Base Station Cooperation for Confidential Broadcasting in Multi-Cell Networks

Biao He, *Student Member, IEEE,* Nan Yang, *Member, IEEE,* Xiangyun Zhou, *Member, IEEE,* and Jinhong Yuan, *Senior Member, IEEE*

***Abstract*—We design linear precoders that perform confidential broadcasting in multi-cell networks for two different forms of base station (BS) cooperation, namely, multi-cell processing (MCP) and coordinated beamforming (CBf). We consider a two-cell network where each cell consists of an N-antenna BS and K single-antenna users. For such a network, we design a linear precoder based on the regularized channel inversion (RCI) for the MCP and a linear precoder based on the generalized RCI for the CBf. For each form of BS cooperation, we derive new channel-independent expressions to approximate the secrecy sum rate achieved by the precoder in the large system regime where $K, N \rightarrow \infty$ with a fixed ratio $\beta = K/N$. Using these results, we determine the optimal regularization parameters of the RCI and the generalized RCI precoders that maximize the secrecy sum rate for the MCP and the CBf, respectively. We further propose power-reduction strategies that significantly increase the secrecy sum rate at high transmit signal-to-noise ratios when the network load is high. Our numerical results substantiate the derived expressions, verify the optimality of the determined optimal regularization parameters, and demonstrate the performance improvement offered by the proposed power-reduction strategies.**

***Index Terms*—Physical layer security, confidential broadcasting, multi-cell processing, coordinated beamforming, linear precoder.**

I. Introduction

WIRELESS devices have become ubiquitous in everyday life with their great flexibility and mobility, which results in a rapid growing amount of private and sensitive data transmitted over wireless channels. Due to the unalterable open nature of the wireless medium, how to secure the data transmissions is one of the core problems that any wireless network designer can face. As a complement to traditional cryptographic techniques, physical layer security techniques have been widely studied [2, 3] to ensure secure wireless data transmission by exploiting the characteristics of wireless channels. The seminal work by Wyner [4] introduced the wiretap channel model as a fundamental framework for physical layer security and defined the secrecy capacity as the maximum rate at which the message can be reliable transmitted to the legitimate receiver without being eavesdropped. This result was then extended to the broadcast channel with confidential messages in [5] and the Gaussian wiretap channel in [6].

In recent years, the increasing demand of high data rates in practical wireless applications, e.g., high-quality video streaming, has sparked a surge in the development of multiple-input multiple-output (MIMO) techniques. This has triggered an enormous amount of research activities investigating physical layer security in MIMO wiretap channels, where the transmitter, the receiver and/or the eavesdropper are equipped with multiple antennas. For instance, the secrecy capacity was analyzed for the MIMO wiretap channel from the information-theoretical perspective, e.g., [7–9], and some signal processing techniques were proposed to improve the secrecy performance of the MIMO wiretap channel, e.g., [10–13]. Apart from the MIMO wiretap channel, some literatures have focused on the physical layer security in multi-antenna broadcast networks, aiming at achieving confidential broadcasting. Different from the wiretap channel, confidential broadcasting requires multiple messages to be securely broadcasted to multiple users in the network. Each of the multiple messages is intended for one of the users but needs to be kept secret from the other users. The secrecy capacity of the two-user multi-antenna broadcast network was examined in [14, 15]. The confidential broadcasting in the multi-user network where a multi-antenna base station (BS) serves an arbitrary number of receivers *in a single cell* was studied in [16–19]. While the confidential broadcasting in a single cell has been elaborately studied, the solution to confidentially broadcasting messages in *multi-cell* networks has not been addressed in the literature. The primary challenge to achieve confidential broadcasting in the multi-cell network is to deal with not only the inter-cell information leakage and interference but the intra-cell information leakage and interference. Thus, the techniques achieving single-cell confidential broadcasting in [16–19] cannot be directly applied to achieve multi-cell confidential broadcasting.

In this work we build up an effective solution to tackle this challenge. To this end, we design linear precoders at BSs that achieve confidential broadcasting in the multi-cell network. In the network, BS cooperation [20] is taken into consideration such that the BSs can share control signals, channel state information (CSI) and/or messages to cooperatively serve users in multiple cells. With BS cooperation, we specifically consider the confidential broadcasting in a symmetric two-cell network where there are K single-antenna users and one N-antenna BS in each cell. The two BSs cooperatively broadcast confidential information to the users. For each message transmitted to the

This work was supported by the Australian Research Council under Discovery Project (DP150103905). This work has been accepted in part for presentation at the 2015 IEEE International Conference on Communications (ICC) [1].

B. He, N. Yang, and X. Zhou are with the Research School of Engineering, Australian National University, Canberra, ACT 0200, Australia (e-mail: biao.he@anu.edu.au, nan.yang@anu.edu.au, xiangyun.zhou@anu.edu.au).

J. Yuan is with the School of Electrical Engineering and Telecommunications, The University of New South Wales, Sydney, NSW 2052, Australia (e-mail: j.yuan@unsw.edu.au).

intended user, we consider the worst-case scenario where the unintended users in both the same cell and the cross cell are regarded as potential cooperating eavesdroppers. We focus on two different forms of cooperation at the BSs: i) multi-cell processing (MCP) and ii) coordinated beamforming (CBf). In the MCP, the BSs fully cooperate such that they share their CSI and messages to transmit. Alternatively, in the CBf the BSs "partially" cooperate. As such, they do not share their messages to transmit but allow users to feed back the CSI to the cross-cell BS. In practice, the MCP is appropriate for the networks where high-capacity backhaul links are established to enable the sharing of CSI and messages between BSs, while the CBf is suitable for the networks where such high-capacity backhaul links are not available. Besides, the investigation of the two-cell network in this work can be extended to general multi-cell networks.

The primary contributions of this paper are summarized as follows.

- We design a linear precoder as per the principles of regularized channel inversion (RCI)[1] [21] to perform confidential broadcasting in the multi-cell network with the MCP. We also design a linear precoder as per the principles of generalized RCI [22] to perform confidential broadcasting in the multi-cell network with the CBf. In each precoder, the precoding matrix is designed to trade off the intended received signal, the intra- and inter-cell information leakage, and the intra- and inter-cell interference via a regularization parameter.
- We derive new channel-independent expressions for the secrecy sum rate achieved by the designed linear precoders for both the MCP and the CBf in the large-system regime. In this regime, we consider $K, N \to \infty$ and keep the ratio $\beta = K/N$ constant. The large-system expressions do not depend on the channel realizations, and thus eliminate the computational burden of performance evaluation incurred by Monte Carlo simulations. Notably, numerical results confirm that our large-system expressions are accurate even for finite K and N.
- We optimize the secrecy performance of confidential broadcasting in the multi-cell network based on our large-system expressions. We first determine the optimal regularization parameters of the RCI and the generalized RCI precoders in order to maximize the secrecy sum rate for the MCP and the CBf, respectively. We then propose power-reduction strategies for the MCP when $\beta > 1$ and the CBf when $\beta > 0.5$, which significantly increase the secrecy sum rate at high transmit signal-to-noise ratios (SNRs) when the network load is high.

Notations: $(\cdot)^T$ and $(\cdot)^H$ denote the transpose and conjugate transpose of a vector or a matrix, respectively, $\mathrm{Tr}(\cdot)$ denotes the trace of a matrix, $\|\cdot\|$ denotes the Euclidean norm of a vector, $\mathbb{E}\{\cdot\}$ denotes the expectation operation, $[x]^+ = \max(x, 0)$, $\xrightarrow{a.s}$ and $\xrightarrow{i.p.}$ denote almost sure convergence and convergence in probability, respectively.

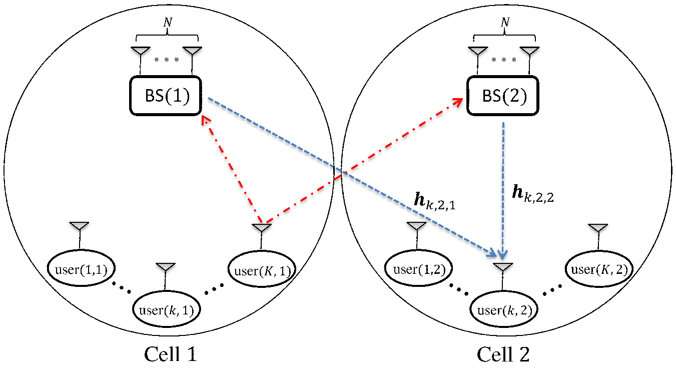


Fig. 1. Illustration of a symmetric two-cell broadcast network, where each cell consists of one N-antenna BS and K single-antenna users.

II. Network Model

We consider a symmetric two-cell broadcast network, as depicted in Figure 1. In each cell, there are K single-antenna users and one N-antenna BS. The two BSs cooperate to serve the users in two cells. For this network, we consider two forms of BS cooperation in this paper, i.e., the MCP and the CBf, the practicality of which are presented in Section I. For the sake of brevity, throughout the paper we denote BS (i) and user (k, j) as the BS in cell i and the user k in cell j, respectively, where $i \in \{1, 2\}$, $j \in \{1, 2\}$ and $k \in \{1, 2, \cdots, K\}$. Moreover, we adopt the following notations to represent the channel coefficients in the two-cell broadcast network:

1) The channel vector from BS (i) to user (k, j) is denoted by the *row* vector $\mathbf{h}_{k,j,i}$.
2) The $2K \times N$ channel matrix from BS (i) to all the users in both cells is denoted by $\mathbf{H}_i = \left[\mathbf{h}_{1,1,i}^H \; \mathbf{h}_{2,1,i}^H \cdots \mathbf{h}_{K,1,i}^H \; \mathbf{h}_{1,2,i}^H \; \mathbf{h}_{2,2,i}^H \cdots \mathbf{h}_{K,2,i}^H\right]^H$.
3) The channel vector from both BSs to user (k, j) is denoted by $\mathbf{h}_{k,j} = [\mathbf{h}_{k,j,1} \; \mathbf{h}_{k,j,2}]$.
4) The $2K \times 2N$ channel matrix from both BSs to all the users in both cells is denoted by $\mathbf{H} = \left[\mathbf{h}_{1,1}^H \; \mathbf{h}_{2,1}^H \cdots \mathbf{h}_{K,1}^H \; \mathbf{h}_{1,2}^H \; \mathbf{h}_{2,2}^H \cdots \mathbf{h}_{K,2}^H\right]^H$.
5) The channel vector between a user and the same-cell BS is denoted by $\mathbf{h}_{k,j,j}$.
6) The channel vector between a user and the cross-cell BS is denoted by $\mathbf{h}_{k,j,\bar{j}}$ where $\bar{j} = 1$ if $j = 2$ and $\bar{j} = 2$ if $j = 1$.

We assume that the antennas at the BSs and the users are sufficiently spaced apart such that all links between the transmit and receive antennas are uncorrelated. We also assume that the data are transmitted over the block fading channel where the coherence time of the channel is larger than the symbol interval. In addition, we consider a homogenous scenario where all users in the same cell to a BS have the same average power. This is a widely-adopted consideration for multi-user networks where the users in the same cell are located at the same distance away from the BS. A practical example of this scenario is that the users in the same cell are close together, e.g., in an office building, but far from the BS. Then, the channels between a user and the same-cell BS are modeled as independent and identically distributed (i.i.d.) complex Gaussian variables with zero mean and unit

[1] The regularized channel inversion (RCI) is also sometimes called as regularized zero forcing (RZF) in some literatures.

variance, i.e., $\mathbf{h}_{k,j,j} \sim \mathcal{CN}(\mathbf{0}, \mathbf{I}_N)$, whereas the channels between a user and the cross-cell BS are modeled as i.i.d. complex Gaussian variables with zero mean and variance ϵ, i.e., $\mathbf{h}_{k,j,\bar{j}} \sim \mathcal{CN}(\mathbf{0}, \epsilon\mathbf{I}_N)$. Here, $0 < \epsilon \leq 1$ represents the cross-cell interference level, which characterizes the severity of interference between two cells. In addition, we assume that each user (k, j) perfectly knows $\mathbf{h}_{k,j}$ and feeds back $\mathbf{h}_{k,j,j}$ to the same-cell BS and $\mathbf{h}_{k,j,\bar{j}}$ to the cross-cell BS through corresponding uplink channels. Finally, we assume that the BSs perfectly recover the CSI from feedback information[2].

Given the aforementioned assumptions and notations, the received signal at user (k, j) is given by

$$y_{k,j} = \mathbf{h}_{k,j,1}\mathbf{x}_1 + \mathbf{h}_{k,j,2}\mathbf{x}_2 + n_{k,j}, \tag{1}$$

where $\mathbf{x}_i \in \mathbb{C}^{N\times 1}, i \in \{1, 2\}$ is the transmitted data from BS (i) and $n_{k,j} \sim \mathcal{CN}(0, \sigma_d^2)$ is the additive white Gaussian noise (AWGN) at user (k, j). We clarify that $\mathbf{x}_i$ consists of the linearly precoded symbols for the users to be served. We also clarify that the generation of $\mathbf{x}_i$ depends on the form of BS cooperation considered, as will be detailed in Sections II-B and II-C. The vector equation of received signals at all users is given by

$$\mathbf{y} = \mathbf{H}_1\mathbf{x}_1 + \mathbf{H}_2\mathbf{x}_2 + \mathbf{n}, \tag{2}$$

where $\mathbf{y} = [y_{1,1}\ y_{2,1} \cdots y_{K,1}\ y_{1,2}\ y_{2,2} \cdots y_{K,2}]^T$ and $\mathbf{n} = [n_{1,1}\ n_{2,1} \cdots n_{K,1}\ n_{1,2}\ n_{2,2} \cdots n_{K,2}]^T$.

A. Confidential Broadcasting and Performance Metric

The aim of this work is to design linear precoders to achieve confidential broadcasting in the two-cell broadcast network. To meet the requirement of confidential broadcasting, the message for each user (k, j) needs to be securely transmitted such that the unintended users obtain zero information. We consider a worst-case scenario in the two-cell network. In such a scenario, we assume that for the message to each user (k, j), all remaining $2K - 1$ users in both cells act as eavesdroppers, and they jointly eavesdrop on the message in a collaborative manner. The cooperating eavesdroppers decode their own signals and share them with each other. It follows that the cooperating eavesdroppers are able to perform interference cancellation, leaving only the signal for the intended user. The alliance of $2K - 1$ cooperating eavesdroppers is equivalent to a single eavesdropper with $2K - 1$ distributed receive antennas, which is denoted by the eavesdropper $(\tilde{k}, \tilde{j})$. The consideration of the worst-case scenario is motivated by the fact that the malicious behaviors of the potential eavesdroppers in the network are not fully controllable or predictable at the BSs. As a result, the weaker assumption of non-colluding eavesdroppers (or equivalently, eavesdroppers are interfered by each other) cannot lead to any true guarantee of security. Furthermore, we clarify that intentionally sharing the received messages by potential eavesdroppers does not disobey the rule of confidential broadcasting. This is due to the fact that confidential broadcasting requires the BSs to securely transmit messages to each user, but does not control the users' behaviors after receiving messages. Due to the aforementioned necessity, we highlight that the consideration of the worst-case scenario is widely adopted in designing confidential broadcasting networks, e.g., [16–19].

The secrecy performance in the two-cell broadcast network is measured by the secrecy sum rate, denoted by R_s. It is mathematically formulated as

$$R_s = \sum_{j=1}^{2}\sum_{k=1}^{K} R_{kj}, \tag{3}$$

where R_{kj} is the secrecy rate for the message to user (k, j). According to the principles of physically layer security, R_{kj} is given by

$$R_{kj} = \left[\log_2\left(1 + \mathrm{SINR}_{k,j}\right) - \log_2\left(1 + \mathrm{SINR}_{\tilde{k},\tilde{j}}\right)\right]^+, \tag{4}$$

where $\mathrm{SINR}_{k,j}$ and $\mathrm{SINR}_{\tilde{k},\tilde{j}}$ denote the signal-to-interference-plus-noise ratios (SINRs) at the intended user (k, j) and the eavesdropper $(\tilde{k}, \tilde{j})$, respectively.

B. Multi-Cell Processing with RCI Precoder

In the MCP, the two BSs fully cooperate to serve the users in the two cells based on the mutually shared CSI and messages to transmit. We note that the two-cell broadcast network with the MCP may appear to be similar to a single-cell broadcast network with $2N$ transmit antennas and $2K$ single-antenna users. However, it is worth mentioning that the design of transmission schemes and the corresponding analysis for confidential broadcasting in the MCP, which take the cross-cell interference level ϵ into consideration, are fundamentally different from those for confidential broadcasting in a single cell, e.g., [17]. As previously mentioned, the cross-cell interference level, ϵ, characterizes the severity of interference between two cells. For the single-cell network considered in [17], the average SNRs for all channels between the BS and the users are assumed to be the same. This implies that all channels are identically distributed. Different from [17], for the MCP in this paper, the average SNRs of the same-cell channels are different from the average SNRs of the cross-cell channels. This implies that all channels are non-identically distributed. Therefore, the large-system analysis of the secrecy sum rate in [17] cannot be directly applied in the MCP, and new large-system analysis needs to be conducted to address the non-identically distributed channel coefficients. Of course, when $\epsilon = 1$, the MCP reduces to the single-cell network, which shows that the result in [17] is a special case of the result for the MCP in this paper.

We next detail the precoder design for the MCP. In our design, the RCI precoder [21] is adopted at BSs to achieve confidential broadcasting. As a linear precoder, the RCI precoder has a low signal-processing complexity and the ability of controlling the information leakage as well as the interference amongst the users [17, 19]. As per the rules of the RCI precoder, the precoding vector for the message to user (k, j) is given by

$$\mathbf{w}_{k,j} = c\left(\mathbf{H}^H\mathbf{H} + \alpha\mathbf{I}_{2N}\right)^{-1}\mathbf{h}_{k,j}^H, \tag{5}$$

[2] Although this work adopts the assumption of perfect CSI at the base station, we note that if channel estimation errors exist, the achievable secrecy rates of the proposed schemes would become worse.

where c is a scaling factor to ensure the power constraint at BSs and α is a real non-negative regularization parameter. Notably, the regularization parameter α achieves a tradeoff between the signal power at the intended receiver and the amount of information leakage as well as interference amongst users. Using $\mathbf{w}_{k,j}$, the transmitted data vector $\mathbf{x} = [\mathbf{x}_1; \mathbf{x}_2]$ is written as

$$\mathbf{x} = \sum_{j=1}^{2}\sum_{k=1}^{K} \mathbf{w}_{k,j} s_{k,j}, \tag{6}$$

where $s_{k,j}$ denotes the message to be transmitted to user (k, j). We assume that the messages for different users are independent and impose a unit average power constraint on $s_{k,j}$ such that $\mathbb{E}\left\{\mathbf{s}\mathbf{s}^H\right\} = \mathbf{I}_{2K}$ with $\mathbf{s} = [\mathbf{s}_1; \mathbf{s}_2]$ and $\mathbf{s}_j = [s_{1,j}\ s_{2,j} \cdots s_{K,j}]^T$. We also assume that the BSs are subject to an average sum-power constraint such that $\mathbb{E}\left\{\|\mathbf{x}\|^2\right\} = P_t$. Accordingly, the scaling factor c is determined by

$$c^2 = \frac{P_t}{\mathrm{Tr}\left(\left(\mathbf{H}^H\mathbf{H} + \alpha\mathbf{I}_{2N}\right)^{-2}\mathbf{H}^H\mathbf{H}\right)}. \tag{7}$$

Based on (5) and (6), the received signal at the intended user (k, j) is written as

$$\begin{aligned} y_{k,j} =& c\mathbf{h}_{k,j}\left(\mathbf{H}^H\mathbf{H} + \alpha\mathbf{I}_{2N}\right)^{-1}\mathbf{H}^H\mathbf{s} + n_{kj} \\ =& c\mathbf{h}_{k,j}\left(\mathbf{H}^H\mathbf{H} + \alpha\mathbf{I}_{2N}\right)^{-1}\mathbf{h}_{k,j}^H s_{k,j} \\ &+ c\mathbf{h}_{k,j}\left(\mathbf{H}^H\mathbf{H} + \alpha\mathbf{I}_{2N}\right)^{-1}\mathbf{H}_{\tilde{k},\tilde{j}}^H\mathbf{s}_{\tilde{k},\tilde{j}} + n_{kj}, \end{aligned} \tag{8}$$

where $\mathbf{H}_{\tilde{k},\tilde{j}}$ and $\mathbf{s}_{\tilde{k},\tilde{j}}$ are obtained from $\mathbf{H}$ and $\mathbf{s}$ by removing the row corresponding to user (k, j), respectively. Moreover, the received signal vector at the eavesdropper $(\tilde{k}, \tilde{j})$ is written as

$$\mathbf{y}_{\tilde{k},\tilde{j}} = c\mathbf{H}_{\tilde{k},\tilde{j}}\left(\mathbf{H}^H\mathbf{H} + \alpha\mathbf{I}_{2N}\right)^{-1}\mathbf{h}_{k,j}^H s_{k,j} + \mathbf{n}_{\tilde{k},\tilde{j}}, \tag{9}$$

where $\mathbf{y}_{\tilde{k},\tilde{j}}$ and $\mathbf{n}_{\tilde{k},\tilde{j}}$ are obtained from $\mathbf{y}$ and $\mathbf{n}$ by removing the row corresponding to user (k, j), respectively. Based on (8) and (9), the SINRs for the message $s_{k,j}$ at the intended user (k, j) and the eavesdropper $(\tilde{k}, \tilde{j})$ are given by

$$\mathrm{SINR}_{k,j} = \frac{c^2\left|\mathbf{h}_{k,j}\left(\mathbf{H}^H\mathbf{H} + \alpha\mathbf{I}_{2N}\right)^{-1}\mathbf{h}_{k,j}^H\right|^2}{c^2\psi + \sigma_d^2} \tag{10}$$

and

$$\mathrm{SINR}_{\tilde{k},\tilde{j}} = \frac{c^2\left|\mathbf{H}_{\tilde{k},\tilde{j}}\left(\mathbf{H}^H\mathbf{H} + \alpha\mathbf{I}_{2N}\right)^{-1}\mathbf{h}_{k,j}^H\right|^2}{\sigma_d^2}, \tag{11}$$

respectively, where

$$\psi = \mathbf{h}_{k,j}\left(\mathbf{H}^H\mathbf{H} + \alpha\mathbf{I}_{2N}\right)^{-1}\mathbf{H}_{\tilde{k},\tilde{j}}^H\mathbf{H}_{\tilde{k},\tilde{j}}\left(\mathbf{H}^H\mathbf{H} + \alpha\mathbf{I}_{2N}\right)^{-1}\mathbf{h}_{k,j}^H. \tag{12}$$

As such, the secrecy sum rate achieved by the RCI precoder for the MCP is obtained as (13), shown at the top of the next page.

C. Coordinated Beamforming with Generalized RCI Precoder

In the CBf, the two BSs partially cooperate based on the CSI from all users. Since the BSs do not know the messages for the cross-cell users, they only transmit data for the users in their own cells. Also, the two BSs cooperate to control the information leakage in both cells. Furthermore, they cooperate to control the interference power amongst the users in both cells (or equivalently, the received signal power at unintended users) by properly designing the precoder and wisely choosing the regularization parameter α [22, 23].

We now detail the precoder design for the CBf. In this design, we consider the generalized RCI precoder [22] at BSs to achieve confidential broadcasting, since using the generalized RCI precoder for the CBf allows each BS to control the interference and information leakage amongst the users not only in the same cell but also in the cross cell[3]. As per the rules of the generalized RCI precoder, the precoding vector for the message to user (k, j) is given by

$$\begin{aligned} \mathbf{w}_{k,j} &= c_j\hat{\mathbf{w}}_{k,j} \\ &= c_j\left(\sum_{(l,m)\neq(k,j)} \mathbf{h}_{l,m,j}^H\mathbf{h}_{l,m,j} + \alpha\mathbf{I}_N\right)^{-1}\mathbf{h}_{k,j,j}^H, \end{aligned} \tag{14}$$

where c_j is the scaling factor to ensure the power constraint at BS (j) and α is the real non-negative regularization parameter achieving the tradeoff between the signal power at the intended receiver and the amount of information leakage as well as interference amongst users. The transmitted data vector at the BS (j) is written as

$$\mathbf{x}_j = \sum_{k=1}^{K} \mathbf{w}_{k,j} s_{k,j}, \tag{15}$$

where $s_{k,j}$ denotes the message to be transmitted to user (k, j) with the same property as that in the MCP. From (14) and (15), we find that BS (j) only requires the CSI from itself to users, $\mathbf{h}_{k,i,j}$, to construct the precoding matrix. That is, BS (j) does not need the CSI from the other BS $(\bar{j})$ to users, $\mathbf{h}_{k,i,\bar{j}}$, for the precoding matrix construction. Different from the average sum-power constraint for two BSs in the MCP, we consider in the CBf that each BS is subject to an average power constraint, such that $\mathbb{E}\left\{\|\mathbf{x}_j\|^2\right\} = P_j$. Then the total power constraint for two BSs is given by $P_t = P_1 + P_2$. Here we assume the same average power constraint at both BSs, i.e., $P_1 = P_2 = P = P_t/2$. Hence, the scaling factor c_j in (14) is determined by

$$c_j^2 = \frac{P_j}{\sum_{k=1}^{K}\|\hat{\mathbf{w}}_{k,j}\|^2}. \tag{16}$$

Based on (14) and (15), the received signal at the intended user (k, j) is written as

$$y_{k,j} = \mathbf{h}_{k,j,j}\mathbf{w}_{k,j}s_{k,j} + \sum_{(k',j')\neq(k,j)} \mathbf{h}_{k,j,j'}\mathbf{w}_{k',j'}s_{k',j'} + n_{k,j}. \tag{17}$$

[3] We clarify that the principle of the generalized RCI precoder is different from that of the RCI precoder. If we adopt the RCI precoder in the CBf, as we do in the MCP, each BS transmits data and controls the interference and information leakage amongst the users only in the same cell.

$$R_{s,\text{MCP}} = \sum_{j=1}^{2}\sum_{k=1}^{K}\left[\log_2\left(\frac{1+\frac{c^2\left|\mathbf{h}_{k,j}\left(\mathbf{H}^H\mathbf{H}+\alpha\mathbf{I}_{2N}\right)^{-1}\mathbf{h}_{k,j}^H\right|^2}{c^2\mathbf{h}_{k,j}(\mathbf{H}^H\mathbf{H}+\alpha\mathbf{I}_{2N})^{-1}\mathbf{H}_{\tilde{k},\tilde{j}}^H\mathbf{H}_{\tilde{k},\tilde{j}}(\mathbf{H}^H\mathbf{H}+\alpha\mathbf{I}_{2N})^{-1}\mathbf{h}_{k,j}^H+\sigma_d^2}}{1+\frac{c^2\left|\mathbf{H}_{\tilde{k},\tilde{j}}(\mathbf{H}^H\mathbf{H}+\alpha\mathbf{I}_{2N})^{-1}\mathbf{h}_{k,j}^H\right|^2}{\sigma_d^2}}\right)\right]^+. \tag{13}$$

Moreover, the received signal vector at the eavesdropper $(\tilde{k},\tilde{j})$ is written as

$$\mathbf{y}_{\tilde{k},\tilde{j}} = \mathbf{H}_{\tilde{k},\tilde{j},j}\mathbf{w}_{k,j}s_{k,j} + \mathbf{n}_{\tilde{k},\tilde{j}}. \tag{18}$$

where $\mathbf{H}_{\tilde{k},\tilde{j},j}$ and $\mathbf{n}_{\tilde{k},\tilde{j}}$ are obtained from $\mathbf{H}_j$ and $\mathbf{n}$ by removing the row corresponding to user (k,j), respectively. Based on (17) and (18), the SINRs for the message $s_{k,j}$ at the intended user (k,j) and the eavesdropper $(\tilde{k},\tilde{j})$ are given by

$$\text{SINR}_{k,j} = \frac{c_j^2\left|\mathbf{h}_{k,j,j}\hat{\mathbf{w}}_{k,j}\right|^2}{\sum_{(k',j')\neq(k,j)} c_{j'}^2\left|\mathbf{h}_{k,j,j'}\hat{\mathbf{w}}_{k',j'}\right|^2+\sigma_d^2} \tag{19}$$

and

$$\text{SINR}_{\tilde{k},\tilde{j}} = \frac{\sum_{(k',j')\neq(k,j)} c_j^2\left|\mathbf{h}_{k',j',j}\hat{\mathbf{w}}_{k,j}\right|^2}{\sigma_d^2}, \tag{20}$$

respectively. Aided by (19) and (20), the secrecy sum rate achieved by the generalized RCI precoder for the CBf is obtained as (21), shown at the top of the next page.

It is evident that the secrecy sum rates in (13) and (21) depend on the realization of each channel, $\mathbf{h}_{k,j,i}$. Based on them, we can only evaluate the secrecy performance by time-consuming numerical simulations. This motivates us to seek channel-independent expressions that reduce the complexity of performance evaluations. Therefore, in the next section we resort to the large-system analysis to explicitly characterize the secrecy sum rate of confidential broadcasting in the two-cell broadcast network.

III. Secrecy Sum Rate in the large-system Regime

In this section, we derive channel-independent expressions for the secrecy sum rate of the two-cell broadcast network in the large-system regime. In such a regime, both the number of users in each cell, K, and the number of transmit antennas at each BS, N, approach infinity with a fixed ratio, $\beta = K/N$. Besides, we denote $\gamma = P_t/(2\sigma_d^2) = P/\sigma_d^2$ as the average *transmit* SNR at *each* BS. As will be shown later in numerical simulations, the analytical result in the large-system regime can accurately approximate the secrecy sum rate of the network even with finite K and N.

A. Large-System Analysis

In the large-system analysis for the symmetric two-cell network with $K, N \to \infty$, the secrecy rate for all messages $s_{k,j}$ converge to the same non-random function. This function does not depend on the realization of each channel $\mathbf{h}_{k,j,i}$. Thus, the secrecy sum rate is analytically approximated by

$$R_s^{\infty} = 2K\left(R_{k,j}^{\infty}\right) = 2K\left[\log_2\frac{1+\text{SINR}_{k,j}^{\infty}}{1+\text{SINR}_{\tilde{k},\tilde{j}}^{\infty}}\right]^+, \tag{22}$$

where $R_{k,j}^{\infty}$ denotes the large-system secrecy rate for each user, $\text{SINR}_{k,j}^{\infty}$ and $\text{SINR}_{\tilde{k},\tilde{j}}^{\infty}$ denote the large-system approximations of the SINRs at the intended user and the eavesdropper, respectively.

In the following *Theorem 1* and *Theorem 2*, we present the large-system secrecy sum rate achieved by the RCI precoder for the MCP and the large-system secrecy sum rate achieved by the generalized RCI precoder for the CBf, respectively.

Theorem 1: In the large-system regime, the secrecy sum rate achieved by the RCI precoder for the MCP converges in probability to a deterministic quantity given by (23), where $\rho_M = (1+\epsilon)^{-1}\alpha/N$ and $g(\beta,\rho_M)$ is the solution of x to $x = \left(\rho_M + \frac{\beta}{1+x}\right)^{-1}$.

Proof: See Appendix A. ∎

Theorem 2: In the large-system regime, the secrecy sum rate achieved by the generalized RCI precoder for the CBf converges almost surely to a deterministic quantity given by (24), where $\rho_C = \alpha/N$, Λ is the solution of x to $x = \left(\rho_C + \frac{\beta\epsilon}{1+\epsilon x} + \frac{\beta}{1+x}\right)^{-1}$ and Λ_0 is the solution of x to $x = \left(\frac{\beta\epsilon}{1+\epsilon x} + \frac{\beta}{1+x}\right)^{-1}$.

Proof: See Appendix B. ∎

We provide several remarks about the large-system secrecy sum rates derived in *Theorems 1* and *2*, as follows:

Remark 1: Theorems 1 and *2* provide closed-form and channel-independent expressions for the large-system secrecy sum rates for the MCP and the CBf, respectively. We highlight that these expressions eliminate the computational burden of performance evaluation incurred by Monte Carlo simulations. Notably, these expressions allow us to evaluate and optimize the secrecy performance efficiently. The comparison of the optimal achievable secrecy performance between the MCP and the CBf will be conducted in Section IV-A.

Remark 2: The results for both the MCP and the CBf contain the parameter ϵ, such that they characterize the impact of the cross-cell interference level on the secrecy sum rate. This demonstrates that the analysis of confidential broadcasting in multi-cell networks is fundamentally different from that in single-cell networks which did not consider ϵ, e.g., [17].

Remark 3: We note that the result in *Theorem 1* with $\epsilon = 1$ reduces to the result for the single-cell confidential broadcasting given in [17], which demonstrates the generality of our analysis. This is due to the fact that the confidential broadcasting in a single cell with one $2N$-antenna BS and $2K$ single-antenna users is equivalent to a special case of the confidential broadcasting in the MCP.

B. Numerical Results

In this subsection, we examine the accuracy of the large-system results by comparing the large-system secrecy sum

$$R_{s,\text{CBf}}=\sum_{j=1}^{2}\sum_{k=1}^{K}\left[\log_2\left(\frac{1+\frac{c_j^2\left|\mathbf{h}_{k,j,j}\hat{\mathbf{w}}_{k,j}\right|^2}{\sum_{(k',j')\neq(k,j)}c_{j'}^2\left|\mathbf{h}_{k,j,j'}\hat{\mathbf{w}}_{k',j'}\right|^2+\sigma_d^2}}{1+\frac{\sum_{(k',j')\neq(k,j)}c_j^2\left|\mathbf{h}_{k',j',j}\hat{\mathbf{w}}_{k,j}\right|^2}{\sigma_d^2}}\right)\right]^+. \tag{21}$$

$$R_{s,\text{MCP}}^{\infty}=\begin{cases}2K\left[\log_2\left(\frac{1+(1+\epsilon)\gamma g(\beta,\rho_M)\frac{1+\frac{\rho_M}{\beta}(1+g(\beta,\rho_M))^2}{(1+\epsilon)\gamma+(1+g(\beta,\rho_M))^2}}{1+\frac{(1+\epsilon)\gamma}{(1+g(\beta,\rho_M))^2}}\right)\right]^+, & \text{if } \alpha\neq 0\\ 2K\log_2\left(1+\frac{(1-\beta)(1+\epsilon)\gamma}{\beta}\right), & \text{if } \alpha=0 \text{ and } \beta\leq 1\\ 2K\left[\log_2\left(\frac{\beta^3(\beta+(\beta-1)(1+\epsilon)\gamma)}{(\beta^2+(\beta-1)^2(1+\epsilon)\gamma)^2}\right)\right]^+, & \text{if } \alpha=0 \text{ and } \beta>1.\end{cases} \tag{23}$$

$$R_{s,\text{CBf}}^{\infty}=\begin{cases}2K\left[\log_2\left(\frac{1+\frac{\frac{\Lambda}{\beta}\left(\rho_C+\frac{\beta\epsilon}{(1+\epsilon\Lambda)^2}+\frac{\beta}{(1+\Lambda)^2}\right)}{\frac{1}{\gamma}+\frac{\epsilon}{(1+\epsilon\Lambda)^2}+\frac{1}{(1+\Lambda)^2}}}{1+\gamma\left(\frac{\epsilon}{(1+\epsilon\Lambda)^2}+\frac{1}{(1+\Lambda)^2}\right)}\right)\right]^+, & \text{if } \alpha\neq 0\\ 2K\log_2\left(1+\frac{(1-2\beta)\gamma}{\beta}\right), & \text{if } \alpha=0 \text{ and } \beta\leq 0.5\\ 2K\left[\log_2\left(\frac{1+\frac{\frac{\Lambda_0}{\beta}\left(\frac{\beta\epsilon}{(1+\epsilon\Lambda_0)^2}+\frac{\beta}{(1+\Lambda_0)^2}\right)}{\frac{1}{\gamma}+\frac{\epsilon}{(1+\epsilon\Lambda_0)^2}+\frac{1}{(1+\Lambda_0)^2}}}{1+\gamma\left(\frac{\epsilon}{(1+\epsilon\Lambda_0)^2}+\frac{1}{(1+\Lambda_0)^2}\right)}\right)\right]^+, & \text{if } \alpha=0 \text{ and } \beta>0.5.\end{cases} \tag{24}$$

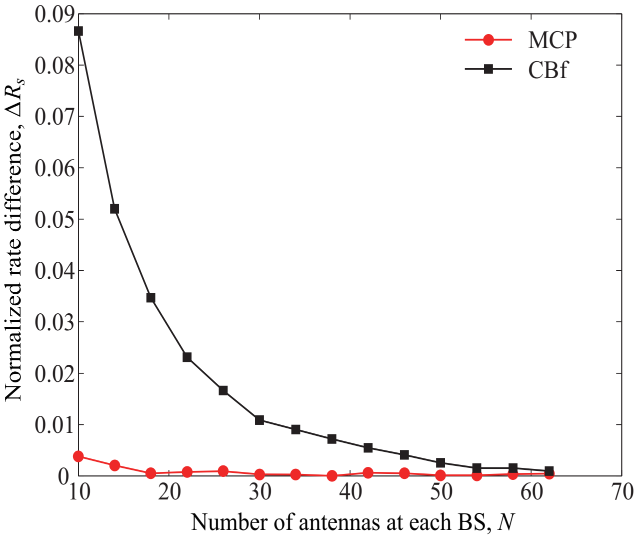


Fig. 2. The normalized rate difference versus the number of antennas at each BS for $\epsilon=0.5,\alpha=0.2,\beta=0.5$ and $\gamma=10$ dB.

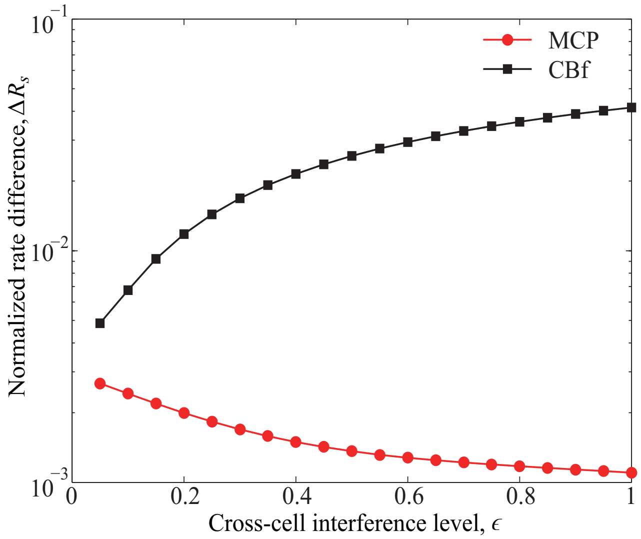


Fig. 3. The normalized rate difference versus the cross-cell interference level for $N=20,\alpha=0.2,\beta=0.5$ and $\gamma=10$ dB.

rate, R_s^{∞}, with the average secrecy sum rate of networks with finite K and N, $\mathbb{E}\left\{R_s\right\}$. To this end, we introduce the normalized rate difference defined by

$$\Delta R_s=\frac{\left|\mathbb{E}\left\{R_s\right\}-R_s^{\infty}\right|}{\mathbb{E}\left\{R_s\right\}}, \tag{25}$$

which quantifies the rate difference between R_s^{∞} and $\mathbb{E}\left\{R_s\right\}$ for finite K and N.

We first demonstrate the accuracy of the large-system approximation over the size of network. Figure 2 plots ΔR_s versus N for the MCP and the CBf[4]. As depicted in the figure, ΔR_s decreases as N increases. This indicates that the large-system approximation becomes more accurate as the size of network increases. Moreover, we find that the rate difference for the MCP is very small across the whole range of N, which indicates that $R_{s,\text{MCP}}^{\infty}$ in (23) is a very accurate approximation.

[4] Throughout this paper we present numerical results by considering some particular examples of networks. For instance, we adopt $\epsilon=0.5,\alpha=0.2,\beta=0.5$ and $\gamma=10$ dB in Figure 2. Of course, these examples do not restrict the generality of our results for arbitrary network parameters, unless otherwise stated.

Furthermore, we find that the rate difference for the CBf is a bit higher than that for the MCP for small N, but decreases rapidly when N grows large. Notably, the rate differences for both the MCP and the CBf are extremely small for large N, e.g., $\Delta R_s < 1\%$ for $N \geq 40$.

We then confirm the accuracy of the large-system approximation over the entire range of ϵ. Figure 3 plots ΔR_s versus ϵ for the MCP and the CBf. In this figure, we consider the network with $N = 20$. We find that the highest rate difference for the MCP is lower than 3×10^{-3} and the highest rate difference for the CBf is approximately 4×10^{-2}. As such, our large-system approximations provide reasonable accuracy across the entire range of ϵ.

IV. Optimization of Secrecy Sum Rate

In this section, we maximize the large-system secrecy sum rate for the MCP and the CBf based on the derived channel-independent large-system approximations. We first determine the optimal regularization parameter that maximizes the large-system secrecy sum rate. Moreover, we propose power-reduction strategies to maintain the maximum large-system secrecy sum rate when an increasing transmit SNR cannot sustain a growing large-system secrecy sum rate for a high network load.

A. Optimal Regularization Parameter

In this subsection, we seek the optimal α which maximizes the secrecy sum rate in the large-system regime. We note that the regularization parameter in the linear precoding matrix, α, plays a pivotal role in determining the network performance. This is due to its ability of handling the trade-off between the signal power at the intended receiver and the amount of information leakage as well as interference amongst users. We denote $\alpha^*_{\text{MCP}} = \arg\max\limits_{\alpha} R^{\infty}_{s,\text{MCP}}$ and $\alpha^*_{\text{CBf}} = \arg\max\limits_{\alpha} R^{\infty}_{s,\text{CBf}}$ as the optimal regularization parameters for the MCP and the CBf, respectively.

1) α^*_{MCP} for MCP: We now determine α^*_{MCP}. By taking the first order derivative of $R^{\infty}_{s,\text{MCP}}$ in (23) with respect to α, we find that there are two possibilities for the sign of $\partial R^{\infty}_{s,\text{MCP}}/\partial\alpha$ when $\alpha \geq 0$: 1) $\partial R^{\infty}_{s,\text{MCP}}/\partial\alpha$ is always negative or 2) $\partial R^{\infty}_{s,\text{MCP}}/\partial\alpha$ is positive for small α and becomes negative as α increases. This implies that the optimal value of α that maximizes $R^{\infty}_{s,\text{MCP}}$ is equal to either zero or a unique positive value. Then we obtain the value of α^*_{MCP} by seeking the solution of α to $\partial R^{\infty}_{s,\text{MCP}}/\partial\alpha = 0$. After performing a series of complicated algebraic manipulations, we obtain α^*_{MCP} as

$$\alpha^*_{\text{MCP}} = \left[\frac{\beta^2 - \phi_1^2 - (\beta+\phi_1)\sqrt{\beta^2+\beta\phi_2+\phi_1^2} + 3\phi_3}{\frac{3\gamma}{N}\left(\beta+\phi_2\right)}\right]^+, \tag{26}$$

where $\phi_1 = (1+\epsilon)(\beta-1)\gamma$, $\phi_2 = (1+\epsilon)(\beta+2)\gamma$ and $\phi_3 = (1+\epsilon)\beta\gamma$. The optimality of α^*_{MCP} will be verified in Section IV-A3.

2) α^*_{CBf} for CBf: We note that the closed-form expression for α^*_{CBf} is mathematically intractable. As such, we present **Algorithm 1** to numerically determine α^*_{CBf}. By taking the first order derivative of $R^{\infty}_{s,\text{CBf}}$ in (24) with respect to α, we find that there are two possibilities for the sign of $\partial R^{\infty}_{s,\text{CBf}}/\partial\alpha$ when $\alpha \geq 0$: 1) $\partial R^{\infty}_{s,\text{CBf}}/\partial\alpha$ is positive for small α and becomes negative as α increases or 2) $\partial R^{\infty}_{s,\text{CBf}}/\partial\alpha$ is always negative. This implies that, from the theoretical perspective, the optimal value of α that maximizes $R^{\infty}_{s,\text{CBf}}$ is a unique positive value or approaches zero. Therefore, the value of α^*_{CBf} can be obtained by numerically searching the value of α that satisfies $\partial R^{\infty}_{s,\text{CBf}}/\partial\alpha = 0$, with the aid of Algorithm 1.

Algorithm 1 Numerical Search for α^*_{CBf}

```
Input: $f(x) = \frac{\partial R^{\infty}_{s,\text{CBf}}}{\partial\alpha}(\alpha = x)$;
       Acceptable error $d$ (e.g., $d = 10^{-10}$);
       Initial search point $\alpha_p$ (e.g., $\alpha_p = 1$);
Output: $\alpha^*_{\text{CBf}}$ that satisfies $|f(\alpha^*_{\text{CBf}})| \leq d$;
Initialize iteration counters: $c = 0$;
if $|f(\alpha_p)| \leq d$ then
    return $\alpha^*_{\text{CBf}} = \alpha_p$; {The value of $\alpha^*_{\text{CBf}}$ is obtained.}
end if
if $f(\alpha_p) > 0$ then
    Initialize the lower bound of $\alpha^*_{\text{CBf}}$ by
    $\alpha_l = \alpha_p$;
    while $f(\alpha_l + 2^c) > 0$ do
        Update the lower bound by $\alpha_l = \alpha_l + 2^c$;
        Exponentially increase the one-side search step $2^c$ by
        $c = c + 1$;
    end while
    Set the upper bound of $\alpha^*_{\text{CBf}}$ by $\alpha_u = \alpha_l + 2^c$;
else
    Initialize the upper bound of $\alpha^*_{\text{CBf}}$ by
    $\alpha_u = \alpha_p$;
    while $f(\alpha_u \times 10^{-1}) < 0$ do
        Update the upper bound by
        $\alpha_u = \alpha_u \times 10^{-1}$;
    end while
    Set the lower bound of $\alpha^*_{\text{CBf}}$ by
    $\alpha_l = \alpha_u \times 10^{-1}$;
end if
if $|f(\alpha_l)| \leq d$ then
    return $\alpha^*_{\text{CBf}} = \alpha_l$; {The value of $\alpha^*_{\text{CBf}}$ is obtained.}
end if
if $|f(\alpha_u)| \leq d$ then
    return $\alpha^*_{\text{CBf}} = \alpha_u$; {The value of $\alpha^*_{\text{CBf}}$ is obtained.}
end if
Initialize the mid-point $\alpha_m = (\alpha_l + \alpha_u)/2$;
while $|f(\alpha_m)| > d$ do
    if $f(\alpha_m) > 0$ then
        $\alpha_l = \alpha_m; \alpha_u = \alpha_u$;
    else
        $\alpha_l = \alpha_l; \alpha_u = \alpha_m$;
    end if
    $\alpha_m = (\alpha_l + \alpha_u)/2$;
end while
return $\alpha^*_{\text{CBf}} = \alpha_m$; {The value of $\alpha^*_{\text{CBf}}$ is obtained.}
```

3) Numerical Results: In the following numerical results, we verify the optimality of the determined α^*_{MCP} and α^*_{CBf}. Figure 4 plots the large-system secrecy rate per transmit

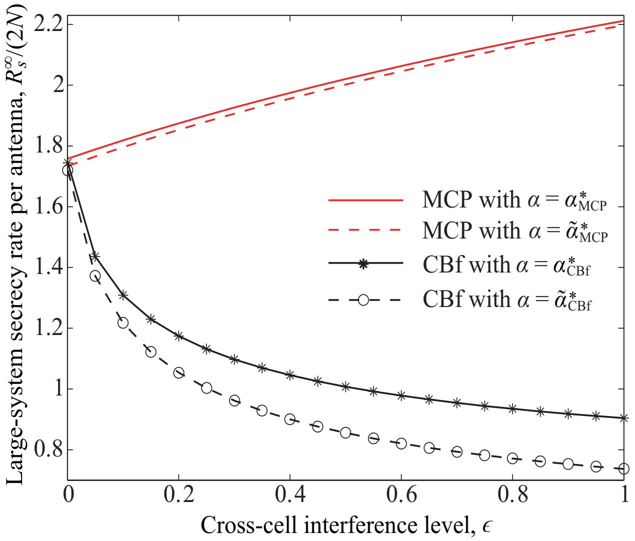


Fig. 4. The large-system secrecy rate per antenna versus the cross-cell interference level for different designs of the regularization parameter with $N = 20, \beta = 0.5$ and $\gamma = 10$ dB.

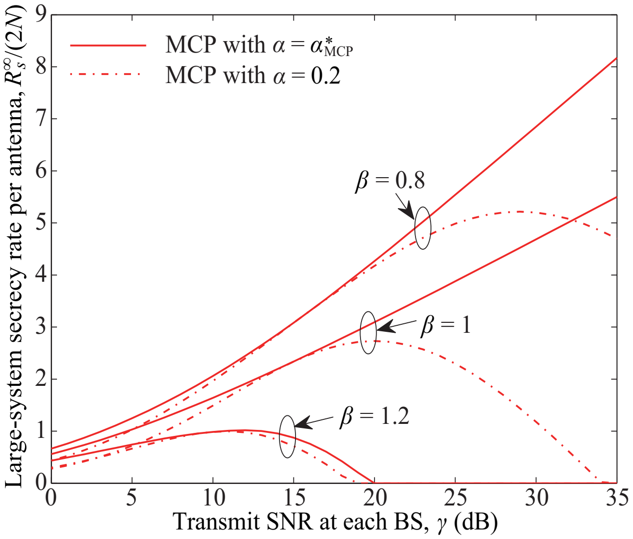


Fig. 5. MCP: the large-system secrecy rate per antenna versus the average transmit SNR per BS for different designs of the regularization parameter with $\beta = 0.8, 1, 1.2$, $N = 20$ and $\epsilon = 0.5$.

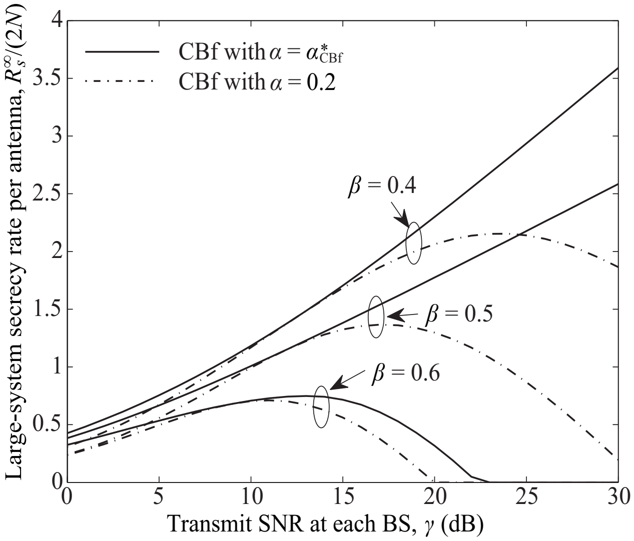


Fig. 6. CBf: the large-system secrecy rate per antenna versus the average transmit SNR per BS for different designs of the regularization parameter with $\beta = 0.4, 0.5, 0.6$, $N = 20$ and $\epsilon = 0.5$.

antenna, $R_s^\infty/(2N)$, versus ϵ. Specifically, we compare the performances for two different designs of α: 1) the optimal α that maximizes the large-system secrecy sum rate, i.e., α^*_{MCP} given by (26) for the MCP or α^*_{CBf} obtained by **Algorithm 1** for the CBf and 2) the optimal α that maximizes the large-system sum rate without secrecy considerations given by [24], i.e., $\tilde{\alpha}^*_{\text{MCP}}$ for the MCP or $\tilde{\alpha}^*_{\text{CBf}}$ for the CBf. We find that the performance achieved by α^*_{MCP} or α^*_{CBf} is always better than that achieved by $\tilde{\alpha}^*_{\text{MCP}}$ or $\tilde{\alpha}^*_{\text{CBf}}$. We note that the difference between the performances achieved by α^*_{MCP} and $\tilde{\alpha}^*_{\text{MCP}}$ is not as obvious as that for the CBf. This is due to the values of network parameters (i.e., β and γ) chosen in the figure. Actually, the advantage of using α^*_{MCP} against $\tilde{\alpha}^*_{\text{MCP}}$ can be very obvious as well if some other network parameters are considered, e.g., $\beta = 1$. These observations indicate that the optimal values of α without secrecy considerations given by [24] are no longer optimal for the networks with secrecy considerations.

Comparing the results for the MCP and the CBf, it is evident that the secrecy rate for the MCP is in general higher than that for the CBf. This is due to the fact that the BSs in the MCP share messages to transmit while the BSs in the CBf do not. Note that such an advantage of secrecy rate necessitates the high-capacity backhaul links in the MCP. Moreover, we find that the secrecy rate for the MCP increases with ϵ. In contrast, the secrecy rate for the CBf decreases with ϵ. This observation can be explained as follows. The value of ϵ determines the average channel gain from the cross-cell BS to the users. In particular, a higher ϵ increases the power of the received signals from the cross-cell BS. In the MCP where BSs share messages to transmit, a higher ϵ increases the received signal power at the intended user, although the interference power at the intended user and the received signal power at the eavesdropper increase as well. Thus, the secrecy rate for the MCP can increase as ϵ increases. On the other hand, the BSs cannot share messages to transmit in the CBf. As such, a higher ϵ only increases the interference power at the intended user and the received signal power at the eavesdropper, but does not increase the received signal power at the intended receiver. It follows that the secrecy rate for the CBf always decreases as ϵ increases.

We next demonstrate the optimality of the determined α^*_{MCP} and α^*_{CBf} over the average transmit SNR per BS, γ, and examine the impact of γ on the large-system secrecy sum rate. Figures 5 and 6 plot $R_s^\infty/(2N)$ versus γ for the MCP and the CBf, respectively. We compare the performance achieved by the obtained optimal α with the performance achieved by an arbitrarily chosen α, i.e., $\alpha = 0.2$, in the figures. As shown in both figures, the secrecy rate achieved by the optimal regularization parameter is always higher than that achieved by $\alpha = 0.2$ for both the MCP and the CBf, which confirms the

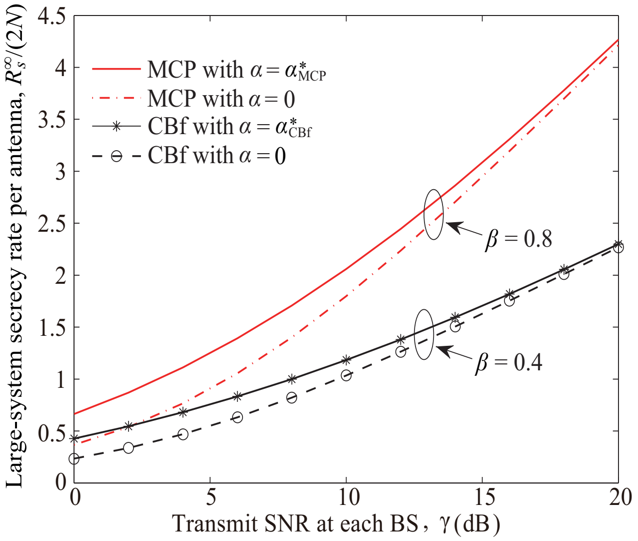


Fig. 7. The large-system secrecy rate per antenna versus the average transmit SNR per BS for different designs of the regularization parameter with $N = 20$ and $\epsilon = 0.5$.

optimality of α^*_{MCP} and α^*_{CBf}. Besides, we note that the secrecy rate achieved by $\alpha = 0.2$ always reduces to zero when γ grows large. This can be explained based on (23) and (24), i.e.,

$$\lim_{\gamma\to\infty} R^\infty_{s,\mathrm{MCP}} = \lim_{\gamma\to\infty} R^\infty_{s,\mathrm{CBf}} = 0, \quad \text{if} \quad \alpha \neq 0. \tag{27}$$

Differently, the secrecy rate achieved by the optimal regularization parameter may not reduce to zero when γ is high. For the MCP, Figure 5 shows that the secrecy rate achieved by $\alpha = \alpha^*_{\mathrm{MCP}}$ monotonically increases with γ if $\beta \leq 1$, but goes to zero at high transmit SNRs if $\beta > 1$. For the CBf, Figure 6 shows that the secrecy rate achieved by $\alpha = \alpha^*_{\mathrm{CBf}}$ monotonically increases with γ if $\beta \leq 0.5$, but goes to zero at high transmit SNRs if $\beta > 0.5$. These observations reveal that the increase in γ benefits the secrecy performance achieved by the optimal α, when the network load is low. We now analytically explain these observations as follows. From the analytical results, we find that the optimal regularization parameter goes to zero as γ increases for both the MCP and the CBf. When $\alpha \to 0$, we find from (23) that $\lim_{\alpha\to 0} R^\infty_{s,\mathrm{MCP}}$ monotonically increases with γ if $\beta \leq 1$, while $\lim_{\alpha\to 0} R^\infty_{s,\mathrm{MCP}}$ approaches to zero at high transmit SNRs if $\beta > 1$. Similarly, it is found from (24) that $\lim_{\alpha\to 0} R^\infty_{s,\mathrm{CBf}}$ monotonically increases with γ if $\beta \leq 0.5$, while $\lim_{\alpha\to 0} R^\infty_{s,\mathrm{CBf}}$ goes to zero at high transmit SNRs if $\beta > 0.5$.

Finally, we demonstrate the advantage of the proposed precoders relative to the channel inversion precoder in the two-cell network. The channel inversion precoder (also called as zero-forcing precoder) is a well-known linear precoder that can eliminate the interference amongst users in the multi-user multi-input single-output (MISO) broadcasting network where the number of users is less than or equal to the number of transmit antennas at the BS, i.e., $\beta \leq 1$ for the MCP or $\beta \leq 0.5$ for the CBf[5]. Figure 7 plots $R_s^\infty/(2N)$ versus γ for the proposed precoders and the channel inversion precoder. The proposed precoders include the RCI precoder with $\alpha = \alpha^*_{\mathrm{MCP}}$ for the MCP and the generalized RCI precoder with $\alpha = \alpha^*_{\mathrm{CBf}}$ for the CBf. For the MCP, the RCI precoder with $\alpha = 0$ reduces to the channel inversion precoder considered for comparison. For the CBf, the generalized RCI precoder with $\alpha = 0$ is considered for comparison, since the conventional channel inversion precoder cannot achieve confidential broadcasting in the CBf. Note that the regularized RCI with $\alpha = 0$ can eliminate the interference amongst users, which has the same effects as the channel inversion precoder in the single-cell network or the MCP. It is evident from the figure that the proposed precoders outperform the channel inversion precoder for both the MCP and the CBf. We find that the proposed precoders exhibit a profound performance gain over the channel inversion precoder in the regime of low transmit SNR. We also find that this performance gain decreases when the transmit SNR increases. This can be explained by the fact that the optimal regularization parameter approaches zero when the transmit SNR grows large. Besides, it is worth mentioning that the channel inversion precoder achieves confidential broadcasting only when the number of users is less than or equal to the number of transmit antennas at the BS, i.e., $\beta \leq 1$ for the MCP or $\beta \leq 0.5$ for the CBf. Differently, the proposed precoders can achieve confidential broadcasting even if $\beta > 1$ for the MCP or $\beta > 0.5$ for the CBf.

B. *Power-Reduction Strategy*

We find from Figures 5 and 6 that the large-system secrecy sum rate achieved by the optimal regularization parameter, denoted by $R_s^{\infty *}$, does not monotonically increase with γ when the network load is high. Specifically, $R_s^{\infty *}$ decreases as γ increases at high transmit SNRs when $\beta > 1$ for the MCP or $\beta > 0.5$ for the CBf. Hence, we propose power-reduction strategies to compensate for the secrecy sum rate loss at high transmit SNRs for a high network load. We highlight that although the principle of the power reduction strategy in our work is similar to that in [17], the prominent challenge of designing our power reduction strategy is to determine the optimal transmit SNR that maximizes the secrecy sum rate using our newly derived expressions for the secrecy sum rate. As such, the design of the power reduction strategy in our paper is different from that in [17]. To this end, we first obtain the optimal transmit SNR that maximizes the large-system secrecy sum rate for each of the MCP and the CBf.

1) Power Reduction for MCP: For the MCP, we focus on the network with $\beta > 1$, since $R^{\infty *}_{s,\mathrm{MCP}}$ does not monotonically increase with γ when $\beta > 1$. We first derive the optimal transmit SNR, γ^*_{MCP}, that maximizes the large-system secrecy sum rate achieved by α^*_{MCP}, i.e., $\gamma^*_{\mathrm{MCP}} = \arg\max\limits_{\gamma} R^{\infty *}_{s,\mathrm{MCP}}$. By taking the first-order derivative of $R^{\infty *}_{s,\mathrm{MCP}}$ with respect to γ and equating it to zero, we obtain γ^*_{MCP} as

$$\gamma^*_{\mathrm{MCP}} = \frac{\beta(2-\beta)}{(1+\epsilon)(\beta-1)^2}. \tag{28}$$

Based on (28), we propose the power-reduction strategy to reduce the total transmit power such that the maximum large-

[5] The well-known block-diagonalization (BD) precoder is a generalization of the channel inversion precoder to the scenario where multiple antennas are equipped at each user [25–27].

system secrecy sum rate is maintained. The precoding vector with the power-reduction strategy is given by

$$\mathbf{w}_{\text{PR}} = \begin{cases} \sqrt{\frac{\gamma^*_{\text{MCP}}}{\gamma}}\,\mathbf{w}^* & \beta > 1 \text{ and } \gamma > \gamma^*_{\text{MCP}}, \\ \mathbf{w} & \text{otherwise,} \end{cases} \tag{29}$$

where $\mathbf{w}$ is the original RCI precoding vector given in (5) with $\alpha = \alpha^*_{\text{MCP}}$ and $\mathbf{w}^*$ is the original RCI precoding vector with $\alpha = \alpha^*_{\text{MCP}}$ at $\gamma = \gamma^*_{\text{MCP}}$. We highlight that $\sqrt{\gamma^*_{\text{MCP}}/\gamma}$ is the power-reduction coefficient for the MCP, which is adopted when $\beta > 1$ and $\gamma > \gamma^*_{\text{MCP}}$. As such, we refer to the RCI precoder using $\mathbf{w}_{\text{PR}}$ in (29) as the RCI-PR precoder. Note that the reduced transmit SNR by adopting the RCI-PR precoder becomes

$$\gamma^{\text{PR}}_{\text{MCP}} = \begin{cases} \gamma^*_{\text{MCP}}, & \beta > 1 \text{ and } \gamma > \gamma^*_{\text{MCP}} \\ \gamma, & \text{otherwise.} \end{cases} \tag{30}$$

2) Power Reduction for CBf: For the CBf, we focus on the network with $\beta > 0.5$, since $R^{\infty *}_{s,\text{CBf}}$ does not monotonically increase with γ when $\beta > 0.5$. We first determine the optimal transmit SNR, γ^*_{CBf}, that maximizes the large-system secrecy sum rate achieved by α^*_{CBf}, i.e., $\gamma^*_{\text{CBf}} = \arg\max\limits_{\gamma} R^{\infty *}_{s,\text{CBf}}$. Since the closed-form expression for γ^*_{CBf} cannot be derived, we obtain γ^*_{CBf} through numerical search. Using γ^*_{CBf}, we propose the power-reduction strategy to reduce the total transmit power and maintain the maximum large-system secrecy sum rate. The precoding vector with the power-reduction strategy is given by

$$\mathbf{w}_{\text{PR}} = \begin{cases} \sqrt{\frac{\gamma^*_{\text{CBf}}}{\gamma}}\,\mathbf{w}^* & \beta > 0.5 \text{ and } \gamma > \gamma^*_{\text{CBf}}, \\ \mathbf{w} & \text{otherwise,} \end{cases} \tag{31}$$

where $\mathbf{w}$ is the original generalized RCI precoding vector given in (14) with $\alpha = \alpha^*_{\text{CBf}}$ and $\mathbf{w}^*$ is the original generalized RCI precoding vector with $\alpha = \alpha^*_{\text{CBf}}$ at $\gamma = \gamma^*_{\text{CBf}}$. We highlight that $\sqrt{\gamma^*_{\text{CBf}}/\gamma}$ is the power-reduction coefficient for the CBf, which is adopted when $\beta > 0.5$ and $\gamma > \gamma^*_{\text{CBf}}$. Therefore, we refer to the generalized RCI precoder using $\mathbf{w}_{\text{PR}}$ in (31) as the generalized RCI-PR precoder. Notably, the reduced transmit SNR by adopting the generalized RCI-PR precoder becomes

$$\gamma^{\text{PR}}_{\text{CBf}} = \begin{cases} \gamma^*_{\text{CBf}}, & \beta > 0.5 \text{ and } \gamma > \gamma^*_{\text{CBf}} \\ \gamma, & \text{otherwise.} \end{cases} \tag{32}$$

3) Numerical Results: Figures 8 and 9 demonstrate the performance improvement offered by the proposed power-reduction strategy for the MCP and the CBf, respectively. Figure 8 plots $R^{\infty}_{s}/(2N)$ versus γ for the MCP, where the curve of MCP RCI-PR is for the proposed power-reduction strategy and the curve of MCP RCI is for the RCI precoding with $\alpha = \alpha^*_{\text{MCP}}$. Figure 9 plots $R^{\infty}_{s}/(2N)$ versus γ for the CBf, where the curve of CBf Generalized RCI-PR is for the proposed power-reduction strategy and the curve of CBf Generalized RCI is for the generalized RCI precoding with $\alpha = \alpha^*_{\text{CBf}}$. We clarify that the actual transmit SNR of the RCI-PR precoder in Figure 8 is γ^*_{MCP} when $\gamma > \gamma^*_{\text{MCP}}$, as indicated by (30), and the actual transmit SNR of the generalized RCI-PR precoder in Figure 9 is γ^*_{CBf} when $\gamma > \gamma^*_{\text{CBf}}$, as indicated by (32). As shown in both figures, the proposed power-reduction strategies efficiently prevent the secrecy rate from decreasing at high transmit SNRs. Particularly, the power-reduction strategy allows the secrecy rate at high transmit SNRs to be equal to the maximum secrecy rate achieved at the optimal transmit SNR. It is worth nothing that the improvement in the secrecy rate at high transmit SNRs is achieved by using a lower transmit power compared with the transmission without the power-reduction strategy.

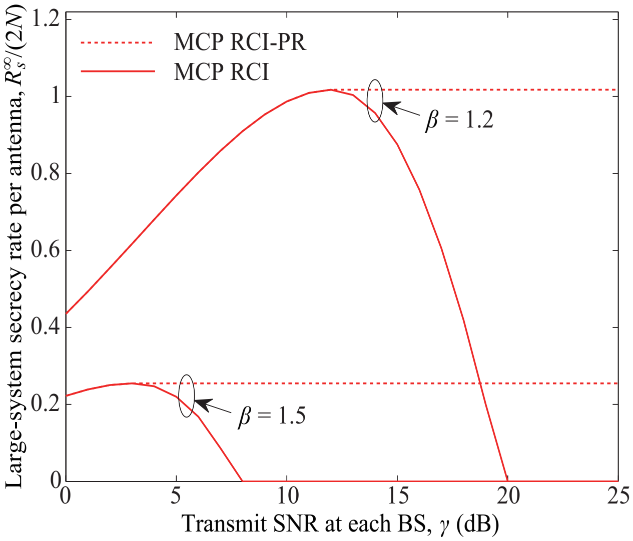


Fig. 8. MCP: the large-system secrecy rate per antenna versus the average transmit SNR per BS for the transmissions with and without power-reduction strategy. The other system parameters are $\beta = 1.2, 1.5$, $N = 20$ and $\epsilon = 0.5$.

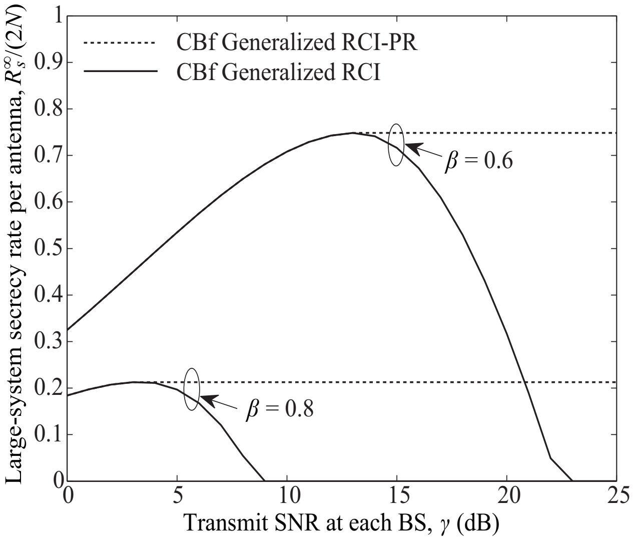


Fig. 9. CBf: the large-system secrecy rate per antenna versus the average transmit SNR per BS for the transmissions with and without power-reduction strategy. The other system parameters are $\beta = 0.6, 0.8$, $N = 20$ and $\epsilon = 0.5$.

V. Conclusion and Future Work

In this paper, we designed the RCI precoder and the generalized RCI precoder for the MCP and the CBf, respectively, to achieve confidential broadcasting in a two-cell broadcast network. For each form of BS cooperation, we derived accurate large-system expressions for the secrecy sum rate achieved by the linear precoder. Based on these expressions, we determined α^*_{MCP} and α^*_{CBf} which are the optimal regularization parameters maximizing the large-system secrecy sum rate for the MCP and the CBf, respectively. Furthermore, we proposed the RCI-PR precoder for the MCP and the generalized RCI-PR precoder for the CBf, which can significantly increase the secrecy sum rate at high transmit SNRs by power-reduction strategies. Using numerical results, we demonstrated the accuracy of our large-system expressions, the optimality of α^*_{MCP} and α^*_{CBf}, and the secrecy sum rate improvement provided by the RCI-PR and the generalized RCI-PR precoders. Notably, our analytical and numerical results allow us to examine the impact of the cross-cell interference level on the secrecy sum rate. Besides, it is worth mentioning that the results in this paper are primarily theoretically oriented and offer a useful theoretical design guide for the two-cell wireless network where in each cell a BS securely broadcasts messages to multiple user terminals.

One direction of future work is to investigate confidential broadcasting in a general N-cell network. For this N-cell network, we can apply the same precoder designs and similar methodologies as described in this paper to examine the impact of the number of cells on the achievable secrecy sum rate. Moreover, an extension from the homogenous scenario considered in this work to the non-homogenous scenario, where the channels from different users to the BS have different average powers, would be of practical interests. Furthermore, using other physical layer security techniques to achieve confidential broadcasting in multi-cell networks is another research direction. For example, it is interesting to study the artificial noise technique in multi-cell networks.

Appendix A
Proof of Theorem 1

We first derive the large-system approximations of the SINRs for message $s_{k,j}$ at the intended receiver and the eavesdropper. Based on the approximations, we then obtain the large-system secrecy sum rate using (22).

We recall that the following equality holds:

$$\left(\mathbf{H}^H\mathbf{H}+\alpha\mathbf{I}_{2N}\right)^{-1}=\left(\mathbf{H}^H_{\tilde{k},\tilde{j}}\mathbf{H}_{\tilde{k},\tilde{j}}+\mathbf{h}^H_{k,j}\mathbf{h}_{k,j}+\alpha\mathbf{I}_{2N}\right)^{-1}. \tag{33}$$

By applying the matrix inversion lemma, we obtain

$$\left(\mathbf{H}^H\mathbf{H}+\alpha\mathbf{I}_{2N}\right)^{-1}=\left(\mathbf{H}^H_{\tilde{k},\tilde{j}}\mathbf{H}_{\tilde{k},\tilde{j}}+\alpha\mathbf{I}_{2N}\right)^{-1} - \frac{\left(\mathbf{H}^H_{\tilde{k},\tilde{j}}\mathbf{H}_{\tilde{k},\tilde{j}}+\alpha\mathbf{I}_{2N}\right)^{-1}\mathbf{h}^H_{k,j}\mathbf{h}_{k,j}\left(\mathbf{H}^H_{\tilde{k},\tilde{j}}\mathbf{H}_{\tilde{k},\tilde{j}}+\alpha\mathbf{I}_{2N}\right)^{-1}}{1+\mathbf{h}_{k,j}\left(\mathbf{H}^H_{\tilde{k},\tilde{j}}\mathbf{H}_{\tilde{k},\tilde{j}}+\alpha\mathbf{I}_{2N}\right)^{-1}\mathbf{h}^H_{k,j}}. \tag{34}$$

Then let us define

$$\mathbf{Z}_{k,j}=\mathbf{O}_{k,j}-\frac{\mathbf{O}_{k,j}\left(\frac{1}{N}\mathbf{h}^H_{k,j}\mathbf{h}_{k,j}\right)\mathbf{O}_{k,j}}{1+\frac{1}{N}\mathbf{h}_{k,j}\mathbf{O}_{k,j}\mathbf{h}^H_{k,j}}, \tag{35}$$

where

$$\mathbf{O}_{k,j}=\left(\frac{1}{N}\mathbf{H}^H_{\tilde{k},\tilde{j}}\mathbf{H}_{\tilde{k},\tilde{j}}+\frac{\alpha}{N}\mathbf{I}_{2N}\right)^{-1}. \tag{36}$$

This allows us to rewrite (34) as

$$\left(\mathbf{H}^H\mathbf{H}+\alpha\mathbf{I}_{2N}\right)^{-1}=\frac{1}{N}\mathbf{Z}_{k,j}. \tag{37}$$

Moreover, we rewrite (10) and (11), respectively, as

$$\text{SINR}_{k,j}=\frac{c^2\left|\frac{A_{k,j}}{1+A_{k,j}}\right|^2}{c^2B_{k,j}+\sigma_d^2}, \tag{38}$$

$$\text{SINR}_{\tilde{k},\tilde{j}}=\frac{c^2B_{k,j}}{\sigma_d^2}, \tag{39}$$

where

$$A_{k,j}=\frac{1}{N}\mathbf{h}_{k,j}\mathbf{O}_{k,j}\mathbf{h}^H_{k,j}, \tag{40}$$

and

$$B_{k,j}=\frac{1}{N}\mathbf{h}_{k,j}\mathbf{Z}_{k,j}\left(\frac{1}{N}\mathbf{H}^H_{\tilde{k},\tilde{j}}\mathbf{H}_{\tilde{k},\tilde{j}}\right)\mathbf{Z}_{k,j}\mathbf{h}^H_{k,j}. \tag{41}$$

Aided by [24], we obtain

$$A_{k,j}\xrightarrow{i.p.}g(\beta,\rho_M), \tag{42}$$

$$B_{k,j}\xrightarrow{i.p.}\frac{1}{\left(1+g(\beta,\rho_M)\right)^2}\left(g(\beta,\rho_M)+\rho_M\frac{\partial g(\beta,\rho_M)}{\partial\rho_M}\right), \tag{43}$$

and

$$c^2\xrightarrow{a.s.}\frac{\frac{1}{2}(1+\epsilon)P_t}{g(\beta,\rho_M)+\rho_M\frac{\partial g(\beta,\rho_M)}{\partial\rho_M}}, \tag{44}$$

where $\rho_M=(1+\epsilon)^{-1}\alpha/N$ and $g(\beta,\rho_M)$ is the solution of x to $x=\left(\rho_M+\frac{\beta}{1+x}\right)^{-1}$. In addition, we find that

$$g(\beta,\rho_M)+\rho_M\frac{\partial g(\beta,\rho_M)}{\partial\rho_M}=\frac{\beta g(\beta,\rho_M)}{\beta+\rho_M(1+g(\beta,\rho_M))^2}. \tag{45}$$

Therefore, substituting (42), (43) and (44) into (38), we derive the large-system approximate SINR at the intended user as

$$\text{SINR}^\infty_{k,j}=(1+\epsilon)\gamma g(\beta,\rho_M)\frac{1+\frac{\rho_M}{\beta}\left(1+g(\beta,\rho_M)\right)^2}{(1+\epsilon)\gamma+\left(1+g(\beta,\rho_M)\right)^2}. \tag{46}$$

Also, substituting (43) and (44) into (39), we derive the large-system approximate SINR at the eavesdropper as

$$\text{SINR}^\infty_{\tilde{k},\tilde{j}}=\frac{(1+\epsilon)\gamma}{\left(1+g(\beta,\rho_M)\right)^2}. \tag{47}$$

Finally, by substituting (46) and (47) into (22), we obtain $R^\infty_{s,\text{MCP}}$ for $\alpha\neq 0$ in (23). If $\alpha=0$, we derive the desired result in (23) by calculating $R^\infty_{s,\text{MCP}}(\alpha=0)=\lim_{\alpha\to 0}R^\infty_{s,\text{MCP}}$. This completes the proof of *Theorem 1*.

Appendix B
Proof of Theorem 2

We first derive the large-system approximations of the SINRs for message $s_{k,j}$ at the intended receiver and the eavesdropper, based on which we obtain the large-system secrecy sum rate with the aid of (22).

Let us define

$$\mathbf{A}_j=\left(\rho_C+\frac{1}{N}\sum_{m=1}^{2}\sum_{l=1}^{K}\mathbf{h}^H_{l,m,j}\mathbf{h}_{l,m,j}\right)^{-1} \tag{48}$$

and

$$\mathbf{A}_{kj}=\left(\rho_C+\frac{1}{N}\sum_{(l,m)\neq(k,j)}\mathbf{h}_{l,m,j}^H\mathbf{h}_{l,m,j}\right)^{-1}, \quad (49)$$

where $\rho_C=\alpha/N$. Due to the consideration of $P_1=P_2=P$, we have $c_j=c_{j'}=c$ in (19) and (20). Then, (19) and (20) can be, respectively, rewritten as

$$\mathrm{SINR}_{k,j}=\frac{c^2\left|\frac{1}{N}\mathbf{h}_{k,j,j}\mathbf{A}_{kj}\mathbf{h}_{k,j,j}^H\right|^2}{\sum_{(k',j')\neq(k,j)}\frac{c^2}{N}\theta_{k,j}+\sigma_d^2}, \quad (50)$$

and

$$\mathrm{SINR}_{\tilde{k},\tilde{j}}=\frac{\sum_{(k',j')\neq(k,j)}\frac{c^2}{N}\theta_{\tilde{k},\tilde{j}}}{\sigma_d^2}, \quad (51)$$

where $\theta_{k,j}=\mathbf{h}_{k,j,j'}\mathbf{A}_{k'j'}\mathbf{h}_{k',j',j'}^H\mathbf{h}_{k',j',j'}\mathbf{A}_{k'j'}\mathbf{h}_{k,j,j'}^H$, $\theta_{\tilde{k},\tilde{j}}=\mathbf{h}_{k',j',j}\mathbf{A}_{kj}\mathbf{h}_{k,j,j}^H\mathbf{h}_{k,j,j}\mathbf{A}_{kj}\mathbf{h}_{k',j',j}^H$, and

$$c^2=\frac{P}{\sum_{k=1}^K\|\hat{\mathbf{w}}_{k.j}\|^2}=\frac{P}{\sum_{k=1}^K\frac{1}{N^2}\mathbf{h}_{k,j,j}\mathbf{A}_{kj}^2\mathbf{h}_{k,j,j}^H}. \quad (52)$$

According to [24], we have

$$\max_{j=1,2,k\leq K}\left|\frac{1}{N}\mathbf{h}_{k,j,j}\mathbf{A}_{kj}\mathbf{h}_{k,j,j}^H-\frac{1}{N}\mathrm{Tr}(\mathbf{A}_j)\right|\xrightarrow{a.s}0, \quad (53)$$

$$\max_{j=1,2,k\leq K}\left|\frac{1}{N^2}\mathbf{h}_{k,j,j}\mathbf{A}_{kj}^2\mathbf{h}_{k,j,j}^H-\frac{1}{N}\mathrm{Tr}(\mathbf{A}_j^2)\right|\xrightarrow{a.s}0, \quad (54)$$

$$\max_{j,j'=1,2,\ k,k'\leq K,\ (k,j)\neq(k',j')}\left|\frac{1}{N}\theta_{k,j}-\vartheta_{j'}\right|\xrightarrow{a.s}0, \quad (55)$$

$$\max_{j,j'=1,2,\ k,k'\leq K,\ (k,j)\neq(k',j')}\left|\frac{1}{N}\theta_{\tilde{k},\tilde{j}}-\vartheta_{j}\right|\xrightarrow{a.s}0, \quad (56)$$

where $\vartheta_{j'}=\frac{\omega_{jj'}\frac{\mathrm{Tr}(\mathbf{A}_{j'}^2)}{N}}{\left(1+\omega_{jj'}\frac{\mathrm{Tr}(\mathbf{A}_{j'})}{N}\right)^2}$, $\vartheta_{j}=\frac{\omega_{jj'}\frac{\mathrm{Tr}(\mathbf{A}_{j}^2)}{N}}{\left(1+\omega_{jj'}\frac{\mathrm{Tr}(\mathbf{A}_{j})}{N}\right)^2}$, and

$$\omega_{jj'}=\begin{cases}1 & \text{if} \quad j=j',\\ \epsilon & \text{if} \quad j\neq j'.\end{cases} \quad (57)$$

In addition, we find that

$$\frac{\mathrm{Tr}(\mathbf{A}_j)}{N}=\frac{\mathrm{Tr}(\mathbf{A}_{j'})}{N}\xrightarrow{a.s.}\Lambda, \quad (58)$$

$$\frac{\mathrm{Tr}(\mathbf{A}_j^2)}{N}=\frac{\mathrm{Tr}(\mathbf{A}_{j'}^2)}{N}\xrightarrow{a.s.}-\frac{\partial\Lambda}{\partial\rho_C}, \quad (59)$$

where Λ is the solution of x to

$$x=\frac{1}{\rho_C+\frac{\beta}{1+x}+\frac{\beta\epsilon}{1+\epsilon x}}. \quad (60)$$

Therefore, we obtain the following approximations as

$$|\mathbf{h}_{k,j,j}\hat{\mathbf{w}}_{k,j}|^2\xrightarrow{a.s.}\Lambda^2, \quad (61)$$

$$\sum_{(k',j')\neq(k,j)}|\mathbf{h}_{k,j,j'}\hat{\mathbf{w}}_{k',j'}|^2 \xrightarrow{a.s.}-\left(\frac{\beta\epsilon}{(1+\epsilon\Lambda)^2}+\frac{\beta}{(1+\Lambda)^2}\right)\frac{\partial\Lambda}{\partial\rho_C}, \quad (62)$$

$$\sum_{(k',j')\neq(k,j)}|\mathbf{h}_{k',j',j}\hat{\mathbf{w}}_{k,j}|^2 \xrightarrow{a.s.}-\left(\frac{\beta\epsilon}{(1+\epsilon\Lambda)^2}+\frac{\beta}{(1+\Lambda)^2}\right)\frac{\partial\Lambda}{\partial\rho_C}, \quad (63)$$

and

$$c^2\xrightarrow{a.s.}-\frac{P}{\beta\frac{\partial\Lambda}{\partial\rho_C}}, \quad (64)$$

with

$$-\frac{\partial\Lambda}{\partial\rho_C}=\frac{\Lambda}{\rho_C+\frac{\beta\epsilon}{(1+\epsilon\Lambda)^2}+\frac{\beta}{(1+\Lambda)^2}}. \quad (65)$$

Substituting (61), (62) and (64) into (50), we derive large-system approximate SINR at the intended user as

$$\mathrm{SINR}_{k,j}^{\infty}=\frac{\frac{\Lambda}{\beta}\left(\rho_C+\frac{\beta\epsilon}{(1+\epsilon\Lambda)^2}+\frac{\beta}{(1+\Lambda)^2}\right)}{\frac{1}{\gamma}+\frac{\epsilon}{(1+\epsilon\Lambda)^2}+\frac{1}{(1+\Lambda)^2}}. \quad (66)$$

Also, substituting (63) and (64) into (51), we derive derive large-system approximate SINR at the eavesdropper as

$$\mathrm{SINR}_{\tilde{k},\tilde{j}}^{\infty}=\gamma\left(\frac{\epsilon}{(1+\epsilon\Lambda)^2}+\frac{1}{(1+\Lambda)^2}\right), \quad (67)$$

Finally, by substituting (66) and (67) into (22), we obtain $R_{s,\mathrm{CBf}}^{\infty}$ for $\alpha\neq0$ in (24). If $\alpha=0$, we derive the desired result in (24) by calculating $R_{s,\mathrm{CBf}}^{\infty}(\alpha=0)=\lim_{\alpha\to0}R_{s,\mathrm{CBf}}^{\infty}$. This completes the proof of Theorem 2.

References

[1] B. He, N. Yang, X. Zhou, and J. Yuan, "Confidential broadcasting via coordinated beamforming in two-cell networks," submitted to *Proc. IEEE ICC*, 2015.

[2] M. Bloch and J. Barros, *Physical-Layer Security: From Information Theory to Security Engineering*. Cambridge University Press, 2011.

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

[4] A. D. Wyner, "The wire-tap channel," *Bell Syst. Tech. J.*, vol. 54, no. 8, pp. 1355–1387, Oct. 1975.

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

[6] S. K. Leung-Yan-Cheong and M. E. Hellman, "The Gaussian wire-tap channel," *IEEE Trans. Inf. Theory*, vol. 24, no. 4, pp. 451–456, July 1978.

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

[8] ——, "Secure transmission with multiple antennas–Part II: The MIMOME wiretap channel," *IEEE Trans. Inf. Theory*, vol. 56, no. 11, pp. 5515–5532, Nov. 2010.

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

[10] S. Goel and R. Negi, "Guaranteeing secrecy using artificial noise," *IEEE Trans. Wireless Commun.*, vol. 7, no. 6, pp. 2180–2189, June 2008.

[11] X. Zhou and M. R. McKay, "Secure transmission with artificial noise over fading channels: Achievable rate and optimal power allocation," *IEEE Trans. Veh. Technol.*, vol. 59, no. 8, pp. 3831–3842, Oct. 2010.

[12] A. Mukherjee and A. L. Swindlehurst, "Robust beamforming for security in MIMO wiretap channels with imperfect CSI," *IEEE Trans. Signal Process.*, vol. 59, no. 1, pp. 351–361, Jan. 2011.

[13] N. Yang, P. L. Yeoh, M. Elkashlan, R. Schober, and I. B. Collings, "Transmit antenna selection for security enhancement in MIMO wiretap channels," *IEEE Trans. Commun.*, vol. 61, no. 1, pp. 144–154, Jan. 2013.

[14] R. Liu, T. Liu, H. V. Poor, and S. Shamai, "Multiple-input multiple-output Gaussian broadcast channels with confidential messages," *IEEE Trans. Inf. Theory,*, vol. 56, no. 9, pp. 4215–4227, Sept. 2010.

[15] D. A. A. Fakoorian and A. L. Swindlehurst, “MIMO interference channel with confidential messages: Achievable secrecy rates and precoder design,” *IEEE Trans. Inf. Forensics Security*, vol. 6, no. 3, pp. 640–649, Sept. 2011.

[16] G. Geraci, M. Egan, J. Yuan, A. Razi, and I. B. Collings, “Secrecy sum-rates for multi-user MIMO regularized channel inversion precoding,” *IEEE Trans. Commun.*, vol. 60, no. 11, pp. 3472–3482, Nov. 2012.

[17] G. Geraci, R. Couillet, J. Yuan, M. Debbah, and I. B. Collings, “Large system analysis of linear precoding in MISO broadcast channels with confidential messages,” *IEEE J. Sel. Areas Commun.*, vol. 31, no. 9, pp. 1660–1671, Sept. 2013.

[18] G. Geraci, A. Y. Al-Nahari, J. Yuan, and I. B. Collings, “Linear precoding for broadcast channels with confidential messages under transmit-side channel correlation,” *IEEE Commun. Lett.*, vol. 17, no. 6, pp. 1164–1167, June 2013.

[19] N. Yang, G. Geraci, J. Yuan, and R. Malaney, “Confidential broadcasting via linear precoding in non-homogeneous MIMO multiuser networks,” *IEEE Trans. Commun.*, vol. 62, no. 7, pp. 2515–2530, July 2014.

[20] D. Gesbert, S. Hanly, H. Huang, S. S. Shitz, O. Simeone, and W. Yu, “Multi-cell MIMO cooperative networks: A new look at interference,” *IEEE J. Sel. Areas Commun.*, vol. 28, no. 9, pp. 1380–1408, Dec. 2010.

[21] C. B. Peel, B. M. Hochwald, and A. L. Swindlehurst, “A vector-perturbation technique for near-capacity multiantenna multiuser communication–Part I: Channel inversion and regularization,” *IEEE Trans. Commun.*, vol. 53, no. 1, pp. 195–202, Jan. 2005.

[22] R. Zakhour and S. Hanly, “Base station cooperation on the downlink: Large system analysis,” *IEEE Trans. Inf. Theory*, vol. 58, no. 4, pp. 2079–2106, Apr. 2012.

[23] H. Dahrouj and W. Yu, “Coordinated beamforming for the multicell multi-antenna wireless system,” *IEEE Trans. Wireless Commun.*, vol. 9, no. 5, pp. 1748–1759, May 2010.

[24] R. Muharar, R. Zakhour, and J. Evans, “Base station cooperation with feedback optimization: A large system analysis,” *IEEE Trans. Inf. Theory*, vol. 60, no. 6, pp. 3620–3644, June 2014.

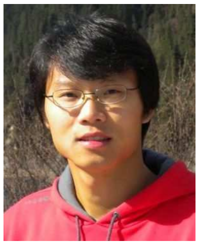
[25] Q. H. Spencer, A. L. Swindlehurst, and M. Haardt, “Zero-forcing methods for downlink spatial multiplexing in multiuser MIMO channels,” *IEEE Trans. Signal Process.*, vol. 52, no. 2, pp. 461–471, Feb. 2004.

[26] H. Sung, S.-R. Lee, and I. Lee, “Generalized channel inversion methods for multiuser MIMO systems,” *IEEE Trans. Commun.*, vol. 57, no. 11, pp. 3489–3499, Nov. 2009.

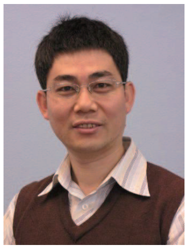
[27] Z. Shen, R. Chen, J. G. Andrews, R. W. Heath, and B. L. Evans, “Low complexity user selection algorithms for multiuser MIMO systems with block diagonalization,” *IEEE Trans. Signal Process.*, vol. 54, no. 9, pp. 3658–3663, Sept. 2006.

Biao He (S’13) received the B.E. (hons.) degree in electronic and communication systems from the Australian National University (ANU) in 2012. At the same year, he received the B.E. degree in information engineering from Beijing Institute of Technology (BIT). Currently, he is pursuing his Ph.D. degree in the Research School of Engineering at the ANU. His research interests include physical layer security, wireless communications, and information theory.

Nan Yang (S’09–M’11) received the B.S. degree in electronics from China Agricultural University in 2005, and the M.S. and Ph.D. degrees in electronic engineering from the Beijing Institute of Technology in 2007 and 2011, respectively. He is currently a Future Engineering Research Leadership Fellow and Lecturer in the Research School of Engineering at the Australian National University. Prior to this he was a Postdoctoral Research Fellow at the University of New South Wales (2012–2014) and a Postdoctoral Research Fellow at the Commonwealth Scientific and Industrial Research Organization (2010–2012). He received the IEEE ComSoc Asia-Pacific Outstanding Young Researcher Award in 2014, the Exemplary Reviewer Certificate of the IEEE Wireless Communications Letters in 2014, the Exemplary Reviewer Certificate of the IEEE Communications Letters in 2012 and 2013, and the Best Paper Award at the IEEE 77th Vehicular Technology Conference in 2013. He serves as an editor of the Transactions on Emerging Telecommunications Technologies. His general research interests lie in the areas of communications theory and signal processing, with specific interests in collaborative networks, network security, massive multi-antenna systems, millimeter wave communications, and molecular communications.



Xiangyun Zhou (M’11) is a Senior Lecturer at the Australian National University (ANU). He received the Ph.D. degree in telecommunications engineering from ANU in 2010. His research interests are in the fields of communication theory and wireless networks. He currently serves on the editorial board of IEEE Transactions on Wireless Communications and IEEE Communications Letters. He also served as a guest editor for IEEE Communications Magazine’s feature topic on wireless physical layer security in 2015. He was a co-chair of the ICC workshop on wireless physical layer security at ICC’14 and ICC’15. He was the chair of the ACT Chapter of the IEEE Communications Society and Signal Processing Society from 2013 to 2014. He is a recipient of the Best Paper Award at ICC’11.



Jinhong Yuan (M’02–SM’11) received the B.E. and Ph.D. degrees in electronics engineering from the Beijing Institute of Technology, Beijing, China, in 1991 and 1997, respectively. From 1997 to 1999, he was a Research Fellow with the School of Electrical Engineering, University of Sydney, Sydney, Australia. In 2000, he joined the School of Electrical Engineering and Telecommunications, University of New South Wales, Sydney, Australia, where he is currently a Telecommunications Professor with the School. He has published two books, three book chapters, over 200 papers in telecommunications journals and conference proceedings, and 40 industrial reports. He is a co-inventor of one patent on MIMO systems and two patents on low-density-parity-check codes. He has co-authored three Best Paper Awards and one Best Poster Award, including the Best Paper Award from the IEEE Wireless Communications and Networking Conference, Cancun, Mexico, in 2011, and the Best Paper Award from the IEEE International Symposium on Wireless Communications Systems, Trondheim, Norway, in 2007. He is currently serving as an Associate Editor for the IEEE Transactions on Communications. He served as the IEEE NSW Chair of Joint Communications/Signal Processions/Ocean Engineering Chapter during 2011-2014. His current research interests include error control coding and information theory, communication theory, and wireless communications.