbf{H}_{n,E} = \mathbf{h}_{n,E}^H \mathbf{h}_{n,E}$, $\mathbf{W}_n = [\mathbf{w}_{n,1}, \mathbf{w}_{n,2}, \ldots, \mathbf{w}_{n,K}]$, and $\mathbf{G}_n \mathbf{W}_n = \mathbf{0}$ ensures that FBS_n does not generate interference to the legitimate MUs. To eliminate the inter-cell inter-user interference of the K FUs served by FBS_n, the beamforming vectors of FBS_n should also satisfy $\mathbf{w}_{n,k}^H \mathbf{h}_{n,nt}^H = 0$, $k, t \in [1, K]$, $k \neq t$. Let us define $\mathbf{w}_{n,k} = \mathbf{V}_n \mathbf{x}_{n,k}$, where the columns of $\mathbf{V}_n$ constitute an orthogonal basis for the null space of $\mathbf{G}_n$. The optimization problem (19) is then equivalent to

$$\max_{\{\mathbf{x}_{n,k}\}_{k=1}^K} \quad \sum_{k=1}^K \mathbf{x}_{n,k}^H \mathbf{R}_{1n} \mathbf{x}_{n,k} \tag{20a}$$

$$\text{s.t.} \quad \sum_{k=1}^K \mathbf{x}_{n,k}^H \mathbf{R}_{2n} \mathbf{x}_{n,k} \leq P_F, \tag{20b}$$

$$\mathbf{x}_{n,k}^H \mathbf{V}_n^H \mathbf{h}_{n,nt}^H = 0, \ k, t \in [1, K], \ k \neq t, \tag{20c}$$

where we have $\mathbf{R}_{1n} = \mathbf{V}_n^H \mathbf{H}_{n,E} \mathbf{V}_n$, and $\mathbf{R}_{2n} = \mathbf{V}_n^H \mathbf{V}_n$. The above problem can be further transformed into a SOCP problem by introducing a slack variable α as follows

$$\max_{\{\mathbf{x}_{n,k}\}_{k=1}^K, \alpha} \quad \alpha \tag{21a}$$

$$\text{s.t.} \quad \left\|[\mathbf{h}_{n,E}\mathbf{V}_n\mathbf{x}_{n,1}, \ldots, \mathbf{h}_{n,E}\mathbf{V}_n\mathbf{x}_{n,K}]^T\right\| \leq \alpha, \tag{21b}$$

$$\left\|[\mathbf{V}_n\mathbf{x}_{n,1}, \ldots, \mathbf{V}_n\mathbf{x}_{n,K}]^T\right\| \leq \sqrt{P_F}, \tag{21c}$$

$$\mathbf{x}_{n,k}^H \mathbf{V}_n^H \mathbf{h}_{n,nt}^H = 0, \ k \neq t, \ k, t \in [1, K]. \tag{21d}$$

As we can see, the problem (21) is a standard SOCP problem and can be solved efficiently via some numerical solvers, such as CVX [43]. For some special case, we can even obtain the closed-form solution. For example, when the number of FU served by FBS_n is 1, i.e., $K = 1$, the problem (20) can be simplified as

$$\max_{\mathbf{x}_{n,1}} \quad \mathbf{x}_{n,1}^H \mathbf{R}_{1n} \mathbf{x}_{n,1}$$

$$\text{s.t.} \quad \mathbf{x}_{n,1}^H \mathbf{R}_{2n} \mathbf{x}_{n,1} \leq P_F. \tag{22}$$

The optimal solution of (22) is given by $\mathbf{x}_{n,1}^* = \alpha \phi_{max}(\mathbf{R}_{1n}, \mathbf{R}_{2n})$, where $\phi_{max}(\mathbf{R}_{1n}, \mathbf{R}_{2n})$ denotes the generalized eigenvector corresponding to the largest generalized eigenvalue of the matrix pair $(\mathbf{R}_{1n}, \mathbf{R}_{2n})$ and $\alpha = \sqrt{P_F} \left(\left\|\mathbf{R}_{2n}^{\frac{1}{2}} \phi_{max}(\mathbf{R}_{1n}, \mathbf{R}_{2n})\right\|\right)^{-1}$. The optimal value of the objective function (22) is $P_F \lambda_{max}(\mathbf{R}_{1n}, \mathbf{R}_{2n})$, where $\lambda_{max}(\mathbf{R}_{1n}, \mathbf{R}_{2n})$ is the largest generalized eigenvalue of matrix pair $(\mathbf{R}_{1n}, \mathbf{R}_{2n})$. As a result, the optimal beamforming vector can be expressed as $\mathbf{w}_{n,1}^* = \mathbf{V}_n \mathbf{x}_{n,1}^*$.

After designing the STB at the cooperative FBSs, we continue to design the STB at the MBS. It is noted that based on the interference temperature generated by the cooperative FBSs (cf. (5)), we can obtain the STB of the MBS by employing the STB-OM with minor modification. Specifically, let us define the interference temperature generated by FBS_n at the eavesdropper as

$$\mathrm{IFT}_n = \sum_{k=1}^K \left|\mathbf{h}_{n,E}\mathbf{w}_{n,k}^*\right|^2, \tag{23}$$

then the sum of such interference from all N cooperative FBSs is $\mathrm{IFT}_{sum} = \sum_{n=1}^N \mathrm{IFT}_n$. It should be noted that IFT_{sum} is calculated by the MBS, after receiving the feedback about IFT_n from FBS_n. Then the MBS performs STB according to STB-OM and IFT_{sum}. For clarity, the proposed STB-SMF is summarized by Algorithm 2 as follows.

Algorithm 2 STB-SMF

---

1) Obtain the beamforming vector $\mathbf{w}_{n,k}^*$ of FBS_n with (21) or (22).
2) Each cooperative FBS_n calculates IFT_n (23) and transmit it to the MBS.
3) The MBS calculates $\mathrm{IFT}_{sum} = \sum_{n=1}^N \mathrm{IFT}_n$ and obtains the beamforming vector of the MBS according to the STB-OM in Algorithm 1.

Remark 4: It is worth mentioning that each cooperative FBS only needs to send a scalar IFT_{sum} to the MBS in this scheme.

Hence, STB-SMF only incurs a small increase of the backhaul traffic loads. Furthermore, only the local CSI is required at each FBS. In contrast, the local CSI and the interference temperature are required at the MBS.

Remark 5: In the STB-SMF, we take the QoS constraints of MUs into consideration while the QoS of FUs is ignored. In other words, we do not intend to ensure or enhance the QoS of FUs. Transmit beamforming vectors are designed for the cooperative FBSs to improve the secrecy rate of the eavesdropped MU, and no interference is generated to the other MUs. The STB-SMF is an altruistic manner from the view point of the FBSs. A more practical scheme is developed in the next subsection, where the QoS of FUs is considered. Despite this fact, the STB-SMF proposed in this subsection serves as a preliminary scheme which provides us the first insight into the interference-aided physical layer security enhancement in Het-Net. Furthermore, the STB-SMF scheme also acts as a design alternative for achieving the tradeoff between the performance and the implementation complexity. Compared to the practical scheme proposed in the next subsection, less cooperation and computation are required by the STB-SMF.

C. Secrecy Transmit Beamforming Jointly Performed in Macrocell and Femtocell (STB-JMF)

In the STB-SMF scheme, CCI is deliberately introduced and exploited. The secrecy rate performance of MU_1 is thus enhanced, and the QoS of the other MUs is also guaranteed. Nevertheless, the QoS of the co-channel FUs is ignored, which implies that we cannot ensure the sum-rate performance of the FUs of the cooperative FBSs.

In this section, we propose a joint secrecy transmit beamforming scheme named STB-JMF to improve the secrecy rate of MU_1 while ensuring the QoS of the other MUs and FUs. Note that the SONOSA is also used in the STB-JMF scheme to take advantage of the CCI from the point of secrecy. Our goal is to maximize the secrecy rate of MU_1 subject to the MBS/FBSs transmit power constraints and the SINR requirements at the other MUs and FUs. The transmit beamforming vectors of both the MBS and the cooperative FBSs are optimized jointly. To be more specific, each cooperative FBS obtains its local CSI and then sends it to the MBS. As a result, global CSI becomes available at the MBS. Then, the MBS jointly optimizes the beamforming vectors with the aid of the global CSI.

Following the analysis in the previous sections, we can formulate the original optimization problem as

$$\max_{\substack{\{\mathbf{w}_m\}_{m=1}^M, \\ \{\{\mathbf{w}_{nk}\}_{k=1}^K\}_{n=1}^N}} \quad \log_2(1+\text{SINR}_1) - \log_2(1+\text{SINR}_E) \quad (24a)$$

$$\text{s.t.} \quad \sum_{m=1}^M \|\mathbf{w}_m\|^2 \leq P_M,$$

$$\sum_{k=1}^K \|\mathbf{w}_{nk}\|^2 \leq P_F, \ n \in [1,N], \quad (24b)$$

$$\text{SINR}_m \geq \gamma_m, \ m \in [2,M], \quad (24c)$$

$$\text{SINR}_{nk} \geq \gamma_{nk}, n \in [1,N], \ k \in [1,K], \quad (24d)$$

where (24b) characterizes the total transmit power constraints at the MBS and the cooperative FBSs, (24c) is the QoS requirement of intact user m in the macrocell, and (24d) is the QoS requirement of FU_{nk}. As we can see, the optimization problem is non-convex and hence is very hard to solve. Despite the challenge, in what follows we will show that the problem can be solved globally optimally by reformulating it as a two-part problem. Let $\mathbf{W}_m = \mathbf{w}_m \mathbf{w}_m^H$, $\mathbf{W}_{nk} = \mathbf{w}_{nk} \mathbf{w}_{nk}^H$, we can use semidefinite relaxation technique [45] to simplify the problem. First, we introduce a slack variable $\tau = \text{SINR}_E$, and (24) can be equivalently transformed into

$$\max_{\substack{\{\mathbf{w}_m\}_{m=1}^M, \\ \{\{\mathbf{w}_{nk}\}_{k=1}^K\}_{n=1}^N}} \quad \frac{1}{1+\tau}\left[1 + \frac{\text{Tr}(\mathbf{H}_1\mathbf{W}_1)}{A'_1}\right] \quad (25a)$$

$$\text{s.t.} \quad \sum_{m=1}^M \text{Tr}(\mathbf{W}_m) \leq P_M, \quad (25b)$$

$$\sum_{k=1}^K \text{Tr}(\mathbf{W}_{nk}) \leq P_F, \ n \in [1,N], \quad (25c)$$

$$\frac{\text{Tr}(\mathbf{H}_m\mathbf{W}_m)}{A'_m} \geq \gamma_m, \ m \in [2,M], \quad (25d)$$

$$\frac{\text{Tr}(\mathbf{H}_{n,nk}\mathbf{W}_{nk})}{C'_{nk}} \geq \gamma_{nk},$$
$$n \in [1,N], \ k \in [1,K], \quad (25e)$$

$$\frac{\text{Tr}(\mathbf{H}_E\mathbf{W}_1)}{B'} \leq \tau, \quad (25f)$$

where A'_1, A'_m, B' and C'_{nk} are respectively defined as

$$A'_1 = \sum_{m\geq2}^M \text{Tr}(\mathbf{H}_m\mathbf{W}_m) + \sum_{n=1}^N\sum_{k=1}^K \text{Tr}(\mathbf{H}_{n,1}\mathbf{W}_{nk}) + 1, \quad (26)$$

$$A'_m = \sum_{q=1,q\neq m}^M \text{Tr}(\mathbf{H}_m\mathbf{W}_q) + \sum_{n=1}^N\sum_{k=1}^K \text{Tr}(\mathbf{H}_{n,m}\mathbf{W}_{nk}) + 1, \quad (27)$$

$$B' = \sum_{m\geq2}^M \text{Tr}(\mathbf{H}_E\mathbf{W}_m) + \sum_{n=1}^N\sum_{k=1}^K \text{Tr}(\mathbf{H}_{n,E}\mathbf{W}_{nk}) + 1, \quad (28)$$

$$C'_{nk} = \sum_{t=1,t\neq k}^K \text{Tr}(\mathbf{H}_{n,nk}\mathbf{W}_{nt}) + \sum_{p=1,p\neq n}^N\sum_{t=1}^K \text{Tr}(\mathbf{H}_{p,nk}\mathbf{W}_{pt})$$
$$+ \sum_{m=1}^M \text{Tr}(\mathbf{H}_{nk}\mathbf{W}_m) + 1, \quad (29)$$

$\mathbf{H}_{n,m} = \mathbf{h}_{n,m}^H\mathbf{h}_{n,m}$, $\mathbf{H}_{n,E} = \mathbf{h}_{n,E}^H\mathbf{h}_{n,E}$, $\mathbf{H}_{n,nk} = \mathbf{h}_{n,nk}^H\mathbf{h}_{n,nk}$, $\mathbf{H}_{p,nk} = \mathbf{h}_{p,nk}^H\mathbf{h}_{p,nk}$ and $\mathbf{H}_{nk} = \mathbf{h}_{nk}^H\mathbf{h}_{nk}$.

To solve the problem (25), we divided it into two parts. The outer part is a one-dimensional line search problem with τ, i.e.,

$$\max_{\tau} \quad \frac{1+G(\tau)}{1+\tau}$$
$$\text{s.t.} \quad 0 \leq \tau \leq \text{Tr}(\mathbf{H}_1)P_M. \quad (30)$$

The function $G(\tau)$ is defined by another optimization problem to be described later. The lower bound about τ can be obtained directly from (25f), while the upper bound is derived from the fact that the secrecy rate is greater than or equal to zero,

hence $\tau \leq \text{Tr}(\mathbf{H}_1)P_M$. For a fixed τ, the inner part can be expressed as

$$\max_{\{\mathbf{W}_m\}_{m=1}^M, \{\{\mathbf{W}_{nk}\}_{k=1}^K\}_{n=1}^N} \frac{\text{Tr}(\mathbf{H}_1\mathbf{W}_1)}{A_1'}$$
$$\text{s.t.} \quad (25b) - (25f), \quad (31)$$

and $G(\tau)$ is equal to the optimal value of (31).

It is observed that the problem (30) is equivalent to the original problem (25). For any fixed τ, we can obtain $G(\tau)$ by solving (31). Then, applying the one-dimensional line search method, e.g., Golden Section Search, to the interval $[1, 1 + \text{Tr}(\mathbf{H}_1)P_M]$, we can solve the problem (25). Hence, the key step is to solve (31) for a fixed τ. In what follows, we will concentrate on it.

Since, the objective function of (31) is a linear fractional function and thus it is quasi-convex [46], then we can use Charnes-Cooper transformation [47] to convert it into a linear one. Upon introducing the auxiliary variables $\mathbf{X}_m, \mathbf{X}_{nk} \succeq 0$, $\zeta > 0$, we can rewrite $\mathbf{W}_m$ and $\mathbf{W}_{nk}$ as $\mathbf{W}_m = \frac{\mathbf{X}_m}{\zeta}$, $\mathbf{W}_{nk} = \frac{\mathbf{X}_{nk}}{\zeta}$, then the problem (31) can be transformed into the problem (32), shown at the bottom of the next page.

It can be seen that the problem (32) is an SDP problem [45], which can be solved efficiently by using numerical solvers such as CVX [43]. The optimal solution of the problem (32) is denoted by $(\mathbf{X}_m^*, \mathbf{X}_{nk}^*, \zeta^*)$. Hence the corresponding optimal solution of the problem (31) can be obtained as $\mathbf{W}_m^* = \frac{\mathbf{X}_m^*}{\zeta^*}$, $\mathbf{W}_{nk}^* = \frac{\mathbf{X}_{nk}^*}{\zeta^*}$. Then, we can solve the problem (30) through the one-dimensional line search method such as Golden Section Search. Note that to get the finial solution, we need to solve a sequence of SDPs.

Let us denote the optimal solution of the problem (30) as $(\tilde{\mathbf{W}}_m, \tilde{\mathbf{W}}_{nk})$. Then, we can obtain the beamforming vector solution as follows: if rank$(\tilde{\mathbf{W}}_m) = 1$, the optimal beamforming vector $\tilde{\mathbf{w}}_m$ is exactly obtained via eigenvalue decomposition; otherwise some rank-one approximation procedures, e.g., Gaussian randomization [48] can be applied to $\tilde{\mathbf{W}}_m$ for obtaining $\tilde{\mathbf{w}}_m$. The same procedure is applicable to $\tilde{\mathbf{W}}_{nk}$. For the sake of clarity, the proposed STB-JMF is summarized in Algorithm 3.

Algorithm 3 STB-JMF

---

1) Initialization: Set $P_M, P_F, \gamma_m, \gamma_{nk}, \varepsilon$ (the search precision of the Golden Section Search);
2) Compute $\tau_{max} = \text{Tr}(\mathbf{H}_1)P_M$;
3) Solve (30) by applying one-dimensional line search method, e.g., the Golden Section Search, on interval $[1, \tau_{max}]$, obtaining the optimal τ^*. To do this, we have to solve (32) to obtain $G^*(\tau)$ for a fixed τ.
4) Obtain $(\mathbf{X}_m^*, \mathbf{X}_{nk}^*, \zeta^*)$ for τ^*.
5) Let $\mathbf{W}_m^* = \frac{\mathbf{X}_m^*}{\zeta^*}$, $\mathbf{W}_{nk}^* = \frac{\mathbf{X}_{nk}^*}{\zeta^*}$.
6) If rank$(\mathbf{W}_m^*) = $ rank$(\mathbf{W}_{nk}^*) = 1$, we can obtain $\mathbf{w}_m^*$ and $\mathbf{w}_{nk}^*$ via eigenvalue decomposition;
7) Otherwise we apply Gaussian randomization method to $\mathbf{W}_m^*$ and $\mathbf{W}_{nk}^*$ for finding approximate $\mathbf{w}_m^*$ and $\mathbf{w}_{nk}^*$.
8) End

Proposition 1: The optimal solution $\{\mathbf{X}_m\}_{m=1}^M$, $\{\{\mathbf{X}_{nk}\}_{k=1}^K\}_{n=1}^N$ of Problem (32) is always rank-one. ∎

Proof: Please see Appendix. ∎

Proposition 1 shows that using semidefinite relaxation is always tight and yields a rank-one solution for the STB-JMF.

Remark 6: In the STB-JMF, not only the QoS of MUs but also the QoS of FUs are taken into consideration. In other words, we can guarantee the QoS of all the legitimate users in both the macrocell and the cooperative femtocells. This is pragmatically attractive because QoS is one of the most important performance metrics for practical HetNet.

Remark 7: The STB-JMF scheme is capable of satisfying the QoS requirements as well as enhancing the secrecy rate performance of the eavesdropped MU, which is in contrast to the sole beamforming in STB-OM and the sequential beamforming in STB-SMF. The cooperative FBSs need to share their local CSI with the MBS. The CSI of all the MUs and FUs are available at the MBS, so that the transmit beamforming vectors for the MBS and FBSs are all designed at the MBS. Then, the MBS delivers the related beamforming matrices to the cooperative FBSs.

Remark 8: The proposed three STB schemes exploit the cooperation among network nodes in varying degrees. In the STB-OM scheme, no cooperation is used. In STB-SMF, each cooperative FBS designs transmit beamforming vectors separately for the sake of enhancing the secrecy rate performance of the eavesdropped MU. A scalar needs to be fed back to the MBS from each cooperative FBS to assist the secrecy beamforming at the MBS. In STB-JMF, all the cooperative FBSs have to share the CSI with the MBS, and the transmit beamforming vectors for the MBS and FBSs are jointly designed at the MBS to satisfy universal QoS requirements, which cannot be supported by the STB-OM and STB-SMF schemes. Moreover, it is worth pointing out that no data sharing is required for any of the proposed STB schemes, which ensures low traffic load on the backhaul links.

Remark 9: Based on [49], we derive the computational complexity of the proposed algorithms as follows. Firstly, the computational complexity of Algorithm 1 is $T_I \cdot \mathcal{O}(N_M M^{3.5} + N_M^3 M^{2.5}) \cdot \log_2(\frac{1}{\epsilon})$. Since Algorithm 2 is based on Algorithm 1 and the only difference is that Algorithm 2 has to first calculate the interference caused by each FBS, the computational complexity of Algorithm 2 is then characterized by $(N \cdot \mathcal{O}(N_F^3 K + N_F K^2) + T_I \cdot \mathcal{O}(N_M M^{3.5} + N_M^3 M^{2.5})) \cdot \log_2(\frac{1}{\epsilon})$. Finally, Algorithm 3 is based on SDP and one-dimensional line search, and its computational complexity is $T_S \cdot \mathcal{O}(NK(N_M^{3.5} + N_F^{3.5}) + N^2 K^2(N_M^{2.5} + N_F^{2.5}) + N^3 K^3(N_M^{0.5} + N_F^{0.5})) \cdot \log_2(\frac{1}{\epsilon})$, where ϵ denotes the accuracy requirement, T_I is the number of iterations required in Algorithms 1 and 2, and T_S is the number of searches carried out in Algorithm 3. As we can see, the computational complexity of Algorithm 3 is higher than that of Algorithms 1 and 2.

Remark 10: It is easy to extend the proposed schemes to the scenario where there are multiple eavesdroppers. The only difference is that the resultant optimization problem has to consider the SINR constraints of multiple eavesdroppers. Then, we can use the proposed algorithms to solve them. For the
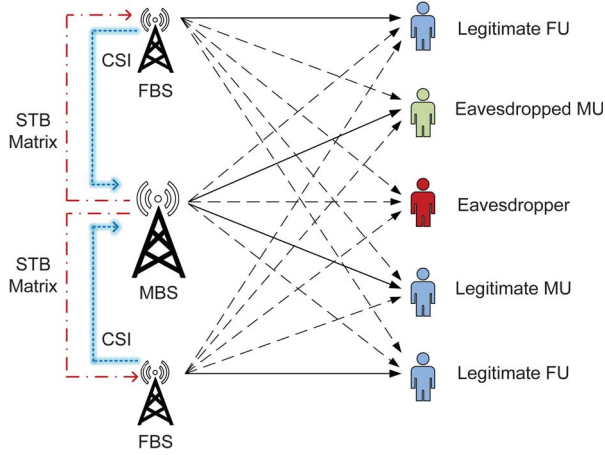
Fig. 6. An example channel model for STB-JMF scheme, consisting of one MBS, $M = 2$ MUs, $N = 2$ FBSs, and $K = 1$ FU at each femtocell. An eavesdropper wiretaps the first MU in the macrocell. As the SONOSA strategy is used, the channel model is equivalent to an interference channel model. The solid lines indicate useful data streams, and the dash lines indicate the interference streams. The blue glow dotted lines indicate the CSI streams delivered from FBSs to the MBS. The red dash-dot lines denote the STB vectors delivered from the MBS to the FBSs.

IV. SIMULATION RESULTS AND DISCUSSIONS

In this section, simulation results are provided to evaluate the secrecy rate of MU_1 for different transmit beamforming schemes conceived. We consider a downlink HetNet with a central MBS serving a circular region C and the area of C is denoted as $\mathcal{C}$. We suppose the radius of C is 500m. The FBSs are spatially distributed according to a Poisson point process φ_f with intensity λ_f [50]. Therefore, the average number of FBSs within the cellular coverage is given by $N_{FBS} = \lambda_f \mathcal{C}$. Femtocells are derived from the Voronoi tessellation and we can attain the stochastic geometry model [36] for the cellular systems illustrated in Fig. 2. The simplified system models of the three proposed STB schemes have been illustrated by Figs. 3, 5, and 6 respectively. In all simulations, the antenna configurations of the MBS and the FBS are $N_M = 10$ and $N_F = 4$, respectively. The number of MUs is $M = 2$, and the number of FUs in each FBS is $K = 1$. We also assume all MUs, FUs and the eavesdropper are single-antenna nodes due to practical constraint. For STB-SMF and STB-JMF schemes, we assume there are two cooperative FBSs helping improve the secrecy rate,[5] and each cooperative FBS serves one FU. According to the ITU-R channel simulation specifications [51], we

scenario where multiple legitimate MUs are targeted by the eavesdroppers, we may maximize either the secrecy sum-rate of the network or the minimum secrecy rate of the legitimate MUs, and the process of solving them is similar to the proposed algorithms.

[5]Our numerical results, which are not provided here due to page limitations, show that two cooperative FBSs are enough for achieving good secrecy performance. This is because when the number of cooperative FBSs increases, the interference imposed on the wiretapped MU also increases, hence the secrecy performance may not see any notable improvement.

$$\max_{\substack{\{\mathbf{x}_m\}_{m=1}^M, \zeta \\ \left\{\{\mathbf{x}_{nk}\}_{k=1}^K\right\}_{n=1}^N}} \mathrm{Tr}(\mathbf{H}_1 \mathbf{X}_1) \tag{32a}$$

$$\text{s.t.} \quad \sum_{m=1}^M \mathrm{Tr}(\mathbf{X}_m) \leq P_M \zeta, \tag{32b}$$

$$\sum_{k=1}^K \mathrm{Tr}(\mathbf{X}_{nk}) \leq P_F \zeta, \tag{32c}$$

$$\mathrm{Tr}(\mathbf{H}_m \mathbf{X}_m) \geq \gamma_m \left(\sum_{\substack{q=1, \\ q \neq m}}^M \mathrm{Tr}(\mathbf{H}_m \mathbf{X}_q) + \sum_{n=1}^N \sum_{k=1}^K \mathrm{Tr}(\mathbf{H}_{n,m} \mathbf{X}_{nk}) + \zeta \right), \tag{32d}$$

$$\mathrm{Tr}(\mathbf{H}_{n,nk} \mathbf{X}_{nk}) \geq \gamma_{nk} \left(\sum_{\substack{t=1, \\ t \neq k}}^K \mathrm{Tr}(\mathbf{H}_{n,nk} \mathbf{X}_{nt}) + \sum_{\substack{p=1 \\ p \neq n}}^N \sum_{t=1}^K \mathrm{Tr}(\mathbf{H}_{p,nk} \mathbf{X}_{pt}) + \sum_{m=1}^M \mathrm{Tr}(\mathbf{H}_{nk} \mathbf{X}_m) + \zeta \right), \tag{32e}$$

$$\mathrm{Tr}(\mathbf{H}_E \mathbf{X}_1) \leq \tau \left(\sum_{m=2}^M \mathrm{Tr}(\mathbf{H}_E \mathbf{X}_m) + \sum_{n=1}^N \sum_{k=1}^K \mathrm{Tr}(\mathbf{H}_{n,E} \mathbf{X}_{nk}) + \zeta \right), \tag{32f}$$

$$\sum_{m=2}^M \mathrm{Tr}(\mathbf{H}_m \mathbf{X}_m) + \sum_{n=1}^N \sum_{k=1}^K \mathrm{Tr}(\mathbf{H}_{n,m} \mathbf{X}_{nk}) + \zeta = 1, \tag{32g}$$

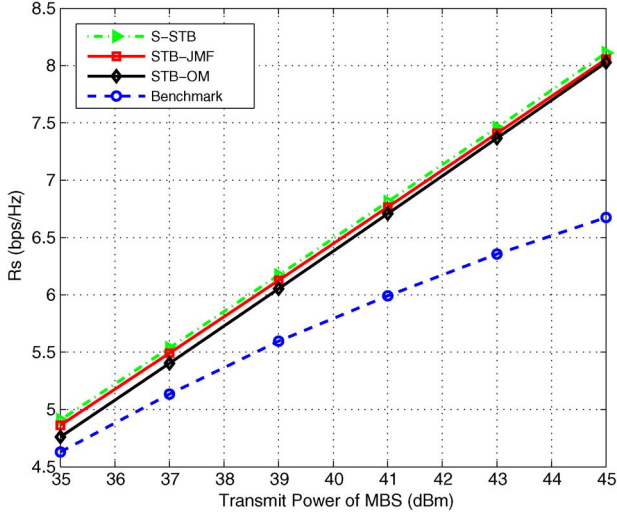$$\mathbf{X}_m, \mathbf{X}_{nk} \succeq 0, \ \zeta > 0. \tag{32h}$$

Fig. 7. The secrecy rate of MU_1 versus the transmit power of the MBS. In the STB-SMF and STB-JMF schemes, two FBSs are used to generate interference.
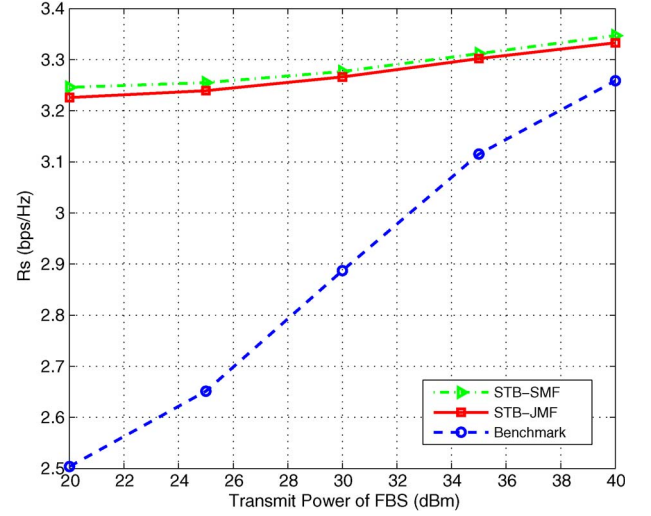

Fig. 8. The secrecy rate of MU_1 versus the transmit power of each FBS.

assume that the MBS has larger transmit power than the FBSs and the specific numerical values are given in the following. Moreover, the channel is modeled as a Rayleigh fading channel in all the simulations.

A. Benchmark Scheme

The benchmark scheme is designed as follows. First, we aim to maximize the rate of the wiretapped MU, i.e., MU_1, without the consideration of secrecy, and obtain the non-secrecy-oriented beamforming vectors for the legitimate MUs and the FUs within the cooperative femtocells. Then, we derive the secrecy rate of MU_1 with the non-secrecy-oriented beamforming vectors, which serves as our benchmark scheme. To be more specific, this optimization problem can be expressed as

$$\max_{\substack{\{\mathbf{w}_m\}_{m=1}^M, \\ \left\{\{\mathbf{w}_{nk}\}_{k=1}^K\right\}_{n=1}^N}} \quad \log_2(1 + \text{SINR}_1) \tag{33a}$$

$$\text{s.t.} \qquad \sum_{m=1}^M \|\mathbf{w}_m\| \leq P_M,$$

$$\sum_{k=1}^K \|\mathbf{w}_{nk}\| \leq P_F, \ n \in [1, N], \tag{33b}$$

$$\text{SINR}_m \geq \gamma_m, \ m \in [2, M], \tag{33c}$$

$$\text{SINR}_{nk} \geq \gamma_{nk}, \ n \in [1, N], \ k \in [1, K], \tag{33d}$$

where (33b) characterizes the transmit power constraint at the MBS and FBSs, while (33c) and (33d) represent the QoS requirements of the legitimate MUs and the FUs, respectively. Note that this nonconvex problem can be transformed into an SDP problem, which is convex, by dropping a rank-one constraint that emerges in the transformation process and has

the form of $\text{rank}(\mathbf{X}) = 1$. For more details, please refer to the process of transforming the problem (31) into the problem (32). Upon finishing the optimization, we can obtain the secrecy rate of MU_1. This scheme has been considered by [15], [28].

B. Performance of the Proposed Schemes

Fig. 7 shows the comparison results regarding MU_1's secrecy rate performances with different schemes for $P_F = 40$ dB. Because the wiretapped MU_1 receives more power but the received noise power does not rise when the transmit power of the MBS increases, so we can observe that the secrecy rate performance of all the four schemes grow as the transmit power of MBS increases. It is also shown that the secrecy rates of the proposed three STB schemes always increase faster than the benchmark scheme, especially when the transmit power of the MBS is high (e.g., 42 dBm and 45 dBm). Obviously, the secrecy rate performance of STB-JMF and STB-SMF is better than that of STB-OM. This observation verifies that the deliberately introduced interference is capable of enhancing enhance the secrecy rate performance of the eavesdropped MU. Furthermore, it is worth noting that R_s of STB-SMF slightly outperforms STB-JMF at all the transmit power values of the MBS, since STB-SMF does not consider the QoS of FUs.

Fig. 8 illustrates the secrecy rate of MU_1 for the STB-SMF and STB-JMF schemes under various FBS transmit power values. It is shown that in all schemes the secrecy rate of MU_1 improves as we increase the transmit power of FBS. Note that the benchmark scheme could finally catch up our schemes at the cost of very high FBS power. However, even with little transmit power at each FBS, the proposed schemes can achieve very high secrecy rate, which is in sharp contract to the benchmark scheme. This indicates that STB-SMF and STB-JMF are able to achieve a better R_s without the need to increase the transmit power of each cooperative FBS. To better illustrate the behaviors of STB-SMF and STB-JMF, we plot the secrecy rate of MU_1 versus the transmit power of the MBS and
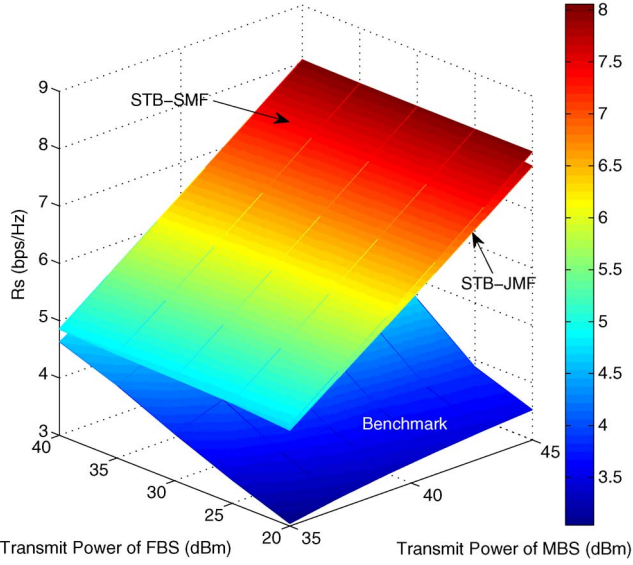
Fig. 9. The secrecy rate region of MU_1 versus the transmit power of the MBS and each FBS.
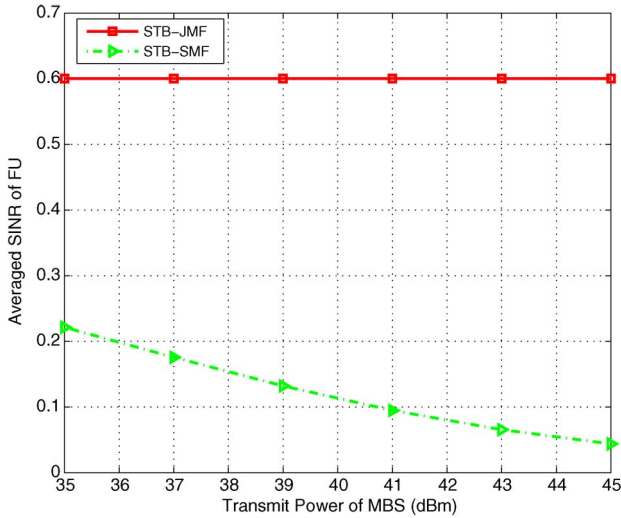

Fig. 10. The receive SINR of FUs versus the transmit power of the MBS.

one cooperative FBS in a three-dimensional figure in Fig. 9, where we can observe the variation tendency of secrecy rate more clearly.

Fig. 10 shows that the averaged SINR of FUs versus the transmit power of the MBS when there is an eavesdropper wiretapping MU_1. Due to symmetry, we only need to evaluate the averaged SINR of the FU in one cooperative femtocell, and we assume the SINR requirement of FUs in STB-JMF scheme is 0.60. From Fig. 10, it is observed that the SINR of FUs in STB-JMF achieves its optimum and is significantly superior to that in STB-SMF. We can also conclude that the SINR constraints (24d) in STB-JMF hold with equality. But for the STB-SMF scheme, as the transmit power of the MBS increases, the SINR of FUs goes down dramatically because more interference is introduced at FUs.

Fig. 11 shows the averaged SINR of each FU versus the transmit power of each FBS when there is an eavesdropper
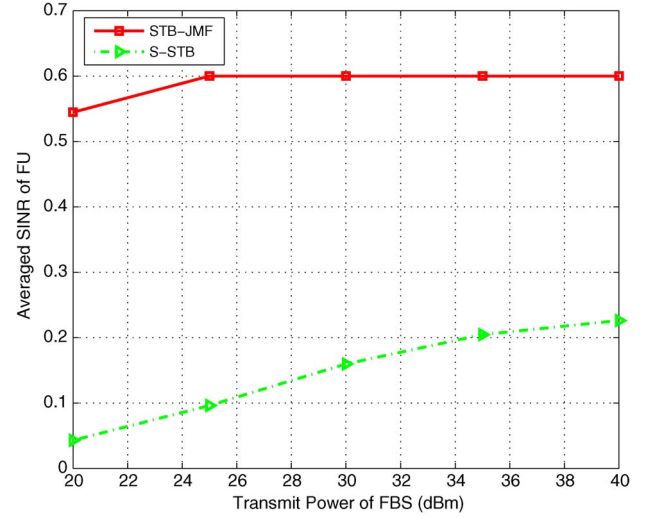

Fig. 11. The receive SINR of FUs versus the transmit power of each FBS.

wiretapping MU_1. Similarly, the SINR requirement of FUs in STB-JMF is set as 0.60. We can also see that STB-JMF has advantages related to the averaged SINR of FU. It is worth noting that when the transmit power of each FBS is relatively low, e.g., around 20 dBm, the SINR constraint in STB-JMF could not be satisfied and thus there is no optimal solution. Hence, we slightly decrease the SINR requirement of FUs to 0.5 to ensure that the optimization problem can be solved. So in Fig. 11, at the point of 20dBm, we can see the averaged SINR decreases slightly. However, from Figs. 10 and 11, we can clearly see that the benefit of STB-JMF is to maximize secrecy rate of the wiretapped MU while maintaining QoS for all related FUs and the intended MU.

C. Impact of Artificial Noise (AN) on the Proposed Schemes

AN plays an important role in the physical layer security and may achieve substantial secrecy performance in some scenarios. In what follows we provide some simulations to verify whether AN is still beneficial for our schemes. To this end, AN is introduced into the STB-OM, the STB-SMF and the STB-JMF in these simulations. Furthermore, except for the beamforming schemes proposed in this paper, we also present two additional schemes for the purpose of comparison in these simulations, which are the "joint beamforming and AN design" as well as the "beamforming design with random AN".

Let us consider the broadcast channel as an example, then the optimization problem of "joint beamforming and AN design" can be expressed as

$$\max_{\{\mathbf{w}_m\}_{m=1}^M, \mathbf{z}} \quad \log(1 + \text{SINR}_1) - \log(1 + \text{SINR}_E) \tag{34a}$$

$$\text{s.t.} \quad \text{SINR}_m \geq \gamma_m, \ m \in [2, M], \tag{34b}$$

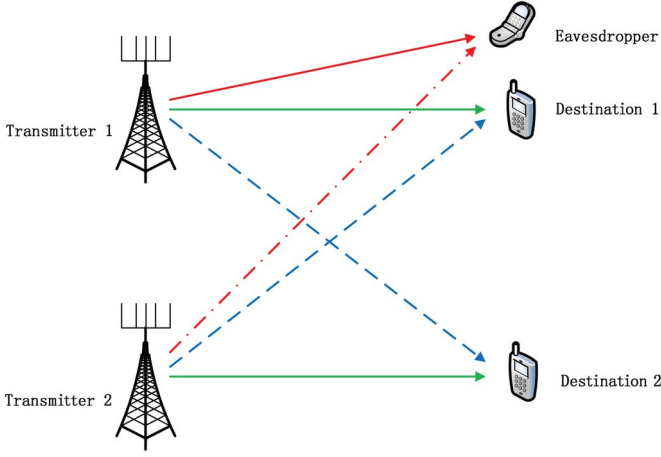$$\sum_{m=1}^M \|\mathbf{w}_m\|^2 + \|\mathbf{z}\| \leq P_M, \tag{34c}$$

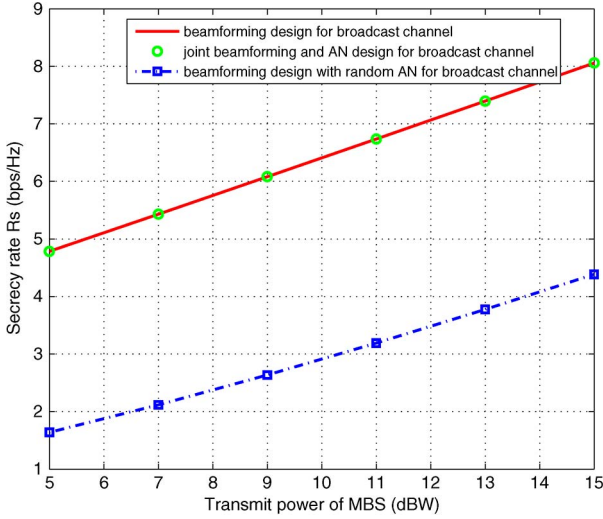Fig. 12. Two-user interference channel with an eavesdropper.

Fig. 14. The secrecy rate versus the transmit power of transmitters in the interference channel with/without AN.

Fig. 13. The secrecy rate versus the transmit power of the MBS in the broadcast channel with/without AN.

where SINR_m and SINR_E are the received SINRs at MU_m and at the eavesdropper E, respectively. These SINRs are given by

$$\text{SINR}_m = \frac{|\mathbf{h}_m \mathbf{w}_m|^2}{\sigma_M^2 + \sum_{q=1, q \neq m}^{M} |\mathbf{h}_m \mathbf{w}_q|^2 + |\mathbf{h}_m \mathbf{z}|^2}, \quad (35)$$

$$\text{SINR}_E = \frac{|\mathbf{h}_E \mathbf{w}_1|^2}{\sigma_E^2 + \sum_{m=2}^{M} |\mathbf{h}_E \mathbf{w}_m|^2 + |\mathbf{h}_E \mathbf{z}|^2}, \quad (36)$$

where $\mathbf{z}$ is the AN vector. Hence, we can solve this optimization problem using Algorithm 1 proposed in this paper. Note that this model mimics the effect of AN in the STB-OM.

On the other hand, considering the "beamforming design with random AN" for the broadcast channel, we transmit random AN and the optimized beamforming vectors at the MBS. The optimization problem is similar to (34) except that the optimization variables are only $\{\mathbf{w}_m\}_{m=1}^{M}$, which do not include $\mathbf{z}$.
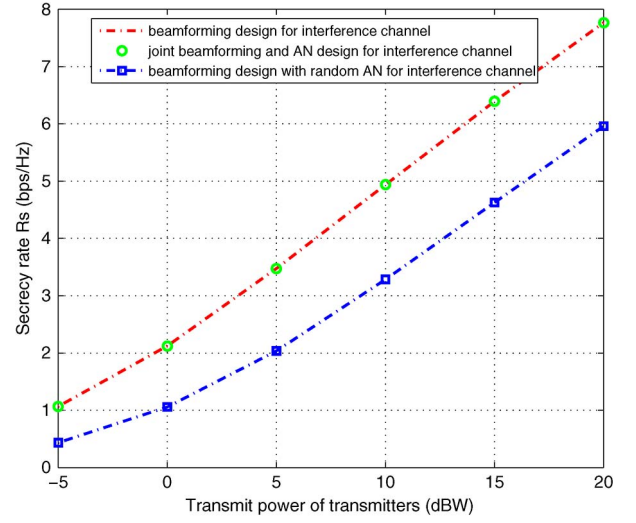
Note that the STB-SMF and the STB-JMF rely on an interference channel. For simplicity, we only consider the typical scenario where there are two transmitters each having four antennas, two receivers each having a single antenna and one single-antenna eavesdropper trying to wiretap one of the transmitters, as shown in Fig. 12.

We present the simulation results for the broadcast channel (as shown in Fig. 13) and for the interference channel (as shown in Fig. 14). From Figs. 13 and 14, we can see that the secrecy rate of the system is almost the same for the proposed schemes whether there exists AN (joint design) or not. Therefore, we can conclude that transmitting AN using the additional $N_M - M$ dimensions does not have any significant impact on the performance of the proposed schemes. This is because in the proposed STB-OM scheme, we assume that there are multiple MUs, thus the MBS has to transmit multiple data flows. Therefore, the STB-OM relies on a broadcast channel. At the eavesdropper, the data from other legitimate MUs can be regarded as interference. For the STB-SMF and the STB-JMF, the data from FBSs can also be treated as interference. These interferences are essentially equivalent to the special ANs imposed on the eavesdropper.

V. CONCLUSION

In this paper, we have investigated the physical-layer security schemes in a two-tier downlink HetNet. On the basis of the two suggested spectrum allocation strategies, the OSA and the SONOSA, three STB schemes, i.e., STB-OM, STB-SMF and STB-JMF, have been proposed to maximize the secrecy rate of the eavesdropped user. According to various considerations of the QoS requirements of the legitimate users, the three proposed secrecy schemes adopt different degrees of collaboration among MBS and its cooperative FBSs. In particular, the complicated nonconvex STB optimization problems have been solved by problem reformulations with SDP and SOCP techniques. Simulation results show the effectiveness of the

proposed schemes. For the future work, it would be interesting to consider the scenario where multiple eavesdroppers and/or targeted MUs exist in the HetNet. Additionally, the robust STB schemes in the context of imperfect CSI may be investigated.

APPENDIX
PROOF OF PROPOSITION 1

The maximization problem (32) can be equivalently transformed into

$$\min_{\substack{\{\mathbf{x}_m\}_{m=1}^{M},\zeta \\ \left\{\{\mathbf{x}_{nk}\}_{k=1}^{K}\right\}_{n=1}^{N}}} \quad \mathrm{Tr}(\mathbf{H}_E \mathbf{X}_1) \tag{37a}$$

$$\text{s.t.} \quad \sum_{m=1}^{M} \mathrm{Tr}(\mathbf{X}_m) \leq P_M \zeta, \tag{37b}$$

$$\sum_{k=1}^{K} \mathrm{Tr}(\mathbf{X}_{nk}) \leq P_F \zeta, \; n \in [1, N], \tag{37c}$$

$$\mathrm{Tr}(\mathbf{H}_m \mathbf{X}_m) \geq \gamma_m \left(\sum_{\substack{q=1,\\q\neq m}}^{M} \mathrm{Tr}(\mathbf{H}_m \mathbf{X}_q) \right. $$
$$\left. + \sum_{n=1}^{N}\sum_{k=1}^{K} \mathrm{Tr}(\mathbf{H}_{n,m}\mathbf{X}_{nk}) + \zeta \right), \; m \in [2, M], \tag{37d}$$

$$\mathrm{Tr}(\mathbf{H}_{n,nk} \mathbf{X}_{nk}) \geq \gamma_{nk} \left(\sum_{\substack{t=1,\\t\neq k}}^{K} \mathrm{Tr}(\mathbf{H}_{n,nk}\mathbf{X}_{nt}) \right. $$
$$+ \sum_{\substack{p=1\\p\neq n}}^{N}\sum_{t=1}^{K} \mathrm{Tr}(\mathbf{H}_{p,nk}\mathbf{X}_{pt}) $$
$$\left. + \sum_{m=1}^{M} \mathrm{Tr}(\mathbf{H}_{nk}\mathbf{X}_m) + \zeta \right), $$
$$n \in [1, N], \; k \in [1, K], \tag{37e}$$

$$\mathrm{Tr}(\mathbf{H}_1 \mathbf{X}_1) \geq \tau \left(\sum_{m=2}^{M} \mathrm{Tr}(\mathbf{H}_m \mathbf{X}_m) \right. $$
$$\left. + \sum_{n=1}^{N}\sum_{k=1}^{K} \mathrm{Tr}(\mathbf{H}_{n,1}\mathbf{X}_{nk}) + \zeta \right), \tag{37f}$$

$$\sum_{m=2}^{M} \mathrm{Tr}(\mathbf{H}_E \mathbf{X}_m) $$
$$+ \sum_{n=1}^{N}\sum_{k=1}^{K} \mathrm{Tr}(\mathbf{H}_{n,E}\mathbf{X}_{nk}) + \zeta = 1, \tag{37g}$$

$$\mathbf{X}_m, \; \mathbf{X}_{nk} \succeq 0, \; \zeta > 0. \tag{37h}$$

It is easy to verify that Problem (37) satisfies the Slater's condition. Then, the Karush-Kuhn-Tucker (KKT) conditions

are the sufficient and necessary optimality conditions. Some KKT conditions needed in the proof are expressed as follows:

$$\mathbf{G}_1^* = a^*\mathbf{I} + \mathbf{H}_E + \sum_{m=2}^{M} b_m^* \gamma_m \mathbf{H}_m $$
$$+ \sum_{n=1}^{N}\sum_{k=1}^{K} c_{nk}^* \gamma_{nk} \mathbf{H}_{nk} - d^* \mathbf{H}_1, \tag{38a}$$

$$\mathbf{G}_1^* \mathbf{X}_1 = 0, \tag{38b}$$

$$\mathbf{G}_m^* = a^*\mathbf{I} + \sum_{q\neq 1,m}^{M} b_q^* \gamma_q \mathbf{H}_q + \sum_{n=1}^{N}\sum_{k=1}^{K} c_{nk}^* \gamma_{nk} \mathbf{H}_{nk} $$
$$+ d^*\tau \mathbf{H}_m + e^* \mathbf{H}_E - b_m^* \mathbf{H}_m, \; m \neq 1, \tag{38c}$$

$$\mathbf{G}_m^* \mathbf{X}_m = 0, \; m \neq 1, \tag{38d}$$

$$\mathbf{G}_{nk}^* = a_n^*\mathbf{I} + \sum_{m=2}^{M} b_m^* \gamma_m \mathbf{H}_{n,m} + \sum_{t\neq k}^{K} c_{nt}^* \gamma_{nt} \mathbf{H}_{n,nt} $$
$$+ \sum_{p\neq n}^{N}\sum_{k=1}^{K} c_{pk}^* \gamma_{pk} \mathbf{H}_{n,pk} + d^*\tau \mathbf{H}_{n,1} - c_{nk}^* \mathbf{H}_{n,nk}, $$
$$n \in [1, N], \; k \in [1, K], \tag{38e}$$

$$\mathbf{G}_{nk}^* \mathbf{X}_{nk} = 0, \; n \in [1, N], \; k \in [1, K], \tag{38f}$$

where $\mathbf{G}_m^* \succeq \mathbf{0}, m \in [1, M], \mathbf{G}_{nk}^* \succeq \mathbf{0}, n \in [1, N], k \in [1, K]$, $a^* \geq 0, a_n^* \geq 0, b_m \geq 0, c_{nk} \geq 0, d \geq 0, e \geq 0$ are the optimal dual variables associated with the constraints $\mathbf{X}_m, \mathbf{X}_{nk} \succeq \mathbf{0}$ and (37b)–(37g), respectively.

Note that (38a), (38c) and (38e) have a similar structure, hence we only focus on the proof of $\mathrm{rank}(\mathbf{X}_1^*) = 1$. $\mathrm{rank}(\mathbf{X}_m^*) = 1, m \in [2, M]$, and $\mathrm{rank}(\mathbf{X}_{nk}^*) = 1, n \in [1, N], k \in [1, K]$, can be proved by using the same method.

If $\mathbf{X}_1^* = \mathbf{0}$, the resultant secrecy rate is zero, which is trivial. Then, we have $\mathbf{X}_1^* \neq \mathbf{0}$. According to (38b), the rank of $\mathbf{G}_1^*$ must be less than or equal to $n - 1$, i.e.,

$$\mathrm{rank}(\mathbf{G}_1^*) \leq n - 1. \tag{39}$$

An important observation is that with the optimal solution, the power constraints (37b) and (37c) have to be satisfied with equality [42]. Therefore, we have $a^* > 0$ and $a_n^* > 0$, $n \in [1, N]$. Let

$$\mathbf{V} = a^*\mathbf{I} + \mathbf{H}_E + \sum_{m=2}^{M} b_m^* \gamma_m \mathbf{H}_m + \sum_{n=1}^{N}\sum_{k=1}^{K} c_{nk}^* \gamma_{nk} \mathbf{H}_{nk} $$
$$= \left(\mathbf{V}^{\frac{1}{2}} \right)^2 \succ \mathbf{0}, \tag{40}$$

where $\mathbf{V}^{\frac{1}{2}} = \left(\mathbf{V}^{\frac{1}{2}} \right)^H \succ 0$, then the rank of $\mathbf{G}_1^*$ can be further expressed as

$$\mathrm{rank}(\mathbf{G}_1^*) = \mathrm{rank}(\mathbf{V} - d^* \mathbf{H}_1) $$
$$= \mathrm{rank}\left(\mathbf{V}^{\frac{1}{2}}(\mathbf{I} - d^* \mathbf{H}_1)\mathbf{V}^{\frac{1}{2}} \right) $$
$$\overset{a}{=} \mathrm{rank}\left(\mathbf{I} - d^* \mathbf{V}^{-\frac{1}{2}}\mathbf{H}_1 \mathbf{V}^{-\frac{1}{2}} \right) $$
$$\geq n - 1, \tag{41}$$

where the equation a holds true relying on the following fact

$$\text{rank}(\mathbf{B}) = \text{rank}(\mathbf{AB}) = \text{rank}(\mathbf{BC}) = \text{rank}(\mathbf{ABC}), \quad (42)$$

where $\mathbf{A}_{m \times m}$ and $\mathbf{C}_{n \times n}$ are both non-singular matrices, and $\mathbf{B}_{m \times n}$ is an arbitrary matrix.

From (39) and (41), we have $\text{rank}(\mathbf{G}_1^*) = n - 1$. According to (38b), we have $\text{rank}(\mathbf{X}_1^*) \leq \dim(\mathcal{N}(\mathbf{G}_1^*)) = n - \text{rank}(\mathbf{G}_1^*) = 1$. Since $\mathbf{X}_1^* \neq \mathbf{0}$, we obtain $\text{rank}(\mathbf{X}_1^*) = 1$.

Following the same procedure, we are capable of proving that $\text{rank}(\mathbf{X}_m^*) = 1$, $m \in [2, M]$, and $\text{rank}(\mathbf{X}_{nk}^*) = 1$, $n \in [1, N]$, $k \in [1, K]$. Hence, we have completed the proof.

ACKNOWLEDGMENT

REFERENCES

[1] "Cisco Visual Networking Index: Global Mobile Data Traffic Forecast, 2013–2018," White Paper, Cisco, Feb. 2014. [Online]. Available: http://www.cisco.com/c/en/us/solutions/collateral/service-provider/visual-networking-index-vni/white_paper_c11-520862.pdf

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

[3] V. Chandrasekhar, J. Andrews, and A. Gatherer, "Femtocell networks: A survey," *IEEE Commun. Mag.*, vol. 46, no. 9, pp. 59–67, Sep. 2008.

[4] W.-C. Liao, M. Hong, Y.-F. Liu, and Z.-Q. Luo, "Base station activation and linear transceiver design for optimal resource management in heterogeneous networks," *IEEE Trans. Signal Process.*, vol. 62, no. 15, pp. 3939–3952, Aug. 2014.

[5] A. Damnjanovic *et al.*, "A survey on 3GPP heterogeneous networks," *IEEE Wireless Commun.*, vol. 18, no. 3, pp. 10–21, Jun. 2011.

[6] A. Ghosh *et al.*, "Heterogeneous cellular networks: From theory to practice," *IEEE Commun. Mag.*, vol. 50, no. 6, pp. 54–64, Jun. 2012.

[7] I. Csiszar and J. Korner, "Broadcast channels with confidential messages," *IEEE Trans. Inf. Theory*, vol. 24, no. 3, pp. 339–348, May 1978.

[8] J. Barros and M. R. D. Rodrigues, "Secrecy capacity of wireless channels," in *Proc. IEEE ISIT*, Seattle, WA, USA, Jul. 2006, pp. 356–360.

[9] C. E. Shannon, "Communication theory of secrecy systems," *Bell. Syst. Tech. J.*, vol. 28, no. 4, pp. 656–715, Oct. 1949.

[10] Y.-S. Shiu, S.-Y. Chang, H.-C. Wu, S.-H. Huang, and H.-H. Chen, "Physical layer security in wireless networks: A tutorial," *IEEE Wireless Commun.*, vol. 18, no. 2, pp. 66–74, Apr. 2011.

[11] Y. Liang, H. V. Poor, and S. Shamai, "Secure communication over fading channels," *IEEE Trans. Inf. Theory*, vol. 54, no. 6, pp. 2470–2492, Jun. 2008.

[12] P. Gopala, L. Lai, and H. El Gamal, "On the secrecy capacity of fading channels," *IEEE Trans. Inf. Theory*, vol. 54, no. 10, pp. 4687–4698, Oct. 2008.

[13] A. Hero, "Secure space-time communication," *IEEE Trans. Inf. Theory*, vol. 49, no. 12, pp. 3235–3249, Dec. 2003.

[14] R. Bustin, R. Liu, H. V. Poor, and S. Shamai, "An MMSE approach to the secrecy capacity of the MIMO Gaussian wiretap channel," *EURASIP J. Wireless Commun. Netw.*, vol. 2009, pp. 1–8, Mar. 2009.

[15] A. Mukherjee and A. L. Swindlehurst, "Fixed-rate power allocation strategies for enhanced secrecy in MIMO wiretap channels," in *Proc. 10th IEEE SPAWC*, Perugia, Italy, Jun. 2009, pp. 344–348.

[16] T. Liu and S. Shamai, "A note on the secrecy capacity of the multiple-antenna wiretap channel," *IEEE Trans. Inf. Theory*, vol. 55, no. 6, pp. 2547–2553, Jun. 2009.

[17] A. Khisti and G. W. Wornell, "Secure transmission with multiple antennas-part II: The MIMOME wiretap channel," *IEEE Trans. Inf. Theory*, vol. 56, no. 11, pp. 5515–5532, Nov. 2010.

[18] F. Oggier and B. Hassibi, "The secrecy capacity of the MIMO wiretap channel," *IEEE Trans. Inf. Theory*, vol. 57, no. 8, pp. 4961–4972, Aug. 2011.

[19] K. Cumanan, Z. Ding, B. Sharif, G. Y. Tian, and K. Leung, "Secrecy rate optimizations for a MIMO secrecy channel with a multiple-antenna eavesdropper," *IEEE Trans. Veh. Technol.*, vol. 63, no. 4, pp. 1678–1690, May 2014.

[20] A. Khisti, A. Tchamkerten, and G. Wornell, "Secure broadcasting over fading channels," *IEEE Trans. Inf. Theory*, vol. 54, no. 6, pp. 2453–2469, Jun. 2008.

[21] E. Ekrem and S. Ulukus, "The secrecy capacity region of the Gaussian MIMO multi-receiver wiretap channel," *IEEE Trans. Inf. Theory*, vol. 57, no. 4, pp. 2083–2114, Apr. 2011.

[22] R. Liu, T. Liu, H. V. Poor, and S. Shamai, "A vector generalization of Costa's entropy-power inequality with applications," *IEEE Trans. Inf. Theory*, vol. 56, no. 4, pp. 1865–1879, Apr. 2010.

[23] Y. Liang and H. V. Poor, "Multiple-access channels with confidential messages," *IEEE Trans. Inf. Theory*, vol. 54, no. 3, pp. 976–1002, Mar. 2008.

[24] E. Tekin and A. Yener, "The Gaussian multiple access wire-tap channel," *IEEE Trans. Inf. Theory*, vol. 54, no. 12, pp. 5747–5755, Dec. 2008.

[25] R. Liu, Y. Liang, and H. V. Poor, "Fading cognitive multiple-access channels with confidential messages," *IEEE Trans. Inf. Theory*, vol. 57, no. 8, pp. 4992–5005, Aug. 2011.

[26] R. Liu, I. Maric, P. Spasojevic, and R. Yates, "Discrete memoryless interference and broadcast channels with confidential messages: Secrecy rate regions," *IEEE Trans. Inf. Theory*, vol. 54, no. 6, pp. 2493–2507, Jun. 2008.

[27] S. Agrawal and S. Vishwanath, "On the secrecy rate of interference networks using structured codes," in *Proc. IEEE ISIT*, Seoul, Korea, Jun. 2009, pp. 2091–2095.

[28] S. A. A. Fakoorian and A. L. Swindlehurst, "MIMO interference channel with confidential messages: Achievable secrecy rates and precoder design," *IEEE Trans. Inf. Forens. Security*, vol. 6, no. 3, pp. 640–649, Sep. 2011.

[29] J. Ni *et al.*, "Robust coordinated beamforming for secure miso interference channels with bounded ellipsoidal uncertainties," *IEEE Wireless Commun. Lett.*, vol. 2, no. 2, pp. 407–410, Aug. 2013.

[30] D. Lopez-Perez *et al.*, "Enhanced intercell interference coordination challenges in heterogeneous networks," *IEEE Wireless Commun.*, vol. 18, no. 3, pp. 22–30, Jun. 2011.

[31] D. Niyato and E. Hossain, "Competitive pricing for spectrum sharing in cognitive radio networks: Dynamic game, inefficiency of nash equilibrium, and collusion," *IEEE J. Sel. Areas Commun.*, vol. 26, no. 1, pp. 192–202, Jan. 2008.

[32] C. H. M. De Lima, M. Bennis, and M. Latva-aho, "Coordination mechanisms for self-organizing femtocells in two-tier coexistence scenarios," *IEEE Trans. Wireless Commun.*, vol. 11, no. 6, pp. 2212–2223, Jun. 2012.

[33] D. Lopez-Perez, X. Chu, A. Vasilakos, and H. Claussen, "On distributed and coordinated resource allocation for interference mitigation in self-organizing LTE networks," *IEEE/ACM Trans. Netw.*, vol. 21, no. 4, pp. 1145–1158, Aug. 2013.

[34] D. Lopez-Perez, X. Chu, A. Vasilakos, and H. Claussen, "Power minimization based resource allocation for interference mitigation in OFDMA femtocell networks," *IEEE J. Sel. Areas Commun.*, vol. 32, no. 2, pp. 333–344, Feb. 2014.

[35] F. Pantisano, M. Bennis, W. Saad, M. Debbah, and M. Latva-Aho, "Improving macrocell-small cell coexistence through adaptive interference draining," *IEEE Trans. Wireless Commun.*, vol. 13, no. 2, pp. 942–955, Feb. 2014.

[36] R. Heath, M. Kountouris, and T. Bai, "Modeling heterogeneous network interference using Poisson point processes," *IEEE Trans. Signal Process.*, vol. 61, no. 16, pp. 4114–4126, Aug. 2013.

[37] M. Hanif, L. Tran, M. Juntti, and S. Glisic, "On linear precoding strategies for secrecy rate maximization in multiuser multiantenna wireless networks," *IEEE Trans. Signal Process.*, vol. 62, no. 14, pp. 3536–3551, May 2014.

[38] G. Geraci, S. Singh, J. Andrews, J. Yuan, and I. Collings, "Secrecy rates in broadcast channels with confidential messages and external eavesdroppers," *IEEE Trans. Wireless Commun.*, vol. 13, no. 5, pp. 2931–2943, May 2014.

[39] G. Zheng, L.-C. Choo, and K.-K. Wong, "Optimal cooperative jamming to enhance physical layer security using relays," *IEEE Trans. Signal Process.*, vol. 59, no. 3, pp. 1317–1322, Mar. 2011.

[40] A. Kalantari, S. Maleki, G. Zheng, S. Chatzinotas, and B. Ottersten, "Joint power control in wiretap interference channels," *IEEE Trans. Wireless Commun.*, to be published. DOI: 10.1109/TWC.2015.2412531.

[41] A. S. Vishwanathan, A. J. Smola, and S. V. N. Vishwanathan, "Kernel methods for missing variables," in *Proc. 10th Int. Workshop Artif. Intell. Stat.*, Barbados, Jan. 2005, pp. 325–332.

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

[43] M. Grant and S. Boyd, "CVX: Matlab Software for Disciplined Convex Programming, Version 1.21 (2011)," 2010. [Online]. Available: cvxr.com/cvx

[44] A. Sheikholeslami, D. Goeckel, H. Pishro-Nik, and D. Towsley, "Physical layer security from inter-session interference in large wireless networks," in *Proc. IEEE INFOCOM*, Orlando, FL, USA, Mar. 2012, pp. 1179–1187.

[45] S. Yang, T. Lv, and L. Hanzo, "Semidefinite programming relaxation based virtually antipodal detection for MIMO systems using Gray-coded high-order QAM," *IEEE Trans. Veh. Tech.*, vol. 62, no. 4, pp. 1667–1677, May 2013.

[46] K. Cheung, S. Yang, and L. Hanzo, "Achieving maximum energy-efficiency in multi-relay OFDMA cellular networks: A fractional programming approach," *IEEE Trans. Commun.*, vol. 61, no. 7, pp. 2746–2757, Jul. 2013.

[47] K. Cheung, S. Yang, and L. Hanzo, "Spectral and energy spectral efficiency optimization of joint transmit and receive beamforming based multi-relay MIMO-OFDMA cellular networks," *IEEE Trans. Wireless Commun.*, vol. 13, no. 11, pp. 6147–6165, Nov. 2014.

[48] Z. Luo, W. K. Ma, A. M.-C. So, Y. Ye, and S. Zhang, "Semidefinite relaxation of quadratic optimization problems," *IEEE Signal Process Mag.*, vol. 27, no. 3, pp. 20–34, May 2010.

[49] A. Ben-Tal and A. Nemirovski, *Lectures on Modern Convex Optimization: Analysis, Algorithms, and Engineering Applications*. ser. MPS-SIAM Series on Optimization,   Philadelphia, PA, USA: SIAM, 2001.

[50] T. M. Nguyen, T. Quek, and H. Shin, "Opportunistic interference alignment in MIMO femtocell networks," in *Proc. IEEE ISIT*, Cambridge, MA, USA, Jul. 2012, pp. 2631–2635.

[51] "Guidelines for evaluation of radio transmission technologies for IMT-2000," ITU-R Recommendation, Geneva, Switzerland, ITU-R Recommendation M.1225, Feb. 1997.

Hui Gao (S'10–M'13) received the B. Eng. degree in information engineering and the Ph.D. degree in signal and information processing from Beijing University of Posts and Telecommunications (BUPT), Beijing, China, in July 2007 and July 2012, respectively. From May 2009 to June 2012, he also served as a Research Assistant for the Wireless and Mobile Communications Technology R&D Center, Tsinghua University, Beijing, China. From April 2012 to June 2012, he visited Singapore University of Technology and Design (SUTD), Singapore, as a Research Assistant. From July 2012 to February 2014, he was a Postdoc Researcher with SUTD. He is now with the School of Information and Communication Engineering, Beijing University of Posts and Telecommunications (BUPT), as an Assistant Professor. His research interests include massive MIMO systems, cooperative communications, ultra-wideband wireless communications.

Tiejun Lv (M'08–SM'12) received the M.S. and Ph.D. degrees in electronic engineering from the University of Electronic Science and Technology of China (UESTC), Chengdu, China, in 1997 and 2000, respectively. From January 2001 to December 2002, he was a Postdoctoral Fellow with Tsinghua University, Beijing, China. From September 2008 to March 2009, he was a Visiting Professor with the Department of Electrical Engineering, Stanford University, Stanford, CA, USA. He is currently a Full Professor with the School of Information and Communication Engineering, Beijing University of Posts and Telecommunications (BUPT). He is the author of more than 200 published technical papers on the physical layer of wireless mobile communications. His current research interests include signal processing, communications theory and networking. He is also a Senior Member of the Chinese Electronics Association. He was the recipient of the Program for New Century Excellent Talents in University Award from the Ministry of Education, China, in 2006.

Shaoshi Yang (S'09–M'13) received the B.Eng. degree in information engineering from Beijing University of Posts and Telecommunications (BUPT), China, in 2006, the first Ph.D. degree in electronics and electrical engineering from University of Southampton, U.K., in 2013, and the second Ph.D. degree in signal and information processing from BUPT in 2014. Since 2013, he has been a Postdoctoral Research Fellow with the University of Southampton, U.K., and from 2008 to 2009, he was an Intern Research Fellow with the Intel Labs China, Beijing, where he focused on channel quality indicator channel design for mobile WiMAX (802.16 m). His research interests include MIMO signal processing, green radio, heterogeneous networks, cross-layer interference management, convex optimization and its applications. He has published in excess of 30 research papers in IEEE journals and conferences.

He has received a number of academic and research awards, including the PMC-Sierra Telecommunications Technology Scholarship at BUPT, the Electronics and Computer Science (ECS) Scholarship of University of Southampton and the Best Ph.D. Thesis Award of BUPT. He serves as a TPC member of a number of IEEE conferences and journals, including IEEE ICC, PIMRC, ICCVE, HPCC and IEEE JOURNAL ON SELECTED AREAS IN COMMUNICATIONS. He is also a Junior Member of the Isaac Newton Institute for Mathematical Sciences, Cambridge University, U.K. (https://sites.google.com/site/shaoshiyang/)