This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TWC.2019.2912611, IEEE Transactions on Wireless Communications

Secure Communications in Tiered 5G Wireless Networks with Cooperative Jamming

Yan Huo, *Member, IEEE,* Xin Fan, Liran Ma, *Member, IEEE,* Xiuzhen Cheng, *Fellow, IEEE,* Zhi Tian, *Fellow, IEEE,* and Dechang Chen

***Abstract*—Cooperative jamming is deemed as a promising physical layer based approach to secure wireless transmissions in the presence of eavesdroppers. In this paper, we investigate cooperative jamming in a two-tier 5G heterogeneous network (HetNet), where the macro base stations (MBSs) at the macrocell tier are equipped with large-scale antenna arrays to provide space diversity and the local base stations (LBSs) at the local cell tier adopt non-orthogonal multiple access (NOMA) to accommodate dense local users. In the presence of imperfect channel state information, we propose three robust secrecy transmission algorithms that can be applied to various scenarios with different security requirements. The first algorithm employs robust beamforming (RBA) that aims to optimize the secrecy rate of a marco user (MU) in a macrocell. The second algorithm provides robust power allocation (RPA) that can optimize the secrecy rate of a local user (LU) in a local cell. The third algorithm tackles a robust joint optimization (RJO) problem across tiers that seeks the maximum secrecy sum rate of a target MU and a target LU robustly. We employ convex optimization techniques to find feasible solutions to these highly non-convex problems. Numerical results demonstrate that the proposed algorithms are highly effective in improving the secrecy performance of a two-tier HetNet.**

***Index Terms*—Heterogeneous networks; cooperative jamming; physical-layer security; collusive eavesdropping; non-orthogonal multiple access; massive MIMO; secrecy rate; imperfect channel state information.**

I. Introduction

Wireless networking has contributed significantly to the ongoing societal developments such as social networks and smart cities. In turn, these developments place great challenges to the design of the fifth generation (5G) and future wireless systems. Particularly, there is an increasing need to deliver on-demand information and various services wirelessly, giving rise to mobile big data. Additionally, it is predicted that human-centric communications would be complemented by a huge increase in device-to-device (D2D) communications (e.g., Internet of Things). The demand on mobile big data and the coexistence of human-centric and D2D applications require 5G wireless systems to be modular, flexible, and extensible. To accommodate these rising needs, tiered heterogeneous networking has been proposed as a promising technology for 5G wireless systems [1]–[3].

An example of a two-tier heterogeneous network (HetNet) under our consideration is illustrated in Fig. 1, in which the macrocell tier consists of one or more macrocell base stations (MBSs) providing access services to macro users (MUs) and the local cell tier consists of a number of local base stations (LBSs) within each macrocell to serve their local users (LUs). This architecture provides an excellent platform to accommodate emerging wireless technologies such as massive multiple-input multiple-output (MaMIMO) [4] and non-orthogonal multiple access (NOMA) [5], offering greating potential for achieving high spectrum efficiency and energy efficiency [6], [7].

However, the rich diversity of devices and applications of HetNets poses unprecedented security challenges. Compared to conventional cellular networks, tiered HetNets are more vulnerable to wireless eavesdropping attacks [8]. Consequently, it is critical to design and implement eavesdropping countermeasures to secure wireless transmissions in a HetNet. Note that although confidentiality can be directly achieved by encryption, there are numerous operating scenarios where key distribution, computational complexity, or management issues prevent the establishment or use of shared keys for encryption.

It has been recognized that the physical layer of wireless systems can enable novel ways to secure transmissions. In this paper, we focus on secure transmissions provided by *cooperative jamming*, where the core idea is to degrade the received signal quality of an eavesdropper by jamming signals emitted from a friendly jammer [9], [10]. There has been considerable work on cooperative jamming for traditional network architectures [11]–[14]. In [11], a power allocation strategy is presented to maximize the secrecy rate for point-to-point wireless communications with multiple eavesdroppers. Then, the secrecy rate of a multiple-input-single-output (MISO) system with a multiple-antenna eavesdropper is investigated in [12], and a secure transmission strategy for multi-point to multi-point wireless networks is investigated in [13] using a non-convex game approach. Considering a relay communication system with multiple eavesdroppers, the authors in

Manuscript received 16 April 2018; revised 7 October 2018 and 30 January 2019; accepted 13 April 2019. This work was supported by the Fundamental Research Funds for the Central Universities (Grant No. 2019JBM001) and the National Science Foundation of the US (Grant No. AST-1443858, AST-1443916, AST-1547329, and OAC-1829553).

Disclaimer: The views expressed are those of the authors and do not necessarily reflect the official views of the Uniformed Services University of the Health Sciences, the Department of Defense, or the U.S. Government.

Y. Huo and X. Fan are with the School of Electronics and Information Engineering, Beijing Jiaotong University, Beijing, China. E-mails: yhuo@bjtu.edu.cn, fanxin@bjtu.edu.cn.

L. Ma is with the Department of Computer Science, Texas Christian University, Fort Worth, Texas, USA. E-mail: l.ma@tcu.edu.

X. Cheng is with the Department of Computer Science, The George Washington University, Washington, DC, USA. E-mail: cheng@gwu.edu.

Z. Tian is with the Department of Electrical & Computer Engineering, George Mason University, Fairfax, VA, USA. E-mail: ztian1@gmu.edu.

D. chen is with the Department of Preventive Medicine and Biostatistics, Uniformed Services University of the Health Sciences, Bethesda, MD 20814 USA. E-mail: dechang.chen@usuhs.edu.

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TWC.2019.2912611, IEEE Transactions on Wireless Communications

[14] have discussed the optimal jamming selection issue and designed the optimal beamforming vectors to achieve secure transmission in [15].

For research on secure heterogeneous transmission, the authors first introduce physical layer security (PLS) to HetNets in [16]; they propose three secrecy transmission beamforming algorithms to maximize the secrecy rate of a legitimate user based on a pre-fixed spectrum allocation in a fixed area. The authors in [17] exploit stochastic geometry theory to derive the closed-form expression for the secrecy outage probability in HetNets, and claim that the secrecy performance could be improved by deploying more low power transmitters in environments with severe path loss. Heterogeneous networks are the basic framework of 5G communications. Thus, it is especially important to study secure data transmission and sharing in such heterogeneous networks. However, little has been done to investigate the use of cooperative jamming for physical layer security in tiered HetNets.

We investigate cooperative jamming in a two-tier HetNet system as depicted in Fig. 1, where an MaMIMO-enabled MBS and multiple NOMA-enabled LBSs are employed to serve legitimate MUs and LUs, respectively. To the best of our knowledge, we are the first to explore cooperative jamming under such a network structure. In our study, we adopt two realistic assumptions that set apart from previous work: i) channel state information (CSI) is imperfectly known; and ii) multiple eavesdroppers may collude. To overcome the challenges brought by these two assumptions, we establish a deterministic error model to characterize the uncertainty of imperfectly known CSI and model the colluding eavesdroppers as a super eavesdropper with multiple antennas.

Based on these two modeling approaches, we propose three robust secrecy transmission algorithms that can be applied to various scenarios with different security requirements. Our contributions are as follows.

- Firstly, we propose a robust beamforming algorithm (RBA) that operates at the macrocell tier. For multiple macro eavesdroppers (MEs) who wiretap a MBS to get the information intended for a particular macro user, RBA aims to maximize the secrecy rate of the target MU subject to the QoS constraints of other MUs. In RBA, we only consider the interference caused by other MUs rather than LBSs because of the low transmit power of LBSs. The novelty of the RBA lies in the transformation of the original non-convex problem of the secrecy rate maximization problem into a second-order cone program (SOCP) by invoking a first-order Taylor approximation.
- Secondly, we propose a robust power allocation algorithm (RPA) that operates at the local cell tier. Considering the transmission distance and radio power, the interference of an LU in a local cell should be derived from other LUs of the same cell and the MBS. The proposed RPA focuses on optimizing the secrecy rate of a target LU based on the beamforming vectors of the MBS under the QoS constraints of other LUs in the same local cell. The beamforming vectors of the MBS can be obtained via applying RBA or zero-forcing beamforming (ZFBF). We transform the original non-convex problem into a convex one.
- Lastly, we study a two-tier scenario, i.e., simultaneous secure transmission for both the macrocell tier and the local cell tier. Different from the aforementioned two schemes for intra-tier secure transmission, we propose a robust joint optimization (RJO) algorithm that intends to maximize the secrecy sum rate of both a target MU and a target LU across both tiers. The RJO takes into account the QoS requirements of all MUs and LUs in the system. Applying the D.C. (difference of convex functions) approximation programming [18], we solve this non-convex optimization problem by an iterative algorithm. In essence, the RJO algorithm employs users' cooperation in both tiers to achieve the overall physical layer security of multiple users.

The rest of the paper is organized as follows. Related work is described in Section II. Our heterogeneous network architecture shown in Fig. 1 and the corresponding data transmission models for the macrocell and the local cells are detailed in Section III. We propose three robust secure transmission algorithms in Section IV based on cooperative jamming, and report our numerical results to demonstrate the effectiveness of these algorithms in Section V. Concluding remarks on future research are provided in Section VI.

Notations: Bold upper and lower case letters denote matrices and vectors, respectively. The expectation operation, Hermitian transpose, trace, and Euclidean norm of a matrix are depicted as $\mathbb{E}[\cdot]$, $(\cdot)^H$, $\mathrm{Tr}(\cdot)$, and $\|\cdot\|$, respectively; $\mathbf{x} \in \mathbb{C}^{i\times j}$ represents that $\mathbf{x}$ is a complex matrix with i rows and j columns; an integer set $\{1, 2, ..., M\}$ is abbreviated as $[1, M]$; and $\mathcal{N}(\mu, \sigma^2)$ and $\mathcal{CN}(\mu, \sigma^2)$ denote a Gaussian variable and a complex Gaussian variable with mean μ and variance σ^2, respectively. For convenience, we provide a list of abbreviations in **Table I**.

TABLE I: List of the major abbreviations

Abbreviation	Definition
ME	A macro eavesdropper who wiretap a MBS
LE	A local eavesdropper who wiretap a LBS
RBA	Robust beamforming algorithm
RPA	Robust power allocation algorithm
RJO	Robust joint optimization
CSI	Channel state information
CCI	Co-channel interference
CSCG	Circularly symmetric complex Gaussian
ZFBF	Zero-forcing beamforming
SOCP	Second-order cone program
MaMIMO	Massive multiple-input multiple-output

II. Related Work

Early studies on PLS can be traced back to Shannon's secure communication theory [19] and Wyner's secrecy analyses on wiretap channels [20]. PLS intends to exploit characteristics of the wireless medium to ensure that eavesdroppers cannot decode private information. It can provide an additional layer of protection without compromising existing cryptography-based security mechanisms [9]. Existing studies on PLS mainly focus on traditional networks such as point-to-point transmissions

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TWC.2019.2912611, IEEE Transactions on Wireless Communications

or single-cell communications [21]. A number of techniques have been developed based on channel characteristics [22], [23], error correction coding [24], [25], or signal processing [26], [27]. These studies validate that PLS can provide reliable transmissions with certain secrecy rates in many practical scenarios [28], especially for low-end devices with limited computational capability.

Cooperative jamming is a signal-based strategies that is first presented in [26] to achieve secure transmissions. With this strategy, a legitimate user transmits information-bearing signals while a neighbor node (called the friendly jammer) transmits artificial noise (AN) signals to interfere with the eavesdroppers' reception [29]. This idea is extended to subsequent investigations from different perspectives [12], [30]–[35]. In [30], the authors have analyzed the achievable rate based on AN for downlink transmissions from a base station with multiple antennas to a user with a single antenna. They also suggest that more AN power should be transmitted when the number of eavesdroppers grows. Considering single- and multi-antenna scenarios, the authors have analyzed the impact of the number of cooperative jammers on secrecy performance in [31]. In [32], the authors develop a friendly jamming strategy to keep information from being wiretapped by an untrusted relay. From the perspective of signal generation, an orthogonal jamming signal is employed in [33] to interfere with the eavesdroppers without affecting the legitimate users. Besides, the authors in [34] focus on secrecy performance via selecting different jammers while the authors in [35] propose a power allocation scheme to maximize the system secrecy capacity subject to power constraints.

Yet, most of the existing secrecy optimization designs hinge on perfect CSI of both the legitimate users and the eavesdroppers. In fact, it is clearly impractical to obtain the perfect CSI due to two reasons. On one hand, weak channel reciprocity and non-robust estimation algorithms cause non-negligible estimation errors, yielding only inaccurate CSI. The impact of these errors on secrecy rate are studied and a series of power allocation strategies to maximize the worst-case secrecy rate are designed [36]–[38]. In [39], a robust cooperative jamming scheme is designed in the case of eavesdroppers with uncertain channel state, where the secrecy rate maximization problem is solved by using a Stackelberg game. On the other hand, passive wiretapping has to deal with completely unknown CSI of the eavesdroppers. To tackle this challenge, various mathematical methods are introduced into the PLS design [40]–[44]. For examples, the stochastic geometry theory [40] is employed in [41] to derive the secrecy outage probability; this work is extended by the authors in [42] who propose a compromised secrecy region (CSR) minimization scheme; and [43], [44] put forward a novel cooperative jamming scheme based on space power synthesis.

Although PLS research has made great progress in traditional wireless networks, it is still in its infancy for 5G wireless systems [45]. In [46], the authors have analyzed the connection probability and secrecy probability of an arbitrarily located user in a HetNet and then evaluated the secrecy throughputs of the whole system and a random user. In [47], a tractable upper bound of the secrecy outage probability is provided for a random user in a MaMIMO aided HetNet; and physical layer-based secure strategies are put forward in [48] for MaMIMO by using matched filter precoding and AN generation. Besides, in [49], the maximization of the secrecy sum rate is studied in a NOMA-enabled single-input single-output (SISO) system, and the authors have demonstrated a feasible region of the transmit power based on all users' QoS requirements. Furthermore, the NOMA-based secrecy transmissions are investigated using stochastic geometry theory in multiple-antenna wireless networks [50]. Despite many works on PLS in 5G networks, little has been done for an MaMIMO-NOMA enabled HetNet, which motivates our work in this paper.

III. System Model and Preliminaries

A. System Description

We consider a two-tier HetNet similar to the one adopted by [7], depicted in Fig. 1, which is composed of a macrocell and several local cells. An MBS with a large-scale antenna array is located at the center of the macrocell. It can provide various services for its legitimate MUs. Each MU communicates with the MBS through its single antenna. To accommodate densely deployed MUs, the MBS exploits space diversity via MaMIMO technology to improve spectral efficiency.

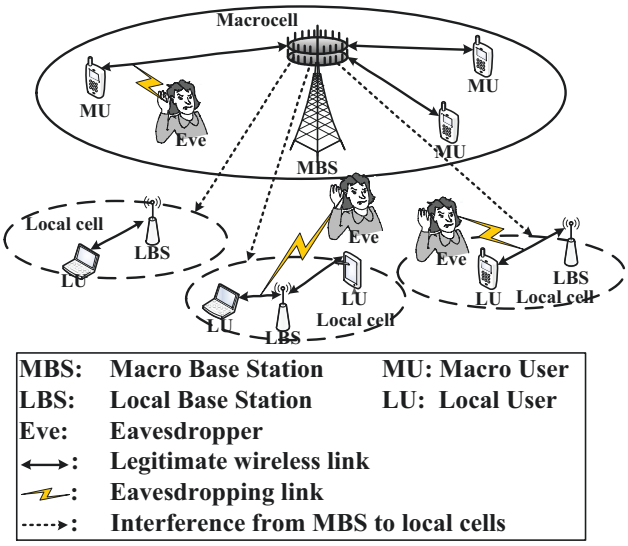


Fig. 1: A heterogeneous network model.

Numerous single-antenna LBSs are scattered within the area covered by the macrocell. The deployment of the LBSs may be ultra-dense to meet the need for high capacity and ubiquitous coverage. Meanwhile, there also exist a number of LUs covered by each LBS. If the number of LUs is too large, LUs' experience may be degraded due to insufficient spectrum resources. To tackle this challenge, we assume that LBSs in our model can exploit the NOMA technique to improve spectral efficiency and utilize successive interference cancellation (SIC) to combat the inter-user interference resulted from the non-orthogonal spectrum use. Note that LBSs transmit at much lower power than that of the MBS and they can communicate with each other directly to achieve cooperative resource allocation.

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TWC.2019.2912611, IEEE Transactions on Wireless Communications

This heterogeneous network model greatly increases the security vulnerability of information transmissions due to the open wireless environment and the flexible user access. Several single-antenna eavesdroppers (abbreviated as Eves in Fig.1) may exist in both the macrocell and the local cells. Generally speaking, these eavesdroppers may passively wiretap private information of either an MU or an LU individually in a non-colluding case. Yet, an even worse scenario occurs when there exist collusive eavesdroppers that can exchange illegally acquired information with each other to enhance their wiretapping capability.

Note that the HetNet model in [7] considers sparsely deployed LUs within a local cell with perfect downlink channel state information, whereas our model assumes the existence of densely deployed LUs in a local cell, imperfect channel state information, and NOMA-incurred interference among LUs. Moreover, our study focuses on the secrecy performance of the HetNet while [7] investigates coverage, spectral efficiency, and energy efficiency.

In this paper, we employ cooperative jamming to prevent Eves from eavesdropping on target users. The key idea is to purposely exploit the inter-user interference emitted from MBSs or LBSs to cooperative legitimate users to degrade the channel quality of the eavesdroppers, without having to generate intentional jamming signals. As we know, intentional jamming of eavesdroppers comes at the cost of extra power emission and hence lowered power efficiency, which can be effectively avoided when treating inter-user interference as cooperative jamming. We can deliberately design one user's information-bearing signals as jamming signals targeted at eavesdroppers. Therefore, we exploit inter-user jamming signals to achieve secure physical layer transmission with power efficiency. For clear exposition of the HetNet structure in Fig. 1, we provide the major variables and their semantic meanings in Table II.

TABLE II: List of the major variables

Variable	Definition
M	The number of MUs
K_M	The number of antennas of the MBS
K_L	The number of LBSs
L	The number of LUs covered by each LBS
P_M	The maximum transmit power of an MBS
P_L	The maximum transmit power of each LBS
MU_m	The mth MU
ME_n	The nth Eve to eavesdrop the information sent to MU_m
LU_l	The lth LU
LE_n	The nth Eve to eavesdrop the information sent to LU_l
$\mathbf{h}_m$	The channel vector from the MBS to MU_m
$\mathbf{h}_{\text{ME}_n}$	The channel vector from the MBS to ME_n
$\mathbf{g}_l$	The channel vector from the MBS to LU_l
$\mathbf{g}_{\text{LE}_n}$	The channel vector from the MBS to LE_n
h_l	The channel gain from LBS to LU_l
h_{LE_n}	The channel gain from LBS to LE_n

B. Uncertainty of Channel Estimation

The transmission performance greatly depends on the accuracy of channel estimation. Various channel estimation techniques can be employed, such as data-aided, blind and semi-blind techniques [51], [52]. Obviously, all channel estimation methods introduce errors. In this case, one can only obtain imperfect CSI, which means that the estimated channel characteristic, $\mathbf{h}$ (or h), is partially uncertain. We can employ an Euclidean ball (or circle) to characterize the uncertainty for the legitimate channels as well as the wiretapping channels, i.e.,

$$\mathcal{H} = \{\mathbf{h} \mid \|\mathbf{h} - \hat{\mathbf{h}}\| \leq \theta\} \text{ (or } \mathcal{H} = \{h \mid |h - \hat{h}| \leq \theta\}), \quad (1)$$

where the estimated result, $\hat{\mathbf{h}}$ (or $\hat{h}$), is the center of the ball (or circle), and the radius θ is determined by the chosen channel estimator and the sensing time. Note that error-free channel estimation corresponds to $\theta = 0$. Then the actual channel state can be formulated as follows:

$$\mathbf{h} = \hat{\mathbf{h}} + \mathbf{\Delta h} \text{ (or } h = \hat{h} + \Delta h), \quad (2)$$

where the uncertainty $\mathbf{\Delta h}$ (or Δh) is norm-bounded by $\|\mathbf{\Delta h}\| \leq \theta$ (or $|\Delta h| \leq \theta$).

Note that channel estimation may be a non-trivial task in practical scenarios, especially for the CSI estimation of the eavesdroppers. In this paper, we assume that only imperfect CSIs of all users can be available.

C. Data Transmissions in Heterogeneous Networks

Within a macrocell, the MBS with K_M antennae sends private information s_m to the mth MU via MaMIMO. Since the MBS has larger power than LBSs, it is reasonable for MUs to ignore signal interference resulted from LBSs. The signal vector transmitted by MBS to M MUs is denoted by $\mathbf{s} = [s_1, ..., s_M]^T \in \mathbb{C}^{M\times 1}$ with $\mathbb{E}[s_m s_m^H] = 1$, where s_i is an information symbol of MU_i. The signal vector $\mathbf{s}$ is multiplied by a transmit beamforming matrix, $\mathbf{\Omega} = [\mathbf{w}_1, ..., \mathbf{w}_M] \in \mathbb{C}^{K_M \times M}$, before transmission. $\mathbf{w}_i \in \mathbb{C}^{K_M \times 1}$ is the beamforming vector for MU_i. Let p_m denote the transmit power allocated to MU_m. Then the received information at the mth MU (MU_m) and the nth Eve (ME_n) can be expressed as

$$y_m = \sqrt{p_m}\mathbf{h}_m\mathbf{w}_m s_m + \sum_{i=1, i\neq m}^{M} \sqrt{p_i}\mathbf{h}_m\mathbf{w}_i s_i + z_m, \quad (3)$$

$$y_{\text{ME}_n} = \sqrt{p_m}\mathbf{h}_{\text{ME}_n}\mathbf{w}_m s_m + \sum_{i=1, i\neq m}^{M} \sqrt{p_i}\mathbf{h}_{\text{ME}_n}\mathbf{w}_i s_i + z_{\text{ME}_n}, \quad (4)$$

where the first term on the right-hand side of (3) and (4) refers to the private information received by MU_m and ME_n, respectively, and the second term represents the interference among the MUs. Since MEs intend to wiretap the information sent to MU_m, the second term can be considered as a cooperative jamming signal for secure transmissions. Here, $\mathbf{h}_i \in \mathbb{C}^{1\times K_M}$ and $\mathbf{h}_{\text{ME}_n} \in \mathbb{C}^{1\times K_M}$, denote the channel state vectors from the MBS to MU_i and to ME_n, respectively. Besides, $z_m \sim \mathcal{CN}(0, \sigma_m^2)$ and $z_{\text{ME}_n} \sim \mathcal{CN}(0, \sigma_{\text{ME}_n}^2)$ are the additive white Gaussian noise (AWGN) at MU_m and ME_n, respectively.

Within a local cell, the lth LU may receive private information from its LBS. Different from the case of the macrocell, LUs may exploit SIC technology to decode different users, in which the interference caused by the decoded users is subtracted before decoding other users. Generally speaking,

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TWC.2019.2912611, IEEE Transactions on Wireless Communications

the decoding order is related to channel fading coefficients, and a user with a better channel state can eliminate the interference of other users with poor channel states. Thus, without artificial noise, the secrecy rate of an LU whose channel gain is lower than those of the eavesdroppers with SIC may be zero. In this case, we may require that the LBS to stop sending any private information to the LU [1]. Thus, if we ignore the cooperation between the macrocell and local cells, we only need to focus on the LUs with better channel conditions than the eavesdroppers.

Taking the same channel fading model as that adopted by [53], [54], we assume that data transmissions from an LBS to all its LUs experience a block fading channel, in which a fading coefficient remains constant within a time slot but changes independently from one slot to another. We assume that the channel gains of the LUs are sorted as $0 < |\hat{h}_1|^2 \leq ... \leq |\hat{h}_l|^2 \leq ... \leq |\hat{h}_L|^2$. Furthermore, we consider a worse case where the eavesdroppers also adopt the SIC technology; thus we have $0 < |\hat{h}_1|^2 \leq ... \leq |\hat{h}_{n_g}|^2 \leq |\hat{h}_{\text{LE}_n}|^2 \leq |\hat{h}_{n_g+1}|^2 \leq ... \leq |\hat{h}_l|^2$, where $n_g \in [0, L-1]$, $0 < |\hat{h}_0|^2 < |\hat{h}_L|^2$, and $\hat{h}_{\text{LE}_n}$ denotes the estimated channel gain from the LBS to the nth Eve (LE_n) when N colluding eavesdroppers wiretap the information sent to LU_l.

Accordingly, the received signals at LU_l and LE_n can be respectively expressed as

$$\begin{aligned} y_l =& h_l\sqrt{\rho_l P_L}x_l + h_l \sum_{j=l+1}^{L} \sqrt{\rho_j P_L}x_j \\ &+ \Delta h_l \sum_{j=1}^{l-1} \sqrt{\rho_j P_L}x_j + \mathbf{g}_l \sum_{i=1}^{M} \sqrt{p_i}\mathbf{w}_i s_i + z_l, \end{aligned} \tag{5}$$

and

$$\begin{aligned} y_{\text{LE}_n} =& h_{\text{LE}_n}\sqrt{\rho_l P_L}x_l + h_{\text{LE}_n} \sum_{\substack{j=n_g+1 \\ j\neq l}}^{L} \sqrt{\rho_j P_L}x_j \\ &+ \Delta h_{\text{LE}_n} \sum_{j=1}^{n_g} \sqrt{\rho_j P_L}x_j + \mathbf{g}_{\text{LE}_n} \sum_{i=1}^{M} \sqrt{p_i}\mathbf{w}_i s_i + z_{\text{LE}_n}, \end{aligned} \tag{6}$$

where the first term on the right-hand side of (5) and (6) refers to the private information received by LU_l and LE_n, respectively. The second term is the inter-user interference among local users after SIC decoding from users of larger channel gains, and the third term is the residual interference due to channel estimation errors from users of smaller channel gains [55]. The fourth term denotes the interference caused by the MBS. Also note that $z_l \sim \mathcal{CN}(0, \sigma_l^2)$ and $z_{\text{LE}_n} \sim \mathcal{CN}(0, \sigma_{\text{LE}_n}^2)$ are the AWGN at LU_l and LE_n. Here, $\mathbf{g}_l$ and $\mathbf{g}_{\text{LE}_n}$ are respectively the channel vectors from the MBS to LU_l and to LE_n, ρ_j ($\sum_{j=1}^{L} \rho_j = 1$) is a power allocation factor that describes the local signal power transmitted to LU_j, and P_L is the maximum power of a local cell.

[1]Particularly, secure transmissions for a user whose channel gain is lower than those of its eavesdroppers should be guaranteed by using cryptography technologies at upper layers [49].

According to the received information of the legitimate user and Eve, we define the corresponding secrecy rate as follows:

$$R_x(\gamma_x, \Gamma_X) = \log(1+\gamma_x) - \log(1+\Gamma_X), \tag{7}$$

where $\gamma_x \in \{\gamma_m, \gamma_l\}$ represents the received SINR of MU_m or LU_l and $\Gamma_X \in \{\Gamma_{\text{ME}}, \Gamma_{\text{LE}}\}$ denotes the aggregate SINR of N collusive eavesdroppers in a macrocell or a local cell. As claimed in [56], one can consider the collusive eavesdroppers as a super eavesdropper with N antennae who intends to wiretap the information sent to either MU_m or LU_l. It is possible to perform equal-gain combining (EGC) of available eavesdroppers' SINR to calculate the aggregate SINR of the super eavesdropper. Here, we believe this is a feasible case for multiple collusive eavesdroppers. As a result, the SINR values in (7) can be computed as

$$\gamma_m = \frac{p_m|\mathbf{h}_m\mathbf{w}_m|^2}{\sum_{i=1,i\neq m}^{M} p_i|\mathbf{h}_m\mathbf{w}_i|^2 + \sigma_m^2}, \tag{8}$$

$$\Gamma_{\text{ME}} = \frac{\sum_{n=1}^{N} p_m|\mathbf{h}_{\text{ME}_n}\mathbf{w}_m|^2}{\sum_{n=1}^{N}(\sum_{i=1,i\neq m}^{M} p_i|\mathbf{h}_{\text{ME}_n}\mathbf{w}_i|^2 + \sigma_{\text{ME}_n}^2)}, \tag{9}$$

$$\gamma_l = \frac{\rho_l P_L|h_l|^2}{Q_l^{(\text{in})} + \sum_{i=1}^{M} p_i|\mathbf{g}_l\mathbf{w}_i|^2 + \sigma_l^2}, \tag{10}$$

and

$$\Gamma_{\text{LE}} = \frac{\sum_{n=1}^{N} \rho_l P_L|h_{\text{LE}_n}|^2}{\sum_{n=1}^{N}(Q_e^{(\text{in})} + \sum_{i=1}^{M} p_i|\mathbf{g}_{\text{LE}_n}\mathbf{w}_i|^2 + \sigma_{\text{LE}_n}^2)}, \tag{11}$$

where $Q_l^{(\text{in})} = |h_l|^2 P_L \sum_{j=l+1}^{L} \rho_j + |\Delta h_l|^2 P_L \sum_{j=1}^{l-1} \rho_j$ and $Q_e^{(\text{in})} = |h_{\text{LE}_n}|^2 P_L \sum_{\substack{j=n_g+1 \\ j\neq l}}^{L} \rho_j + |\Delta h_{\text{LE}_n}|^2 P_L \sum_{j=1}^{n_g} \rho_j$ are the interference powers of the local cell for LU_l and LE_n, respectively. Note that the numerators in these SINR expressions represent the powers of the received signals, while the denominators denote the power sum of the cooperative jamming signals and AWGN.

IV. Secure Transmission Algorithms with Imperfect CSI

Based on the above preliminary definitions, we present three robust optimization formulations for secrecy maximization under channel uncertainty in this section. First, for a macrocell with cooperative jammers, we present a robust beamforming algorithm to mitigate the wiretapping capability of collusive macro eavesdroppers. Then, for a local cell with NOMA-enabled inter-user interference, we provide a robust power allocation algorithm to counter against collusive local eavesdroppers. Finally, we develop a joint optimization algorithm that can simultaneously satisfy the secrecy requirements of a target MU and a target LU in a tiered system.

A. Robust Beamforming Algorithm (RBA) at a Macrocell

Generally speaking, we need to increase the secrecy rate of a target MU_m as much as possible while satisfying the SINR requirements of other MUs. In addition, the total power of the wireless system should be bounded. Taking into account these

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TWC.2019.2912611, IEEE Transactions on Wireless Communications

constraints, we obtain the following optimization problem for MU_m:

$$\max_{\{\mathbf{w}_i\}_{i=1}^M} \quad R_m(\gamma_m, \Gamma_{\text{ME}}) \tag{12a}$$

$$\text{s.t.} \quad \gamma_i \geq \epsilon_i, \quad i \in [1, M] \tag{12b}$$

$$\sum_{i=1}^{M} p_i \|\mathbf{w}_i\|^2 \leq P_M, \tag{12c}$$

where ϵ_i is the threshold of the minimum acceptable SINR of each MU_i and P_M represents the maximum transmit power of the MBS.

The beamforming design in (12) hinges on the CSI $\mathbf{h}$, but we only have an estimated $\hat{\mathbf{h}}$ at hand. We opt to a robust design based on the worst feasible case. The **Lemma 1** specifies the minimum γ_m and the maximum Γ_{ME} with respect to the channel uncertainty.

Lemma 1. *Considering the channel uncertainty defined in* (1)*, the minimum γ_m and the maximum Γ_{ME} are*

$$\tilde{\gamma}_m = \frac{\text{Tr}(\hat{\mathbf{H}}_m^{\downarrow} \mathbf{W}_m)}{\sum\limits_{\substack{i=1 \\ i \neq m}}^{M} \text{Tr}(\hat{\mathbf{H}}_m^{\uparrow} \mathbf{W}_i) + \sigma_m^2}, \tag{13}$$

and

$$\tilde{\Gamma}_{ME} = \frac{\sum\limits_{n=1}^{N} \text{Tr}(\hat{\mathbf{H}}_{ME_n}^{\uparrow} \mathbf{W}_m)}{\sum\limits_{n=1}^{N} \sum\limits_{\substack{i=1 \\ i \neq m}}^{M} \left(\text{Tr}(\hat{\mathbf{H}}_{ME_n}^{\downarrow} \mathbf{W}_i) + \sigma_{ME_n}^2 \right)}, \tag{14}$$

where $\mathbf{W}_i = \mathbf{w}_i \mathbf{w}_i^H$, $\hat{\mathbf{H}}^{\uparrow} \triangleq \hat{\mathbf{h}}^H \hat{\mathbf{h}} + \zeta \mathbf{I}$, $\hat{\mathbf{H}}^{\downarrow} \triangleq \hat{\mathbf{h}}^H \hat{\mathbf{h}} - \zeta \mathbf{I}$, and $\zeta \triangleq \theta^2 + 2\theta \|\mathbf{h}\|$ is an upper bound of the uncertainty.

Proof. See Appendix A. □

Using the worst-case SINR results in **Lemma 1**, we transform (12) into a robust formulation as follows:

$$\textbf{RBA:} \quad \max_{\{\mathbf{w}_i\}_{i=1}^M} \quad R_m(\tilde{\gamma}_m, \tilde{\Gamma}_{\text{ME}}) \tag{15a}$$

$$\text{s.t.} \quad \tilde{\gamma}_i \geq \epsilon_i, \quad i \in [1, M] \tag{15b}$$

$$\sum_{i=1}^{M} p_i \|\mathbf{w}_i\|^2 \leq P_M \tag{15c}$$

Intuitively, (15) consists of a fractional objective function and a set of affine inequalities. Thus, it is non-convex and is hard to solve. In the following we relax some constraints in (15) and employ the Taylor series expansion to transform it into a second-order cone program (SOCP).

Lemma 2. *(Taylor series expansion) Let $f_{a,\mathbf{H}}(\mathbf{w}, x) = \frac{\mathbf{w}^H \mathbf{H} \mathbf{w}}{x - a}$ and $u_{b,\mathbf{H}}(\mathbf{w}) = b \mathbf{w}^H \mathbf{H} \mathbf{w}$. The first-order Taylor series expansions around certain points $(\mathbf{w}^*, x^*)$ and $\mathbf{w}^*$ are as follows [57]:*

$$F_{a,\mathbf{H}}(\mathbf{w}, x, \mathbf{w}^*, x^*) = \frac{2\text{Re}\{\mathbf{w}^{*H} \mathbf{H} \mathbf{w}\}}{x^* - a} - \frac{\mathbf{w}^{*H} \mathbf{H} \mathbf{w}^*}{(x^* - a)^2}(x - a),$$

$$U_{b,\mathbf{H}}(\mathbf{w}, \mathbf{w}^*) = (-\mathbf{w}^{*H} \mathbf{H} \mathbf{w}^* + 2\text{Re}\{\mathbf{w}^{*H} \mathbf{H} \mathbf{w}\}) b.$$

Proof. See Appendix B. □

Theorem 1. *The non-convex problem* (15) *can be transformed into* (16)*, which is a tractable SOCP problem* [2]*, where $\mathbf{I}_\zeta \triangleq \zeta \mathbf{I}$ and α_0, α_1, α_2 are three slack variables satisfying $0 \leq \alpha_1 \leq 1 + \tilde{\gamma}_m$, $0 \leq \alpha_2 \leq \frac{1}{1 + \tilde{\Gamma}_{ME}}$, $\alpha_1 \alpha_2 \geq \alpha_0^2$.*

Proof. See Appendix C. □

It is generally known that a SOCP form problem is convex. Thus, (16) can be solved by existing convex optimization problem solvers such as CVX [58]. The algorithm of our proposed RBA is summarized as **Algorithm 1**.

Remark 1. *(Convergence) Our RBA employs an iterative process to find the optimal beamforming vectors for the considered secrecy rate maximization. The optimal beamforming vectors $\{\mathbf{w}_1, ..., \mathbf{w}_M\}$ is calculated by solving problem* (16) *for a given $\{\mathbf{w}_1^*, ..., \mathbf{w}_M^*, \alpha_1^*, \alpha_2^*\}$. For each iteration, $\{\mathbf{w}_1^*, ..., \mathbf{w}_M^*, \alpha_1^*, \alpha_2^*\}$ is updated from the optimal solutions of the last iteration. Hence, $\{\mathbf{w}_1^*, ..., \mathbf{w}_M^*, \alpha_1^*, \alpha_2^*\}$ is always feasible for the next iteration. As a result, the objective metric α_0 which reveals the secrecy rate increases (or at least non-decreasing) during the whole iterative process. Yet, it has an upper limit due to the constraint of MBS's transmit power. Thus, the proposed RBA can converge.*

Remark 2. *(Conservative solutions) Our RBA is mainly aimed at maximizing the secrecy rate of the MUs. The CSI of all legitimate MUs and eavesdroppers are imperfect and are available at the MBS. Note that the result of our optimization problem indicates the worst case secrecy rate of the system. Thus, our algorithm provides a conservative strategy. And our solution subsumes the perfect CSI case by setting $\theta = 0$.*

Remark 3. *(Non-collusive solutions) Although the scenario of collusive eavesdroppers is taken into account in RBA, it is applicable to the case of non-collusive eavesdroppers (i.e., set $N = 1$): when the eavesdroppers are non-collusive, we only consider the one with the best channel state.*

B. Robust Power Allocation Algorithm (RPA) at Local Cells

The above analysis on the MUs' secrecy rate only considers the inter-MU interference, while ignoring the interference caused by the LBSs. This is because the transmit powers of the LBSs are low and do not produce strong interference on the MUs. Nevertheless, at the local cell tier, an LU is subject to not only the interference of other LUs of the same local cell, but also the interference from the MBS. Considering the complex interference structure in NOMA-enabled local cells, we now develop a robust power allocation algorithm for the LUs in the case of collusive eavesdropping.

Similar to the optimization problem presented in the previous subsection, we formulate a power allocation optimization problem aiming at maximizing the worst-case achievable secrecy rate. Suppose that the imperfect CSIs of all LUs are available to their LBSs as well as the MBS. We focus on the secrecy rate of an LU (i.e., LU_l) whose information is wiretapped by collusive eavesdroppers. Note that the total power

[2]Without loss of generality, we assume all variances of AWGN are equal to 1 in our article.

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TWC.2019.2912611, IEEE Transactions on Wireless Communications

$$\max_{\substack{\{\mathbf{w}_i\}_{i=1}^{M} \\ \alpha_0,\alpha_1,\alpha_2}} \quad \alpha_0 \tag{16a}$$

$$\text{s.t.} \quad \|[2\mathbf{w}_1^H\hat{\mathbf{h}}_m^H, ..., 2\mathbf{w}_{m-1}^H\hat{\mathbf{h}}_m^H, 2\mathbf{w}_{m+1}^H\hat{\mathbf{h}}_m^H, ..., 2\mathbf{w}_M^H\hat{\mathbf{h}}_m^H, 2\sqrt{\zeta_1}\mathbf{w}_1^H, ..., 2\sqrt{\zeta_{m-1}}\mathbf{w}_{m-1}^H,$$
$$2\sqrt{\zeta_{m+1}}\mathbf{w}_{m+1}^H, ..., 2\sqrt{\zeta_M}\mathbf{w}_M^H, (t_1-1)]^T\| \le t_1+1 \tag{16b}$$
$$\|[2\mathbf{w}_1^H\hat{\mathbf{h}}_{\text{ME}_1}^H, ..., 2\mathbf{w}_M^H\hat{\mathbf{h}}_{\text{ME}_1}^H, 2\mathbf{w}_1^H\hat{\mathbf{h}}_{\text{ME}_2}^H, ..., 2\mathbf{w}_M^H\hat{\mathbf{h}}_{\text{ME}_2}^H, ...,$$
$$2\mathbf{w}_1^H\hat{\mathbf{h}}_{\text{ME}_N}^H, ..., 2\mathbf{w}_M^H\hat{\mathbf{h}}_{\text{ME}_N}^H, 2\mathbf{w}_m^H\sqrt{\zeta_{\text{ME}_1}}, ..., 2\mathbf{w}_m^H\sqrt{\zeta_{\text{ME}_N}}, 2\sqrt{N}, (t_2-1)]^T\| \le t_2+1 \tag{16c, 16d}$$
$$\|[2\mathbf{w}_1^H\hat{\mathbf{h}}_i^H\sqrt{\epsilon_i}, ..., 2\mathbf{w}_{i-1}^H\hat{\mathbf{h}}_i^H\sqrt{\epsilon_i}, 2\mathbf{w}_{i+1}^H\hat{\mathbf{h}}_i^H\sqrt{\epsilon_i},$$
$$..., 2\mathbf{w}_M^H\hat{\mathbf{h}}_i^H\sqrt{\epsilon_i}, 2\mathbf{w}_i^H\sqrt{\zeta_i}, 2\sqrt{\epsilon_i}, (t_{3i}-1)]^T\| \le t_{3i}+1, \quad i\in[1,M] \tag{16e}$$
$$\|[\sqrt{p_1}\mathbf{w}_1^H, \sqrt{p_2}\mathbf{w}_2^H, ..., \sqrt{p_M}\mathbf{w}_M^H]^T\| \le \sqrt{P_M} \tag{16f}$$
$$\|[2\alpha_0, (\alpha_1-\alpha_2)]^T\| \le \alpha_1+\alpha_2 \tag{16g}$$
$$\alpha_0, \alpha_1, \alpha_2 > 0 \tag{16h}$$

Algorithm 1 A Robust Beamforming Algorithm

Initialization:

δ: a convergence threshold;

k: the number of iterations.

1: Transform the original problem (12) into the worst-case optimization problem (15) based on **Lemma 1**;
2: Transform the non-convex problem (15) into a SOCP solvable one (16) based on **Lemma 2** and **Theorem 1**;
3: Initialize beamforming vector set $\{\mathbf{w}_1^*, ..., \mathbf{w}_M^*\}$ satisfying (15c); set α_1^* and α_2^* to any positive values; $k=0$;
4: **while** $|\alpha_0^{(k)} - \alpha_0^{(k-1)}| \le \delta$ **do**
5: Set $k = k+1$;
6: Solve problem (16) with $\{\mathbf{w}_1^*, ..., \mathbf{w}_M^*, \alpha_1^*, \alpha_2^*\}$ to find an optimal solution for $\{\mathbf{w}_1^{(k)}, ..., \mathbf{w}_M^{(k)}, \alpha_1^{(k)}, \alpha_2^{(k)}\}$ and α_0^k;
7: $\{\mathbf{w}_1^*, ..., \mathbf{w}_M^*, \alpha_1^*, \alpha_2^*\} = \{\mathbf{w}_1^{(k)}, ..., \mathbf{w}_M^{(k)}, \alpha_1^{(k)}, \alpha_2^{(k)}\}$;
8: **end while**
9: **return** $\{\mathbf{w}_1, ..., \mathbf{w}_M\} = \{\mathbf{w}_1^*, ..., \mathbf{w}_M^*\}$.

of all the transmitters should satisfy the power constraint. Therefore, the power allocation optimization for LU_l can be formulated as follows:

$$\textbf{RPA:} \max_{\{\rho_j\}_{j=1}^{L}} \quad R_l(\tilde{\gamma}_l, \tilde{\Gamma}_{\text{LE}}) \tag{19a}$$
$$\text{s.t.} \quad \tilde{\gamma}_j \ge \epsilon_j, \quad j\in[1,L] \tag{19b}$$
$$\sum_{j=1}^{L}\rho_j = 1, \tag{19c}$$

where ϵ_j is a threshold of the minimum acceptable SINR for LU_j. Considering the uncertainty of channel estimation, we employ $\hat{h}^{\uparrow} \triangleq \hat{h}+\theta$, $\hat{h}^{\downarrow} \triangleq \hat{h}-\theta$, $\hat{\mathbf{G}}^{\uparrow} = \hat{\mathbf{g}}^H\hat{\mathbf{g}} + \mathbf{I}_\zeta$ and $\hat{\mathbf{G}}^{\downarrow} = \hat{\mathbf{g}}^H\hat{\mathbf{g}} - \mathbf{I}_\zeta$. Therefore, the minimum SINR of LU_l and the maximum SINR of the collusive eavesdroppers can be expressed as below,

$$\tilde{\gamma}_l = \frac{\rho_l P_L |\hat{h}_l^{\downarrow}|^2}{\sum_{j=l+1}^{L}\rho_j P_L|\hat{h}_l^{\uparrow}|^2 + \theta_l^2\sum_{j=1}^{l-1}\rho_j P_L + \sum_{i=1}^{M}\text{Tr}(\hat{\mathbf{G}}_l^{\uparrow}\mathbf{W}_i) + \sigma_l^2},$$

and

$$\tilde{\Gamma}_{\text{LE}} = \frac{\sum_{n=1}^{N}\rho_l P_L|\hat{h}_{\text{LE}_n}^{\uparrow}|^2}{\sum_{n=1}^{N}\left(|\hat{h}_{\text{LE}_n}^{\downarrow}|^2\sum_{\substack{j=n_g+1 \\ j\neq l}}^{L}\rho_j P_L + \sum_{i=1}^{M}\text{Tr}(\hat{\mathbf{G}}_{\text{LE}_n}^{\downarrow}\mathbf{W}_i) + \sigma_{\text{LE}_n}^2\right)}.$$

Obviously, (19) is non-convex; thus we introduce two slack variables β_1, and β_2, and employ Taylor series expansion (i.e., **Lemma 3**) to transform it into a convex optimization problem shown in (20).

Lemma 3. *(Taylor series expansion) Let* $v_{a,b}(x,y) = \frac{ay}{x-b}$. *The first-order Taylor series expansion of* $v_{a,b}(x,y)$ *at a certain point* (x^*, y^*) *is:*

$$V_{a,b}(x,y,x^*,y^*) = \frac{ay}{x^*-b} + \frac{ay^*}{(x^*-b)^2}(x-x^*).$$

Proof. Please refer to **Appendix B** for the prove of **Lemma 3**. We omit the proof here because of its similarity to **Lemma 2**. □

Theorem 2. *The non-convex problem* (19) *can be transformed into the tractable problem* (20)*, where* β_1 *and* β_2 *are two slack variables satisfying* $0 \le \beta_1 \le 1+\tilde{\gamma}_l$ *and* $0 \le \beta_2 \le \frac{1}{1+\tilde{\Gamma}_{LE}}$.

Proof. See Appendix D. □

Obviously, the problem (20) can be efficiently solved by available solvers. Similar to **Algorithm 1**, we employ an iterative method to find the optimal power allocation factor ρ_j. Note that RPA needs the beamforming vectors of the MBS in advance; thus the optimal ρ_j of RPA is affected by the solution of RBA.

Remark 4. *(Convergence) At each iteration, new solutions, i.e.,* $(\rho_1^*, ..., \rho_L^*, \beta_1^*, \beta_2^*)$*, are calculated by solving the problem*

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TWC.2019.2912611, IEEE Transactions on Wireless Communications

$$\max_{\substack{\{\rho_j\}_{j=1}^{L}\\ \beta_1,\beta_2}} \quad \log\beta_1+\log\beta_2 \tag{20a}$$

$$\text{s.t.} \quad \sum_{j=l+1}^{L}\rho_j P_L|\hat{h}_l^{\uparrow}|^2+\theta_l^2\sum_{j=1}^{l-1}\rho_j P_L+\sum_{i=1}^{M}\mathrm{Tr}(\hat{\mathbf{G}}_l^{\uparrow}\mathbf{W}_i)+1-V_{P_L|\hat{h}_l^{\downarrow}|^2,1}(\beta_1,\rho_l,\beta_1^*,\rho_l^*)\le 0 \tag{20b}$$

$$\sum_{n=1}^{N}\sum_{\substack{j=n_g+1\\ j\neq l}}^{L}\Big(\rho_j P_L|\hat{h}_{\mathrm{LE}_n}^{\downarrow}|^2+\rho_l P_L|\hat{h}_{\mathrm{LE}_n}^{\uparrow}|^2-V_{P_L|\hat{h}_{\mathrm{LE}_n}^{\downarrow}|^2,0}(\beta_2,\rho_j,\beta_2^*,\rho_j^*)$$
$$+\frac{(\beta_2^*)^2-2\beta_2^*+\beta_2}{(\beta_2^*)^2}\left(\sum_{i=1}^{M}\mathrm{Tr}(\hat{\mathbf{G}}_{\mathrm{LE}_n}^{\downarrow}\mathbf{W}_i)+1\right)\Big)\le 0 \tag{20c}$$

$$\epsilon_j\left(\sum_{q=j+1}^{L}\rho_q P_L|\hat{h}_j^{\uparrow}|^2+\theta_j^2\sum_{q=1}^{j-1}\rho_q P_L+\sum_{i=1}^{M}\mathrm{Tr}(\hat{\mathbf{G}}_j^{\uparrow}\mathbf{W}_i)+1\right)-\rho_j P_L|\hat{h}_j^{\downarrow}|^2\le 0,\qquad j\in[1,L] \tag{20d}$$

$$\sum_{j=1}^{L}\rho_j=1 \tag{20e}$$

$$\beta_1>0,\beta_2>0 \tag{20f}$$

(20). *These solutions can be considered as the initial values for the next iteration. The initial values are always feasible for solving the problem* (20) *in the current iteration, and thus the objective function* $\log\beta_1+\log\beta_2$ *is non-decreasing with each iteration. Yet,* $\log\beta_1+\log\beta_2$ *cannot exceed an upper bound due to the power constraint of the LBSs. Thus, the convergence of RPA is guaranteed.*

Remark 5. *(Non-collusive and conservative solutions) RPA provides an optimal secrecy rate for both collusive and individual eavesdropping. The secrecy rate is computed under the premise that the imperfect CSIs of the users (including MUs, LUs, and eavesdroppers) are available at the LBSs. Therefore, the RPA algorithm is conservative and can be employed in the case of individual eavesdropping.*

Remark 6. *(ZFBF-based sub-optimization problem) It is noted that if we only consider the secrecy rates of the LUs, the MBS can be considered as a friendly jammer to send cooperative jamming signals. In this case, we may use ZFBF to eliminate the co-channel interference (CCI) from the MBS to a target LU in an LBS, while still interfering with the reception of the eavesdroppers. More specifically, the MBS calculates its ZFBF vectors based on the known CSI of the target LU. Then the LBS implements RPA based on the ZFBF vectors sent by the MBS. According to this ZFBF-based design, the secrecy rates of the LUs can be improved. The detailed process to obtain the ZFBF vectors can be found in [59], [60].*

C. Robust Joint Optimization (RJO) across Tiers

We have developed two algorithms focusing on the secrecy rate optimization of either a target MU or a target LU individually. On one hand, RBA achieves the maximum secrecy rate for the MU by the optimal design of beamforming vectors at the MBS while ignoring the interferences of the signals sent by the MBS to the LUs. On the other hand, RPA considers the interferences from the MBS to the LU as a constant to achieve a sequential optimization, and the LU's secrecy rates can be optimized only after completing the optimization of the MUs, i.e., after obtaining the beamforming vectors. As a result, neither RBA nor RPA can achieve system-level optimal solutions (including both MUs and LUs).

For system-level optimization of the two-tier network, it is also viable to jointly optimize the secrecy sum rate of a target MU and a target LU, at the expense of increased design complexity. To this end, we now develop a robust joint optimization algorithm (RJO) under collusive eavesdropping in this subsection. RJO is subject to the power constraints of the MBS and the LBSs as well as the received SINR requirements of the MUs and the LUs in all local cells. Without loss of generality, we select the first local cell as the cooperative local cell. This problem is formulated as (21).

$$\textbf{RJO:}\quad \max_{\substack{\{\mathbf{w}_i\}_{i=1}^{M}\\ \{\rho_{1,j}\}_{j=1}^{L}}} \quad R_m(\tilde{\gamma}_m,\tilde{\Gamma}_{\mathrm{ME}})+R_l(\tilde{\gamma}_l,\tilde{\Gamma}_{\mathrm{LE}}) \tag{21a}$$

$$\text{s.t.} \quad \tilde{\gamma}_i\ge\epsilon_i,\ i\in[1,M] \tag{21b}$$

$$\tilde{\gamma}_{k,j}\ge\epsilon_{k,j},\ j\in[1,L],k\in[1,K_L] \tag{21c}$$

$$\sum\nolimits_{i=1}^{M}p_i\|\mathbf{w}_i\|^2\le P_M \tag{21d}$$

$$\sum\nolimits_{j=1}^{L}\rho_{k,j}=1,\quad k\in[1,K_L], \tag{21e}$$

where $k\in[1,K_L]$ represents the kth local cell, and $\{\rho_{k,j}\}_{j=1}^{L}$ denotes the power allocation factors of the kth local cell. The objective function in (21) denotes a secrecy sum rate of MU_m and $\mathrm{LU}_{1,l}$.

Because of the fractional form and logarithmic function in the objective function, (21) is a non-convex problem that is difficult to solve. Applying the D.C. approximation program-

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TWC.2019.2912611, IEEE Transactions on Wireless Communications

ming [18], we can rewrite the objective function as follow.

$$\max_{\substack{\{\mathbf{W}_i\}_{i=1}^M \\ \{\rho_{1,j}\}_{j=1}^L}} \Phi, \tag{22}$$

where

$$\begin{aligned}\Phi =&\phi_1(\mathbf{W}_1,...,\mathbf{W}_M,\rho_{1,1},...,\rho_{1,L}) \\ &-\phi_2(\mathbf{W}_1,...,\mathbf{W}_M,\rho_{1,1},...,\rho_{1,L}),\end{aligned} \tag{23}$$

and

$$\begin{aligned}&\phi_1(\mathbf{W}_1,...,\mathbf{W}_M,\rho_{1,1},...,\rho_{1,L}) \\ &\quad=\log(\varphi_{1,1})+\log(\varphi_{1,2})+\log(\varphi_{1,3})+\log(\varphi_{1,4}), \\ &\phi_2(\mathbf{W}_1,...,\mathbf{W}_M,\rho_{1,1},...,\rho_{1,L}) \\ &\quad=\log(\varphi_{2,1})+\log(\varphi_{2,2})+\log(\varphi_{2,3})+\log(\varphi_{2,4}),\end{aligned}$$

where $\{\varphi_{1,i}\}_{i=1}^4$ and $\{\varphi_{2,i}\}_{i=1}^4$ are all functions about $(\mathbf{W}_1,...,\mathbf{W}_M,\rho_{1,1},...,\rho_{1,L})$, which are defined as follows.

$$\begin{aligned}\varphi_{1,1} =&\mathrm{Tr}(\hat{\mathbf{H}}_m^{\downarrow}\mathbf{W}_m)+\sum_{\substack{i=1\\i\neq m}}^{M}\mathrm{Tr}(\hat{\mathbf{H}}_m^{\uparrow}\mathbf{W}_i)+\sigma_m^2, \\ \varphi_{1,2} =&\rho_l P_L|\hat{h}_l^{\downarrow}|^2+\sum_{j=l+1}^{L}\rho_j P_L|\hat{h}_l^{\uparrow}|^2+\theta_l^2\sum_{j=1}^{l-1}\rho_j P_L \\ &+\sum_{i=1}^{M}\mathrm{Tr}(\hat{\mathbf{G}}_l^{\uparrow}\mathbf{W}_i)+\sigma_l^2, \\ \varphi_{1,3} =&\sum_{n=1}^{N}\left(\sum_{\substack{i=1\\i\neq m}}^{M}\mathrm{Tr}(\hat{\mathbf{H}}_{\mathrm{ME}_n}^{\downarrow}\mathbf{W}_i)+\sigma_{\mathrm{ME}_n}^2\right), \\ \varphi_{1,4} =&\sum_{n=1}^{N}\left(|\hat{h}_{\mathrm{LE}_n}^{\downarrow}|^2\sum_{\substack{j=n_g+1\\j\neq l}}^{L}\rho_j P_L\right. \\ &\left.+\sum_{i=1}^{M}\mathrm{Tr}(\hat{\mathbf{G}}_{\mathrm{LE}_n}^{\downarrow}\mathbf{W}_i)+\sigma_{\mathrm{LE}_n}^2\right), \\ \varphi_{2,1} =&\sum_{n=1}^{N}\mathrm{Tr}(\hat{\mathbf{H}}_{\mathrm{ME}_n}^{\uparrow}\mathbf{W}_m) \\ &+\sum_{n=1}^{N}\left(\sum_{\substack{i=1\\i\neq m}}^{M}\mathrm{Tr}(\hat{\mathbf{H}}_{\mathrm{ME}_n}^{\downarrow}\mathbf{W}_i)+\sigma_{\mathrm{ME}_n}^2\right), \\ \varphi_{2,2} =&\sum_{n=1}^{N}\rho_l P_L|\hat{h}_{\mathrm{LE}_n}^{\uparrow}|^2+\sum_{n=1}^{N}\left(|\hat{h}_{\mathrm{LE}_n}^{\downarrow}|^2\sum_{\substack{j=n_g+1\\j\neq l}}^{L}\rho_j P_L\right. \\ &\left.+\sum_{i=1}^{M}\mathrm{Tr}(\hat{\mathbf{G}}_{\mathrm{LE}_n}^{\downarrow}\mathbf{W}_i)+\sigma_{\mathrm{LE}_n}^2\right), \\ \varphi_{2,3} =&\sum_{\substack{i=1\\i\neq m}}^{M}\mathrm{Tr}(\hat{\mathbf{H}}_m^{\uparrow}\mathbf{W}_i)+\sigma_m^2, \\ \varphi_{2,4} =&\sum_{j=l+1}^{L}\rho_j P_L|\hat{h}_l^{\uparrow}|^2+\theta_l^2\sum_{j=1}^{l-1}\rho_j P_L \\ &+\sum_{i=1}^{M}\mathrm{Tr}(\hat{\mathbf{G}}_l^{\uparrow}\mathbf{W}_i)+\sigma_l^2.\end{aligned}$$

Note that the optimization variables of the above optimization problem are $\{\mathbf{W}_i\}_{i=1}^M$ rather than $\{\mathbf{w}_i\}_{i=1}^M$. It can be seen that ϕ_1 and ϕ_2 are both concave functions, so the objective function remains non-convex. To deal with it, we approximate ϕ_2 by its first order Taylor approximation.

Assuming that $\{\{\mathbf{W}_i^*\}_{i=1}^M,\{\rho_{1,j}^*\}_{j=1}^L\}$ is a feasible solution of RJO, we can replace ϕ_2 by its first order Taylor series expansion at the feasible solution $\{\{\mathbf{W}_i^*\}_{i=1}^M,\{\rho_{1,j}^*\}_{j=1}^L\}$, i.e., the objective function of (22) can be transformed into

$$\max_{\substack{\{\mathbf{W}_i\}_{i=1}^M \\ \{\rho_{1,j}\}_{j=1}^L}} \left\{\Phi^*-Y_1-Y_1-Y_3-Y_4\right\}, \tag{24}$$

where Φ^*,Y_1, Y_2, Y_3, Y_4 are given by (25).

As a result, the initial optimization problem (21) can be transformed into a convex one as follows.

$$\begin{aligned}\textbf{RJO:}\quad &\max_{\substack{\{\mathbf{W}_i\}_{i=1}^M \\ \{\rho_{1,j}\}_{j=1}^L}} \{\Phi^*-Y_1-Y_1-Y_3-Y_4\} && \text{(26a)}\\ &\text{s.t.}\quad \tilde{\gamma}_i\geq\epsilon_i,\ i\in[1,M] && \text{(26b)}\\ &\quad \tilde{\gamma}_{k,j}\geq\epsilon_{k,j},\ j\in[1,L],k\in[1,K_L] && \text{(26c)}\\ &\quad \sum\nolimits_{i=1}^{M}p_i\mathrm{Tr}(\mathbf{W}_i)\leq P_M && \text{(26d)}\\ &\quad \sum\nolimits_{j=1}^{L}\rho_{k,j}=1,\quad k\in[1,K_L] && \text{(26e)}\\ &\quad Rank(\mathbf{W}_i)=1,\quad i\in[1,M], && \text{(26f)}\end{aligned}$$

To solve (26), we can first drop the rank-one constraint on $\{\mathbf{W}_i\}_{i=1}^M$, and then by utilizing a similar iterative method to find a feasible solution set, including the beamforming vectors $\{\mathbf{W}_i\}_{i=1}^M$ and the power allocation factors $\{\rho_{1,j}\}_{j=1}^L$. Finally, RT method in [61] can be used to obtain the optimal rank-one solution $\{\mathbf{w}_i\}_{i=1}^M$ from $\{\mathbf{W}_i\}_{i=1}^M$. In brief, the entire D.C. approximation programming can be summarized as follows.

Algorithm 2 The D.C. Approximation Programming Algorithm

Initialization:

δ: a convergence threshold;

k: the number of iterations.

1: Set $\Phi^{(0)}=0$, $k=1$,

2: Initialize $\{\mathbf{W}_1^*,...,\mathbf{W}_M^*,\rho_{1,1}^*,...,\rho_{1,L}^*\}$ satisfying (26);

3: **repeat**

4: Set $k=k+1$;

5: Solve problem (26) with $\{\mathbf{W}_1^*,...,\mathbf{W}_M^*,\rho_{1,1}^*,...,\rho_{1,L}^*\}$ to find an optimal solution for $\{\mathbf{W}_1,...,\mathbf{W}_M,\rho_{1,1},...,\rho_{1,L}\}$;

6: $\{\mathbf{W}_1^*,...,\mathbf{W}_M^*,\rho_{1,1}^*,...,\rho_{1,L}^*\}$= $\{\mathbf{W}_1,...,\mathbf{W}_M,\rho_{1,1},...,\rho_{1,L}\}$;

7: **until** $|\Phi^{(k)}-\Phi^{(k-1)}|\leq\delta$

8: Obtain the optimal rank-one solution $\{\mathbf{w}_i\}_{i=1}^M$ by using RT method in [61].

9: **return** $\{\mathbf{w}_i\}_{i=1}^M$ and $\{\rho_{1,j}\}_{j=1}^L$.

Remark 7. *(Convergence) For the same reason as that elaborated for the previous two algorithms, the iterative convergence of the proposed RJO is guaranteed [18].*

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TWC.2019.2912611, IEEE Transactions on Wireless Communications

$$\Phi^* = \phi_1(\mathbf{W}_1, ..., \mathbf{W}_M, \rho_{1,1}, ..., \rho_{1,L}) - \phi_2(\mathbf{W}_1^*, ..., \mathbf{W}_M^*, \rho_{1,1}^*, ..., \rho_{1,L}^*), \tag{25a}$$

$$Y_1 = \frac{\sum_{n=1}^{N}\left(\sum_{\substack{i=1\\ i\neq m}}^{M} \mathrm{Tr}\left(\hat{\mathbf{H}}_{\mathrm{ME}_n}^{\downarrow}(\mathbf{W}_i - \mathbf{W}_i^*)\right) + \mathrm{Tr}\left(\hat{\mathbf{H}}_{\mathrm{ME}_n}^{\uparrow}(\mathbf{W}_m - \mathbf{W}_m^*)\right)\right)}{\varphi_{2,1}(\mathbf{W}_1^*, ..., \mathbf{W}_M^*, \rho_{1,1}^*, ..., \rho_{1,L}^*)\ln 2}, \tag{25b}$$

$$Y_2 = \frac{\sum_{n=1}^{N}(\rho_{1,l} - \rho_{1,l}^*)P_L|\hat{h}_{\mathrm{LE}_n}^{\uparrow}|^2 + \sum_{n=1}^{N}\left(|\hat{h}_{\mathrm{LE}_n}^{\downarrow}|^2 \sum_{\substack{j=n_g+1\\ j\neq l}}^{L}(\rho_{1,j} - \rho_{1,j}^*)P_L + \sum_{i=1}^{M}\mathrm{Tr}\left(\hat{\mathbf{G}}_{\mathrm{LE}_n}^{\downarrow}(\mathbf{W}_i - \mathbf{W}_i^*)\right)\right)}{\varphi_{2,2}(\mathbf{W}_1^*, ..., \mathbf{W}_M^*, \rho_{1,1}^*, ..., \rho_{1,L}^*)\ln 2}, \tag{25c}$$

$$Y_3 = \frac{\sum_{\substack{i=1\\ i\neq m}}^{M}\mathrm{Tr}\left(\hat{\mathbf{H}}_m^{\uparrow}(\mathbf{W}_i - \mathbf{W}_i^*)\right)}{\varphi_{2,3}(\mathbf{W}_1^*, ..., \mathbf{W}_M^*, \rho_{1,1}^*, ..., \rho_{1,L}^*)\ln 2}, \tag{25d}$$

$$Y_4 = \frac{\sum_{j=l+1}^{L}(\rho_{1,j} - \rho_{1,j}^*)P_L|\hat{h}_l^{\uparrow}|^2 + \theta_l^2\sum_{j=1}^{l-1}(\rho_{1,j} - \rho_{1,j}^*)P_L + \sum_{i=1}^{M}\mathrm{Tr}\left(\hat{\mathbf{G}}_l^{\uparrow}(\mathbf{W}_i - \mathbf{W}_i^*)\right)}{\varphi_{2,4}(\mathbf{W}_1^*, ..., \mathbf{W}_M^*, \rho_{1,1}^*, ..., \rho_{1,L}^*)\ln 2}. \tag{25e}$$

Remark 8. *(Non-collusive and conservative solutions) Similarly, RJO is designed for collusive eavesdropping based on imperfect CSIs. Thus its solution is conservative and it can be degenerated to an individual eavesdropping scenario.*

Remark 9. *(systematic design) The proposed RJO is mainly aimed at the secrecy sum rate of multiple users under collusive eavesdropping. It takes into account the SINR requirements of all the legitimate users (including all MUs and LUs in the system). Obviously, it has a great practical significance in real-world heterogeneous network applications.*

V. Numerical Analyses

In this section, we evaluate the secrecy performance of our algorithms in a typical heterogeneous network. This network consists of a central MBS and two LBSs. The number of MUs is $M = 5$, while the number of LUs in each local cell is assumed to be $L = 3$. Suppose that there are two collusive MEs for a target MU and two collusive LEs for a target LU. The MBS has a larger transmit power than the LBSs in our simulations. All multi-antenna channel vectors are generated by an independent circularly symmetric complex Gaussian (CSCG) distribution, and all single-antenna channel vectors follow an independent and identically distributed Gaussian distribution.

A. The Convergence of the Proposed Algorithms

We first investigate the convergence of our proposed algorithms and report the results in Fig. 2. In testing the RBA, the number of antennas of the MBS in Fig. 2(a) is set to $K_M = 192$. All channel vectors of the MUs and MEs are i.i.d. and follow $\mathcal{CN}(0, 1)$. We employ the same threshold of the minimum acceptable SINR for each MU_i, i.e., $\epsilon_i = 5$. It is evident from Fig. 2(a) that the secrecy rate increases as the number of iterations increases and eventually converges to constants. And the larger the MBS's transmit power, the higher value of the converged secrecy rate.

To test RPA, we randomly generate five channel parameters in an LBS, with each satisfying a standard normal distribution, i.e., $h_l \sim \mathcal{N}(0, 1)$ and $h_{\mathrm{LE}_n} \sim \mathcal{N}(0, 1)$. Here, we assume that collusive eavesdroppers may target LU_2. The transmit power of the LBS is about 10 dBm lower than that of the MBS. Besides, the threshold of the received SINR for each LU is set to 0.50. From Fig. 2(b), one can see that the secrecy rate of the LU is low due to the low transmit power of the LBS. Yet, the secrecy rate still grows along with the increasing transmit power of the LBS.

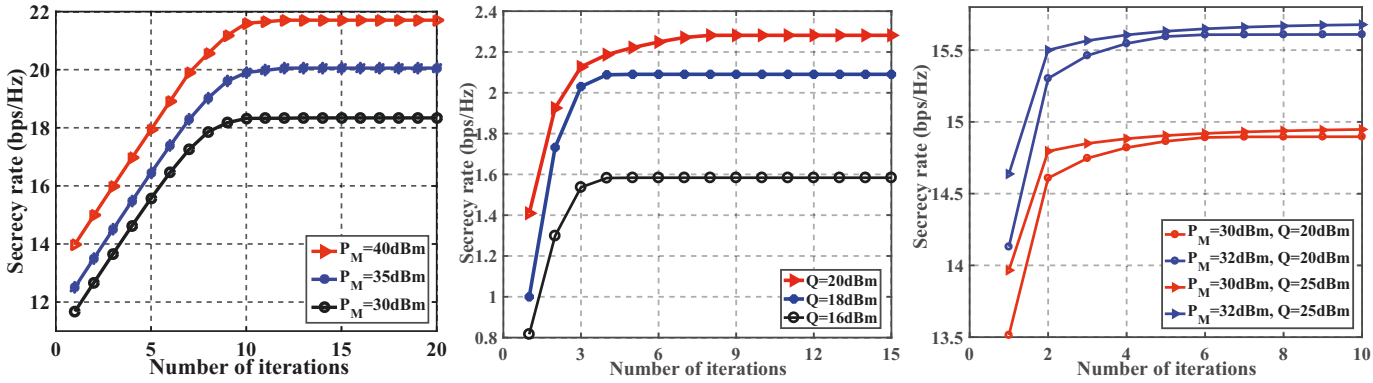
Moreover, we consider a more practical application scenario in which the local cells are deployed in areas where the signals from the MBS are weak. In this case, these signals may interfere with those of the LUs, but not too much. Thus, we set that $\mathbf{g}_l \sim \mathcal{CN}(0, 0.1)$ and $\mathbf{g}_{\mathrm{LE}_n} \sim \mathcal{CN}(0, 0.1)$. Fig. 2(c) provides the secrecy sum rate of a target MU and a target LU. One can see that the rate improves with the increasing transmit power of the MBS or the LBSs. On the other hand, compared with the LBSs, the MBS's power has a greater impact on the secrecy sum rate, due to the fact that the MBS has a higher transmit power.

Note that the results in Fig. 2 are obtained under the assumption of error-free channel estimation, i.e., $\theta = 0$. The impact of channel uncertainty is to be discussed in Subsection V-D.

B. The Effect of the Number of Antennas

Next, we analyze the secrecy performance of RBA when the number of antennas of the MBS varies. Here, we provide three results based on various transmit powers of the MBS. It can be seen from Fig. 3 that more antennas leads to higher secrecy rates, due to larger array gain steered toward the target MU. Besides, one can conclude that more antennas with a lower power may result in a higher secrecy rate than that of less antennas with a higher power. This indicates that we may increase the complexity of the MBS antennas to save the transmit power, which is an advantage of MaMIMO.

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TWC.2019.2912611, IEEE Transactions on Wireless Communications



(a) RBA (b) RPA (c) RJO

Fig. 2: The convergence of different algorithms in various scenarios.

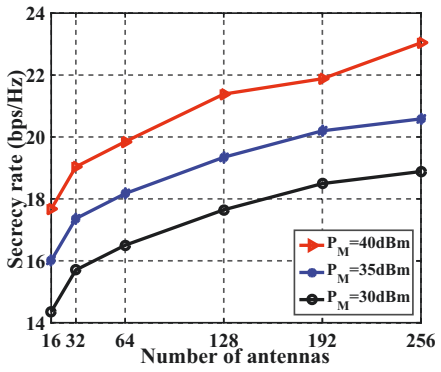


Fig. 3: Secrecy rate *vs.* the number of antennas for different transmit power of the MBS.

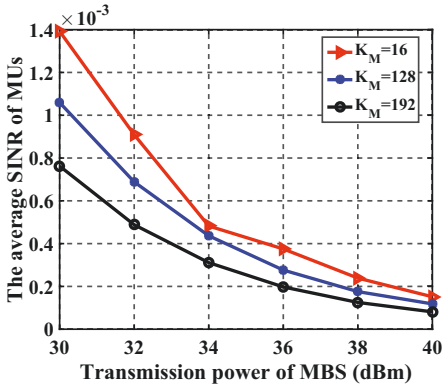


Fig. 4: The average SINR of the MUs *vs.* the transmit power of the MBS.

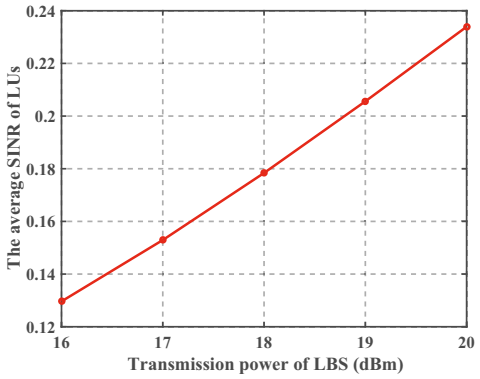


Fig. 5: The average SINR of the LUs *vs.* the transmit power of an LBS.

C. *The Effect of SINR Constraints*

Taking into account different transmit powers of the MBS, we present the average received SINR of the MUs (except for the target MU) in Fig. 4. Here, we omit the SINR constraints of the MUs (i.e., removing (12b) from the optimization). Similarly, we depict the average SINR of the LUs (except for the target LU) *vs.* the transmit power of the LBS when ignoring all the SINR constraints, i.e., removing the constraint (19b), in Fig. 5.

From these figures, we notice that the average SINR of both the MUs and the LUs is relatively low once we remove the SINR constraints. Besides, one can see that the average SINR decreases with the increase of the MBS's transmit power, as shown in Fig. 4. This is because more power may be allocated to the target MU rather than other MUs when the MBS's transmit power increases. Besides, the average SINR decreases along with the increasing number of antennas in the MBS, as the MBS transmits messages to the target MU with more power on the main lobe when using beamforming with more antennas. As a result, other MUs get less signal power but experience more interference.

On the contrary, the average SINR of the LUs improves with the increasing transmit power of the LBS as shown in Fig. 5. This can be explained by the fact that the LBSs employ NOMA to transmit signals. Particularly, the principle of NOMA suggests that more power should be allocated to the users with poor channel quality. Thus, the growth of the transmit power of an LBS can increase not only the power of the target LU but also those of other LUs.

We illustrate the secrecy performance under different SINR constraints of the MU and the LU in Fig. 6 and Fig. 7, respectively. The transmit power of the MBS is set to $P_M = 30$ dBm in Fig. 6. Intuitively, higher SINR constraints of the MUs lead to worse secrecy performance of the target MU because the MBS needs to allocate more power to other MUs to meet their SINR demands. Moreover, as the number of antennas increases, the decrease in the secrecy rate due to the increased SINR demands become less obvious. This phenomenon demonstrates that MaMIMO has a strong ability to handle multi-user SINR demands. Yet, the decrease in the target LU's secrecy rate in Fig. 7 is much clearer. This indicates that low-power nodes require more power to meet the multi-user SINR demands. Note that the optimization problem does not yield any feasible solution with $Q = 16$ dBm because the SINR demands are overly high for the limited resource in transmit power. Thus, we assume that the SINR demands of the LUs cannot exceed 2.0.

According to our observations on the secrecy performance under different SINR constraints, it is of great practical significance to take into account other users' QoSs when optimizing the secrecy rate of a target user. Further, there is an additional advantage of adopting MaMIMO, which can satisfy the multi-

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TWC.2019.2912611, IEEE Transactions on Wireless Communications

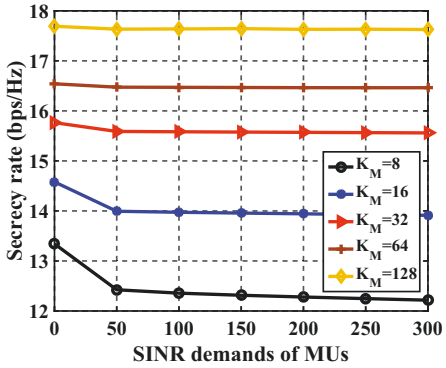


Fig. 6: Secrecy rate *vs.* SINR constraint of the MUs.

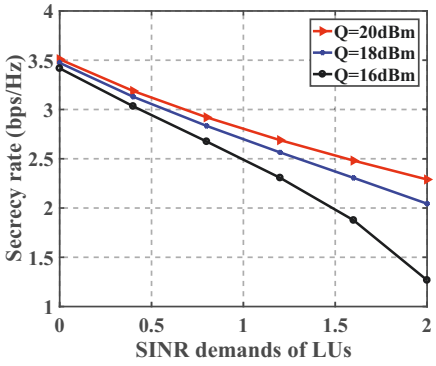


Fig. 7: Secrecy rate *vs.* SINR constraint of the LUs.

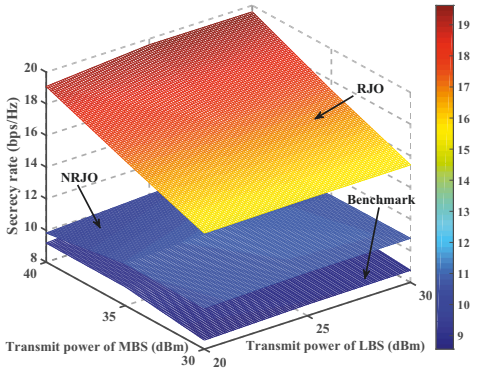


Fig. 8: Secrecy rate *vs.* transmit power of MBS and LBSs.

user SINR demands.

D. Security performance Analysis

Since there are no existing secure transmission schemes of the tiered HetNets, we design a benchmark based on [62] to analyze the secure performance of the proposed algorithms. The benchmark is designed to optimize the throughput of target users while guaranteeing the QoS of other users. We first maximize the sum rate of a target MU and a target LU without considering security. The goal is to obtain the non-security-oriented beamforming vectors $\{\mathbf{w}_i^*\}_{i=1}^M$ and the power allocation factors $\{\rho_{1,j}^*\}_{j=1}^L$. And then we derive the final secrecy rate based on these non-security-oriented parameters. More specifically, the optimization problem can be expressed as follows.

$$\textbf{Benchmark:} \max_{\substack{\{\mathbf{w}_i\}_{i=1}^M \\ \{\rho_{1,j}\}_{j=1}^L}} \quad \log(1+\gamma_m)+\log(1+\gamma_{1,l}) \tag{27a}$$

$$\text{s.t.} \quad \gamma_i \geq \epsilon_i,\ i \in [1,M] \tag{27b}$$

$$\gamma_{k,j} \geq \epsilon_{k,j},\ j \in [1,L], k \in [1,K_L] \tag{27c}$$

$$\sum\nolimits_{i=1}^{M} p_i \|\mathbf{w}_i\|^2 \leq P_M \tag{27d}$$

$$\sum\nolimits_{j=1}^{L} \rho_{k,j} = 1, \quad k \in [1,K_L]. \tag{27e}$$

Note that we still consider the QoS requirements of all users in the system. However, we do not consider robustness, i.e., the channel estimation errors are ignored.

The benchmark optimization problem is a non-convex optimization problem. We can transform it into a semi-definite program (SDP) problem by applying the semidefinite relaxation technique. We can also apply the D.C. approximation programming in Subsection IV-C. Here, we omit the specific solution process.

Moreover, we design a non-robust joint optimization (NRJO) scheme as the baseline to compare the robustness with our proposed algorithms. The NRJO is simply a special case of RJO by setting $\theta = 0$, that is, ignoring the channel estimation errors.

In our RJO scheme, we conservatively set $\theta = 0.05$ as the maximum channel estimation errors. Then, both RJO and NRJO are run to produce their respective optimal solutions in terms of the beamforming vectors and power allocation factors. These solutions are then used to calculate the achieved secrecy rate when the actual channel estimation error is $\theta = 0.01$.

The results in Fig. 8 show the secure performance of the three schemes. Here, the non-security-oriented benchmark scheme does guarantee a certain level of security, as claimed in [62]. The secure performance of the security-oriented schemes, i.e., NRJO and RJO perform better than that of the benchmark scheme. In addition, RJO demonstrates strong robustness in resisting channel estimation errors.

VI. Conclusion

In this paper, we have studied secure transmissions in a MaMIMO and NOMA enabled 5G HetNet with cooperative jamming. Three secrecy transmission algorithms, RBA, RPA and RJO, have been developed to be respectively applied in the macrocell tier, the local cell tier, and both tiers of the HetNet. Different from the existing literature, these algorithms can cope with two realistic yet challenging issues, imperfect CSI and collusive eavesdroppers. To make these problems tractable, the original non-convex optimization problems have been transformed into the corresponding convex ones. Finally, the secrecy performance of our proposed algorithms has been evaluated under different parameter settings by considering the number of antennas in the MBS, the SINR constraints of both the MUs and the LUs, as well as the channel uncertainty. Numerical results corroborate the effectiveness of our proposed algorithms. As future work, it is of interest to investigate secure transmissions when the CSI of the eavesdroppers is completely unknown.

Appendix A
Proof of Lemma 1

For robust beamformer design, here we evaluate the worst-case SINR quantities at the macro cell. In the presence of the channel uncertainty modeled in (1), the minimum $\tilde{\gamma}$ of the target MU's SINR γ_m in (8) is given by

$$\tilde{\gamma}_m = \min_{\|\Lambda_m\|} \frac{p_m |\mathbf{h}_m \mathbf{w}_m|^2}{\sum_{i=1, i\neq m}^{M} p_i |\mathbf{h}_m \mathbf{w}_i|^2 + \sigma_m^2}, \tag{28}$$

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TWC.2019.2912611, IEEE Transactions on Wireless Communications

where $\Lambda \triangleq \hat{\mathbf{h}}^H\mathbf{\Delta h} + \mathbf{\Delta h}^H\hat{\mathbf{h}} + \mathbf{\Delta h}^H\mathbf{\Delta h}$. Obviously, we can derive a bound of $\|\Lambda\|$, i.e.,

$$\begin{aligned}\|\Lambda\| &= \|\hat{\mathbf{h}}^H\mathbf{\Delta h} + \mathbf{\Delta h}^H\hat{\mathbf{h}} + \mathbf{\Delta h}^H\mathbf{\Delta h}\| \\ &\leq \|\hat{\mathbf{h}}^H\|\|\mathbf{\Delta h}\| + \|\mathbf{\Delta h}^H\|\|\hat{\mathbf{h}}\| + \|\mathbf{\Delta h}^H\|\|\mathbf{\Delta h}\| \\ &\leq \theta^2 + 2\theta\|\hat{\mathbf{h}}^H\| \triangleq \zeta.\end{aligned}$$

According to a lower bound and a upper bound proposed by [63], [64], one can minimize the numerator of (28) and maximize its denominator to obtain $\tilde{\gamma}_m$. Assuming $\hat{\mathbf{H}}^{\uparrow} = \hat{\mathbf{h}}^H\hat{\mathbf{h}} + \zeta\mathbf{I}$ and $\hat{\mathbf{H}}^{\downarrow} = \hat{\mathbf{h}}^H\hat{\mathbf{h}} - \zeta\mathbf{I}$, the minimum value of the numerator is

$$\begin{aligned}\min_{\|\Lambda_m\|} \mathbf{w}_m^H(\hat{\mathbf{H}}_m + \Lambda_m)\mathbf{w}_m =& \mathbf{w}_m^H(\hat{\mathbf{H}}_m - \zeta_m\mathbf{I})\mathbf{w}_m \\ =& \mathrm{Tr}(\hat{\mathbf{H}}_m^{\downarrow}\mathbf{W}_m),\end{aligned}$$

and the maximum value of the denominator is

$$\begin{aligned}&\max_{\|\Lambda_m\|} \sum_{i=1,i\neq m}^{M} \mathbf{w}_i^H(\hat{\mathbf{H}}_m + \Lambda_m)\mathbf{w}_i + \sigma_m^2 \\ &= \sum\nolimits_{i=1,i\neq m}^{M} \mathbf{w}_i^H(\hat{\mathbf{H}}_m + \zeta_m\mathbf{I})\mathbf{w}_i + \sigma_m^2 \\ &= \sum\nolimits_{i=1,i\neq m}^{M} \mathrm{Tr}(\hat{\mathbf{H}}_m^{\uparrow}\mathbf{W}_i) + \sigma_m^2.\end{aligned}$$

Thus we can obtain (13). Similarly, the maximum $\mathit{\Gamma}_{\text{ME}}$ can be derived as (14). This completes the proof of **Lemma 1**.

Appendix B
Proof of Lemma 2

For given functions $f_{a,\mathbf{H}}(\mathbf{w},x) = \frac{\mathbf{w}^H\mathbf{H}\mathbf{w}}{x-a}$ and $u_{b,\mathbf{H}}(\mathbf{w}) = b\mathbf{w}^H\mathbf{H}\mathbf{w}$, their first-order Taylor series expansions around the points $(\mathbf{w}^*,x^*)$ and $\mathbf{w}^*$ can be expressed as

$$\begin{aligned}F_{a,\mathbf{H}}(\mathbf{w},x,\mathbf{w}^*,x^*) =& f_{a,\mathbf{H}}(\mathbf{w}^*,x^*) \\ &+ \left.\frac{\partial f_{a,\mathbf{H}}(\mathbf{w},x)}{\partial\mathbf{w}}\right|_{(\mathbf{w}^*,x)}(\mathbf{w}-\mathbf{w}^*) \\ &+ \left.\frac{\partial f_{a,\mathbf{H}}(\mathbf{w},x)}{\partial x}\right|_{(\mathbf{w},x^*)}(x-x^*),\end{aligned} \tag{29}$$

$$U(\mathbf{w},\mathbf{w}^*) = u_{b,\mathbf{H}}(\mathbf{w}^*) + \left.\frac{\partial u_{b,\mathbf{H}}(\mathbf{w})}{\partial\mathbf{w}}\right|_{(\mathbf{w}^*)}(\mathbf{w}-\mathbf{w}^*). \tag{30}$$

According to [57], the differentiations of functions $f_{a,\mathbf{H}}(\mathbf{w},x) = \frac{\mathbf{w}^H\mathbf{H}\mathbf{w}}{x-a}$ and $g_{b,\mathbf{H}}(\mathbf{w}) = b\mathbf{w}^H\mathbf{H}\mathbf{w}$ can be given by

$$\frac{\partial f_{a,\mathbf{H}}(\mathbf{w},x)}{\partial\mathbf{w}} = \frac{\mathbf{w}^H(\mathbf{H}+\mathbf{H}^H)}{x-a} \overset{a}{=} 2\frac{\mathbf{w}^H\mathbf{H}}{x-a}, \tag{31}$$

$$\frac{\partial f_{a,\mathbf{H}}(\mathbf{w},x)}{\partial x} = -\frac{\mathbf{w}^H\mathbf{H}\mathbf{w}}{(x-a)^2}, \tag{32}$$

$$\frac{\partial g_{b,\mathbf{H}}(\mathbf{w})}{\partial\mathbf{w}} = b\mathbf{w}^H(\mathbf{H}+\mathbf{H}^H) \overset{b}{=} 2b\mathbf{w}^H\mathbf{H}, \tag{33}$$

where the reason for the existence of steps $\overset{a}{=}$ and $\overset{b}{=}$ is that $\mathbf{H}$ is a symmetric matrix.

Accordingly, we can deduce the first order Taylor expansions in **Lemma 2**.

Appendix C
Proof of Theorem 1

For the non-convex problem, we introduce two slack variables α_1 and α_2. Then (15) can be rewritten as follows:

$$\max_{\{\mathbf{w}_i\}_{i=1}^M,\alpha_1,\alpha_2} \quad \alpha_1\alpha_2 \tag{34a}$$

$$\text{s.t.} \quad 1 + \tilde{\gamma}_m \geq \alpha_1 \tag{34b}$$

$$1 + \tilde{\mathit{\Gamma}}_{\text{ME}} \leq \frac{1}{\alpha_2} \tag{34c}$$

$$\tilde{\gamma}_i \geq \epsilon_i, \quad i \in [1,M] \tag{34d}$$

$$\sum_{i=1}^{M} p_i\|\mathbf{w}_i\|^2 \leq P_M. \tag{34e}$$

Here, (34b) and (34c) are two newly introduced constraints. They, together with (34a), transform (15) into a relaxed optimization problem. Obviously, (34b) to (34e) are non-convex functions because of the fractional forms. Next, we employ **Lemma 1** and **Lemma 2** to transform these constraints into the convex ones, i.e., (16b) to (16e).

Firstly, by substituting (13) and (14), the above optimization problem can be transformed as follows,

$$\max_{\substack{\{\mathbf{w}_i\}_{i=1}^M,\\ \alpha_1,\alpha_2}} \quad \alpha_1\alpha_2 \tag{35a}$$

$$\text{s.t.} \quad 1 + \sum_{\substack{i=1,\\ i\neq m}}^{M} \mathbf{w}_i^H\hat{\mathbf{H}}_i^{\uparrow}\mathbf{w}_i \leq \frac{\mathbf{w}_m^H\hat{\mathbf{H}}_m^{\downarrow}\mathbf{w}_m}{\alpha_1 - 1} \tag{35b}$$

$$\sum_{n=1}^{N}\left(\sum_{\substack{i=1,\\ i\neq m}}^{M} \mathbf{w}_i^H\hat{\mathbf{H}}_{m,n}\mathbf{w}_i + \mathbf{w}_m^H\hat{\mathbf{H}}_{\text{ME}_n}^{\uparrow}\mathbf{w}_m + 1\right) \leq \sum_{n=1}^{M}\left\{\sum_{\substack{i=1,\\ i\neq m}}^{M}\left(\frac{\mathbf{w}_i^H\hat{\mathbf{H}}_{\text{ME}_n}^{\downarrow}\mathbf{w}_i}{\alpha_2} + \mathbf{w}_i^H\mathbf{I}_{\zeta_{\text{ME}_n}}\mathbf{w}_i\right) + \frac{1}{\alpha_2}\right\} \tag{35c}$$

$$\left(1 + \sum_{\substack{j=1,\\ j\neq i}}^{M} \mathbf{w}_j^H\hat{\mathbf{H}}_i\mathbf{w}_j\right)\epsilon_i + \mathbf{w}_i^H\mathbf{I}_{\zeta_i}\mathbf{w}_i \leq \mathbf{w}_i^H\hat{\mathbf{H}}_i\mathbf{w}_i + \epsilon_i\sum_{\substack{j=1,\\ j\neq i}}^{M}\mathbf{w}_j^H\mathbf{I}_{\zeta_j}\mathbf{w}_j \ , \ i \in [1,M] \tag{35d}$$

$$\sum_{i=1}^{M}\|\mathbf{w}_i\|^2 \leq P_M, \tag{35e}$$

where (35b), (35c) and (35d) are non-convex. The reason is that these can be expressed as $f(x_1) \leq f(x_2)$, where both $f(x_1)$ and $f(x_2)$ are convex functions but $f(x_1) - f(x_2)$ is non-convex. Based on **Lemma 2**, for the points (w^*,x^*) and w^*, we can transform the right sides of (35b), (35c) and (35d) into linear form.

Moreover, we introduce another slack variable α_0 to transform the quasi-convex objective function ($\max\alpha_1\alpha_2$) into a convex function ($\max\alpha_0^2$). As a result, we should add an additional constraint, $\alpha_1\alpha_2 \geq \alpha_0^2$, to ensure an equivalent transformation. Because $\alpha_1 \geq 0$ and $\alpha_2 \geq 0$, $\alpha_0^2 \leq \alpha_1\alpha_2 \Leftrightarrow 4\alpha_0^2 + (\alpha_1-\alpha_2)^2 \leq (\alpha_1+\alpha_2)^2$ and then this additional constraint can be rewritten as the form of inequality (16g).

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TWC.2019.2912611, IEEE Transactions on Wireless Communications

To sum up, the non-convex problem (15) can be transformed into a tractable SOCP form as shown in (16), where three auxiliary linear functions t_1, t_2, t_{3i} are defined as follows,

$$\begin{aligned}
t_1 =& F_{1,\hat{\mathbf{H}}_m^{\downarrow}}(\mathbf{w}_m, \alpha_1, \mathbf{w}_m^*, \alpha_1^*) - 1, \\
t_2 =& \sum_{n=1}^{N} \Bigg\{ \sum_{\substack{i=1 \\ i\neq m}}^{M} \Bigg(F_{0,\hat{\mathbf{H}}_{\mathrm{ME}_n}^{\downarrow}}(\mathbf{w}_i, \alpha_2, \mathbf{w}_i^*, \alpha_2^*) \\
& + U_{1,\mathbf{I}_{\zeta_{\mathrm{ME}_n}}}(\mathbf{w}_i, \mathbf{w}_i^*) \Bigg) + \frac{2\alpha_2^* - \alpha_2}{(\alpha_2^*)^2} \Bigg\}, \\
t_{3i} =& U_{1,\hat{\mathbf{H}}_i}(\mathbf{w}_i, \mathbf{w}_i^*) + \sum_{\substack{j=1 \\ j\neq i}}^{M} U_{\epsilon_i,\mathbf{I}_{\zeta_i}}(\mathbf{w}_j, \mathbf{w}_j^*), \quad i \in [1, M].
\end{aligned}$$

This completes the proof of **Theorem 1**.

Appendix D
Proof of Theorem 2

Similar to the proof of **Theorem 1**, (19) can be rewritten via the relaxation technique as follows:

$$\begin{aligned}
\max_{\{\rho_j\}_{j=1}^{L}, \beta_1, \beta_2} \quad & \log \beta_1 + \log \beta_2 && \text{(36a)} \\
\text{s.t.} \quad & 1 + \tilde{\gamma}_l \geq \beta_1 && \text{(36b)} \\
& 1 + \tilde{I}_{\mathrm{LE}} \leq \frac{1}{\beta_2} && \text{(36c)} \\
& \tilde{\gamma}_j \geq \epsilon_j, \quad j \in [1, L] && \text{(36d)} \\
& \sum_{j=1}^{L} \rho_j = 1. && \text{(36e)}
\end{aligned}$$

Here, we can utilize (20), (20), and **Lemma 3** to transform the non-convex constraints (from (36b) to (36d)) into convex forms (from (20b) to (20d)).

Firstly, by substituting (20) and (20), (36b) and (36c) can be transformed as follows,

$$\begin{aligned}
& \sum_{j=l+1}^{L} \rho_j P_L |\hat{h}_l^{\uparrow}|^2 + \theta_l^2 \sum_{j=1}^{l-1} \rho_j P_L \\
& \qquad + \sum_{i=1}^{M} \mathrm{Tr}(\hat{\mathbf{G}}_l^{\uparrow} \mathbf{W}_i) + 1 \leq \frac{P_L |\hat{h}_l^{\downarrow}|^2 \rho_l}{\beta_1 - 1}, \qquad (37) \\
& \sum_{n=1}^{N} \sum_{\substack{j=n_g+1 \\ j\neq l}}^{L} \Bigg(\rho_j P_L |\hat{h}_{l,n}^{\downarrow}|^2 + \rho_l P_L |\hat{h}_{l,n}^{\uparrow}|^2 \\
& \qquad + \sum_{i=1}^{M} \mathrm{Tr}(\hat{\mathbf{G}}_{\mathrm{LE}_n}^{\downarrow} \mathbf{W}_i) + 1 \Bigg) \leq \\
& \sum_{n=1}^{N} \sum_{\substack{j=n_g+1 \\ j\neq l}}^{L} \left(\frac{P_L |\hat{h}_{l,n}^{\downarrow}|^2 \rho_j}{\beta_2} + \frac{\sum_{i=1}^{M} \mathrm{Tr}(\hat{\mathbf{G}}_{\mathrm{LE}_n}^{\downarrow} \mathbf{W}_i) + 1}{\beta_2} \right). \qquad (38)
\end{aligned}$$

Here, the optimization problem is still non-convex and non-linear due to the righthand sides of the constraints (37) and (38). Again, we can apply the first-order Taylor series expansion approximations to further transform it into a convex and solvable optimization problem. According to **Lemma 3**, the righthand sides of (37) and (38) can be approximated by their first-order Taylor series expansions at $\{\{\rho_j^*\}_{j=1}^{L}, \beta_1^*, \beta_2^*\}$. Eventually, the initial optimization problem can be transformed into a convex optimization problem, due to its concave objective function and linear constraints.

This completes the proof of **Theorem 2**.

References

[1] J. G. Andrews, S. Buzzi, C. Wan, S. V. Hanly, A. Lozano, A. C. K. Soong, and J. C. Zhang, "What will 5G be?" *IEEE Journal on Selected Areas in Communications*, vol. 32, no. 6, pp. 1065–1082, 2014.

[2] A. Damnjanovic, J. Montojo, Y. Wei, T. Ji, T. Luo, M. Vajapeyam, T. Yoo, O. Song, and D. Malladi, "A survey on 3GPP heterogeneous networks," *IEEE Wireless Communications*, vol. 18, no. 3, pp. 10–21, 2011.

[3] A. Ghosh, N. Mangalvedhe, R. Ratasuk, B. Mondal, M. Cudak, E. Visotsky, T. A. Thomas, J. G. Andrews, X. Ping, and S. J. Han, "Heterogeneous cellular networks: from theory to practice," *IEEE Communications Magazine*, vol. 50, no. 6, pp. 54–64, 2012.

[4] J. Zhang, L. Dai, Z. He, S. Jin, and X. Li, "Performance analysis of mixed-ADC massive MIMO systems over rician fading channels," *IEEE Journal on Selected Areas in Communications*, vol. 35, no. 6, pp. 1327–1338, June 2017.

[5] W. Shin, M. Vaezi, B. Lee, D. J. Love, J. Lee, and H. V. Poor, "Non-orthogonal multiple access in multi-cell networks: theory, performance, and practical challenges," *IEEE Communications Magazine*, vol. 55, no. 10, pp. 176–183, Oct 2017.

[6] M. Agiwal, A. Roy, and N. Saxena, "Next generation 5G wireless networks: A comprehensive survey," *IEEE Communications Surveys Tutorials*, vol. 18, no. 3, pp. 1617–1655, thirdquarter 2016.

[7] Y. Liu, Z. Qin, M. Elkashlan, A. Nallanathan, and J. A. McCann, "Non-orthogonal multiple access in large-scale heterogeneous networks," *IEEE Journal on Selected Areas in Communications*, vol. 35, no. 12, pp. 2667–2680, Dec 2017.

[8] Y. Liu, H. H. Chen, and L. Wang, "Physical layer security for next generation wireless networks: theories, technologies, and challenges," *IEEE Communications Surveys Tutorials*, vol. 19, no. 1, pp. 347–376, Firstquarter 2017.

[9] A. Mukherjee, S. A. A. Fakoorian, J. Huang, and A. L. Swindlehurst, "Principles of physical layer security in multiuser wireless networks: A survey," *IEEE Communications Surveys Tutorials*, vol. 16, no. 3, pp. 1550–1573, Third 2014.

[10] Y. Huo, Y. Tian, L. Ma, X. Cheng, and T. Jing, "Jamming strategies for physical layer security," *IEEE Wireless Communications*, vol. 25, no. 1, pp. 148–153, February 2018.

[11] K. Cumanan, G. C. Alexandropoulos, Z. Ding, and G. K. Karagiannidis, "Secure communications with cooperative jamming: optimal power allocation and secrecy outage analysis," *IEEE Transactions on Vehicular Technology*, vol. 66, no. 8, pp. 7495–7505, Aug 2017.

[12] H. Wu, X. Tao, Z. Han, N. Li, and J. Xu, "Secure transmission in misome wiretap channel with multiple assisting jammers: maximum secrecy rate and optimal power allocation," *IEEE Transactions on Communications*, vol. 65, no. 2, pp. 775–789, Feb 2017.

[13] P. Siyari, M. Krunz, and D. N. Nguyen, "Friendly jamming in a mimo wiretap interference network: A nonconvex game approach," *IEEE Journal on Selected Areas in Communications*, vol. 35, no. 3, pp. 601–614, March 2017.

[14] Q. Gao, Y. Huo, L. Ma, X. Xing, X. Cheng, T. Jing, and H. Liu, "Optimal stopping theory based jammer selection for securing cooperative cognitive radio networks," in *2016 IEEE Global Communications Conference (GLOBECOM)*, Dec 2016, pp. 1–6.

[15] ——, "Joint design of jammer selection and beamforming for securing mimo cooperative cognitive radio networks," *IET Communications*, vol. 11, no. 8, pp. 1264–1274, 2017.

[16] T. Lv, H. Gao, and S. Yang, "Secrecy transmit beamforming for heterogeneous networks," *IEEE Journal on Selected Areas in Communications*, vol. 33, no. 6, pp. 1154–1170, 2015.

[17] H. Wu, X. Tao, N. Li, and J. Xu, "Secrecy outage probability in multi-RAT heterogeneous networks," *IEEE Communications Letters*, vol. 20, no. 1, pp. 53–56, 2016.

[18] H. H. Kha, H. D. Tuan, and H. H. Nguyen, "Fast global optimal power allocation in wireless networks by local d.c. programming," *IEEE Transactions on Wireless Communications*, vol. 11, no. 2, pp. 510–515, 2012.

[19] C. E. Shannon, "Communication theory of secrecy systems," *Bell Labs Technical Journal*, vol. 28, no. 4, pp. 656–715, 1949.

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

[21] Y. S. Shiu, S. Y. Chang, H. C. Wu, S. C. H. Huang, and H. H. Chen, "Physical layer security in wireless networks: a tutorial," *IEEE Wireless Communications*, vol. 18, no. 2, pp. 66–74, April 2011.

[22] C. Y. Wu, P. C. Lan, P. C. Yeh, C. H. Lee, and C. M. Cheng, "Practical physical layer security schemes for MIMO-OFDM systems using precoding matrix indices," *IEEE Journal on Selected Areas in Communications*, vol. 31, no. 9, pp. 1687–1700, September 2013.

[23] K. Ren, H. Su, and Q. Wang, "Secret key generation exploiting channel characteristics in wireless communications," *IEEE Wireless Communications*, vol. 18, no. 4, pp. 6–12, August 2011.

[24] Y. Hwang and H. C. Papadopoulos, "Physical-layer secrecy in AWGN via a class of chaotic DS/SS systems: analysis and design," *IEEE Transactions on Signal Processing*, vol. 52, no. 9, pp. 2637–2649, Sept 2004.

[25] J. S. Sousa and J. P. Vilela, "Uncoordinated frequency hopping for wireless secrecy against non-degraded eavesdroppers," *IEEE Transactions on Information Forensics and Security*, vol. 13, no. 1, pp. 143–155, Jan 2018.

[26] R. Negi and S. Goel, "Secret communication using artificial noise," in *VTC-2005-Fall. 2005 IEEE 62nd Vehicular Technology Conference, 2005.*, vol. 3, Sept 2005, pp. 1906–1910.

[27] Y. Li, M. Jiang, Q. Zhang, Q. Li, and J. Qin, "Secure beamforming in downlink MISO nonorthogonal multiple access systems," *IEEE Transactions on Vehicular Technology*, vol. 66, no. 8, pp. 7563–7567, Aug 2017.

[28] K. Cumanan, H. Xing, P. Xu, G. Zheng, X. Dai, A. Nallanathan, Z. Ding, and G. K. Karagiannidis, "Physical layer security jamming: Theoretical limits and practical designs in wireless networks," *IEEE Access*, vol. 5, no. 99, pp. 3603–3611, 2017.

[29] M. Atallah, G. Kaddoum, and K. Long, "A survey on cooperative jamming applied to physical layer security," in *IEEE International Conference on Ubiquitous Wireless Broadband*, 2015, pp. 1–5.

[30] X. Zhou and M. R. Mckay, "Secure transmission with artificial noise over fading channels: Achievable rate and optimal power allocation," *IEEE Transactions on Vehicular Technology*, vol. 59, no. 8, pp. 3831–3842, 2010.

[31] E. A. Jorswieck, "Secrecy capacity of single- and multi-antenna channels with simple helpers," in *International Itg Conference on Source and Channel Coding*, 2010, pp. 1–6.

[32] R. Zhang, L. Song, Z. Han, and B. Jiao, "Physical layer security for two-way untrusted relaying with friendly jammers," *IEEE Transactions on Vehicular Technology*, vol. 61, no. 8, pp. 3693–3704, Oct 2012.

[33] T. T. Tran and H. Y. Kong, "CSI-secured orthogonal jamming method for wireless physical layer security," *IEEE Communications Letters*, vol. 18, no. 5, pp. 841–844, May 2014.

[34] H. Hui, A. L. Swindlehurst, G. Li, and J. Liang, "Secure relay and jammer selection for physical layer security," *IEEE Signal Processing Letters*, vol. 22, no. 8, pp. 1147–1151, 2015.

[35] Z. Li, T. Jing, X. Cheng, Y. Huo, W. Zhou, and D. Chen, "Cooperative jamming for secure communications in MIMO cooperative cognitive radio networks," in *2015 IEEE International Conference on Communications (ICC)*, June 2015, pp. 7609–7614.

[36] Z. Li, T. Jing, Y. Huo, and J. Qian, "Worst-case jamming for secure communications in multi-antenna cooperative cognitive radio networks with energy harvesting," in *2015 International Conference on Identification, Information, and Knowledge in the Internet of Things (IIKI)*, Oct 2015, pp. 110–115.

[37] Z. Li, T. Jing, L. Ma, Y. Huo, and J. Qian, "Worst-case cooperative jamming for secure communications in CIoT networks," *Sensors*, vol. 16, no. 3, p. 339, 2016.

[38] W. Wang, T. Lv, and H. Gao, "Robust beamforming and power allocation for secrecy in df relay networks with imperfect channel state information," *IEEE Access*, vol. 4, pp. 9520–9527, 2016.

[39] C. Zheng, K. Cumanan, Z. Ding, M. Johnston, and S. Y. L. Goff, "Secrecy rate optimizations for a mimo secrecy channel with a cooperative jammer," *IEEE Transactions on Vehicular Technology*, vol. 64, no. 5, pp. 1833–1847, 2015.

[40] M. Haenggi, J. G. Andrews, F. Baccelli, O. Dousse, and M. Franceschetti, "Stochastic geometry and random graphs for the analysis and design of wireless networks," *IEEE Journal on Selected Areas in Communications*, vol. 27, no. 7, pp. 1029–1046, 2009.

[41] M. Ghogho and A. Swami, "Physical-layer secrecy of MIMO communications in the presence of a poisson random field of eavesdroppers," in *IEEE International Conference on Communications Workshops*, 2011, pp. 1–5.

[42] H. Li, X. Wang, and W. Hou, "Security enhancement in cooperative jamming using compromised secrecy region minimization," in *2013 13th Canadian Workshop on Information Theory*, June 2013, pp. 214–218.

[43] F. Xin, H. Liang, H. Yan, C. Hu, Y. Tian, and Q. Jin, "Space power synthesis-based cooperative jamming for unknown channel state information," in *International Conference on Wireless Algorithms*, 2017.

[44] L. Huang, X. Fan, Y. Huo, C. Hu, Y. Tian, and J. Qian, "A novel cooperative jamming scheme for wireless social networks without known CSI," *IEEE Access*, vol. 5, pp. 26 476–26 486, 2017.

[45] N. Yang, L. Wang, G. Geraci, and M. Elkashlan, "Safeguarding 5G wireless communication networks using physical layer security," *Communications Magazine IEEE*, vol. 53, no. 4, pp. 20–27, 2016.

[46] H. M. Wang, T. X. Zheng, J. Yuan, D. Towsley, and M. H. Lee, "Physical layer security in heterogeneous cellular networks," *IEEE Transactions on Communications*, vol. 64, no. 3, pp. 1204–1219, 2016.

[47] Y. Deng, L. Wang, K. K. Wong, and A. Nallanathan, "Safeguarding massive MIMO aided hetnets using physical layer security," in *International Conference on Wireless Communications & Signal Processing*, 2015, pp. 1–5.

[48] Y. Wu, R. Schober, D. W. K. Ng, C. Xiao, and G. Caire, "Secure massive MIMO transmission with an active eavesdropper," *IEEE Transactions on Information Theory*, vol. 62, no. 7, pp. 3880–3900, July 2016.

[49] Y. Zhang, H. M. Wang, Q. Yang, and Z. Ding, "Secrecy sum rate maximization in non-orthogonal multiple access," *IEEE Communications Letters*, vol. 20, no. 5, pp. 930–933, 2016.

[50] Y. Liu, Z. Qin, M. Elkashlan, Y. Gao, and L. Hanzo, "Enhancing the physical layer security of non-orthogonal multiple access in large-scale networks," *IEEE Transactions on Wireless Communications*, vol. 16, no. 3, pp. 1656–1672, March 2017.

[51] K. Abed-Meraim, P. Loubaton, and E. Moulines, "A subspace algorithm for certain blind identification problems," *IEEE Transactions on Information Theory*, vol. 43, no. 2, pp. 499–511, March 1997.

[52] T. Lv, S. Yang, and H. Gao, "Semi-blind channel estimation relying on optimum pilots designed for multi-cell large-scale MIMO systems," *IEEE Access*, vol. 4, pp. 1190–1204, 2016.

[53] C. Chen, L. Bai, B. Wu, and J. Choi, "Downlink throughput maximization for OFDMA systems with feedback channel capacity constraints," *IEEE Transactions on Signal Processing*, vol. 59, no. 1, pp. 441–446, 2011.

[54] M. You, H. Sun, J. Jiang, and J. Zhang, "Unified framework for the effective rate analysis of wireless communication systems over MISO fading channels," *IEEE Transactions on Communications*, vol. 65, no. 4, pp. 1775–1785, April 2017.

[55] Q. Zhang, Q. Li, and J. Qin, "Robust beamforming for nonorthogonal multiple-access systems in miso channels." *IEEE Trans. Vehicular Technology*, vol. 65, no. 12, pp. 10 231–10 236, 2016.

[56] Y. Zhang, Y. Shen, H. Wang, J. Yong, and X. Jiang, "On secure wireless communications for iot under eavesdropper collusion," *IEEE Transactions on Automation Science and Engineering*, vol. 13, no. 3, pp. 1281–1293, July 2016.

[57] EricZiegel, "Matrix differential calculus with applications in statistics and econometrics," *Technometrics*, vol. 31, no. 4, pp. 501–502, 1989.

[58] M. Grant and S. Boyd, "Cvx: Matlab software for disciplined convex programming, version 1.21," *Global Optimization*, pp. 155–210, 2008.

[59] T. Yoo, "Optimality of zero-forcing beamforming with multiuser diversity," *IEEE Int.conf.commun*, vol. 1, pp. 542–546, 2005.

[60] Q. Li, Q. Zhang, and J. Qin, "Secure relay beamforming for SWIPT in amplify-and-forward two-way relay networks," *IEEE Transactions on Vehicular Technology*, vol. 65, no. 11, pp. 9006–9019, 2016.

[61] Z. Q. Luo, W. K. Ma, M. C. So, Y. Ye, and S. Zhang, "Semidefinite relaxation of quadratic optimization problems," *IEEE Signal Processing Magazine*, vol. 27, no. 3, pp. 20–34, 2010.

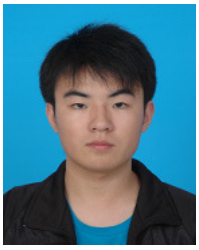
[62] A. Mukherjee and A. L. Swindlehurst, "Fixed-rate power allocation strategies for enhanced secrecy in mimo wiretap channels," in *Signal Processing Advances in Wireless Communications, 2009. Spawc '09. IEEE Workshop on*, 2009, pp. 344–348.

[63] M. Bengtsson and B. Ottersten, "Optimal downlink beamforming using semidefinite optimization," in *37th Annual Allerton Conference on Communication, Control, and Computing*, 1999, pp. 987–996.

[64] ——, "Optimum and suboptimum transmit beamforming," in *Chapter 18 of Handbook of Antennas in Wireless Communications*. CRC Press, 2001.

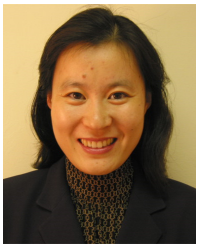
This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TWC.2019.2912611, IEEE Transactions on Wireless Communications

Yan Huo is currently a Professor in School of Electronics and Information Engineering at Beijing Jiaotong University. He received the B.E. and Ph.D. degrees in Communication and Information System from Beijing Jiaotong University, Beijing, China, in 2004 and 2009 respectively. He was a visiting scholar to the Department of Computer Science at the George Washington University from 2015 to 2016. His current research interests include wireless communications, security and privacy, and vehicular networks. He has served as an associate editor for IEEE Access and a reviewer for a number of journals including IEEE Wireless Communications, IEEE Transactions on Wireless Communications, and IEEE Transactions on Mobile Computing. He is a member of IEEE.



Xin Fan received his B.E. and M.S. degrees in School of Electronic and Information Engineering, Beijing Jiaotong University, Beijing, China. He is currently pursuing the Ph.D. degree in Beijing Jiaotong University. His current research interests include 5G wireless networks, cooperative communications and physical layer security.

Liran Ma is currently an Associate Professor in the Department of Computer Science at Texas Christian University. He received his D.Sc. degree in Computer Science from the George Washington University. His current research focuses on wireless, mobile, and embedded systems, including security and privacy, smartphones, smart health, mobile computing, data analytics, Internet of Things, and security education.



Xiuzhen Cheng received her MS and PhD degrees in computer science from the University of Minnesota – Twin Cities, in 2000 and 2002, respectively. She is a professor at the Department of Computer Science, The George Washington University, Washington DC. Her current research focuses on Blockchain computing, intelligent Internet of Things, privacy-aware computing, wireless and mobile security, and algorithm design and analysis. She is the founder and steering committee chair of the International Conference on Wireless Algorithms, Systems, and Applications (WASA, launched in 2006). She served/is serving on the editorial boards of several technical journals (e.g. IEEE Transactions on Computers, IEEE Transactions on Parallel and Distributed Systems, IEEE Wireless Communications) and the technical program committees of many professional conferences/workshops (e.g. ACM Mobihoc, ACM Mobisys, IEEE INFOCOM, IEEE ICDCS, IEEE ICC, IEEE/ACM IWQoS). She also chaired several international conferences (e.g. ACM Mobihoc'14, IEEE PAC'18). Xiuzhen worked as a program director for the US National Science Foundation (NSF) from April to October in 2006 (full time), and from April 2008 to May 2010 (part time). She published more than 200 peer-reviewed papers. She is a Fellow of IEEE.

Zhi Tian is a Professor in the Electrical and Computer Engineering Department of George Mason University, Fairfax, VA, since 2015. Prior to that, she was on the faculty of Michigan Technological University from 2000 to 2014, and she served a three-year term as a Program Director at the US National Science Foundation. Her current research focuses on 5G wireless communications, high-dimensional statistical signal processing, and decentralized optimization and learning. She is an IEEE Fellow. She was an IEEE Distinguished Lecturer for both the IEEE Communications Society and the IEEE Vehicular Technology Society. She served as Associate Editor for IEEE Transactions on Wireless Communications and IEEE Transactions on Signal Processing. She served on many posts with the IEEE, such as General Chair of the 2016 IEEE GlobalSIP Conference, Chair of the IEEE Signal Processing Society Big Data Special Interest Group, and Member-at-large of the Signal Processing Society Board of Governors. She won the 2018 Communication Society TCCN Publication Award.

Dechang Chen received the B.S. degree in applied mathematics from Southeast University, China, in 1983, the M.S. degree in mathematics from Peking University, China, in 1988, the M.S. degree in statistics and the Ph.D. degree in mathematics from SUNY Buffalo, USA, in 1998. He is a Professor with the Division of Epidemiology and Biostatistics, Department of Preventive Medicine and Biometrics, Uniformed Services University of the Health Sciences. His research interests include bioinformatics, computational medicine, machine learning, wireless networks, applied statistics, and differential equations.