Coordinated Beamforming for Secure Transmission in the Downlink Multicell MIMO Systems

Juan Bai, Tao Dong, Qin Zhang, Shiqiang Wang, and Yanhong Lin

Air Force Engineering University, Xi'an 710051, China

Correspondence should be addressed to Juan Bai; b_juan@163.com

Received 7 November 2019; Revised 28 March 2020; Accepted 30 April 2020; Published 20 May 2020

Academic Editor: Francesco Riganti-Fulginei

Copyright © 2020 Juan Bai et al. This is an open access article distributed under the Creative Commons Attribution License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

In this paper, we consider secure transmission in the downlink of a multicell multiple-input multiple-output (MIMO) system with $M$ cells; each cell consists of an $N$-antenna base station (BS) and $K$ single-antenna users. Coordinated beamforming (CBf) is employed for secrecy enhancement. For CBf, the BSs can jointly design their respective beamformers to control intercell interference and information leakage. Based on regularized channel inversion (RCI) precoding structures, we derive the concise formulas for the signal-to-interference-plus-noise ratio (SINR) for the legitimate users and the colluding malicious users and the achievable secrecy sum rate for the CBf. Furthermore, we obtain a novel closed-form expression of the secrecy sum in the large-system regime where $N$ and $K$ tend to infinity with a fixed ratio $\beta = K/N$. Based on the large-system regime result, the regularization parameter is optimized to maximize the secrecy sum rate. It shows that the optimal regularization parameter decreases with the signal-to-noise ratio (SNR) and stays constant at high SNR if $\beta > (1/M)$. Compared with single-cell processing (SCP) without BS cooperation, simulation results show that the secrecy performance can be significantly enhanced by exploiting CBf. The analytical results are validated with the finite-size system by simulation.

1. Introduction

Multicell multiuser multiple-input and multiple-output (MIMO) has been considered a classical scenario for 5G networks. Due to the unalterable open nature of the wireless medium, wireless multicell multiantenna communications are very susceptible to secrecy outage caused by cochannel interference and intercell information leakage. Thus, security becomes a more crucial issue in the downlink multicell MIMO systems. In addition to the widely used cryptographic approach, information-theoretic security by exploiting the physical layer to achieve perfect secrecy, known as physical layer security, has attracted attention widely [1–3]. The pioneering work made by Wyner introduced the wiretap channel in [4], and secrecy capacity was defined to measure the performance of physical layer security. Then, it was extended to the broadcast channel with a confidential message [5] and the Gaussian wiretap channel [6].

In recent years, wireless communication has grown rapidly due to MIMO techniques. Many studies investigated the physical layer security in MIMO wiretap channels [7–9], where the transmitter, the receiver, and/or the eavesdropper were equipped with multiple antennas. Physical layer security for single-cell multiuser MIMO communications was first studied in the broadcast channel, where a multiantenna BS transmitted confidential messages to multiple users at the same time. The secrecy capacity region for MIMO broadcast channel was characterized in [10, 11]. Secret communication in the single-cell multiuser MIMO systems has been elaborately studied, particularly in the downlink [12–15]. The primary challenge to achieve confidential broadcasting in the single cell system is to deal with the intracell interference. Linear precoding based on regularized channel inversion (RCI) has been proven to be an effective transmission scheme to control intracell interference [16, 17].

Most practical systems have more than one cell, e.g., the 4G and 5G wireless cellular network. When the base station
Mathematical Problems in Engineering

(BS) in each cell uses the same frequency, the main challenge that limits the secure transmission, besides intracell interference and leakage, is the extra intercell interference and leakage; i.e., the intercell interference will cause information leakage to inter-cell malicious users, which cannot be controlled by the BS. It was shown that intercell interference could result in the secrecy outage probability to tend to 1 in high signal-to-noise ratio (SNR) regime [18]. In the existing literature, base station (BS) cooperation has been exploited to suppress the intercell interference to improve the secrecy performance in [19–23]. There are two different forms of BS cooperation, namely, multicell processing (MCP) and coordinated beamforming (CBf). In the MCP, the BSs fully cooperate to share both their channel state information (CSI) and messages to transmit. However, in the CBf, the BSs only share the CSI, but they do not share the messages to transmit. Many studies, such as [19–22], employed the MCP to improve the secrecy rate in multicell MIMO systems. However, the MCP needs high-capacity backhaul links, which are hard for practical settings. However, the CBf is suitable for the networks where such high-capacity backhaul links are not available. Different from the existing studies (see, e.g., [20, 22]), in our work, we exploit the CBf cooperation scheme. The coordinated beamforming was optimized in the relay networks [23, 24]. Although the authors in [19, 25] investigated the secrecy performance for multicell networks with the CBf, the two-cell special scenario was considered and the path loss was not taken into account. Hence, the results presented in [19, 25] are not directly applicable to the multicell system with M cells ($M > 2$) studied in this paper.

In our work, we extend to study the achievable ergodic secrecy sum rate in the downlink multicell MIMO system with $M$ cells, where there are one N-antenna BS and $K$ single-antenna users in each cell. We focus on the CBf scheme, and the BSs partially cooperate based on the CSI of all users. From a worst-case perspective, we assume that the unintended users in the same cell and the cross cells are regarded as malicious users, and they can collude to eavesdrop the transmitted message for the intended user. The main contributions of the work can be summarized as follows:

(i) We investigate the secrecy performance in the downlink multicell ($M > 2$) MIMO system with the CBf cooperation scheme. RCI precoding is considered to trade off the intracell and intercell interference and information leakage. Based on CBf and RCI, we derive a novel closed-form expression for the secrecy sum rate in the large-system regime, where $N$ and $K$ tend to infinity with a fixed ratio $\beta = K/N$. It is sufficiently accurate for the finite-size system and can reduce the computational complexity entailed by the large-scale matrix inversions of RCI.

(ii) We use the closed-form expression of the secrecy sum rate as an objective function to optimize the regularization parameter of the RCI. It shows that the regularization parameter decreases with SNR and stays constant at the high SNR if $N < KM$, i.e., $\beta > 1/M$.

(iii) We also characterize the secrecy sum rate with respect to key parameters $M$, $\beta$, and $\epsilon$. These theoretical results can provide useful insights into practical system design.

The remainder of the paper is organized as follows: Section 2 presents the system model. Sections 3 and 4 describe our main work in detail. Based on RCI precoding, we derive the achievable secrecy sum rate with coordinated beamforming. Simulation and numerical results are presented in Section 5. Section 6 gives concluding remarks.

Notations. $(\cdot)^T$ and $(\cdot)^H$ denote the transpose and conjugate transpose of a vector or a matrix, respectively. $\mathbb{C}^{1 \times N}$ denotes complex-valued $1 \times N$ vector. A capital bold letter $\mathbf{H}$ and lower bold letter $\mathbf{h}$ represent a matrix and a vector, respectively. $\mathbf{x} \sim \mathbb{C}^{1 \times N} \sim \mathcal{CN}(\mathbf{0}, \mathbf{I}_N)$ denotes a complex Gaussian vector with zero mean and covariance $\mathbf{I}$. $\mathbb{E}[\cdot]$ denotes the expectation operation. The trace of a matrix is denoted by $\text{Tr}(\cdot)$, $(\cdot)^{-1}$ denotes the inversion operator, and $\overset{a.s.}{\rightarrow}$ denotes almost sure convergence.

2. System Model

We consider the downlink of a multicell MIMO cellular network with $M$ cells. Each BS is equipped with $N$ antennas and transmits $K$-independent confidential messages to $K$ users at the same time. We denote the small-scale fading channel between the user $k$ in the cell $i$ and the BS in the cell $j$ by row vector $\mathbf{h}_{k,i,j}$. We assume that the antennas at the BSs and the users are sufficiently spaced apart such that all links between the transmitter and receiver antennas are uncorrelated. We assume that the users undergo independent Rayleigh fading, where the coherence time of the channel is larger than the system interval. The Rayleigh fading is one of the most comment and effective statistical channel model for wireless communication. Many studies such as [17, 19–21] (and the references therein) had considered the Rayleigh fading channel. Without loss of generality, the entries of $\mathbf{h}_{k,i,j}$ are modeled as independent and identically distributed (i. i. d.) complex Gaussian random variables with zero mean and unit variance [19, 21], i.e., $\mathbf{h}_{k,i,j} \sim \mathcal{CN}(0, \mathbf{I}_N)$. For simplicity, we denote the typical cell as Cell 1, as shown in Figure 1. Thus, the received signal of the user $k$ in Cell 1 can be written as

$$y_{k,1} = \sqrt{\gamma_{k,1}} \mathbf{h}_{k,1} \mathbf{x}_1 + \sum_{m=2}^{M} \sqrt{\gamma_{k,m}} \mathbf{h}_{k,m} \mathbf{x}_m + n_{k,1},$$

(1)

where $\mathbf{x}_1 \in \mathbb{C}^{N \times 1}$ and $\mathbf{x}_m \in \mathbb{C}^{N \times 1}$ are the transmitted data from BS in Cell 1 and from BS in Cell $m$, respectively. $\gamma_{k,j}$ represents the path loss from the BS in the cell $j$ to the user $k$ in the cell $i$ and $n_{k,j} \sim \mathcal{CN}(0, \sigma_n^2)$ is the noise at the user $k$.

We consider the RCI precoding, which performs better than other linear precoding (i.e., zero-forcing (ZF)) [17]. The transmitted vectors $\mathbf{x}_1$ and $\mathbf{x}_m$ can be obtained at BS in Cell 1 and in Cell $m$ by performing a linear processing on the
vector of confidential messages $s_1 = [s_{1,1}, \ldots, s_{K,1}]^T$ and $s_m = [s_{1,m}, \ldots, s_{K,m}]^T, m = 2, \ldots, M$, respectively. It is assumed that the messages to be transmitted to each user are independent identically distributed, satisfying $E(\|s_{k,m}\|^2) = 1$ and $E(\|s_{k,m}\|^2) = 1, m = 2, \ldots, M$. The same power constraint $E(\|x_k\|^2) = E(\|x_{1,k}\|^2), \ldots, E(\|x_{K,1}\|^2) = P_1, P_2, \ldots, P_M = P$ for each BS is considered.

For conventional downlink cellular networks, single-cell processing (SCP) is employed, i.e., each BS serves its own users with the out-of-cell interference being treated as noise. For the CBf scheme, each BS sends messages to users in its own cell, as done in SCP, but the CSI is shared among BSs. Taking the intercell interference into consideration, the BSs can do a beamformer-lever coordination. Thus, for Cell 1 and Cell $m$, the transmitted data vectors $x_1$ and $x_m$ can be expressed as

$\begin{align*}
x_1 &= c \sum_{k=1}^{K} w_{k,1}s_{k,1}, \\
x_m &= c \sum_{k'=1}^{K} w_{k',m}s_{k',m}
\end{align*}$

where $c$ is a constant chosen to satisfy the per-BS power constraint $P$, which can be expressed by

$\text{c}^2 = \frac{P}{\sum_{k=1}^{K} \|w_{k,m}\|^2}, \quad 1 \leq m \leq M. \quad (4)$

For the CBf, the base stations cooperate with each other and design their transmit beamformers in a coordinated manner. We are interested in RCI precoding, and the beamforming vector $w_{k,1}$ is given by [25]

$w_{k,1} = \left( \sum_{\ell, m \neq (k,1)} h_{\ell,m,1}^H h_{\ell,m,1} + \alpha I_N \right)^{-1} h_{k,1,1}^H, \quad (5)$

where $\alpha$ is the regularized parameter. Define $\xi = (\alpha/N)$ as the normalized regularization parameter, whose function is to achieve a tradeoff between the signal power at the legitimate user and the interference from the other users in the same cell. So, (5) can be rewritten as

$w_{k,1} = \frac{1}{N} \left( \xi I_N + \frac{1}{N} \sum_{\ell, m \neq (k,1)} h_{\ell,m,1}^H h_{\ell,m,1} \right)^{-1} h_{k,1,1}^H. \quad (6)$

Similarly, the beamforming vector in the cell $m$ is given by

$w_{k',m} = \frac{1}{N} \left( \xi I_N + \frac{1}{N} \sum_{\ell, m' \neq (k',m)} h_{\ell,m',m}^H h_{\ell,m',m} \right)^{-1} h_{k',m,m}. \quad (7)$

### 3. Achievable Secrecy Sum Rate with Coordination Beamforming

In this section, we derive the achievable secrecy sum rate by using the RCI precoder with CBf scheme in the downlink multicell MIMO systems.

#### 3.1. SINR at a Legitimate User

We consider a legitimate user $k$ in the reference Cell 1. Due to RCI precoding, the user $k$ receives intracell interference caused by the other messages transmitted by the BS in Cell 1 and intercell interference caused by the messages transmitted by the BS in other Cell $m$. The SINR of the user $k$ in Cell 1 can be expressed as

$\text{SINR}_{k,1} = \frac{c^2 y_{k,1,1} |h_{k,1,1} w_{k,1}|^2}{c^2 \sum_{(k',j) \neq (k,1)} |y_{k',j}|^2 |h_{k',j} w_{k',j}|^2 + \sigma^2}
\begin{align*}
&= \frac{c^2 y_{k,1,1} |h_{k,1,1} w_{k,1}|^2}{c^2 \sum_{k'=1, k' \neq k} y_{k,1,1} |h_{k,1,1} w_{k',1}|^2 + \sigma^2}
&\quad + \frac{c^2 \sum_{m=2}^{M} \sum_{k'=1}^{K} y_{k,1,m} |h_{k,1,m} w_{k',m}|^2 + \sigma^2}{\text{intracell interference}}
&\quad + \frac{c^2 \sum_{m=2}^{M} \sum_{k'=1}^{K} y_{k,1,m} |h_{k,1,m} w_{k',m}|^2 + \sigma^2}{\text{cell interference}}
\end{align*}
\quad (8)$
For brevity in the following presentation, we denote
\[
\mathbf{T}_1 = \left( \mathbf{I}_N + \frac{1}{N} \sum_{m=1}^{M} \sum_{k=1}^{K} h_{\ell,m}^{H} h_{\ell,m} \right)^{-1}, \tag{9}
\]
\[
\mathbf{T}_{k,1} = \left( \mathbf{I}_N + \frac{1}{N} \sum_{(\ell,m) \neq (k,1)} h_{\ell,m}^{H} h_{\ell,m} \right)^{-1}, \tag{10}
\]
\[
\mathbf{T}_{k,m_{1},m_{2}} = \left( \mathbf{I}_N + \frac{1}{N} \sum_{(\ell,m) \neq (k,1)} h_{\ell,m}^{H} h_{\ell,m} \right)^{-1}. \tag{11}
\]

By plugging the beamforming vectors \( \mathbf{w}_{k,1} \) and \( \mathbf{w}_{k',m} \) in (6) and (7) into (8), we can write the numerator of the SINR, excluding \( c^2 Y_{k,1} \), as
\[
|\mathbf{h}_{k,1}^{H} \mathbf{w}_{k,1}|^2 = \frac{1}{\mathbf{h}_{k,1}^{H} \mathbf{T}_{k,1} \mathbf{h}_{k,1}} = |A_{k,1}|^2. \tag{12}
\]
In denominator, the terms \( |\mathbf{h}_{k,1}^{H} \mathbf{w}_{k',1}|^2 \) and \( |\mathbf{h}_{k,2}^{H} \mathbf{w}_{k',2}|^2 \) can be expanded as follows:
\[
|\mathbf{h}_{k,1}^{H} \mathbf{w}_{k',1}|^2 = \frac{1}{N^2} \mathbf{h}_{k,1}^{H} \mathbf{T}_{k',1} \mathbf{h}_{k,1} = B_{k',1}, \tag{13}
\]
\[
|\mathbf{h}_{k,2}^{H} \mathbf{w}_{k',2}|^2 = \frac{1}{N^2} \mathbf{h}_{k,2}^{H} \mathbf{T}_{k',2} \mathbf{h}_{k,2} = B_{k',2}. \tag{14}
\]
By applying the matrix inversion lemma [22], we know that
\[
(\mathbf{H}^{H} \mathbf{H} + \alpha \mathbf{I})^{-1} = (\mathbf{H}^{H} \mathbf{k}_{k,1} + \alpha \mathbf{I})^{-1} \tag{15}
\]
where \( \mathbf{H}_{k,1} \) is \( \mathbf{H} \) with the \( k \)th row removed.

Thus, we can rewrite \( B_{k',1} \) and \( B_{k',m} \) as follows:
\[
B_{k',1} = \frac{1}{N} \frac{1}{(1 + (1/N) \mathbf{h}_{k,m}^{H} \mathbf{T}_{k',1} \mathbf{h}_{k,m})^2}, \tag{16}
\]
\[
B_{k',m} = \frac{1}{N} \frac{1}{(1 + (1/N) \mathbf{h}_{k,m}^{H} \mathbf{T}_{k',1} \mathbf{h}_{k,m})^2}. \tag{17}
\]

Thus, the SINR \( k \) can be rewritten as
\[
\text{SINR}_{k} = c^2 Y_{k,1} |A_{k,1}|^2 + \frac{c^2 \sum_{s=1}^{K} Y_{k,1,s} B_{k',s} + \sigma^2}{\sigma^2}. \tag{18}
\]

3.2. SINR at the Eavesdropper. We assume that for each legitimate user, its confidential message can be eavesdropped by other users in the same cell and the users in the other cells, i.e., the remaining \( MK - 1 \) users act maliciously as eavesdroppers. From a worst-case perspective, we take into account collusion amongst the malicious users, i.e., the cooperative eavesdroppers are able to cancel the interference, leaving only the signal for the intended user. The consideration of the worst-case scenario is motivated by the fact that the malicious behaviors of the potential eavesdropper in the network are not fully controllable or predictable at the BSs. The consideration of the worst-case scenario is widely adopted in broadcasting networks (e.g., [17, 19, 20, 23]). 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 the BSs are required to securely transmit messages to each user but do not control the user behaviors after receiving messages. Thus, the SINR for the colluding eavesdropper can be expressed as
\[
\text{SINR}_{\varepsilon} = \frac{c^2 \sum_{s=1}^{K} Y_{k,1,s} B_{k',1} + \sigma^2 \sum_{m=2}^{M} \sum_{s=1}^{K} Y_{k,1,m} B_{k',m}}{\sigma^2}. \tag{19}
\]

3.3. Ergodic Secrecy Rate. The ergodic secrecy rate for the typical user \( k \) in the Cell 1 can be obtained as
where $E(\cdot)$ denotes the mean operator.

In order to obtain the ergodic secrecy sum rate, we need to know the distributions of SINR$_{k,1}$ and SINR$_e$, which are complicated and hard to derive [17]. We instead consider deriving the nonrandom equivalents for SINR$_{k,1}$ and SINR$_e$ in the large system limit. The number of antennas at the BS and the number of users in each cell $K$ both grow large together, while their ratio $\beta = (K/N)$ (also known as cell load) remains a constant. So we can obtain the closed-form expression of the secrecy sum rate in a large-system limit.

4. Large-System Analysis

In this section, we first derive the expressions for the SINRs for the legitimate user and the colluding malicious users with CBf cooperation scheme. The expression can reduce the complexity of system design and analysis incurred by Monte Carlo simulation. Many studies, e.g., [13, 14, 17], have exploited the approach and shown that the large-system result can provide useful insights into the secrecy performance for the finite-size system.

We obtain the following propositions.

**Proposition 1.** Let $\rho = (P/\sigma^2)$ and $g(M\beta, \xi)$ be the solution of $g(M\beta, \xi) = (\xi + (M\beta/(1 + g(M\beta, \xi)))^{-1}$. In the large-system limit, the SINR$_{k,1}$ with CBf given in (18) converges in probability to a deterministic quantity given by

$$\text{SINR}_{k,1}^\infty = \frac{M\rho g_{k,1,1} g(M\beta, \xi) K (\xi/M\beta)(1 + g(M\beta, \xi)^2 + 1}{\rho K (K - 1) g_{k,1,1} + \rho K \sum_{m=2}^M \beta_{k,1,m} + K (1 + g(M\beta, \xi)^2)^2}$$

$$\text{SINR}_e^\infty = \frac{\rho (K - 1) g_{k,1,1} + \rho K \sum_{m=2}^M \beta_{k,1,m} + K (1 + g(M\beta, \xi)^2)}{K (1 + g(M\beta, \xi)^2)^2} \tag{21}$$

**Proof.** See the appendix.

By substituting (21) and (22) into (20), it is easy to obtain the following proposition.

**Proposition 2.** Based on RCI precoding, the secrecy sum rate with CBf can be obtained in the large-system regime as

$$R_s^\infty = \sum_{k=1}^K R_{k,1}^\infty$$

$$= MK \left[ \log_2 \left( 1 + \left( M\rho g_{k,1,1} g(M\beta, \xi) K \left( \frac{\xi}{M\beta}(1 + g(M\beta, \xi)^2 + 1) \right)(\rho K (K - 1) g_{k,1,1} + \rho K \sum_{m=2}^M \beta_{k,1,m} + K (1 + g(M\beta, \xi)^2)^2) \right) \right] \right].$$

$$\xi^{\text{opt}} = \arg \max_\xi R_s^\infty \quad \text{s.t.} \quad 0 < \xi < 1$$

$$= \frac{\partial R_s^\infty}{\partial \xi} \tag{24}$$

The value of $\xi$ has a significant impact on the secrecy sum rate in the large-system regime. To obtain the optimal regularization parameter $\xi$ that maximizes the secrecy sum rate, we can take the derivative of the asymptotic $R_s^\infty$ in (23) with respect to $\xi$ to zero, i.e.,

$$\xi^{\text{opt}} = \arg \max_\xi R_s^\infty \quad \text{s.t.} \quad 0 < \xi < 1$$

$$= \frac{\partial R_s^\infty}{\partial \xi} \tag{24}$$

$$= \frac{\rho K (K - 1) g_{k,1,1} + \rho K \sum_{m=2}^M \beta_{k,1,m} + K (1 + g(M\beta, \xi)^2)}{K (1 + g(M\beta, \xi)^2)^2} \tag{26}$$

**Remark 1.** Proposition 2 provides the novel closed-form expression of the secrecy sum rate in the large-system limit with CBf cooperation scheme. The expression can reduce the complexity of system design and analysis incurred by Monte Carlo simulation. We can evaluate and optimize the

**Remark 2.** The secrecy sum rate contains the parameter, which characterize the impact of the path loss (or
equivalently, the cross-cell interference level) on the secrecy performance.

5. Numerical Results

In this section, we evaluate the secrecy performance of the considered multicell MIMO system with CBf. In order to gain some insight for system analysis, we only consider the small-scale fading channel. The simulation results for the ergodic secrecy rate of the user $k$ in Cell 1 in (22) are averaged over 3,000 random channel realizations.

Figures 2 and 3 illustrate the per-antenna secrecy sum rate for different values of the regularization parameter $\xi$ and SNR $\rho$ and examine the impact of $\xi$ on the large-system secrecy sum rate. $M = 4$, $N = 100$, $K = 25$ and $M = 4$, $N = 100$, $K = 30$ are considered, respectively. It is obvious there exists an optimal value of the regularization parameter $\xi$ that maximizes the secrecy sum rate. $\xi^{\text{opt}}$ can be numerically obtained from the plots. We find that $\xi^{\text{opt}}$ decreases with $\rho$. In particular, $\xi^{\text{opt}}$ converges to a constant value at a high transmit SNR when $N < KM$, i.e., the cell load $\beta > 1/M$, as shown in Figure 3.

Figure 4 shows the per-antenna secrecy sum rate versus the transmit SNR $\rho$ for the CBf with $M = 5$ and $N = 100$. Different number of users $K = 10, 20, 25, 30$, i.e., the cell load $\beta = 0.1, 0.2, 0.25, 0.3$, are considered. For SCP without cooperation, the intercell interference and information leakage cannot be suppressed effectively by the BS, which results in nonpositive secrecy sum rate. By exploiting the CBf, a significant performance gain in the secrecy sum rate can be obtained with a beamformer-level coordination. It shows that the secrecy sum rate monotonically increases with $\rho$ if $\beta \leq (1/M)$ but becomes zero at high $\rho$ if $\beta < (1/M)$. The results are reasonable. When $\beta < 1/5$, i.e., $N < MK$, there is not sufficient spacial degrees of freedom to cancel the intercell interference with CBf. This implies that more antennas are required for the BS if $M$ is large. Our large-system analytical results are proved to be accurate at lower values of $\rho$ by simulation. The loss of accuracy at high SNR mainly comes from the limitations of the large-system assumption in the finite-size systems.

Figure 5 further compares the secrecy sum rate for different values of $N$ and $K$. It shows that the large-system results are pretty accurate even at lower values of $N$ and $K$. This means that the large-system result is sufficiently accurate for finite size systems, which can reduce the complexity of system design and analysis. In addition, the secrecy performance of RCI precoding is better than that of ZF precoding, especially at lower SNR, but the secrecy performance of ZF approached that of RCI at an asymptotically high SNR.
value of $K$ for $M = 6$ is smaller than that for $M = 3$. Furthermore, the secrecy sum rate decreases fast for higher $\rho$ and the power allocation becomes an important factor affecting the secrecy sum rate for higher SNR.

6. Conclusion

In this paper, we considered a multicell MIMO system with CBf for secure downlink transmission. For CBf, the BSs can jointly design their beamforming matrix to control intercell interference and information leakage. Based on RCI precoding, we derived the ergodic secrecy sum rate and obtained its closed-form expression in the large-system regime. Based on the results, we optimized the regularization parameter that maximized the secrecy sum rate. The analytical expression allowed us to gain significant insight into the impact of the system parameters on performance. The analysis in this paper focused on the perfect CSI. Generalizing the results to the case of imperfect CSI is part of our going research effort.

Appendix

Proof of Proposition 1

Proof. For the clarity in presentation, we first list two important results in a random matrix to derive Proposition 1. □

Lemma A.1 (see [26]). Let $A$ be a deterministic $N \times N$ complex matrix with uniformly bounded spectral radius for all $N$. Let $q = (1/\sqrt{N})[q_1,q_2,\ldots,q_N]$, where the $q_i$s are i. i. d. with zero mean and unit variance. Let $r$ be a similar vector independent of $q$. Then, we have

$$qAq^H \rightarrow \frac{1}{N} \text{Tr}(A), \quad (A.1)$$

$$qAr^H \rightarrow \frac{1}{N} \cdot 0. \quad (A.2)$$

Theorem A.1 (see [26]). Let $H$ be a $[cN] \times [dN]$ random matrix with independent entries $[H]_{ij}$ which are zero mean and variance $E[[H]_{ij}]^2 = N^{-1}P_{ij}$, such that $P_{ij}$ are uniformly bounded from above. For each $N$, let $\gamma_N(x,y)\colon [0,c] \times [0,d] \rightarrow \mathbb{R}$, be the variance profile function given by

$$\gamma_N(x,y) = P_{ij}, \quad \frac{i}{N} \leq x \leq \frac{i+1}{N}, \quad \frac{j}{N} \leq y \leq \frac{j+1}{N}. \quad (A.4)$$

Suppose that $\gamma_N(x,y)$ converges uniformly to a limiting bounded function $\nu(x,y)$. Then, for each $a,b \in [0,c)$, $a < b$, and $z \in \mathbb{C}^*$,

$$\frac{1}{N} \sum_{i \leq |a|N} (HH^H - zI)^{-1} \rightarrow \int_a^b u(x,z)dz, \quad (A.5)$$

where $u(x,z)$ satisfies
Moreover, almost surely, the empirical eigenvalue distribution of $H|\{H\}^T|$ converges weakly to a limiting distribution whose Stieltjes transform is given by

$$
\ell(\xi) = \frac{1}{N} Tr(T_k) \xrightarrow{a.s.} 0.
$$

By applying rank-1 perturbation lemma [27], we have

$$
\max_{k \leq K} |A_{k,1} - \frac{1}{N} Tr(T_k)| \xrightarrow{a.s.} 0.
$$

Let $H_1 = [h_{1,1,1}, h_{2,1,1}, \ldots, h_{K,1,1,1}, h_{1,2,1,1}, \ldots, h_{K,2,1,1}, \ldots, h_{1,M,1,1}, \ldots, h_{K,M,1,1}]^T$, then, $T_1 = (c I_N + (1/N) \sum_{\ell=1}^K h_{\ell,m}^H h_{\ell,m})^{-1} = (c I_N + (1/N) H H^T)^{-1}$, and we have

$$
\frac{1}{N} Tr(T_1) = \int_0^1 u(x, -\xi) dx,
$$

where

$$
u(x, -\xi) = \frac{1}{\xi + (M\beta/(1 + u(-\xi)))}.
$$

Let $g(\beta, M\beta)$ be the positive solution of $g(\beta, M\beta) = (\xi + (M\beta/g(\beta, M\beta)))^{-1}$, and we have [17]

$$
g(M\beta, \xi) = \left(\sqrt{(\xi + M\beta - 1)^2 + 4\xi - (\xi + M\beta - 1)^2}\right) / 2\xi.
$$

Similarly, by applying rank-1 perturbation lemma twice, we can obtain

$$
\max_{k \leq K} \left| B_{k,1} - \frac{1}{N} Tr(T_2) \right| \xrightarrow{a.s.} 0.
$$

Following Lemma A.1, $A_{k,1}$ in (12) converges (almost surely) to

$$
\max_{k \leq K} \left| A_{k,1} - \frac{1}{N} Tr(T_k) \right| \xrightarrow{a.s.} 0.
$$

By making the derivative with respect to $\xi$ at both sides of (A.11), we can obtain

$$
- \frac{\partial g(M\beta, \xi)}{\partial \xi} = g'(M\beta, \xi) = \frac{g(M\beta, \xi)}{\xi + (M\beta(1 + g(M\beta, \xi))^2)}.
$$

To sum up, we can express the limiting SINR for legitimate user as

$$
\text{SINR}^{\infty}_{\delta} = \frac{\left( 1 + g(M\beta, \xi)^2 \right) / \beta \rho \rho' (M\beta, \xi)}{(P/\beta \rho (M\beta, \xi)) \left( (1 + g(M\beta, \xi)^2) + (K \sum_{m=1}^M y_{k,m}^T y_{k,m} + K(1 + g(M\beta, \xi))^2) \right) + g'(M\beta, \xi) + \sigma^2}
$$

The limiting SINR for the colluding eavesdroppers is given by

$$
\text{SINR}^{\infty}_{\delta} = \rho (K - 1) y_{k,1} + \rho K \sum_{m=2}^M y_{k,m} + K(1 + g(M\beta, \xi))^2.
$$
Data Availability
The simulation code data used to support the findings of this study are available from the corresponding author (Juan Bai, e-mail: b_juan@163.com) upon request.

Conflicts of Interest
The authors declare that they have no conflicts of interest.

Acknowledgments
This work was supported by the National Natural Science Foundation of China under Grant 61601503 and 61601499.

References