Confidential Broadcasting via Coordinated Beamforming in Two-Cell Networks

Biao He†, Nan Yang†, Xiangyun Zhou†, and Jinhong Yuan‡
†Research School of Engineering, Australian National University, Canberra, Australia
‡School of Electrical Engineering and Telecommunications, The University of New South Wales, Sydney, Australia
Email: biao.he@anu.edu.au, nan.yang@anu.edu.au, xiangyun.zhou@anu.edu.au, j.yuan@unsw.edu.au

***Abstract*—We design a linear precoder based on the principles of the generalized regularized channel inversion (RCI) precoder that achieves confidential broadcasting in a two-cell network. In each cell of the network, an N-antenna base station (BS) communicates with K single-antenna users. We consider coordinated beamforming where the BSs in the two cells do not share messages but the users in the two cells feed back their channel state information to both BSs. In the precoder design, we determine the optimal regularization parameter that maximizes the secrecy sum rate. To this end, we derive new channel-independent expressions for the secrecy sum rate in the large-system regime, where K and N approach infinity with a fixed ratio $\mu = K/N$. Moreover, we propose a power-reduction strategy that significantly improves the secrecy sum rate at high transmit signal-to-noise ratios when μ is higher than 0.5.**

I. Introduction

Wireless technologies have been deeply embedded in the modern life to bring great convenience for everyone. Along with the unchangeable open nature of wireless medium, security has become a critical issue for wireless data transmissions. As a complement to the traditional cryptographic technique, physical (PHY) layer security has been extensively investigated [1, 2] to provide secure wireless communications by exploiting the characteristics of wireless channels. In Wyner's pioneering study [3], the wiretap channel was introduced as a fundamental framework for PHY layer security. In this study, Wyner defined the secrecy capacity as the maximum rate at which confidential messages can be reliably decoded by the legitimate receiver, while the eavesdropper obtains zero information. This result was subsequently extended to the broadcast channel with confidential messages and the Gaussian wiretap channel in [4] and [5], respectively. Recently, PHY layer security in multi-antenna wiretap channels has attracted a significant amount of attention, where the transmitter, the receiver and/or the eavesdropper are equipped with multiple antennas. This is triggered by the rapid development in multi-input multi-output (MIMO) techniques that provide high-rate data transmissions. From the information-theoretical perspective, the secrecy capacity in the multi-antenna wiretap channel was analyzed in, e.g., [6–8]. From a signal processing perspective, various PHY layer security techniques have been proposed to improve the secrecy performance of the multi-antenna wiretap channel, e.g., [9–13].

This work was supported by the Australian Research Council under Discovery Project Grant DP150103905.

Apart from the multi-antenna wiretap channel, PHY layer security in multi-antenna broadcast networks has also drawn considerable attention. The research in this direction is based on the concept of confidential broadcasting [4], where confidential messages are broadcasted to intended users in multi-user networks and the unintended users should be kept in full ignorance. The secrecy capacity of confidential broadcasting in the two-user network was evaluated in [14, 15]. In [16–19], confidential broadcasting was investigated in the *single-cell* network with one base station (BS) and arbitrary number of users. Among these studies, [16] designed a linear precoder based on the principles of regularized channel inversion (RCI) in order to achieve confidential broadcasting for single-antenna users. Considering the same precoder, the achievable secrecy sum rate was evaluated in [17]. The impact of channel correlation at the BS on the secrecy sum rate was examined in [18]. Taking multi-antenna users into consideration, [19] designed a linear RCI precoder and addressed unequal path loss from the BS to users. While [16–19] have thoroughly studied confidential broadcasting in the *single-cell* network, the precoder for confidential broadcasting in the *multi-cell* network has yet been explored in the literature. In the multi-cell network, the primary challenge in performing confidential broadcasting is to conduct the inter-cell secrecy control apart from the intra-cell secrecy control. Therefore, the results from [16–19] cannot be used in multi-cell confidential broadcasting.

In this paper, we propose an effective solution to tackle the challenge of performing confidential broadcasting in multi-cell networks. Specifically, we designed a linear precoder based on the rules of generalized RCI [20] under the consideration of coordinated beamforming. In coordinated beamforming, the BSs in different cells do not share messages but the users in different cells are allowed to feed back the channel state information (CSI) to all BSs [21]. As such, coordinated beamforming applies to the practical scenario where the high-capacity backhaul links between BSs are not available. Motivated by this, the benefits of coordinated beamforming on multi-cell network without secrecy consideration have been studied in, e.g., [22]. With secrecy considerations, we study confidential broadcasting in a symmetric two-cell network with coordinated beamforming in this work. Each cell in the network consists of K single-antenna users and one N-antenna BS. The two BSs coordinate at the beamforming level to broadcast confidential messages to intended users, while unintended users in the same cell and the cross cell are regarded as potential eavesdroppers.

Certainly, 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:

1) We design a linear precoder that achieves confidential broadcasting in two-cell networks with coordinated beamforming. In the design of the precoder matrix, we strike a balance between the received signal at the intended user and the crosstalk at the unintended users in both cells through a regularization parameter.
2) We derive new channel-independent expressions for the secrecy sum rate achieved by the linear precoder in the large-system regime, where $K, N \to \infty$ with a fixed ratio $\mu = K/N$. The newly derived expressions allow us to examine the secrecy performance without time-consuming simulations.
3) We propose an algorithm to determine the optimal regularization parameter that maximizes the secrecy sum rate in the large-system regime. Using the optimal regularization parameter, the secrecy sum rate always increases with the transmit signal-to-noise ratio (SNR) for $\mu \leq 0.5$.
4) We propose a power-reduction strategy that significantly increases the secrecy sum rate at high transmit SNRs for $\mu > 0.5$. Based on the generalized RCI and the power reduction strategy, we further design a power-reduction precoder, named generalized RCI-PR precoder.

Notations: $(\cdot)^H$ and $(\cdot)^T$ denote the conjugate transpose and the transpose, 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; $[x]^+ = \max(x, 0)$; $\xrightarrow{a.s}$ denotes almost sure convergence.

II. Confidential Broadcasting in Two-Cell Broadcast Networks

A. Network Model

We consider a symmetric two-cell broadcast network, as depicted in Figure 1, where each cell consists of K single-antenna users and one N-antenna BS. In this network, we assume that each BS transmits confidential messages to the users in the same cell. We also assume that the users in both cells feed back their CSI to the same-cell BS and the cross-cell BS. The two BSs cooperate to control the inter-cell information leakage and the inter-cell interference. 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 $k \in \{1, 2, \cdots, K\}$. We also denote the row vector $\mathbf{h}_{k,j,i}$ as the channel vector from BS (i) to user (k, j). We further denote the $2K \times N$ matrix $\mathbf{H}_i = \left[\mathbf{h}_{1,1,i}^H\ \mathbf{h}_{2,1,i}^H \cdots \mathbf{h}_{K,1,i}^H\ \mathbf{h}_{1,2,i}^H\ \mathbf{h}_{2,2,i}^H \cdots \mathbf{h}_{K,2,i}^H\right]^H$ as the channel matrix from BS (i) to all the users in both cells.

We assume that all links between the transmit and receive antennas are uncorrelated, as the antennas are all sufficiently spaced apart. We also assume that the data transmission is performed over block fading channels, where the symbol interval is much smaller than the coherence time of channel.

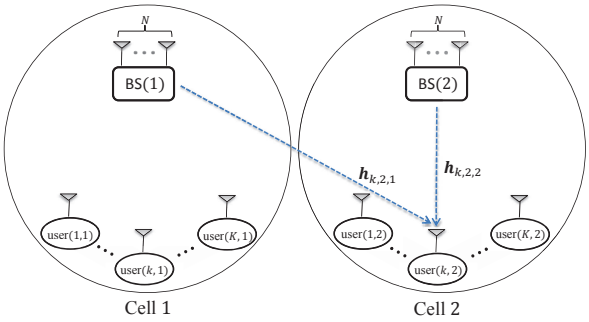

Fig. 1. Illustration of a symmetric two-cell broadcast network.

We further assume that channels between the BS and the same-cell users are modeled as independent and identically distributed (i.i.d.) complex Gaussian variables with zero mean and unit variance, i.e., $\mathbf{h}_{k,j,j} \sim \mathcal{CN}(\mathbf{0}, \mathbf{I}_N)$, and the channels between the BS and the cross-cell users are modeled as i.i.d. complex Gaussian variables with zero mean and variance δ, i.e., $\mathbf{h}_{k,j,\bar{j}} \sim \mathcal{CN}(\mathbf{0}, \delta\mathbf{I}_N)$, where $\bar{j} = 1$ if $j = 2$ and $\bar{j} = 2$ if $j = 1$. Here, $0 < \delta \leq 1$ denotes the cross-cell interference level between the two cells. We assume that each user obtains perfect knowledge of its own channel, and then 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 each BS (i) obtains perfect knowledge of $\mathbf{H}_i$ from the feedback information.

In the two-cell broadcast network, 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 $\mathbf{x}_i \in \mathbb{C}^{N\times 1}$, $i \in \{1, 2\}$, denotes the transmitted data from BS (i) and $n_{k,j} \sim \mathcal{CN}(0, \sigma_d^2)$ denotes the additive white Gaussian noise (AWGN) at user (k, j). Based on (1), the received signals at all users can be expressed as

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

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

As required by confidential broadcasting, the message needs to be securely transmitted to the intend user while the unintended users obtain zero information. In this work, we consider a worst-case scenario where all the other $2K - 1$ users act as potential eavesdroppers for the message to the intend user, since BSs cannot fully control the behavior of the users. In this scenario, we assume that the $2K-1$ eavesdroppers collaborate to jointly eavesdrop on the message to the intend user. Under this assumption, they decode their own signals and share them with each other, leaving only the signal for the intended user. The alliance of $2K-1$ cooperating eavesdroppers is equivalent to a single eavesdropper with $2K - 1$ receive antennas. For the message to user (k, j), we denote eavesdropper $(\tilde{k}, \tilde{j})$ as the eavesdropper with $2K - 1$ antennas. We note that the consideration of the worst-case scenario is widely adopted in designing confidential broadcasting networks; see, e.g., [16–19]. The performance of confidential broadcasting in the

network is measured by the secrecy sum rate. Mathematically the secrecy sum rate is 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).

B. Secrecy Sum Rate with Generalized RCI Precoder

In this work, we adopt the generalized RCI precoder [20] at BSs to perform confidential broadcasting in the two-cell broadcast network. Using this precoder, each BS controls the information leakage and interference amongst the users in both the same cell and the cross cell. Under the requirement of confidential broadcasting, the generalized RCI precoding vector for the message to user (k, j) is given by

$$\mathbf{w}_{k,j} = c_j \hat{\mathbf{w}}_{k,j} = c_j \left(\alpha \mathbf{I}_N + \sum_{(l,m)\neq(k,j)} \mathbf{h}_{l,m,j}^H \mathbf{h}_{l,m,j} \right)^{-1} \mathbf{h}_{k,j,j}^H, \tag{4}$$

where c_j denotes the scaling factor that adjusts the transmit power at BS (j) and α denotes the real non-negative regularization parameter that trades off the received signal power at the intended receiver and the amount of information leakage as well as interference amongst users. Based on (4), the transmitted data at BS (j) is given by

$$\mathbf{x}_j = \sum_{k=1}^{K} \mathbf{w}_{k,j} s_{k,j}, \tag{5}$$

where $s_{k,j}$ denotes the message to user (k, j). We assume that the messages are independent with a unit average power constraint, such that $\mathbb{E}\{\mathbf{s}\mathbf{s}^H\} = \mathbf{I}_{2K}$ with $\mathbf{s} = [s_{1,1}\ s_{2,1}\ \cdots\ s_{K,1}\ s_{1,2}\ s_{2,2}\ \cdots\ s_{K,2}]^T$. In addition, we consider that there is a long-term power constraint at each BS, such that $\mathbb{E}\{\|\mathbf{x}_j\|^2\} = P_j$. Hence, the scaling factor c_j in (4) is determined by

$$c_j^2 = \frac{P_j}{\sum_{k=1}^{K} \|\hat{\mathbf{w}}_{k,j}\|^2}. \tag{6}$$

Without loss of generality, we assume that the long-term power constraints at the two BSs are the same with $P_1 = P_2 = P$. From (4), (5) and (6), we find that each BS (j) only needs $\mathbf{h}_{k,i,j}$ to construct the precoding matrix, while $\mathbf{h}_{k,i,\tilde{j}}$ is not required.

Based on the precoding vector, the received signal at the intended user (k, j) is given by

$$y_{k,j} = \mathbf{h}_{k,j,j} \mathbf{w}_{k,j} s_{k,j} + \sum_{(k',j')\neq(k,j)} \mathbf{h}_{k,j,j'} \mathbf{w}_{k',j'} s_{k',j'} + n_{k,j} \tag{7}$$

and the received signal vector at the eavesdropper $(\tilde{k}, \tilde{j})$ is given by

$$\mathbf{y}_{\tilde{k},\tilde{j}} = \mathbf{H}_{\tilde{k},\tilde{j},j} \mathbf{w}_{k,j} s_{k,j} + \mathbf{n}_{\tilde{k},\tilde{j}}, \tag{8}$$

where $\mathbf{H}_{\tilde{k},\tilde{j},j}$ denotes the matrix obtained from $\mathbf{H}_j$ by removing the row corresponding to user (k, j) and $\mathbf{n}_{\tilde{k},\tilde{j}}$ denotes vector obtained from $\mathbf{n}$ by removing the row corresponding to user (k, j). Based on (7) and (8), the signal-to-interference-plus-noise ratios (SINRs) for the message $s_{k,j}$ at the intended user (k, j) and the eavesdropper $(\tilde{k}, \tilde{j})$ are given by

$$\mathrm{SINR}_{k,j} = \frac{c_j^2 \left| \mathbf{h}_{k,j,j} \hat{\mathbf{w}}_{k,j} \right|^2}{\sigma_d^2 + \sum\limits_{(k',j')\neq(k,j)} c_{j'}^2 \left| \mathbf{h}_{k,j,j'} \hat{\mathbf{w}}_{k',j'} \right|^2} \tag{9}$$

and

$$\mathrm{SINR}_{\tilde{k},\tilde{j}} = \sum_{(k',j')\neq(k,j)} \frac{c_j^2 \left| \mathbf{h}_{k',j',j} \hat{\mathbf{w}}_{k,j} \right|^2}{\sigma_d^2}, \tag{10}$$

respectively. Accordingly, the secrecy sum rate achieved by the generalized RCI precoder is given by

$$R_s = \sum_{j=1}^{2} \sum_{k=1}^{K} \left[\log_2(1+\mathrm{SINR}_{k,j}) - \log_2\left(1+\mathrm{SINR}_{\tilde{k},\tilde{j}}\right) \right]^+. \tag{11}$$

Substituting (9) and (10) into (11), we obtain the secrecy sum rate depending on the realization of each channel, $\mathbf{h}_{k,j,i}$. As such, we have to use the time-consuming Monte Carlo simulations for evaluating the secrecy performance based on (11). This motivates us to seek channel-independent expressions that eliminate the computation burden of performance evaluation via Monte Carlo simulations.

III. Secrecy Sum Rate in Large-System Regime

In this section, we derive channel-independent expressions for R_s of the two-cell broadcast network by the large-system analysis. In the large-system regime, the number of users in each cell, K, and the number of antennas at each BS, N, approach infinity with a fixed ratio, $\mu = K/N$. Besides, we denote $\gamma = P/\sigma_d^2$ as the *transmit* SNR at each BS.

A. Large-System Secrecy Sum Rate

As $K, N \to \infty$, all secrecy rates R_{kj} for all messages $s_{k,j}$ converge to the same non-random function, which does not depend on the realization of $\mathbf{h}_{k,j,i}$. Then, the secrecy sum rate is analytically approximated as

$$R_s^{\infty} = 2K \left(R_{k,j}^{\infty} \right) = 2K \left[\log_2 \left(\frac{1 + \mathrm{SINR}_{k,j}^{\infty}}{1 + \mathrm{SINR}_{\tilde{k},\tilde{j}}^{\infty}} \right) \right]^+, \tag{12}$$

where $R_{k,j}^{\infty}$ is the large-system secrecy rate for each user, $\mathrm{SINR}_{k,j}^{\infty}$ is the large-system approximation of the SINR at the intended user, and $\mathrm{SINR}_{\tilde{k},\tilde{j}}^{\infty}$ is the large-system approximation of the SINR at the eavesdropper. Throughout this paper, we refer to R_s^{∞} as the large-system secrecy sum rate. As will be shown in Section III-B, the large-system secrecy sum rate can accurately approximate the secrecy sum rate of the network even with finite K and N.

Theorem 1. *The large-system secrecy sum rate achieved by the generalized RCI precoder is derived as* (13) *on the next page, where* $\rho = \alpha/N$, Θ *is the solution of* x *to* $x = \left(\rho + \frac{\mu\delta}{1+\delta x} + \frac{\mu}{1+x} \right)^{-1}$ *and* Θ_0 *is the solution of* x *to* $x = \left(\frac{\mu\delta}{1+\delta x} + \frac{\mu}{1+x} \right)^{-1}$.

$$R_s^{\infty} = \begin{cases} 2K\left[\log_2\left(\dfrac{1+\frac{\frac{\Theta}{\mu}\left(\rho+\frac{\mu\delta}{(1+\delta\Theta)^2}+\frac{\mu}{(1+\Theta)^2}\right)}{\frac{1}{\gamma}+\frac{\delta}{(1+\delta\Theta)^2}+\frac{1}{(1+\Theta)^2}}}{1+\gamma\left(\frac{\delta}{(1+\delta\Theta)^2}+\frac{1}{(1+\Theta)^2}\right)}\right)\right]^+, & \text{if } \alpha \neq 0 \\ 2K\log_2\left(1+\dfrac{(1-2\mu)\gamma}{\mu}\right), & \text{if } \alpha = 0 \text{ and } \mu \leq 0.5 \\ 2K\left[\log_2\left(\dfrac{1+\frac{\frac{\Theta_0}{\mu}\left(\frac{\mu\delta}{(1+\delta\Theta_0)^2}+\frac{\mu}{(1+\Theta_0)^2}\right)}{\frac{1}{\gamma}+\frac{\delta}{(1+\delta\Theta_0)^2}+\frac{1}{(1+\Theta_0)^2}}}{1+\gamma\left(\frac{\delta}{(1+\delta\Theta_0)^2}+\frac{1}{(1+\Theta_0)^2}\right)}\right)\right]^+, & \text{if } \alpha = 0 \text{ and } \mu > 0.5. \end{cases} \tag{13}$$

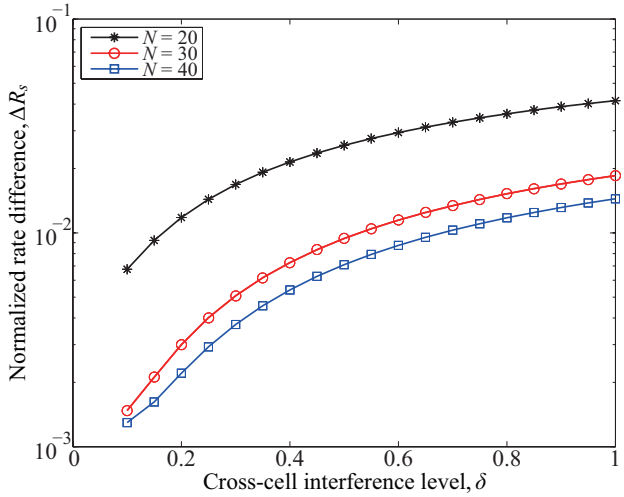

Fig. 2. The normalized rate difference versus the cross-cell interference level for $\alpha = 0.2, \mu = 0.5$ and $\gamma = 10$ dB.

Proof: See Appendix A. ■

B. Numerical Results

We now verify the accuracy of our large-system analysis by numerical results. Specifically, we compare the large-system secrecy sum rate, R_s^{∞} given by (13), and the average secrecy sum rate of the network with finite K and N obtained via Monte Carlo simulations, denoted by $\mathbb{E}\{R_s\}$. To facilitate this comparison, we define the normalized rate difference to quantify the rate difference between R_s^{∞} and $\mathbb{E}\{R_s\}$, which is given by

$$\Delta R_s = \frac{|\mathbb{E}\{R_s\} - R_s^{\infty}|}{\mathbb{E}\{R_s\}}. \tag{14}$$

We demonstrate the accuracy of the large-system approximations for different sizes of networks over the entire range of δ. Figure 2 plots ΔR_s versus δ for $N = 20$, 30, and 40.[1] As shown in the figure, ΔR_s decreases as N increases for any given δ. This indicates that the large-system approximation becomes more accurate as the size of network increases. For the entire range of δ, we find that the highest ΔR_s for the network with $N = 20$ is approximately 4%, the highest ΔR_s for the network with $N = 30$ is approximately 2%, and the highest ΔR_s for the network with $N = 40$ is approximately 1.4%. These observations confirm that the large-system approximations provide high accuracy across the entire range of δ, even for the finite network.

[1]In this paper, we often present the numerical results by considering some particular network parameters. For instance, we adopt $\alpha = 0.2, \mu = 0.5$ and $\gamma = 10$ dB in Figure 2. However, this does not restrict the generality of our results for arbitrary network parameters.

IV. Performance Optimization

In this section, we optimize the network performance by maximizing the large-system secrecy sum rate. We first determine the optimal regularization parameter that maximizes the large-system secrecy sum rate. Second, we propose a power-reduction strategy that maintains the maximum large-system secrecy sum rate when increasing transmit power cannot sustain a growing large-system secrecy sum rate.

A. Optimal Regularization Parameter

In the precoder design, the regularization parameter, α, trades off the received signal power at the intended receiver and the amount of information leakage as well as interference amongst users. Thus, the value of α in the precoding matrix directly determines the performance of confidential broadcasting in the two-cell network. In this subsection, we determine the optimal regularization parameter, denoted by α^*, that maximizes the large-system secrecy sum rate.

1) Determination of α^*: Mathematically, α^* is formulated as

$$\alpha^* = \arg\max_{\alpha} R_s^{\infty}. \tag{15}$$

Observing R_s^{∞} in (13), we find that the closed-form expression for α^* is mathematically intractable, due to the complexity of the expression involved. As such, we propose **Algorithm 1** to efficiently determine α^* numerically. In this algorithm, we first decide the searching range of α^* by the one-side-search technique [23]. We then adopt the bisection-search technique to find α^* within the searching range. The optimality of α^* obtained from **Algorithm 1** will be verified by the following numerical results.

2) Numerical Results: First, we demonstrate the optimality of α^* over the entire range of δ. Figure 3 plots the large-system secrecy rate per transmit antenna, denoted by $R_s^{\infty}/(2N)$, versus δ. In this figure, we specifically consider three different values of α: 1) α^* obtained by **Algorithm 1**, 2) an arbitrarily

Algorithm 1 Numerical Search for α^*

Input: $f(x) = \frac{\partial R_s^{\infty}}{\partial \alpha}(\alpha = x)$;
Acceptable error d (e.g., $d = 10^{-10}$);
Initial search point α_p (e.g., $\alpha_p = 1$);
Output: α^* that satisfies $|f(\alpha^*)| \leq d$;
Initialize iteration counters: $c = 0$;
if $|f(\alpha_p)| \leq d$ **then**
  return $\alpha^* = \alpha_p$; {The value of α^* is obtained.}
end if
if $f(\alpha_p) > 0$ **then**
  Initialize the lower bound of α^* 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 α^* by $\alpha_u = \alpha_l + 2^c$;
else
  Initialize the upper bound of α^* 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 α^* by $\alpha_l = \alpha_u \times 10^{-1}$;
end if
if $|f(\alpha_l)| \leq d$ **then**
  return $\alpha^* = \alpha_l$; {The value of α^* is obtained.}
end if
if $|f(\alpha_u)| \leq d$ **then**
  return $\alpha^* = \alpha_u$; {The value of α^* 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 $\alpha^* = \alpha_m$; {The value of α^* is obtained.}

chosen α, i.e., $\alpha = 0.2$ and 3) the optimal α that maximizes the large-system sum rate without secrecy considerations, which is obtained from [24] and denoted by $\tilde{\alpha}^*$. As depicted in the figure, the secrecy rate achieved by α^* is always higher than the secrecy rates achieved by the other two values of α. This observation confirms the optimality of α^* over the entire range of δ. Note that the optimal value of α without secrecy considerations, $\tilde{\alpha}^*$, is no longer optimal in the secrecy network. Besides, we find that the secrecy rate always decreases as δ

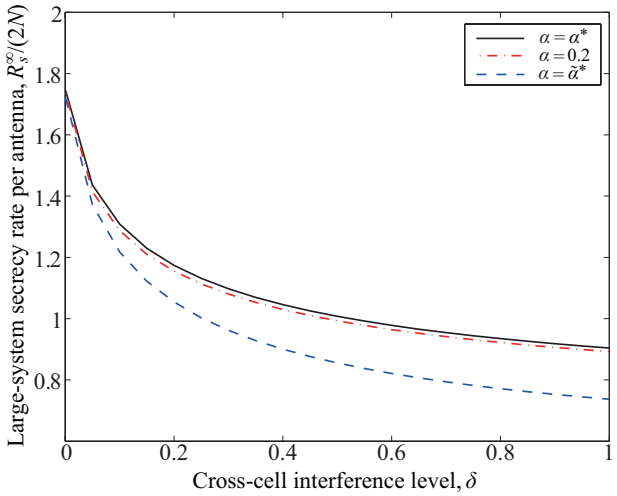

Fig. 3. The large-system secrecy rate per antenna versus the cross-cell interference level for different values of the regularization parameter with $N = 20, \mu = 0.5$ and $\gamma = 10$ dB.

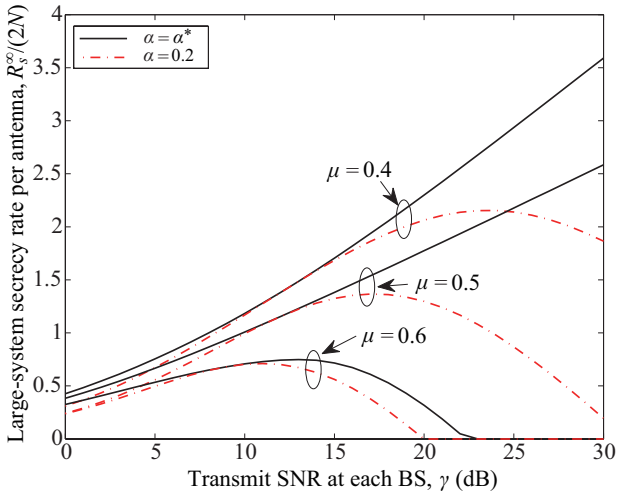

Fig. 4. The large-system secrecy rate per antenna versus the transmit SNR at each BS for different values of the regularization parameter with $\mu = 0.4, 0.5, 0.6, N = 20$ and $\delta = 0.5$.

increases. This observation can be explained as follows. Since each BS transmit messages to the users only in the same cell, the increase in δ does not increase the received signal power at the intended receiver. However, the increase in δ leads to the increasing interference power at the intended user and the increasing received signal power at the eavesdropper. Thus, the secrecy rate decreases as δ increases.

Now we verify the optimality of α^* against the transmit SNR at each BS, γ, and examine the impact of γ on the secrecy rate. Figure 4 plots $R_s^{\infty}/(2N)$ versus γ. As the figure shows, the secrecy rate achieved by $\alpha = \alpha^*$ is always higher than that achieved by $\alpha = 0.2$. This confirms the optimality of the obtained α^*. Notably, the secrecy rate achieved by $\alpha = 0.2$ always reduces to zero when γ grows large. This can be explained from (13), i.e., $\lim_{\gamma \to \infty} R_s^{\infty} = 0$ if $\alpha \neq 0$.

Differently, the secrecy rate achieved by $\alpha = \alpha^*$ may not reduce to zero when γ is high. Specifically, we observe that the secrecy rate achieved by $\alpha = \alpha^*$ monotonically increases with γ if $\mu \leq 0.5$. This observation reveals that the increase in the transmit power always benefits the secrecy performance achieved by the optimal regularization parameter when the network load is low. We also observe that if $\mu > 0.5$, the secrecy rate achieved by $\alpha = \alpha^*$ increases with γ at low and medium transmit SNRs, but goes to zero at high transmit SNRs. This observation reveals that the increase in the transmit power is first beneficial and then detrimental to the secrecy performance when the network load is high. These observations can be explained as follows. From the analytical results, we note that α^* goes to zero as γ increases. When $\alpha \to 0$, we find that $\lim_{\alpha \to 0} R_s^{\infty}$ in (13) monotonically increases with γ if $\mu \leq 0.5$, while $\lim_{\alpha \to 0} R_s^{\infty}$ goes to zero at high transmit SNRs if $\mu > 0.5$.

B. Power-Reduction Strategy

In this subsection, we propose a power-reduction strategy to compensate the secrecy rate loss at high transmit SNRs when $\mu > 0.5$. Based on this strategy, we design a new linear precoder named the generalized RCI-PR precoder.

1) Generalized RCI-PR Precoder: We first obtain the optimal transmit SNR that maximizes the large-system secrecy sum rate achieved by the RCI precoder with $\alpha = \alpha^*$, denoted by $R_s^{\infty *}$, for $\mu > 0.5$. This optimal transmit SNR is formulated as $\gamma^* = \arg\max_{\gamma} R_s^{\infty *}$. Although the closed-form expression for γ^* cannot be derived, we are able to obtain γ^* through numerical search.

Based on γ^*, we now propose the power-reduction strategy for $\mu > 0.5$. In this strategy, the actual transmit power is reduced when $\gamma > \gamma^*$ such that the maximum large-system secrecy sum rate is maintained. The precoding vector with the power-reduction strategy is designed as

$$\mathbf{w}_{\text{PR}} = \begin{cases} \sqrt{\frac{\gamma^*}{\gamma}}\mathbf{w}^*, & \mu > 0.5 \text{ and } \gamma > \gamma^* \\ \mathbf{w}, & \text{otherwise,} \end{cases} \tag{16}$$

where $\mathbf{w}$ is the generalized RCI precoding vector given in (4) with $\alpha = \alpha^*$ and $\mathbf{w}^*$ is the vector obtained from the generalized RCI precoding vector with $\alpha = \alpha^*$ at $\gamma = \gamma^*$. We refer to the linear precoder using $\mathbf{w}_{\text{PR}}$ in (16) as the generalized RCI-PR precoder. In (16), we highlight that $\sqrt{\gamma^*/\gamma}$ is the power-reduction coefficient, which is adopted when $\mu > 0.5$ and $\gamma > \gamma^*$. Notably, the reduced transmit SNR by adopting the generalized RCI-PR precoder becomes

$$\gamma_{\text{PR}} = \begin{cases} \gamma^*, & \mu > 0.5 \text{ and } \gamma > \gamma^* \\ \gamma, & \text{otherwise.} \end{cases} \tag{17}$$

2) Numerical Results: We now demonstrate the performance improvement offered by the proposed power-reduction strategy. Figure 5 plots $R_s^{\infty}/(2N)$ versus γ. In the figure, we compare the secrecy performance achieved by the generalized RCI-PR precoder and that achieved by the generalized RCI precoder with $\alpha = \alpha^*$. We clarify that the actual transmit SNR of the generalized RCI-PR precoder is γ^* when $\gamma > \gamma^*$,

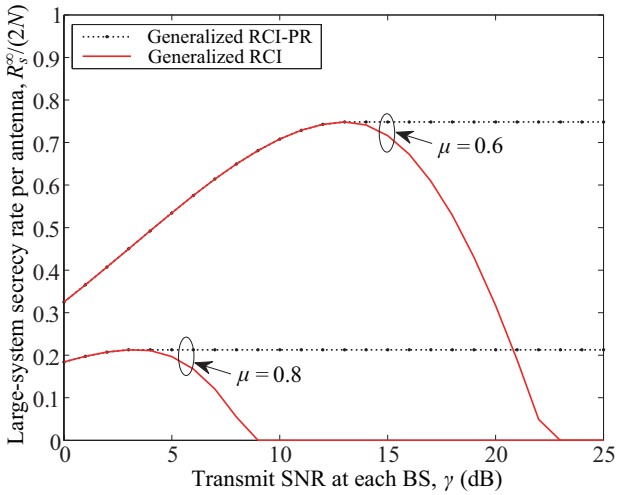

Fig. 5. The large-system secrecy rate per antenna versus the transmit SNR at each BS for transmissions with and without the power-reduction strategy. The other network parameters are $\mu = 0.6, 0.8$, $N = 20$ and $\delta = 0.5$.

as indicated by (17). It is evident that the decrease in the secrecy rate at high transmit SNRs, caused by the generalized RCI precoder, is effectively prevented by the proposed power-reduction strategy. Notably, the power-reduction strategy maintains the maximum secrecy rate achieved at γ^* when γ grows large. In addition, we highlight that such an improvement is achieved by using a lower transmit power, compared with the generalized RCI precoder without power reduction.

V. Conclusions

In this paper, we designed a linear precoder based on the principles of generalized RCI in order to perform confidential broadcasting in the two-cell network with coordinated beamforming. We derived accurate and channel-independent large-system expressions for the secrecy sum rate achieved by the proposed precoder. To optimize the network performance, we proposed an algorithm to determine the optimal regularization parameter in the precoding matrix that maximizes the large-system secrecy sum rate. Furthermore, we proposed the power-reduction strategy, based on which the generalized RCI-PR precoder was designed. The generalized RCI-PR precoder significantly increases the secrecy sum rate at high transmit SNRs when the network load is high.

Appendix A
Proof of Theorem 1

We first derive the large-system approximations of the SINRs for the message $s_{k,j}$ to the intended receiver and the eavesdropper. To commence our analysis, we define

$$\mathbf{A}_j = \left(\rho + \frac{1}{N} \sum_{m=1}^{2} \sum_{l=1}^{K} \mathbf{h}_{l,m,j}^H \mathbf{h}_{l,m,j} \right)^{-1} \tag{18}$$

and

$$\mathbf{A}_{kj} = \left(\rho + \frac{1}{N} \sum_{(l,m) \neq (k,j)} \mathbf{h}_{l,m,j}^H \mathbf{h}_{l,m,j} \right)^{-1}, \tag{19}$$

where $\rho = \alpha/N$. Under the consideration of $P_1 = P_2 = P$, we have $c_j = c_{j'} = c$ in (9) and (10). We rewrite (9) and (10) as

$$\text{SINR}_{k,j} = \frac{c^2 \left| \frac{\mathbf{h}_{k,j,j}\mathbf{A}_{kj}\mathbf{h}_{k,j,j}^H}{N} \right|^2}{\sigma_d^2 + \sum\limits_{(k';j')\neq(k,j)} \frac{c^2 \mathbf{h}_{k,j,j'}\mathbf{A}_{k'j'}\mathbf{h}_{k',j',j}^H \mathbf{h}_{k',j',j'}\mathbf{A}_{k'j'}\mathbf{h}_{k,j,j'}^H}{N}} \tag{20}$$

and

$$\text{SINR}_{\tilde{k},\tilde{j}} = \sum_{(k',j')\neq(k,j)} \frac{c^2 \mathbf{h}_{k',j',j}\mathbf{A}_{kj}\mathbf{h}_{k,j,j}^H \mathbf{h}_{k,j,j}\mathbf{A}_{kj}\mathbf{h}_{k',j',j}^H}{N\sigma_d^2}, \tag{21}$$

respectively, where

$$c^2 = \frac{P}{\sum_{k=1}^K \|\hat{\mathbf{w}}_{k.j}\|^2} = \frac{P}{\sum_{k=1}^K \frac{1}{N^2}\mathbf{h}_{k,j,j}\mathbf{A}_{kj}^2\mathbf{h}_{k,j,j}^H}. \tag{22}$$

Aided by [24], we obtain

$$\frac{1}{N}\mathbf{h}_{k,j,j}\mathbf{A}_{kj}\mathbf{h}_{k,j,j}^H \xrightarrow{a.s} \frac{1}{N}\text{Tr}(\mathbf{A}_j), \tag{23}$$

$$\frac{1}{N^2}\mathbf{h}_{k,j,j}\mathbf{A}_{kj}^2\mathbf{h}_{k,j,j}^H \xrightarrow{a.s} \frac{1}{N}\text{Tr}(\mathbf{A}_j^2), \tag{24}$$

$$\frac{1}{N}\mathbf{h}_{k,j,j'}\mathbf{A}_{k'j'}\mathbf{h}_{k',j',j'}^H \mathbf{h}_{k',j',j'}\mathbf{A}_{k'j'}\mathbf{h}_{k,j,j'}^H \xrightarrow{a.s} \frac{\omega_{jj'}\frac{\text{Tr}(\mathbf{A}_{j'}^2)}{N}}{\left(1+\omega_{jj'}\frac{\text{Tr}(\mathbf{A}_{j'})}{N}\right)^2}, \tag{25}$$

$$\frac{1}{N}\mathbf{h}_{k',j',j}\mathbf{A}_{kj}\mathbf{h}_{k,j,j}^H \mathbf{h}_{k,j,j}\mathbf{A}_{kj}\mathbf{h}_{k',j',j}^H \xrightarrow{a.s} \frac{\omega_{jj'}\frac{\text{Tr}(\mathbf{A}_j^2)}{N}}{\left(1+\omega_{jj'}\frac{\text{Tr}(\mathbf{A}_j)}{N}\right)^2}, \tag{26}$$

where

$$\omega_{jj'} = \begin{cases} 1\,, & \text{if } j = j' \\ \delta\,, & \text{if } j \neq j'. \end{cases} \tag{27}$$

Moreover, we find

$$\frac{\text{Tr}(\mathbf{A}_j)}{N} = \frac{\text{Tr}(\mathbf{A}_{j'})}{N} \xrightarrow{a.s.} \Theta, \tag{28}$$

$$\frac{\text{Tr}(\mathbf{A}_j^2)}{N} = \frac{\text{Tr}(\mathbf{A}_{j'}^2)}{N} \xrightarrow{a.s.} -\frac{\partial\Theta}{\partial\rho}, \tag{29}$$

$$-\frac{\partial\Theta}{\partial\rho} = \frac{\Theta}{\rho + \frac{\mu\delta}{(1+\delta\Theta)^2} + \frac{\mu}{(1+\Theta)^2}}, \tag{30}$$

where Θ is the solution of x to

$$x = \left(\rho + \frac{\mu}{1+x} + \frac{\mu\delta}{1+\delta x}\right)^{-1}. \tag{31}$$

Therefore, we obtain the approximations as follows:

$$\text{SINR}_{k,j}^{\infty} = \frac{\frac{\Theta}{\mu}\left(\rho + \frac{\mu\delta}{(1+\delta\Theta)^2} + \frac{\mu}{(1+\Theta)^2}\right)}{\frac{1}{\gamma} + \frac{\delta}{(1+\delta\Theta)^2} + \frac{1}{(1+\Theta)^2}} \tag{32}$$

and

$$\text{SINR}_{\tilde{k},\tilde{j}}^{\infty} = \gamma\left(\frac{\delta}{(1+\delta\Theta)^2} + \frac{1}{(1+\Theta)^2}\right). \tag{33}$$

Finally, by substituting (32) and (33) into (12), we obtain R_s^{∞} for $\alpha \neq 0$. For $\alpha = 0$, we can derive $R_s^{\infty}(\alpha = 0)$ by computing $\lim_{\alpha\to 0} R_s^{\infty}$. This completes the proof of Theorem 1.

REFERENCES

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

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

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

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

[5] 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.

[6] 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.

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

[8] 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.

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

[10] 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.

[11] 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.

[12] 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.

[13] N. Yang, P. L. Yeoh, M. Elkashlan, R. Schober, and J. Yuan, "MIMO wiretap channels: Secure transmission using transmit antenna selection and receive generalized selection combining," *IEEE Commun. Lett.*, vol. 17, no. 9, pp. 1754–1757, Sept. 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] 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.

[21] 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.

[22] 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.

[23] J. L. Bentley and A. C.-C. Yao, "An almost optimal algorithm for unbounded searching," *Inf. Process. Lett. (Elsevier)*, vol. 5, no. 3, pp. 82–87, June 1976.

[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.