IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received August 1, 2016, accepted August 22, 2016, date of publication September 5, 2016, date of current version October 6, 2016.

Digital Object Identifier 10.1109/ACCESS.2016.2605918

Adaptive Base Station Cooperation for Physical Layer Security in Two-Cell Wireless Networks

LIN HU[1], HONG WEN[1], BIN WU[2], (Member, IEEE), JIE TANG[1], AND FEI PAN[1]

[1]National Key Laboratory of Science and Technology on Communications, University of Electronic Science and Technology of China, Chengdu 611731, China
[2]School of Computer Science and Technology, Tianjin University, Tianjin 300072, China

Corresponding author: H. Wen (sunlike@uestc.edu.cn)

This work was supported in part by the 863 High Technology Plan under Grant 2015AA01A707 and in part by NSFC under Grant 61271172, Grant 61372085, and Grant 61572114.

ABSTRACT We study physical layer security in two-cell wireless networks in which a base station (Alice) intends to send a confidential message to a legitimate user (Bob) with the help of a cooperative base station (Charlie), in the presence of an eavesdropper (Eve). Adaptive base station cooperation is explored to secure communication between Alice and Bob, and ensure the desired quality of service (QoS) at Charlie's user. In particular, we consider two different scenarios where the channel state information of Eve is perfectly and statistically known, respectively. In either scenario, we provide a cooperative transmission scheme for secrecy rate maximization, subject to both security and QoS constraints. Unlike the conventional cooperative security with a fixed transmission scheme, we propose a mechanism for transmit strategy adaptation with security protection. Specifically, the cooperative transmission is replaced by a cooperative jamming scheme if either security or QoS constraint is not satisfied. Our design enables adaptive secure transmission, and thus is flexible and environment-adaptive. Moreover, numerical results confirm that our scheme is efficient in power resource utilization.

INDEX TERMS Physical layer security, adaptive secure transmission, cooperative jamming, security protection, secrecy rate maximization.

I. INTRODUCTION

Confidential data traffic (e.g., financial data, bank account, and credit card information) grows rapidly in recent years, fuelled by the popularity of wireless devices and the ever-increasing demands on sensitive data-centric applications. However, wireless communication systems are particularly susceptible to security attacks (e.g., malicious interception and eavesdropping) due to the broadcasting nature of wireless medium. Thus guarantying confidentiality is one of the top issues in future network designs. Specifically, high data rate, low latency [1], and unrivalled security are necessary requirements in future wireless communication systems [2]. Traditionally, security issues are addressed by cryptographic encryption and decryption techniques implemented in upper layers of the network protocol stacks, which have inherent difficulties and vulnerabilities in secret key distribution and high computational complexity [3], [4]. By exploring only physical properties of wireless channel, physical layer security [5]–[7] can support confidential transmission, and is identified as an important complement to cryptographic techniques.

In terms of information-theoretic secrecy, the notion of perfect secrecy was first studied by Shannon [8]. Subsequently, a pioneering work by Wyner [9] introduced the wiretap channel model. It demonstrates that, when the main channel (between source and destination) is better than the eavesdropper channel (between source and eavesdropper), both reliability (i.e., low error probability at the destination) and security (i.e., substantial confusion at the eavesdropper) can be achieved simultaneously. This result was further extended to the Gaussian degraded wiretap channel by Cheong et al. in [10], and to the general non-degraded wiretap channel by Csiszár et al. in [11]. Based on those works, physical layer security has been intensively studied to enlarge the signal quality difference at the destination and the eavesdropper, with focus on transmit design and resource allocation [12]–[14].

A. RELATED WORKS

There are a lot of works on secrecy-enhancing transmit designs, such as secrecy beamforming [15]–[24], cooperative secure transmission [25]–[40], mode selection [41],

and secure broadcasting [42]. Those investigations are based on either different secrecy criteria, or different assumptions on the channel knowledge, or different network topologies. The essential of physical layer security is to maximize the secrecy rate, which is defined as the nonnegative rate difference between the main channel and the eavesdropper channel [43], [44].

The secrecy rate maximization (SRM) problem in multiple-input single-output (MISO) and multiple-input multiple-output (MIMO) systems are investigated in [15] and [16], respectively, and the optimal transmit schemes are provided based on the assumption of perfect channel state information (CSI) of eavesdropper. This assumption is reasonable if the eavesdropper is part of the communication systems. For example, in the digital TV broadcasting systems, we can obtain CSI of the unpaid user who tries to receive the authorized services. In addition, the work [45] investigates a method to detect eavesdropper from local oscillator power that is inadvertently leaked from radio-frequency front end.

However, if the eavesdropper's CSI is unknown, it is impossible to support a steady secrecy rate over all realizations of fading channels. In this context, the transmission of artificial noise (AN) on top of the information-bearing signal is proposed to enhance secrecy [17]. Based on AN generation, secure transmission is investigated for both fast and slow fading channels [18]–[21]. If channels are fast varying, the work [19] verifies that there is a need to inject AN into the main channel. However, the result in [21] shows that the optimal AN is orthogonal to the information-bearing signal for slow fading channels.

For cooperative networks, the state-of-the-art in physical layer security are summarized in [25]–[27]. In particular, secure transmission schemes are designed for different cooperative protocols, e.g., amplify-and-forward (AF) in [29] and [30], decode-and-forward (DF) in [31]–[33], and cooperative jamming (CJ) in [34]–[38]. In the CJ scheme, rather than forwarding confidential information, relays emit AN to interfere with eavesdropper.

In this paper, we study the physical layer security in two-cell wireless networks, where a base station (Alice) intends to transmit a confidential message to a legitimate user (Bob), in the presence of an eavesdropper (Eve). The cooperative base station (Charlie) emits AN to deteriorate the eavesdropper channel, and provides service to its intended user simultaneously. Adaptive base station cooperation is explored to secure communication between Alice and Bob, while ensuring the desired quality of service (QoS) at Charlie's user. Our work is significantly different from the existing cooperative security [28]–[40] in the following aspects:

1) We adopt the secrecy rate as the performance metric under perfect CSI of Eve. Nevertheless, when only the statistical CSI of Eve is available, the outage constrained secrecy rate is considered as the performance measure, which is defined as the secrecy rate subject to a maximum allowable secrecy outage probability. Specifically, we utilize the outage formulation developed in [20] instead of [46].
2) In addition to emitting AN for secrecy enhancing, the cooperative base station also provides service to its own user and guarantee the QoS, which is not considered in the existing cooperative security schemes. Moreover, the aforementioned works do not take into account the security performance guarantee, which is denoted by a minimum secrecy rate threshold.
3) Unlike the conventional cooperative security with fixed protocols (e.g., AF, DF, and CJ), we propose a mechanism for transmit strategy adaptation. Although transmit strategy adjustment between cooperative relaying and jamming is studied in [33], the authors assume that each node is equipped with a single antenna, and the ergodic secrecy rate is adopted as the secrecy metric. However, we concentrate on multi-antenna secure transmit design, and the proposed adaptive secure transmission can be applied under both perfect and statistical CSI of Eve.

B. OUR CONTRIBUTIONS

The main contributions of this paper are summarized as follows:

1) We present a framework of physical layer security in two-cell downlink networks through adaptive base station cooperation. In particular, we propose a mechanism for transmit strategy adaptation with security protection. Numerical results show that the proposed scheme is flexible and efficient in resource utilization.
2) We propose a cooperative transmit design for an SRM problem under perfect CSI of Eve. Since the problem is difficult to solve directly, we divide the solution process into two steps: we first characterize the Pareto boundary of Charlie's power gain region as in [47]; and then find an explicit solution based on Pareto boundary. As a distinct feature of our approach, it can guarantee security performance by automatically adjust the transmit strategy. Specifically, the proposed transmit scheme is replace by a CJ scheme if either of the following two situations are encountered: 1) the secrecy rate is less than a minimum threshold; or 2) the signal-to-interference-plus-noise ratio (SINR) requirement at Charlie's user is not fulfilled. Moreover, we propose a modified CJ scheme to further improve security at the physical layer.
3) For the statistical CSI case, we propose an AN assisted transmission design for SRM, subject to a constraint on secrecy outage probability. We again take two steps to solve this complex problem: we first transfer it into a power allocation problem; and then derive a closed-form solution to the new problem. Transmission strategy adaptation is also enabled (with both security and performance guarantee), which is achieved by invoking the CJ scheme in [38] if the outage constrained secrecy rate is less than a minimum thresh-

old, or the SINR requirement at Charlie's user is not satisfied.

C. PAPER ORGANIZATION AND NOTATIONS

The rest of this paper is organized as follows. Section II describes the system model. The adaptive base station cooperation for physical layer security under perfect and statistical CSI of Eve are respectively presented in Section III and IV. We conclude the paper in Section V.

Notations: The uppercase and lowercase boldface letters denote matrices and column vectors, respectively, and the standard lowercase letters denote scalars. $\mathbf{I}$ is the identity matrix with appropriate size. The superscript $(\cdot)^H$ and $(\cdot)^{-1}$ denote the Hermitian (conjugate transpose) and the inverse of a matrix, respectively. $\mathbf{A} \succeq \mathbf{0}$ ($\mathbf{A} \succ \mathbf{0}$) means that $\mathbf{A}$ is positive semidefinite (positive definite). $\Pi_{\mathbf{X}}^{\perp}$ is the projection onto the orthogonal complement of the column space of $\mathbf{X}$, i.e., $\Pi_{\mathbf{X}}^{\perp} = \mathbf{I} - \Pi_{\mathbf{X}}$, where $\Pi_{\mathbf{X}} = \mathbf{X}\left(\mathbf{X}^H\mathbf{X}\right)^{-1}\mathbf{X}^H$. null($\mathbf{X}$) is the null space of $\mathbf{X}$. The largest eigenvalue of $\mathbf{Z}$ is specified as $\mu_{\max}(\mathbf{Z})$, and the corresponding eigenvector is specified as $\mathbf{x}_{\max}(\mathbf{Z})$. $\mathbb{C}^n$ is the n-dimensional complex space. $|\cdot|$ and $\|\cdot\|$ denote absolute value and ℓ_2 norm, respectively. The probability measure is given by $\Pr(\cdot)$. $\mathcal{CN}(\boldsymbol{\mu}, \mathbf{Q})$, $\Gamma(k, \mu)$, and $\mathrm{Exp}(\lambda)$ represent circularly symmetric complex Gaussian distribution with mean $\boldsymbol{\mu}$ and covariance $\mathbf{Q}$, gamma distribution with shape k and scale μ, and exponential distribution with rate parameter λ, respectively. $\Gamma(x)$ is the gamma function , and $[x]^+$ is the max-function $\max(x, 0)$ with $x \in \mathbb{R}$. The symbols $\triangleq$, $\Longrightarrow$, and $\Longleftrightarrow$ denote "defined as", "implies", and the equivalence relation, respectively.

II. SYSTEM MODEL

As shown in Fig. 1, we consider a downlink transmission in two-cell wireless networks. In cell 1, Alice intends to send a confidential message to Bob, in the presence of an eavesdropper, who tries to decode this message. Specifically, we focus on the eavesdropper who complies with the protocols and does not attempt to tamper with the confidential message. In cell 2, Charlie acts as a cooperative base station that assists in enhancing secure transmission from Alice to Bob, while also providing service to its intended user Rx2.

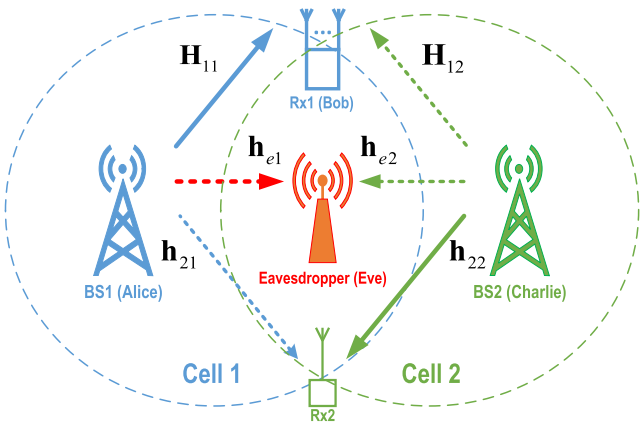


FIGURE 1. A model of two-cell downlink networks with physical layer security.

A. BASE STATION COOPERATION

In order to guarantee confidentiality of information transfer from Alice to Bob, and ensure that Charlie provides the desired QoS to Rx2, base station cooperation [48] is taken into account such that Alice and Charlie can share control signals and CSI to cooperatively provide services to users. In addition, we assume that Alice and Charlie cannot exchange user messages. In practice, this setting is more appropriate when the infrastructure of high-capacity backhaul links are not readily available.

B. CHANNEL MODEL

We consider a non-line-of-sight rich scattering environment, and assume the messages intended for Bob and Rx2 are transmitted over the slow fading channels. The coherence time is assumed to be long enough to support the wiretap code [9]. It is also assumed that Alice, Bob, and Charlie are equipped with N_a, N_b, and N_c antennas, respectively, whereas Eve and Rx2 are both equipped with a single antenna. The channels from Alice to Bob, Eve, and Rx2 are denoted by $\mathbf{H}_{11} \in \mathbb{C}^{N_b \times N_a}$, $\mathbf{h}_{e1} \in \mathbb{C}^{N_a}$, and $\mathbf{h}_{21} \in \mathbb{C}^{N_a}$, respectively, and those from Charlie to Bob, Eve, and Rx2 are denoted by $\mathbf{H}_{12} \in \mathbb{C}^{N_b \times N_c}$, $\mathbf{h}_{e2} \in \mathbb{C}^{N_c}$, and $\mathbf{h}_{22} \in \mathbb{C}^{N_c}$, respectively. Note that $\mathbf{H}_{11}$ and $\mathbf{h}_{e1}$ are also referred to as the main channel and the eavesdropper channel, respectively.

Besides, we assume that Bob can estimate $\mathbf{H}_{11}$ and $\mathbf{H}_{12}$ accurately, and feeds them back to Alice. It is also assumed that Rx2 can estimate $\mathbf{h}_{21}$ and $\mathbf{h}_{22}$ accurately, and feeds them back to Charlie. In addition, the time used for channel estimation and CSI feedback is assumed to be negligible. Then, Alice and Charlie can share these channel knowledge through base station cooperation. Specifically, we consider two different assumptions on the CSI of Eve. In Section III, we assume that the CSI of $\mathbf{h}_{e1}$ and $\mathbf{h}_{e2}$ are available at Alice and Charlie. In Section IV, we relax this strong assumption by assuming the statistical information of $\mathbf{h}_{e1}$ and $\mathbf{h}_{e2}$.

Based on the above notations and assumptions, the received signals at Bob, Eve, and Rx2 can be expressed as

$$\mathbf{y}_1 = \mathbf{H}_{11}\mathbf{s}_1 + \mathbf{H}_{12}\mathbf{s}_2 + \mathbf{n}_1, \tag{1}$$

$$y_e = \mathbf{h}_{e1}^H\mathbf{s}_1 + \mathbf{h}_{e2}^H\mathbf{s}_2 + n_e, \tag{2}$$

$$y_2 = \mathbf{h}_{21}^H\mathbf{s}_1 + \mathbf{h}_{22}^H\mathbf{s}_2 + n_2, \tag{3}$$

where $\mathbf{s}_1 \in \mathbb{C}^{N_a}$ and $\mathbf{s}_2 \in \mathbb{C}^{N_c}$ denote signals transmitted by Alice and Charlie, respectively; $\mathbf{n}_1 \sim \mathcal{CN}(\mathbf{0}, \mathbf{I}_{N_b})$, n_e, $n_2 \sim \mathcal{CN}(0, 1)$ are mutually independent, and denote the additive complex white Gaussian noise (AWGN) at Bob, Eve and Rx2, respectively. In particular, all channels are assumed to be independent, and all entries of each channel matrix are independent and identically distributed (i.i.d.) complex Gaussian variables with zero mean and unit variance.

C. SECURE TRANSMISSION AND PERFORMANCE METRICS

Utilizing Wyner's wiretap code, the confidential information transmitted by Alice is encoded before transmission. We denote the rate of the transmitted codeword as R_b, and the rate of the secret message as R_s. Then, the rate of redundant information $R_e \triangleq R_b - R_s$ is deliberately added to provide secrecy against eavesdropping. Let C_b and C_e denote the main channel capacity and eavesdropper channel capacity, respectively. For the main channel, the secret message transmitted by Alice can be correctly recovered by Bob if $R_b \leq C_b$, or capacity outage occurs otherwise. Based on base station cooperation, C_b can be obtained with the channel knowledge at Alice. Accordingly, Alice can choose R_b such that $R_b = C_b$, and thus eliminate capacity outage at Bob. In addition, for the eavesdropper channel, the confidential information can be protected against eavesdropping if $C_e \leq R_e$. Otherwise, perfect secrecy cannot be guaranteed and secrecy outage occurs [20].

Specifically, when the CSI of $\mathbf{h}_{e1}$ and $\mathbf{h}_{e2}$ are available (which is assumed in Section III), Alice cooperates with Charlie, and then determines a maximum secrecy rate R_s such that $C_e = C_b - R_s$. In this case, the secrecy outage does not happen. Thus, we characterize the secrecy performance by the achievable secrecy rate in Section III.

However, when only the statistical CSI of Eve is available (which is assumed in Section IV), the eavesdropper channel capacity C_e becomes a random variable, and thus secrecy outage cannot be prevented with absolute certainty. In this case, we adopt the outage constrained secrecy rate as the performance measure.

Furthermore, to compare efficiency in power utilization between the proposed adaptive transmission scheme and the CJ scheme, we utilize the system service rate (i.e., the sum of the secrecy rate and the transmission rate of Charlie) as the performance measure.

D. COOPERATIVE SECURITY AT THE PHYSICAL LAYER

In the system model, the inter-cell interference due to full frequency reuse pattern has a great impact on downlink transmission. On one hand, the signal transmitted by Charlie deteriorates the secret information reception at Eve, and thus degrade the performance of the eavesdropper channel; on the other, Alice and Charlie interfere with each other during transmission, reducing useful signal quality at both Bob and Rx2. However, the harmful interference can be exploited for physical layer security as an efficient tool of anti-eavesdropping. Specifically, through adaptive base station cooperation, signals transmitted by Alice and Charlie can be carefully designed, such that the interference is constructed in a positive way.

In the following two sections, we provide a comprehensive analysis of physical layer security in two-cell wireless networks. Transmit strategies are designed to maximize the secrecy rate under perfect and statistical CSI of Eve. Taking security and performance guarantee into account, we provide a new mechanism for dynamic transmit strategy adjustment.

III. ADAPTIVE BASE STATION COOPERATION UNDER PERFECT CSI OF EVE

In this section, we design the cooperative secure transmission scheme through adaptive base station cooperation. Our objective is to maximize the secrecy rate, while ensuring both security performance and the SINR requirement at Rx2.

A. PROBLEM FORMULATION WITH COOPERATIVE TRANSMISSION

Since perfect CSI of Eve is available, it is sufficient for Alice to transmit confidential information in the direction (i.e., spatial dimension) that generates the maximum difference in signal quality at Bob and Eve. Hence, transmit beamforming is utilized to maximize the secrecy rate. Let $\mathbf{v} \in \mathbb{C}^{N_a}$ and $\mathbf{w} \in \mathbb{C}^{N_c}$ represent transmit beamforming vector at Alice and Charlie, respectively. Then, signals transmitted by Alice and Charlie can be constructed as

$$s_1 = \sqrt{P_1}\mathbf{v}x, \quad s_2 = \sqrt{P_2}\mathbf{w}z, \tag{4}$$

where P_1 and P_2 represent transmit powers at Alice and Charlie, respectively; $x, z \sim \mathcal{CN}(0, 1)$ correspond to the encoded symbols for Bob and Rx2, respectively. From (1)-(4), the received signals at Bob, Eve, and Rx2 can be expressed as

$$\begin{aligned} y_1 &= \sqrt{P_1}\mathbf{u}^H\mathbf{H}_{11}\mathbf{v}x + \sqrt{P_2}\mathbf{u}^H\mathbf{H}_{12}\mathbf{w}z + \mathbf{u}^H\mathbf{n}_1, \\ y_e &= \sqrt{P_1}\mathbf{h}_{e1}^H\mathbf{v}x + \sqrt{P_2}\mathbf{h}_{e2}^H\mathbf{w}z + n_e, \\ y_2 &= \sqrt{P_1}\mathbf{h}_{21}\mathbf{v}x + \sqrt{P_2}\mathbf{h}_{22}^H\mathbf{w}z + n_2, \end{aligned}$$

where $\mathbf{u} \in \mathbb{C}^{N_b}$ denotes the receive combining vector at Bob. Therefore, the SINR at Bob, Eve and Rx2 can be calculated as

$$\gamma_b = \frac{P_1|\mathbf{u}^H\mathbf{H}_{11}\mathbf{v}|^2}{1 + P_2|\mathbf{u}^H\mathbf{H}_{12}\mathbf{w}|^2}, \quad \gamma_e = \frac{P_1|\mathbf{h}_{e1}^H\mathbf{v}|^2}{1 + P_2|\mathbf{h}_{e2}^H\mathbf{w}|^2},$$
$$\gamma_2 = \frac{P_2|\mathbf{h}_{22}^H\mathbf{w}|^2}{1 + P_1|\mathbf{h}_{21}^H\mathbf{v}|^2}.$$

According to the essential of physical layer security, the achievable secrecy rate is given by

$$\begin{aligned} R_s &= \left[C_b - C_e\right]^+ \\ &= \left[\log_2\left(1 + \frac{P_1|\mathbf{u}^H\mathbf{H}_{11}\mathbf{v}|^2}{1 + P_2|\mathbf{u}^H\mathbf{H}_{12}\mathbf{w}|^2}\right)\right. \\ &\quad \left. - \log_2\left(1 + \frac{P_1|\mathbf{h}_{e1}^H\mathbf{v}|^2}{1 + P_2|\mathbf{h}_{e2}^H\mathbf{w}|^2}\right)\right]^+, \end{aligned} \tag{5}$$

where $C_b = \log_2(1 + \gamma_b)$ and $C_e = \log_2(1 + \gamma_e)$ denote the main channel capacity and the eavesdropper channel capacity, respectively. These two capacities jointly determine the achivable secrecy rate.

The achievable secrecy rate expression in (5) can be taken as the difference of two logarithmic (concave) functions, the resulting SRM problem is nonconvex, and thus difficult to solve in most cases. With the tradeoff between security performance and complexity in mind, we simplify the transmit

design at Charlie by imposing a zero forcing (ZF) constraint, i.e., the beamforming vector $\mathbf{w}$ is designed to completely null out the interference at Bob. Besides, we simplify the beamformer design at Alice and Bob, by choosing beamforming vector $\mathbf{v}$ ($\mathbf{u}$) as the right (left) singular vector, corresponding to the largest singular value of $\mathbf{H}_{11}$. This transmission scheme is often referred to as the max-eigenmode beamforming, i.e., secure transmission is performed over the dimension corresponding to the largest eigenmode of the main channel. Thus, the achievable secrecy rate in (5) can be rewritten as

$$R_s = \left[\log_2(1+P_1\sigma^2) - \log_2\left(1+\frac{P_1|\mathbf{h}_{e1}^H\mathbf{v}|^2}{1+P_2|\mathbf{h}_{e2}^H\mathbf{w}|^2}\right)\right]^+, \quad (6)$$

where σ is the maximum singular value of $\mathbf{H}_{11}$.

Based on the above analysis, we optimize the transmit strategy at Charlie to maximize the secrecy rate in (6). Let R_{th} be a minimum secrecy rate threshold, which corresponds to the security performance requirement. Besides, the desired QoS at Rx2 is denoted by a minimum SINR requirement γ_{th}. Then, the SRM problem can be formulated as

$$\begin{aligned} \max \quad & R_s \\ \text{s.t.} \quad & \mathbf{u}^H\mathbf{H}_{12}\mathbf{w} = 0, \\ & R_s \geq R_{th}, \\ & \gamma_2 \geq \gamma_{th}. \end{aligned} \quad (7)$$

Note that the first constraint in problem (7) corresponds to the ZF constraint. It can be verified that the secrecy rate in (6) increases with the interference from Charlie to Eve (i.e., $P_2|\mathbf{h}_{e2}^H\mathbf{w}|^2$). Accordingly, the problem (7) can be equivalently formulated as

$$\begin{aligned} \max \quad & P_2|\mathbf{h}_{e2}^H\mathbf{w}|^2 \\ \text{s.t.} \quad & \mathbf{u}^H\mathbf{H}_{12}\mathbf{w} = 0, \\ & R_s \geq R_{th}, \\ & P_2|\mathbf{h}_{22}^H\mathbf{w}|^2 \geq \left(1+P_1|\mathbf{h}_{21}^H\mathbf{v}|^2\right)\gamma_{th}. \end{aligned} \quad (8)$$

Note that both R_{th} and γ_{th} can be determined according to the security and performance requirement. In this paper, we choose R_{th} as the maximum achievable secrecy rate without the help of Charlie. In this case, the SINR at Alice and Eve can be expressed as

$$\gamma_b = P_1\left|\mathbf{u}^H\mathbf{H}_{11}\mathbf{v}\right|^2, \quad \gamma_e = P_1\left|\mathbf{h}_{e1}^H\mathbf{v}\right|^2.$$

Hence, we can calculate the achievable secrecy rate as

$$\begin{aligned} R_{th} &= \left[\log_2(1+\gamma_b) - \log_2(1+\gamma_e)\right]^+ \\ &= \left[\log_2\left(1+P_1\left|\mathbf{u}^H\mathbf{H}_{11}\mathbf{v}\right|^2\right) - \log_2\left(1+P_1\left|\mathbf{h}_{e1}^H\mathbf{v}\right|^2\right)\right]^+ \\ &= \left[\log_2\left(1+P_1\|\mathbf{H}_{11}\mathbf{v}\|^2\right) - \log_2\left(1+P_1\left|\mathbf{h}_{e1}^H\mathbf{v}\right|^2\right)\right]^+ \\ &= \left[\log_2\left(\frac{\mathbf{v}^H\left(\mathbf{I}+P_1\mathbf{H}_{11}^H\mathbf{H}_{11}\right)\mathbf{v}}{\mathbf{v}^H\left(\mathbf{I}+P_1\mathbf{h}_{e1}\mathbf{h}_{e1}^H\right)\mathbf{v}}\right)\right]^+. \end{aligned}$$

Here, the third equation follows from the fact that the optimal receive combining vector at Bob can be calculated as $\mathbf{u} = (\mathbf{H}_{11}\mathbf{v})/\|\mathbf{H}_{11}\mathbf{v}\|$. According to [49], the optimal beamforming vector that maximizes the achievable secrecy rate is given by

$$\mathbf{v} = \mathbf{x}_{\max}\left(\left(\mathbf{I}+P_1\mathbf{h}_{e1}\mathbf{h}_{e1}^H\right)^{-1}\left(\mathbf{I}+P_1\mathbf{H}_{11}^H\mathbf{H}_{11}\right)\right).$$

By utilizing the above beamforming vectors $\mathbf{u}$ and $\mathbf{v}$, the maximum achievable secrecy rate can be expressed as

$$R_{th} = \left[\log_2\left(\mu_{\max}\left(\left(\mathbf{I}+P_1\mathbf{h}_{e1}\mathbf{h}_{e1}^H\right)^{-1} \times \left(\mathbf{I}+P_1\mathbf{H}_{11}^H\mathbf{H}_{11}\right)\right)\right)\right]^+. \quad (9)$$

B. PROBLEM FORMULATION WITH COOPERATIVE JAMMING

Due to the channel fading and transmit power limits, the problem (8) may be infeasible with stringent constraints on the minimum secrecy rate threshold and the SINR requirement at Rx2. Therefore, the proposed cooperative beamforming strategy needs to be adjusted for security protection. To enhance the security, we employ a CJ scheme if either of the following two conditions are satisfied: 1) $R_s < R_{th}$; or 2) $\gamma_2 < \gamma_{th}$. In the proposed CJ scheme, Charlie only emits AN without providing service to Rx2, whereas Alice performs secrecy beamforming to maximize the secrecy rate.

Let $\mathbf{v}_c \in \mathbb{C}^{N_a}$, $\mathbf{u}_c \in \mathbb{C}^{N_b}$, and $\mathbf{w}_c \in \mathbb{C}^{N_c}$ denote secrecy beamforming vector at Alice, receive combining vector at Bob, and transmit vector at Charlie, respectively. Taking ZF constraint into account, the SINR at Bob and Eve can be calculated as

$$\gamma_b = P_1\left|\mathbf{u}_c^H\mathbf{H}_{11}\mathbf{v}_\mathbf{c}\right|^2, \quad \gamma_e = \frac{P_1\left|\mathbf{h}_{e1}^H\mathbf{v}_\mathbf{c}\right|^2}{1+P_2\left|\mathbf{h}_{e2}^H\mathbf{w}_\mathbf{c}\right|^2}.$$

Accordingly, the achievable secrecy rate with CJ scheme can be expressed as

$$\begin{aligned} R_s &= \left[\log_2(1+\gamma_b) - \log_2(1+\gamma_e)\right]^+ \\ &= \left[\log_2\left(1+P_1\left|\mathbf{u}_c^H\mathbf{H}_{11}\mathbf{v}_c\right|^2\right) - \log_2\left(1+\frac{P_1\left|\mathbf{h}_{e1}^H\mathbf{v}_c\right|^2}{1+P_2\left|\mathbf{h}_{e2}^H\mathbf{w}_c\right|^2}\right)\right]^+. \end{aligned} \quad (10)$$

Then, the SRM problem with CJ scheme can be formulated as

$$\begin{aligned} \max \quad & R_s \\ \text{s.t.} \quad & \mathbf{u}^H\mathbf{H}_{12}\mathbf{w} = 0. \end{aligned} \quad (11)$$

Note that under the ZF constraint, the AN transmitted by Charlie has no impact on Bob while causing interference to Eve. Therefore, the maximum achievable secrecy rate with CJ scheme (i.e., the optimal value of R_s in (11)) is greater than that without the help of Charlie (i.e., R_{th} in (9)).

C. COOPERATIVE BEAMFORMING DESIGN

In this subsection, we provide the explicit solution to problem (8). It is difficult to solve (8) directly, and thus we divide our design into two steps: we first characterize Charlie's power gain region according to [47]; and then we provide the explicit solution for cooperative beamforming scheme.

Let $\mathrm{PG}_{e2}(\mathbf{w}) = |\mathbf{h}_{e2}^H\mathbf{w}|^2$ and $\mathrm{PG}_{22}(\mathbf{w}) = |\mathbf{h}_{22}^H\mathbf{w}|^2$ represent power gains achieved by Charlie at Eve and Rx2, respectively. Then, Charlie's power gain region can be defined as

$$\mathrm{PGR} \triangleq \left\{ \left(\mathrm{PG}_{e2}(\mathbf{w}), \mathrm{PG}_{22}(\mathbf{w}) \right) \,\middle|\, \mathbf{w} \in \mathbb{C}^{N_c},\ \|\mathbf{w}\| = 1 \right\}. \quad (12)$$

Note that $\mathrm{PG}_{e2}(\mathbf{w})$ can also be taken as the interference power gain at Eve. Taking ZF constraint in problem (8) into account, transmit beamforming vector of Charlie can be uniquely expressed as

$$\mathbf{w} = \mathbf{N}\mathbf{g}, \quad (13)$$

where $\mathbf{N} \in \mathbb{C}^{N_c \times (N_c-1)}$ denotes an orthonormal basis for null $\left(\mathbf{u}^H\mathbf{H}_{12}\right)$, and $\mathbf{g} \in \mathbb{C}^{N_c-1}$ is a Gaussian noise vector. Thus, the remaining task is to choose $\mathbf{g}$ such that the interference to Eve is maximized under the SINR constraint, which corresponds to a point on the Pareto boundary of PGR in (12).

Proposition 1: The Pareto boundary points of PGR can be achieved by

$$\mathbf{g}(\lambda) = \mathbf{x}_{\max}\left(\lambda\mathbf{N}^H\mathbf{h}_{22}\mathbf{h}_{22}^H\mathbf{N} + (1-\lambda)\mathbf{N}^H\mathbf{h}_{e2}\mathbf{h}_{e2}^H\mathbf{N}\right), \quad (14)$$

where $\lambda \in [0, 1]$. **Proposition 1** can be proved directly from [47, Th. 1] and interested readers may refer to [47, Appendix D] for a detailed proof. Therefore, from (13), transmit beamforming vector at Charlie can be expressed as $\mathbf{w}(\lambda) = \mathbf{N}\mathbf{g}(\lambda)$, which is a function of λ.

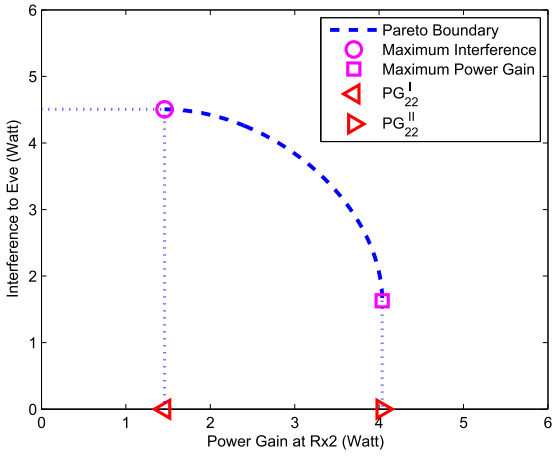


FIGURE 2. An example of the power gain region and its Pareto boundary.

In Fig. 2, we give an example of the Pareto boundary of PGR with $N_c = 4$, $N_b = 2$, and $P_1 = P_2 = 0$ dB. There are two extreme points on the boundary (i.e., the empty circle and square in Fig. 2), corresponding to the maximum interference at Eve and the maximum power gain at Rx2, respectively. Let $\mathrm{PG}_{22}^{\mathrm{I}}$ and $\mathrm{PG}_{22}^{\mathrm{II}}$ denote the power gains at Rx2 achieved by these two extreme points, and let $I_{th} = \gamma_{th}\left(1 + P_1\left|\mathbf{h}_{21}^H\mathbf{v}\right|^2\right)/P_2$ denote a power gain threshold related to γ_{th}. Then, we can obtain the optimal transmit strategy for Charlie. Some different cases are listed below.

1) Case 1: $I_{th} \le \mathrm{PG}_{22}^{\mathrm{I}}$.
In this case, we can find that

$$\frac{P_2|\mathbf{h}_{22}^H\mathbf{w}|^2}{1 + P_1|\mathbf{h}_{21}^H\mathbf{v}|^2} \ge \gamma_{th}.$$

Hence, the SINR requirement at Rx2 (i.e., the third constraint in problem (8)) is satisfied. In addition, the maximum interference point on Pareto boundary (i.e., the empty circle in Fig. 2) can be achieved. Specifically, the optimal transmit beamforming vector at Charlie can be obtained by solving the following interference maximization problem:

$$\max\ P_2|\mathbf{h}_{e2}^H\mathbf{w}|^2 \quad \text{s.t. (13).} \quad (15)$$

The objective function in problem (15) can be rewritten as $P_2\left|\left(\mathbf{N}^H\mathbf{h}_{e2}\right)^H\mathbf{g}\right|^2$, and thus the optimal vector $\mathbf{g}$ can be expressed as $\mathbf{g} = \mathbf{N}^H\mathbf{h}_{e2}$. Consequently, the optimal beamforming vector $\mathbf{w}$ is given by

$$\mathbf{w} = \frac{\mathbf{N}\mathbf{N}^H\mathbf{h}_{e2}}{\left\|\mathbf{N}\mathbf{N}^H\mathbf{h}_{e2}\right\|} = \frac{\Pi_{\mathbf{N}}\mathbf{h}_{e2}}{\|\Pi_{\mathbf{N}}\mathbf{h}_{e2}\|} = \frac{\Pi^{\perp}_{\mathbf{H}_{12}^H\mathbf{u}}\mathbf{h}_{e2}}{\left\|\Pi^{\perp}_{\mathbf{H}_{12}^H\mathbf{u}}\mathbf{h}_{e2}\right\|}. \quad (16)$$

Here, the second equation follows from $\mathbf{N}^H\mathbf{N} = \mathbf{I}$, and the third follows from $\left(\mathbf{H}_{12}^H\mathbf{u}\right)^H\mathbf{N} = \mathbf{0}$.
In particular, (16) can also be obtained by setting $\lambda = 0$ in (14). Then, we can find that

$$\mathbf{w} = \mathbf{N}\mathbf{g}(0) = \mathbf{N}\mathbf{x}_{\max}\left(\mathbf{N}^H\mathbf{h}_{e2}\mathbf{h}_{e2}^H\mathbf{N}\right) = \frac{\mathbf{N}\mathbf{N}^H\mathbf{h}_{e2}}{\left\|\mathbf{N}\mathbf{N}^H\mathbf{h}_{e2}\right\|}. \quad (17)$$

Here, the last equation follows from the fact that for any rank-one positive semidefinite (PSD) matrix $\mathbf{A} = \mathbf{a}\mathbf{a}^H$, we have

$$\mathbf{x}_{\max}(\mathbf{A}) = \mathbf{a}/\|\mathbf{a}\|$$

Therefore, the optimal vector $\mathbf{w}$ in (16) can also be derived from (17). Finally, by substituting (16) into (6), we can calculate the secrecy rate R_s. Note that we still need to check whether or not the required security performance (i.e., the seconde constraint in problem (8)) can be satisfied. If $R_s \ge R_{th}$, the max-eigenmode beamforming is performed at Alice, and transmit beamforming in (16) is performed at Charlie. However, if $R_s < R_{th}$, the cooperative beamforming scheme is replaced by the CJ scheme through adaptive base station cooperation. The corresponding SRM problem is formulated in (11), and the explicit solution is detailed in Section III-D.

2) Case 2: $\mathrm{PG}_{22}^{\mathrm{I}} < I_{th} \le \mathrm{PG}_{22}^{\mathrm{II}}$.
In this case, the SINR requirement at Rx2 can also be satisfied. Specifically, if $I_{th} = \mathrm{PG}_{22}^{\mathrm{II}}$, the maximum

power gain point on Pareto boundary (i.e., the empty square in Fig. 2) can be achieved. The transmit beamforming vector at Charalie can be obtained by solving the following problem:

$$\max P_2|\mathbf{h}_{22}^H\mathbf{w}|^2 \quad \text{s.t.} \quad (13).$$

Similar to the derivation of (16), the optimal solution to the above problem can be expressed as

$$\mathbf{w} = \left(\Pi^{\perp}_{\mathbf{H}_{12}^H\mathbf{u}}\mathbf{h}_{22}\right) \Big/ \left\|\Pi^{\perp}_{\mathbf{H}_{12}^H\mathbf{u}}\mathbf{h}_{22}\right\|.$$

However, for a general case (i.e., $\mathrm{PG}_{22}^{\mathrm{I}} < I_{th} < \mathrm{PG}_{22}^{\mathrm{II}}$), the optimal beamforming vector $\mathbf{w}$ corresponding to the Pareto boundary point cannot be expressed in a closed form. We will utilize numerical method to get the optimal solution.

From (13) and (14), the power gains corresponding to the Pareto boundary point can be expressed as

$$\mathrm{PG}_{22}(\lambda) = |\mathbf{h}_{22}^H\mathbf{w}(\lambda)|^2 = \left|\mathbf{h}_{22}^H\mathbf{N}\mathbf{g}(\lambda)\right|^2, \quad (18)$$

$$\mathrm{PG}_{e2}(\lambda) = |\mathbf{h}_{e2}^H\mathbf{w}(\lambda)|^2 = \left|\mathbf{h}_{e2}^H\mathbf{N}\mathbf{g}(\lambda)\right|^2. \quad (19)$$

Both (18) and (19) can be considered as two functions of λ. In particular, we have the following proposition.

Proposition 2: $\mathrm{PG}_{22}(\lambda)$ in (18) is an increasing function of λ, and $\mathrm{PG}_{e2}(\lambda)$ in (19) is a decreasing function of λ.

Proof: Please refer to Appendix A. ■

Therefore, by performing a binary search over λ, $\lambda \in [0, 1]$, and choosing the one such that $\mathrm{PG}_{22}(\lambda) = I_{th}$, we can obtain the beamforming vector $\mathbf{w} = \mathbf{N}\mathbf{g}(\lambda)$. Then, we can get the corresponding secrecy rate R_s from (6).

Similar to the Case 1, we also need to check whether or not the required security performance can be satisfied. If $R_s \geq R_{th}$, the proposed cooperative beamforming scheme is performed. If $R_s < R_{th}$, cooperative beamforming scheme is replaced by the CJ scheme due to adaptive base station cooperation. The corresponding SRM problem is formulated in (11), and the explicit solution will be detailed in Section III-D.

3) Case 3: $I_{th} > \mathrm{PG}_{22}^{\mathrm{II}}$.

In this case, we have

$$\frac{P_2|\mathbf{h}_{22}^H\mathbf{w}|^2}{1 + P_1|\mathbf{h}_{21}^H\mathbf{v}|^2} < \gamma_{th}.$$

Hence, the required SINR at Rx2 cannot be guaranteed. Therefore, the CJ scheme is carried out. The corresponding SRM problem is formulated in (11), and the explicit solution will be provided in the next subsection.

D. COOPERATIVE JAMMING DESIGN

In this subsection, we provide the explicit solution to problem (11). In particular, we consider two scenarios with different complexity levels: 1) the AN transmitted by Charlie is designed without using the combining vector at Bob (i.e., $\mathbf{u}$); and 2) based on the first scenario, the receive combining vector at Bob is chosen to be fixed, then we optimize the transmit beamforming vector for Alice.

Without using $\mathbf{u}$, the CJ scheme can be obtained by solving the following problem:

$$\max \quad P_2|\mathbf{h}_{e2}^H\mathbf{w}|^2 \quad \text{s.t.}\ \mathbf{H}_{12}\mathbf{w} = 0.$$

Similar to the derivation of (16), the optimal solution to the above problem can be expressed as

$$\mathbf{w}_c = \left(\Pi^{\perp}_{\mathbf{H}_{12}^H}\mathbf{h}_{e2}\right) \Big/ \left\|\Pi^{\perp}_{\mathbf{H}_{12}^H}\mathbf{h}_{e2}\right\|. \quad (20)$$

In the CJ scheme, the AN transmitted by Charlie is restricted in null $(\mathbf{H}_{12})$. According to [49], the condition for null $(\mathbf{H_{12}}) \neq \{\mathbf{0}\}$ is given by

$$\dim\{\mathrm{null}\,(\mathbf{H}_{12})\} = N_c - \min(N_b, N_c) > 0,$$

where dim is the dimension of a subspace, and the equation follows from the fact that the matrix $\mathbf{H}_{12}$ has full rank, i.e., $\mathrm{rank}\{\mathbf{H}_{12}\} = \min(N_b, N_c)$. Hence, (20) is applicable when the number of antennas at Charlie is greater than that at Bob, i.e., $N_c > N_b$. With (20), the achievable secrecy rate in (10) can be rewritten as

$$\begin{aligned} R_{s1} &= \Big[\log_2\left(1 + P_1|\mathbf{u}_c^H\mathbf{H_{11}}\mathbf{v_c}|^2\right) \\ &\quad - \log_2\left(1 + \frac{P_1|\mathbf{h}_{e1}^H\mathbf{v_c}|^2}{1 + P_2|\mathbf{h}_{e2}^H\mathbf{w_c}|^2}\right)\Big]^+ \\ &= \left[\log_2\left(\frac{\mathbf{v}_c^H\left(\mathbf{I} + P_1\mathbf{H}_{11}^H\mathbf{u}_c\mathbf{u}_c^H\mathbf{H}_{11}\right)\mathbf{v}_c}{\mathbf{v}_c^H\left(\mathbf{I} + \frac{P_1\mathbf{h}_{e1}\mathbf{h}_{e1}^H}{1+P_2|\mathbf{h}_{e2}^H\mathbf{w}_c|^2}\right)\mathbf{v}_c}\right)\right]^+ \\ &= \left[\log_2\left(\frac{\mathbf{v}_c^H\left(\mathbf{I} + P_1\mathbf{H}_{11}^H\mathbf{H}_{11}\right)\mathbf{v}_c}{\mathbf{v}_c^H\left(\mathbf{I} + \frac{P_1\mathbf{h}_{e1}\mathbf{h}_{e1}^H}{1+P_2|\mathbf{h}_{e2}^H\mathbf{w}_c|^2}\right)\mathbf{v}_c}\right)\right]^+. \end{aligned} \quad (21)$$

Here, the third equation follows from the fact that the optimal receive combining vector at Bob is

$$\mathbf{u}_c = (\mathbf{H}_{11}\mathbf{v}_c) \big/ \|\mathbf{H}_{11}\mathbf{v}_c\|. \quad (22)$$

Then, according to [49], the optimal beamforming vector at Alice that maximizes secrecy rate can be calculated as

$$\mathbf{v}_c = \mathbf{x}_{\max}(\mathbf{Z}_1), \quad (23)$$

where

$$\mathbf{Z}_1 = \left(\mathbf{I} + \frac{P_1\mathbf{h}_{e1}\mathbf{h}_{e1}^H}{1 + P_2|\mathbf{h}_{e2}^H\mathbf{w}_c|^2}\right)^{-1}\left(\mathbf{I} + P_1\mathbf{H}_{11}^H\mathbf{H}_{11}\right). \quad (24)$$

Substituting (23) into (22), we have the receive combining vector at Bob. Then, by utilizing beamforming vectors $\mathbf{u}_c$ and $\mathbf{v}_c$, the achievable secrecy rate in (21) can be calculated as

$$R_{s1} = \left[\log_2\left(\mu_{\max}(\mathbf{Z}_1)\right)\right]^+. \quad (25)$$

To further enhance secrecy, we propose a modified CJ scheme, where the receive combining vector at Bob is fixed

as in (22). Based on this, the AN transmitted by Charlie can be obtained by solving the following problem:

$$\max \quad P_2|\mathbf{h}_{e2}^H\mathbf{w}|^2 \quad \text{s.t. } \mathbf{u}_c^H\mathbf{H}_{12}\mathbf{w}=0.$$

Similar to the derivation of (16), the optimal solution to the above problem can be expressed as

$$\mathbf{w}_m = \left(\Pi^{\perp}_{\mathbf{H}_{12}^H\mathbf{u}_c}\mathbf{h}_{e2}\right) \Big/ \left\|\Pi^{\perp}_{\mathbf{H}_{12}^H\mathbf{u}_c}\mathbf{h}_{e2}\right\|. \tag{26}$$

Therefore, the AN is restricted in null $\left(\mathbf{u}_c^H\mathbf{H}_{12}\right)$. According to [49], the condition for null $\left(\mathbf{u}_c^H\mathbf{H}_{12}\right) \neq \{\mathbf{0}\}$ is given by

$$\dim\left\{\text{null}\left(\mathbf{u}_c^H\mathbf{H}_{12}\right)\right\} = N_c - \text{rank}\left\{\mathbf{u}_c^H\mathbf{H}_{12}\right\} = N_c - 1 > 0.$$

Hence, the modified CJ scheme in (26) is applicable as long as Charlie has multiple antennas. With (22) and (26), the achievable secrecy rate in (10) can be rewritten as

$$\begin{aligned} R_s &= \Big[\log_2\left(1+P_1|\mathbf{u}_c^H\mathbf{H_{11}}\mathbf{v_c}|^2\right) \\ &\qquad - \log_2\left(1+\frac{P_1|\mathbf{h}_{e1}^H\mathbf{v_c}|^2}{1+P_2|\mathbf{h}_{e2}^H\mathbf{w_c}|^2}\right)\Big]^+ \\ &= \left[\log_2\left(\frac{\mathbf{v}_m^H\left(\mathbf{I}+P_1\mathbf{H}_{11}^H\mathbf{u}_c\mathbf{u}_c^H\mathbf{H}_{11}\right)\mathbf{v}_m}{\mathbf{v}_m^H\left(\mathbf{I}+\frac{P_1\mathbf{h}_{e1}\mathbf{h}_{e1}^H}{1+P_2|\mathbf{h}_{e2}^H\mathbf{w}_m|^2}\right)\mathbf{v}_m}\right)\right]^+. \end{aligned}$$

Then, according to [49], the optimal transmit beamforming vector at Alice that maximizes secrecy rate is given by

$$\mathbf{v}_m = \mathbf{x}_{\max}(\mathbf{Z}), \tag{27}$$

where

$$\mathbf{Z} = \left(\mathbf{I}+\frac{P_1\mathbf{h}_{e1}\mathbf{h}_{e1}^H}{1+P_2|\mathbf{h}_{e2}^H\mathbf{w}_m|^2}\right)^{-1}\left(\mathbf{I}+P_1\mathbf{H}_{11}^H\mathbf{u}_c\mathbf{u}_c^H\mathbf{H}_{11}\right). \tag{28}$$

Accordingly, the secrecy rate in the modified CJ scenario can be derived as

$$R_s = \left[\log_2\left(\mu_{\max}(\mathbf{Z})\right)\right]^+. \tag{29}$$

Compared with the CJ scheme, there is an extra calculation step in the the modified CJ scheme. Nevertheless, the requirement on the number of transmit antennas at Charlie is relaxed, i.e., in the modified CJ scheme, ZF constraint can be satisfied as long as Charlie is equipped with multiple antennas. Moreover, for security performance comparison, we have the following proposition.

Proposition 3: Compared with the CJ scheme, the modified one can achieve a higher secrecy rate. Specifically, we have the following result.

$$\begin{cases} R_s \geq R_{s1} > 0, & \text{if } \mu_{\max}(\mathbf{Z}_1) > 1 \\ R_s > R_{s1} = 0, & \text{if } \mu_{\max}(\mathbf{Z}_1) \leq 1 < \mu_{\max}(\mathbf{Z}) \\ R_s = R_{s1} = 0, & \text{if } \mu_{\max}(\mathbf{Z}) \leq 1 \end{cases}$$

where R_{s1} and R_s are given in (25) and (29), respectively; $\mathbf{Z}_1$ and $\mathbf{Z}$ are given in (24) and (28), respectively.

Algorithm 1 Solve SRM Problem (7)

1) Initialization: Given $R_{th}, I_{th}, P_1, P_2, N_a, N_b, N_c$, and all channel state information.
2) Characterize the Pareto boundary of PGR in (12) by utilizing $\mathbf{g}(\lambda)$ in (14).
   a) If $I_{th} > \text{PG}_{22}^{\text{II}}$, carry out the modified CJ scheme, and solve problem (11).
   b) Otherwise, calculate R_s according to the Case 1 and Case 2 as discussed in Section III-C.
      - If $(R_s < R_{th})$, carry out the modified CJ scheme, and solve (11).
      - Otherwise, carry out the proposed cooperative beamforming scheme.
3) The transmit strategy is determined as the result of 2), and then calculate the maximum achievable secrecy rate.

Proof: Please refer to Appendix B. ■

Accordingly, we adopt the modified CJ scheme for secure transmission if either of the following two conditions are satisfied: 1) the achievable secrecy rate is less than R_{th}; or 2) the SINR at Rx2 is less than γ_{th}. The process of solving the primal problem (7) can be summarized in **Algorithm 1**.

E. PERFORMANCE ANALYSIS

In this subsection, we demonstrate the performance of the proposed adaptive base station cooperation. System parameters are set as $N_a = N_b = 2$, $N_c = 4$, $\gamma_{th} = 1$, and $P_1 = 10$ dB. Specifically, R_{th} is the maximum achievable secrecy rate without the help of Charlie, which is given in (9). The secrecy rate and transmission rate of Charlie are measured by bits per channel use (bpcu).

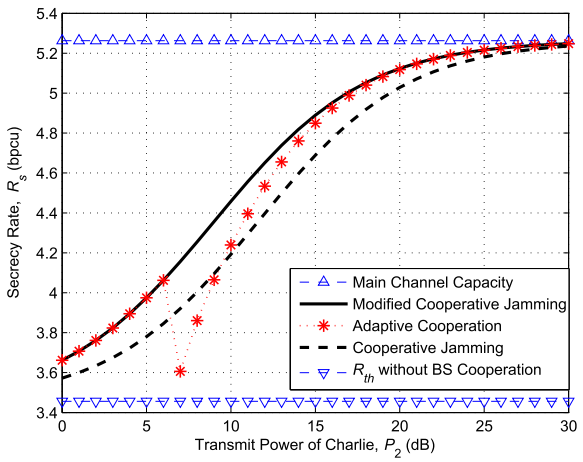


FIGURE 3. Secrecy rate versus transmit power of Charlie.

Fig. 3 shows numerical results of the secrecy rate. Compared with the CJ scheme, security performance can be improved by performing the modified CJ scheme. Fig. 3 also shows that the proposed cooperation scheme enables dynamic strategy adjustment. For example, when $P_2 \leq 6$ dB, the

modified CJ scheme is performed. As P_2 increases to 7 dB, Charlie begins to provide service to Rx2, as shown in Fig. 4. Although the secrecy rate is reduced due to transmit strategy adjustment, it is still higher than the threshold R_{th}.

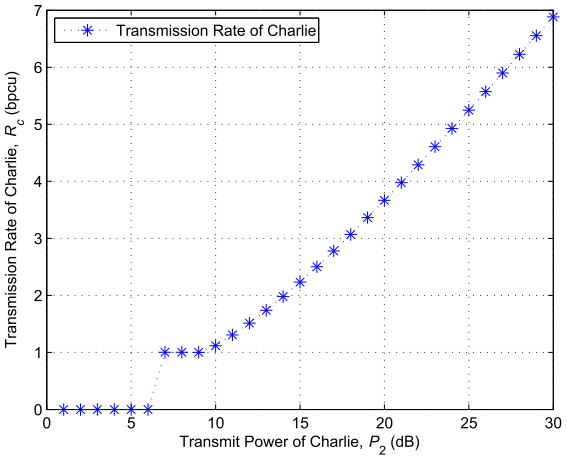


FIGURE 4. Transmission rate of Charlie versus transmit power of Charlie.

Fig. 4 provides the transmission rate of Charlie. It can be observed that when P_2 increases from 7 dB to 9 dB, the transmission rate remains at $\log_2(1+\gamma_{th})$. During this stage, the power gain threshold I_{th} satisfies the condition that $\mathrm{PG}_{22}^{\mathrm{I}} < I_{th} \leq \mathrm{PG}_{22}^{\mathrm{II}}$. In this case, Charlie creates the maximal interference to Eve under the SINR constraint $\gamma_2 = \gamma_{th}$. It can also be observed that the secrecy rate is increased during this stage, as shown in Fig. 3. Furthermore, as P_2 keeps increasing, both secrecy rate and transmission rate of Charlie are increased. Moreover, the secrecy rate achieved by adaptive base station cooperation will converge to that of the modified CJ scheme.

Note that in both CJ schemes, all transmit power of Charlie is used to emit AN without providing service to Rx2, thus leading to a higher secrecy rate. However, for a wide range of P_2, the proposed cooperation scheme achieves much higher system service rate, as shown in Fig. 5. Therefore, our scheme achieves more efficient utilization of power resources.

IV. ADAPTIVE BASE STATION COOPERATION UNDER STATISTIC CSI OF EVE

In this section, we design the cooperative secure transmission to maximize the secrecy rate, subject to a secrecy outage constraint. Specifically, we propose a mechanism for transmit strategy adaptation with security protection.

A. PROBLEM FORMULATION WITH COOPERATIVE TRANSMISSION

Let $\mathbf{v} \in \mathbb{C}^{N_a}$ and $\mathbf{u} \in \mathbb{C}^{N_b}$ denote secrecy beamforming vector for Alice and receive combining vector for Bob, respectively. With the tradeoff between security performance and complexity in mind, we simplify the beamformer design by choosing $\mathbf{v}$ ($\mathbf{u}$) as the right (left) singular vector corresponding

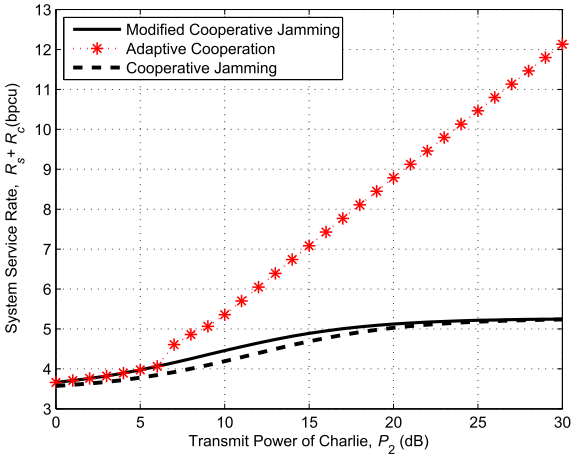


FIGURE 5. System service rate versus transmit power of Charlie.

to the largest singular value of $\mathbf{H}_{11}$. We also simplify the transmit design at Charlie by imposing the ZF constraint, i.e., the signal transmitted by Charlie creates no interference to Bob. From (1), the received signal at Bob can be rewritten as

$$y_1 = \sqrt{P_1}\mathbf{u}^H\mathbf{H}_{11}\mathbf{v}x + \mathbf{u}^H\mathbf{n}_1,$$

where $x \sim \mathcal{CN}(0,1)$ represents the encoded symbols for Bob.

In addition to providing service to Rx2, Charlie also transmits AN to further interfere with Eve. Let $[\mathbf{w}, \mathbf{W}_n] \in \mathbb{C}^{N_c \times (N_c-1)}$ denote an orthonormal basis for null $\left(\mathbf{u}^H\mathbf{H}_{12}\right)$, where $\mathbf{w}$ is used for beamforming, and $\mathbf{W}_n$ for AN generation. Then, the signal transmitted by Charlie can be constructed as

$$\mathbf{s}_2 = \sqrt{P_2\phi}\mathbf{w}u + \sqrt{\frac{P_2(1-\phi)}{N_c-2}}\mathbf{W}_n\mathbf{z},$$

where $u \sim \mathcal{CN}(0,1)$ and $\mathbf{z} \sim \mathcal{CN}(\mathbf{0}, \mathbf{I})$ are mutually independent, and denote the data symbols for Rx2 and a Gaussian noise vector, respectively; $\phi \in [0,1]$ represents the fraction of P_2 allocated to information-bearing signal. To maximize the useful signal at Rx2, the beamforming vector for Charlie can be obtained by solving the following problem:

$$\max P_2|\mathbf{h}_{22}^H\mathbf{w}|^2 \quad \text{s.t. } \mathbf{u}^H\mathbf{H}_{12}\mathbf{w} = 0.$$

Similar to the derivation of (16), the optimal solution to the above problem is

$$\mathbf{w} = \left(\Pi_{\mathbf{H}_{12}^H\mathbf{u}}^{\perp}\mathbf{h}_{22}\right) \Big/ \left\|\Pi_{\mathbf{H}_{12}^H\mathbf{u}}^{\perp}\mathbf{h}_{22}\right\|. \tag{30}$$

Then, from (2)-(3), the received signals at Eve and Rx2 can be rewritten as

$$y_e = \sqrt{P_1}\mathbf{h}_{e1}^H\mathbf{v}x + \sqrt{P_2\phi}\mathbf{h}_{e2}^H\mathbf{w}u + \sqrt{\frac{P_2(1-\phi)}{N_c-2}}\mathbf{h}_{e2}^H\mathbf{W}_n\mathbf{z} + n_e,$$

$$y_2 = \sqrt{P_1}\mathbf{h}_{21}\mathbf{v}x + \sqrt{P_2\phi}\mathbf{h}_{22}^H\mathbf{w}u + \sqrt{\frac{P_2(1-\phi)}{N_c-2}}\mathbf{h}_{22}^H\mathbf{W}_n\mathbf{z} + n_2.$$

Let σ denote the maximum singular value of $\mathbf{H}_{11}$. The SINR at Bob, Eve and Rx2 can be calculated as

$$\gamma_b = P_1|\mathbf{u}^H\mathbf{H_{11}}\mathbf{v}|^2 = P_1\sigma^2,$$
$$\gamma_e(\phi) = \frac{P_1\left|\mathbf{h}_{e1}^H\mathbf{v}\right|^2}{1+P_2\phi\left|\mathbf{h}_{e2}^H\mathbf{w}\right|^2+\frac{P_2(1-\phi)}{N_c-2}\left\|\mathbf{h}_{e2}^H\mathbf{W}_n\right\|^2}, \quad (31)$$
$$\gamma_2(\phi) = \frac{P_2\phi\left\|\mathbf{h}_{22}^H\mathbf{w}\right\|^2}{1+P_1\left|\mathbf{h}_{21}^H\mathbf{v}\right|^2+\frac{P_2(1-\phi)}{N_c-2}\left\|\mathbf{h}_{22}^H\mathbf{W}_n\right\|^2}. \quad (32)$$

Hence, the achievable secrecy rate is given by

$$R_s = \left[\log_2(1+\gamma_b)-\log_2(1+\gamma_e(\phi))\right]^+ = \left[\log_2\left(1+P_1\sigma^2\right) - \log_2\left(1+\frac{P_1\left|\mathbf{h}_{e1}^H\mathbf{v}\right|^2}{1+P_2\phi\left|\mathbf{h}_{e2}^H\mathbf{w}\right|^2+\frac{P_2(1-\phi)}{N_c-2}\left\|\mathbf{h}_{e2}^H\mathbf{W}_n\right\|^2}\right)\right]^+. \quad (33)$$

As discussed in Section II-C, the secrecy outage constraint can be expressed as

$$\Pr\left(C_e > R_b - R_s\right) = \Pr\left(1+\gamma_e(\phi) > 2^{R_b-R_s}\right) \le \varepsilon, \quad (34)$$

where ε is a maximum allowable secrecy outage probability. Since the secrecy outage probability increases with R_s, (34) is equivalent to

$$\Pr\left(\gamma_e(\phi) > \mu\right) = \varepsilon, \quad (35)$$

where $\mu = 2^{R_b-R_s}-1$. Let R_{th} and γ_{th} represent a minimum secrecy rate threshold and a minimum SINR requirement at Rx2, respectively. Then the SRM problem is formulated as

$$\begin{aligned} \max \quad & R_s = \log_2\left(\frac{1+P_1\sigma^2}{1+\mu}\right) \\ \text{s.t.} \quad & 0 \le \phi \le 1, \\ & \Pr\left(\gamma_e(\phi) > \mu\right) = \varepsilon, \\ & R_{th} \le R_s \le R_b, \\ & \gamma_2(\phi) \ge \gamma_{th}. \end{aligned} \quad (36)$$

Note that both R_{th} and γ_{th} can be determined according to the security and performance requirement. Specifically, we choose R_{th} as the maximum achievable secrecy rate without the help of Charlie, which can be obtained according to [21].

B. PROBLEM FORMULATION WITH COOPERATIVE JAMMING

Due to the channel fading and transmit power limits, the problem (36) may be infeasible with stringent constraints on the minimum secrecy rate threshold and the SINR requirement at Rx2. Therefore, the proposed cooperative transmit strategy needs to be adjusted for security protection. In particular, the CJ scheme proposed in [38] can enhance security and secure energy efficiency. To enhance secrecy, we employ this CJ scheme if either of the following two conditions are satisfied: 1) $R_s < R_{th}$; or 2) $\gamma_2 < \gamma_{th}$. With the CJ scheme in [38], Charlie only emits AN without providing service to Rx2, whereas Alice performs AN assisted secrecy beamforming. The signal transmitted by Alice can be constructed as

$$\mathbf{s}_1 = \sqrt{P_1\theta}\mathbf{v}x + \sqrt{\frac{P_1(1-\theta)}{N_a-1}}\mathbf{N_v}\mathbf{n}, \quad (37)$$

where $\theta \in [0,1]$ represents the fraction of P_1 allocated to the information-bearing signal; $x \sim \mathcal{CN}(0,1)$ and $\mathbf{n} \sim \mathcal{CN}(\mathbf{0},\mathbf{I})$ are mutually independent, and denote data symbols for Bob and a Gaussian noise vector, respectively; $\mathbf{v}$ is the secrecy beamforming vector; and $\mathbf{N_v} \in \mathbb{C}^{N_a\times(N_a-1)}$ is an orthonormal basis for null$\left(\mathbf{u}^H\mathbf{H}_{11}\right)$. Based on ZF constraint $\mathbf{u}^H\mathbf{H}_{12}\mathbf{s}_2 = 0$, the signal transmitted by Charlie can be expressed as

$$\mathbf{s}_2 = \sqrt{\frac{P_2}{N_c-1}}\mathbf{W}\mathbf{g}, \quad (38)$$

where $\mathbf{g} \sim \mathcal{CN}(\mathbf{0},\mathbf{I})$ denotes a Gaussian noise vector; $\mathbf{W}$ denotes an orthonormal basis for null$\left(\mathbf{u}^H\mathbf{H}_{12}\right)$. Then, according to (37)-(38), we can calculate the SINR at Bob and Eve as

$$\gamma_b(\theta) = P_1\theta|\mathbf{u}^H\mathbf{H_{11}}\mathbf{v}|^2,$$
$$\gamma_e(\theta) = \frac{P_1\theta|\mathbf{h}_{e1}^H\mathbf{v}|^2}{1+\frac{P_1(1-\theta)}{N_a-1}|\mathbf{h}_{e1}^H\mathbf{N_v}|^2+\frac{P_2}{N_c-1}\|\mathbf{h}_{e2}^H\mathbf{W}\|^2}.$$

Specifically, we also simplify the secure transmission by choosing beamforming vector $\mathbf{v}$ ($\mathbf{u}$) as the right (left) singular vector corresponding to the largest singular value of $\mathbf{H}_{11}$ (denoted by σ). Then, the achievable secrecy rate can be calculated as

$$R_s = \left[\log_2(1+\gamma_b(\theta)) - \log_2(1+\gamma_b(\theta))\right]^+, = \left[\log_2\left(1+P_1\sigma^2\right) - \log_2\left(1+\frac{P_1\theta|\mathbf{h}_{e1}^H\mathbf{v}|^2}{1+\frac{P_1(1-\theta)}{N_a-1}|\mathbf{h}_{e1}^H\mathbf{N_v}|^2+\frac{P_2}{N_c-1}\|\mathbf{h}_{e2}^H\mathbf{W}\|^2}\right)\right]^+.$$

Hence, the SRM problem with CJ scheme is formulated as

$$\begin{aligned} \max \quad & R_s \\ \text{s.t.} \quad & 0 \le \theta \le 1, \\ & \Pr\left(\gamma_e(\theta) > \mu\right) = \varepsilon, \end{aligned} \quad (39)$$

where $\mu = 2^{R_b-R_s}-1$. Note that under the ZF constraint, the AN emitted by Charlie only interferes with Eve. Therefore, the maximum achievable secrecy rate with CJ scheme is greater than that without help of Charlie. The explicit solution to problem (39) can be obtained in [38].

C. PROBLEM REFORMULATION

In this subsection, we provide the solution process to problem (36). It is difficult to solve (36) directly, and thus we reformulate it as a tractable power allocation problem. We first check that whether the required SINR at Rx2 can be satisfied. From (32), the maximum achievable SINR at Rx2 is given by $\gamma_2(1)$. If $\gamma_2(1) < \gamma_{th}$, the SINR constraint cannot be satisfied. Thus, the proposed transmission scheme is replaced by CJ scheme through adaptive base station cooperation. The corresponding SRM problem is formulated in (39), and the explicit solution can be found in [38]. If $\gamma_2(1) \geq \gamma_{th}$, we optimize the power allocation ratio ϕ in problem (36). In the following, we assume that $\gamma_2(1) \geq \gamma_{th}$ is satisfied.

It is obvious that $\gamma_2(\phi)$ in (32) is an increasing function of ϕ. In addition, the SINR constraint in problem (36) can be rewritten as

$$P_2\phi\left\|\mathbf{h}_{22}^H\mathbf{w}\right\|^2 \geq \gamma_{th}\left(1+P_1\left|\mathbf{h}_{21}^H\mathbf{v}\right|^2+\frac{P_2(1-\phi)\left\|\mathbf{h}_{22}^H\mathbf{W}_n\right\|^2}{N_c-2}\right).$$

Then, we can calculate a lower bound on ϕ as

$$\phi_L=\frac{\left(1+P_1\left|\mathbf{h}_{21}^H\mathbf{v}\right|^2+\frac{P_2\left\|\mathbf{h}_{22}^H\mathbf{W}_n\right\|^2}{N_c-2}\right)\gamma_{th}}{P_2\left\|\mathbf{h}_{22}^H\mathbf{w}\right\|^2+\frac{P_2\left\|\mathbf{h}_{22}^H\mathbf{W}_n\right\|^2}{N_c-2}\gamma_{th}}. \tag{40}$$

Since the objective function in problem (36) is a monotone decreasing function of μ, problem (36) is equivalent to the following problem:

$$\begin{aligned}&\min \quad \mu\\ &\text{s.t.} \quad \phi_L\leq\phi\leq 1,\\ &\qquad \Pr\left(\gamma_e\left(\phi\right)>\mu\right)=\varepsilon,\\ &\qquad R_{th}\leq R_s\leq C_b.\end{aligned} \tag{41}$$

This problem can be solved in two steps. First, by dropping the security performance constraint, we solve the relaxed version of (41), which can be formulated as

$$\begin{aligned}&\min \quad \mu\\ &\text{s.t.} \quad \phi_L\leq\phi\leq 1,\\ &\qquad \Pr\left(\gamma_e\left(\phi\right)>\mu\right)=\varepsilon.\end{aligned} \tag{42}$$

Let μ^* be the optimal solution of (42), then the secrecy rate can be calculated as

$$R_s^*=\log_2\left(\frac{1+P_1\sigma^2}{1+\mu^*}\right). \tag{43}$$

Then, we check whether or not the required security performance can be guaranteed. If $R_s^* \geq R_{th}$, the proposed transmit strategy is performed, and R_s^* in (43) is the maximum achievable secrecy rate. Otherwise, transmit strategy will be replaced by CJ scheme through adaptive base station cooperation. The corresponding SRM problem is formulated in (39), and the explicit solution can be obtained accoring to [38]. Finally, the process of solving the primal problem (36) can be summarized in **Algorithm 2**.

Algorithm 2 Solve SRM Problem (36)

1) Initialization: Given R_{th}, γ_{th}, P_1, P_2, N_a, N_b, N_c, ε, CSI of $\mathbf{H}_{11}$, $\mathbf{h}_{21}$, $\mathbf{H}_{12}$, $\mathbf{h}_{22}$, and the statistical CSI of $\mathbf{h}_{e1}$ and $\mathbf{h}_{e2}$.
2) Calculate $\gamma_2(1)$ according to (32).
   a) If $\gamma_2(1) < \gamma_{th}$, carry out the CJ scheme, and solve problem (39).
   b) If $\gamma_2(1) \geq \gamma_{th}$, solve problem (42) to obtain μ^*, and calculate R_s^* according to (43).
      - If $R_s < R_{th}$, carry out the CJ scheme, and solve problem (39).
      - Otherwise, carry out the proposed transmission scheme.
3) The transmit strategy is determined as the result of 2), and then calculate the maximum achievable secrecy rate.

D. POWER ALLOCATION

In this subsection, we provide the explicit solution to problem (42). First, we can obtain a suboptimal solution by fixing $\phi = \phi_L$. Hence, the power $P_2\phi_L$ is utilized for data transmission, while the remaining power is utilized for AN generation. In the following, we solve problem (42) by optimizing ϕ.

For simplicity, we define new variables

$$X=P_1\left|\mathbf{h}_{e1}^H\mathbf{v}\right|^2,\quad X_1=P_2\phi\left\|\mathbf{h}_{e2}^H\mathbf{w}\right\|^2,$$
$$X_2=\frac{P_2\left(1-\phi\right)\left\|\mathbf{h}_{e2}^H\mathbf{W}_n\right\|^2}{N_c-2},\quad Y=X_1+X_2.$$

Then, the secrecy outage constraint in problem (42) can be rewritten as

$$\Pr\left(X>\mu+\mu Y\right)=\varepsilon. \tag{44}$$

It can be verified that $X\sim\text{Exp}\left(\lambda\right)$, $X_1\sim\text{Exp}\left(\lambda_1\right)$, and $X_2\sim\Gamma\left(N_c-2,\lambda_2\right)$, where $\lambda=\frac{1}{P_1}$, $\lambda_1=\frac{1}{P_2\phi}$, and $\lambda_2=\frac{N_c-2}{P_2(1-\phi)}$. The probability density function (PDF) of X, X_1, and X_2 are given by

$$f_X\left(x\right)=\lambda e^{-\lambda x},\quad x\geq 0,$$
$$f_{X_1}\left(x_1\right)=\lambda_1 e^{-\lambda_1 x_1},\quad x_1\geq 0,$$
$$f_{X_2}\left(x_2\right)=\frac{\lambda_2^{N_c-2}}{\Gamma\left(N_c-2\right)}x_2^{N_c-3}e^{-\lambda_2 x_2},\quad x_2\geq 0.$$

Note that the PDF of X_2 and Y changes with N_c, and thus the secrecy outage probability changes with N_c. For simplicity, we assume that $N_c=4$, and $N_a=N_b=2$. The study under this parameter settings can be extended to a general multi-antenna scenario.

Based on the above notations and assumptions, we can obtain the PDF of Y as

$$\begin{aligned} f_Y(y) &= \int_{-\infty}^{+\infty} f_{X_1}(y-x_2) f_{X_2}(x_2)\, dx_2 \\ &= \lambda_1\lambda_2^2 e^{-\lambda_1 y} \int_0^y x_2 e^{(\lambda_1-\lambda_2)x_2} dx_2 \\ &= \lambda_1\lambda_2^2 e^{-\lambda_1 y}\left[\frac{x_2 e^{(\lambda_1-\lambda_2)x_2}}{\lambda_1-\lambda_2} - \frac{e^{(\lambda_1-\lambda_2)x_2}}{(\lambda_1-\lambda_2)^2}\right]_0^y \\ &= \frac{\lambda_1\lambda_2^2}{(\lambda_1-\lambda_2)^2}\left[(\lambda_1-\lambda_2)\, y e^{-\lambda_2 y} - e^{-\lambda_2 y} + e^{-\lambda_1 y}\right], \end{aligned}$$

where $y \geq 0$. Then, the secrecy outage constraint in (44) can be expressed as

$$\begin{aligned} \varepsilon &= \int_0^{+\infty}\int_{\mu+\mu y}^{+\infty} f_X(x) f_Y(y) dx dy \\ &= \int_0^{+\infty}\left[e^{-\lambda x}\right]_{+\infty}^{\mu+\mu y} f_Y(y)\, dy \\ &= \frac{\lambda_1\lambda_2^2 e^{-\lambda\mu}}{(\lambda_1-\lambda_2)^2}\int_0^{\infty}[(\lambda_1-\lambda_2)y-1]e^{-(\lambda_2+\lambda\mu)y} \\ &\quad + e^{-(\lambda_1+\lambda\mu)y} dy \\ &= \frac{\lambda_1\lambda_2^2 e^{-\lambda\mu}}{(\lambda_1-\lambda_2)^2}\left[\frac{[1+(\lambda_2+\lambda\mu)y](\lambda_1-\lambda_2)e^{-(\lambda_2+\lambda\mu)y}}{(\lambda_2+\lambda\mu)^2}\right. \\ &\quad \left. + \frac{e^{-(\lambda_1+\lambda\mu)y}}{\lambda_1+\lambda\mu} - \frac{e^{-(\lambda_2+\lambda\mu)y}}{\lambda_2+\lambda\mu}\right]_{\infty}^{0} \\ &= \frac{\lambda_1\lambda_2^2 e^{-\lambda\mu}}{(\lambda_1+\lambda\mu)(\lambda_2+\lambda\mu)^2}. \end{aligned}$$

After rearranging terms, it can be rewritten as

$$\ln\left(\frac{1}{\varepsilon}\right) = \lambda\mu + \ln\left(1+\frac{\lambda\mu}{\lambda_1}\right) + 2\ln\left(1+\frac{\lambda\mu}{\lambda_2}\right). \quad (45)$$

Given P_1, P_2, and ε, μ in (45) can be taken as an implicit function of ϕ. Specifically, we have the following proposition.

Proposition 4: The function $\mu(\phi)$ determined by (45) decreases with ϕ when $\phi \in \left[0, \frac{1}{3}\right]$, and increases with ϕ when $\phi \in \left[\frac{1}{3}, 1\right]$

Proof: Taking the derivative on both sides of (45) with respect to ϕ, we have

$$\begin{aligned} &\left[\lambda + \frac{\lambda P_2\phi}{1+\lambda P_2\phi\mu(\phi)} + \frac{2\lambda P_2(1-\phi)}{2+\lambda P_2(1-\phi)\mu(\phi)}\right]\mu'(\phi) \\ &\quad = \frac{2\lambda P_2\mu(\phi)}{2+\lambda P_2(1-\phi)\mu(\phi)} - \frac{\lambda P_2\mu(\phi)}{1+\lambda P_2\phi\mu(\phi)}. \end{aligned} \quad (46)$$

For simplicity, we define the following new functions

$$\begin{aligned} T_1(\phi) &= \lambda(P_2\mu)^2\left(3-\frac{1}{\phi}\right), \\ T_2(\phi) &= \frac{1}{\phi} + \lambda P_2\mu, \\ T_3(\phi) &= 2+\lambda P_2\mu(1-\phi). \end{aligned}$$

Then, according to (46), $\mu'(\phi)$ can be expressed as

$$\begin{aligned} \mu'(\phi) &= \frac{\dfrac{2\lambda P_2\mu(\phi)}{2+\lambda P_2(1-\phi)\mu(\phi)} - \dfrac{\lambda P_2\mu(\phi)}{1+\lambda P_2\phi\mu(\phi)}}{\lambda + \dfrac{\lambda P_2\phi}{1+\lambda P_2\phi\mu(\phi)} + \dfrac{2\lambda P_2(1-\phi)}{2+\lambda P_2(1-\phi)\mu(\phi)}} \\ &= \frac{T_1(\phi)}{T_2(\phi)T_3(\phi)+P_2T_3(\phi)+2P_2(1-\phi)T_2(\phi)}. \end{aligned} \quad (47)$$

It can be verified that $T_2(\phi)$ is $T_3(\phi)$ are both positive. In addition, we can infer that $T_1(\phi) \leq 0$ when $\phi \in \left[0, \frac{1}{3}\right]$, and $T_1(\phi) \geq 0$ when $\phi \in \left[\frac{1}{3}, 1\right]$. This completes the proof of **Proposition 4**. ■

Based on this, we can find the optimal solution to problem (42) by the following proposition.

Proposition 5: The optimal solution to problem (42) is

$$\phi^* = \begin{cases} \dfrac{1}{3} & \phi_L \leq \dfrac{1}{3}; \\ \phi_L & \phi_L > \dfrac{1}{3}. \end{cases}$$

where ϕ_L is given in (40).

Proof: According to **Proposition 4**, we can find the global minimum of $\mu(\phi)$ by solving the following equation

$$\mu'(\phi) = 0. \quad (48)$$

where $\mu'(\phi)$ is given in (47). It can be verified that the solution to (48) is $\phi = \frac{1}{3}$. Finally, taking the lower bound on ϕ into account, we can obtain the **Proposition 5**. ■

E. PERFORMANCE ANALYSIS

In this subsection, we demonstrate the performance of the proposed adaptive base station cooperation. System parameters are set as $N_a = N_b = 2$, $N_c = 4$, $P_1 = 10$ dB, $\varepsilon = 0.01$, and $\gamma_{th} = 1$. Specifically, R_{th} is the maximum achievable secrecy rate without the help of Charlie, which can be obtained according to [21]. The secrecy rate and

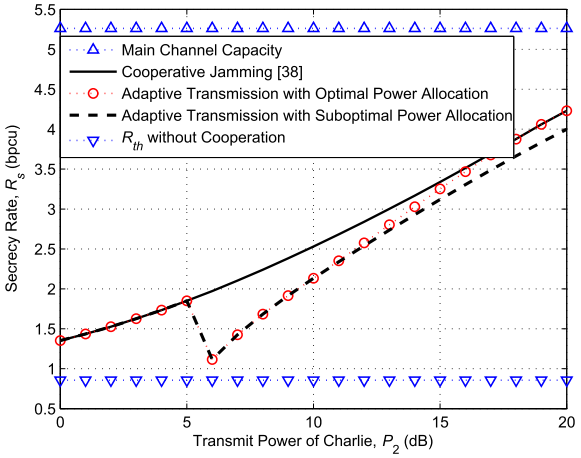


FIGURE 6. Secrecy rate versus transmit power of Charlie.

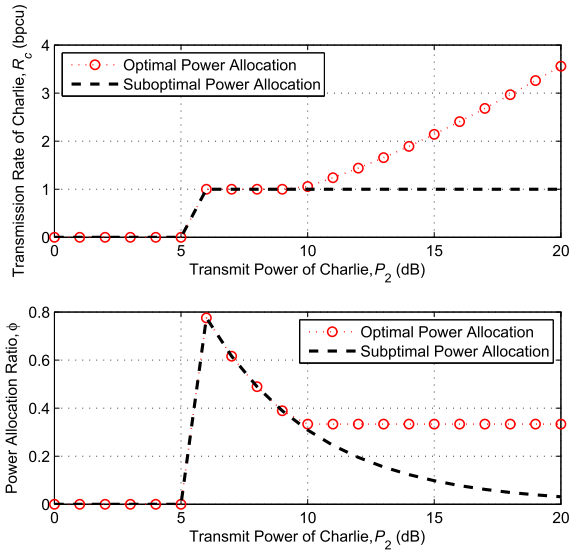


FIGURE 7. Transmission rate of Charlie and the power allocation ratio.

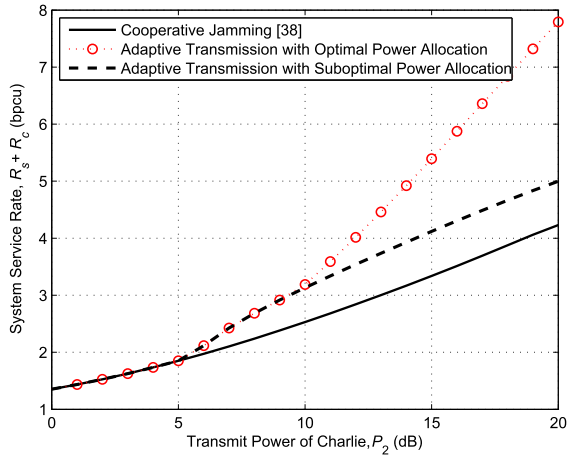


FIGURE 8. System service rate versus transmit power of Charlie.

transmission rate of Charlie are measured by bits per channel use (bpcu).

Fig. 6 shows the numerical results on secrecy rate. We can observe that the proposed adaptive transmission with optimal power allocation scheme outperforms that with suboptimal power allocation scheme. Fig. 6 also demonstrates that the proposed transmission scheme enables dynamic strategy adjustment. For example, when $P_2 \leq 5$ dB, the CJ scheme is carried out. As P_2 increases to 6 dB, Charlie begins to provide service to Rx2, as shown in Fig. 7. Although the secrecy rate is reduced due to transmit strategy adjustment, it is still higher than the threshold R_{th}.

Fig. 7 shows the numerical results on the transmission rate of Charlie and the power allocation ratio. We can observe that the performance gain achieved by optimizing power allocation can be verified for a wide range of P_2. Specifically, the transmission rate remains at $\log_2(1+\gamma_{th})$ when P_2 increases from 6 dB to 9 dB. The reason is that during this stage, the optimal power allocation ratio equals ϕ_L. As P_2 keeps increasing, the optimal power allocation comes into play, and then the transmission rate is increased.

Note that in the CJ schemes, all transmit power of Charlie is used to emit AN without providing service to Rx2, thus leading to a higher secrecy rate. However, for a wide range of P_2, the proposed cooperative transmission scheme achieves much higher system service rate, as shown in Fig. 8. Therefore, the proposed adaptive transmission with optimal power allocation achieves more efficient utilization of power resources.

V. CONCLUSION

We studied the physical layer security in two-cell wireless networks. The main contribution of this paper is the proposition of the adaptive base station cooperation for security protection. By taking both security and performance guarantee into account, we provided a mechanism for dynamic transmit strategy adjustment. The explicit transmit design for secrecy rate maximization was provided under both perfect and statistical channel state information of eavesdropper. Our evaluation results demonstrate both the effectiveness and flexibility of our solution. More importantly, our scheme is efficient in power resource utilization.

In future work, the secure transmission scheme will be further investigated for a more severe wiretap channel model, where the eavesdropper is equipped with multiple antennas. Also, the joint decoding scenario where the eavesdropper can decode and remove the jamming signal emitted by the cooperative base station, will be of practical interests.

APPENDIX A
PROOF OF PROPOSITION 2

Proof: First, $\mathbf{g}(\lambda)$ in (14) can be rewritten as

$$\begin{aligned}\mathbf{g}(\lambda) &= \arg\max_{\|\mathbf{x}\|=1} \mathbf{x}^H \left(\lambda \mathbf{N}^H \mathbf{h}_{22}\mathbf{h}_{22}^H \mathbf{N} + (1-\lambda)\mathbf{N}^H \mathbf{h}_{e2}\mathbf{h}_{e2}^H \mathbf{N}\right)\mathbf{x} \\ &= \arg\max_{\|\mathbf{x}\|=1} \left(\lambda \left|\mathbf{h}_{22}^H \mathbf{N}\mathbf{x}\right|^2 + (1-\lambda)\left|\mathbf{h}_{e2}^H \mathbf{N}\mathbf{x}\right|^2\right). \quad (49)\end{aligned}$$

Here, the first equation follows from the fact that for any Hermitian matrix $\mathbf{A}$, we have

$$\mathbf{x}_{\max}(\mathbf{A}) = \arg\max_{\|\mathbf{x}\|=1} \mathbf{x}^H \mathbf{A}\mathbf{x}.$$

We assume that $\lambda_1, \lambda_2 \in [0,1]$, and $\lambda_1 < \lambda_2$. Then, from (49), we can conclude that

$$\begin{aligned}&\lambda_1 \left|\mathbf{h}_{22}^H \mathbf{N}\mathbf{g}(\lambda_2)\right|^2 + (1-\lambda_1)\left|\mathbf{h}_{e2}^H \mathbf{N}\mathbf{g}(\lambda_2)\right|^2 \\ &\quad \leq \lambda_1 \left|\mathbf{h}_{22}^H \mathbf{N}\mathbf{g}(\lambda_1)\right|^2 + (1-\lambda_1)\left|\mathbf{h}_{e2}^H \mathbf{N}\mathbf{g}(\lambda_1)\right|^2, \quad (50)\end{aligned}$$

and

$$\begin{aligned}&\lambda_2 \left|\mathbf{h}_{22}^H \mathbf{N}\mathbf{g}(\lambda_1)\right|^2 + (1-\lambda_2)\left|\mathbf{h}_{e2}^H \mathbf{N}\mathbf{g}(\lambda_1)\right|^2 \\ &\quad \leq \lambda_2 \left|\mathbf{h}_{22}^H \mathbf{N}\mathbf{g}(\lambda_2)\right|^2 + (1-\lambda_2)\left|\mathbf{h}_{e2}^H \mathbf{N}\mathbf{g}(\lambda_2)\right|^2. \quad (51)\end{aligned}$$

In the following, two cases are considered.

1) Case 1: $0 = \lambda_1 < \lambda_2 \leq 1$.

In this case, (50) can be rewritten as

$$\left|\mathbf{h}_{e2}^H\mathbf{N}\mathbf{g}(\lambda_1)\right|^2 \geq \left|\mathbf{h}_{e2}^H\mathbf{N}\mathbf{g}(\lambda_2)\right|^2. \quad (52)$$

In addition, from (51), we can get

$$\left|\mathbf{h}_{22}^H\mathbf{N}\mathbf{g}(\lambda_2)\right|^2 - \left|\mathbf{h}_{22}^H\mathbf{N}\mathbf{g}(\lambda_1)\right|^2 \geq \frac{1-\lambda_2}{\lambda_2}\left(\left|\mathbf{h}_{e2}^H\mathbf{N}\mathbf{g}(\lambda_1)\right|^2 - \left|\mathbf{h}_{e2}^H\mathbf{N}\mathbf{g}(\lambda_2)\right|^2\right). \quad (53)$$

Substituting (52) into (53), we can conclude that

$$\left|\mathbf{h}_{22}^H\mathbf{N}\mathbf{g}(\lambda_2)\right|^2 \geq \left|\mathbf{h}_{22}^H\mathbf{N}\mathbf{g}(\lambda_1)\right|^2. \quad (54)$$

Hence, from (52) and (54), the monotonic properties are proved for the case $0 = \lambda_1 < \lambda_2 \leq 1$.

2) Case 2: $0 < \lambda_1 < \lambda_2 \leq 1$.
In this case, we can rewrite (50) and (51) as

$$\left|\mathbf{h}_{22}^H\mathbf{N}\mathbf{g}(\lambda_2)\right|^2 - \left|\mathbf{h}_{22}^H\mathbf{N}\mathbf{g}(\lambda_1)\right|^2 \leq \frac{1-\lambda_1}{\lambda_1}\left(\left|\mathbf{h}_{e2}^H\mathbf{N}\mathbf{g}(\lambda_1)\right|^2 - \left|\mathbf{h}_{e2}^H\mathbf{N}\mathbf{g}(\lambda_2)\right|^2\right), \quad (55)$$

and

$$\left|\mathbf{h}_{22}^H\mathbf{N}\mathbf{g}(\lambda_2)\right|^2 - \left|\mathbf{h}_{22}^H\mathbf{N}\mathbf{g}(\lambda_1)\right|^2 \geq \frac{1-\lambda_2}{\lambda_2}\left(\left|\mathbf{h}_{e2}^H\mathbf{N}\mathbf{g}(\lambda_1)\right|^2 - \left|\mathbf{h}_{e2}^H\mathbf{N}\mathbf{g}(\lambda_2)\right|^2\right). \quad (56)$$

Combining (55) with (56), we have

$$\frac{1-\lambda_2}{\lambda_2}\left(\left|\mathbf{h}_{e2}^H\mathbf{N}\mathbf{g}(\lambda_1)\right|^2 - \left|\mathbf{h}_{e2}^H\mathbf{N}\mathbf{g}(\lambda_2)\right|^2\right) \leq \frac{1-\lambda_1}{\lambda_1}\left(\left|\mathbf{h}_{e2}^H\mathbf{N}\mathbf{g}(\lambda_1)\right|^2 - \left|\mathbf{h}_{e2}^H\mathbf{N}\mathbf{g}(\lambda_2)\right|^2\right),$$

Then, we can conclude that

$$\left(\frac{1}{\lambda_1} - \frac{1}{\lambda_2}\right)\left(\left|\mathbf{h}_{e2}^H\mathbf{N}\mathbf{g}(\lambda_1)\right|^2 - \left|\mathbf{h}_{e2}^H\mathbf{N}\mathbf{g}(\lambda_2)\right|^2\right) \geq 0.$$

Since $\frac{1}{\lambda_1} > \frac{1}{\lambda_2}$, we can obtain the expression in (52). Furthermore, substituting (52) into (56), we can obtain the expression in (54). Accordingly, the monotonic properties are proved for the case $0 < \lambda_1 < \lambda_2 \leq 1$.

This completes the proof of **Proposition 2**. ■

APPENDIX B
PROOF OF PROPOSITION 3

Proof: The proof consists of two steps. First, we show that, compared with the CJ scheme, the modified CJ scenario creates more interference to Eve. Then, we compare the secrecy rate performance of these two strategies.

1) First step: Let $\mathbf{N}_c \in \mathbb{C}^{N_c\times(N_c-N_b)}$ and $\mathbf{N}_m \in \mathbb{C}^{N_c\times(N_c-1)}$ represent the orthonormal bases for null($\mathbf{H}_{12}$) and null($\mathbf{u}_c^H\mathbf{H}_{12}$), respectively. Then, we have

$$\Pi^{\perp}_{\mathbf{H}_{12}^H} = \mathbf{N}_c\mathbf{N}_c^H, \quad \Pi^{\perp}_{\mathbf{H}_{12}^H\mathbf{u}_c} = \mathbf{N}_m\mathbf{N}_m^H. \quad (57)$$

Given $\mathbf{w}_c$ in (20) is utilized to generate AN, the interference created by Charlie in the CJ scheme can be calculated as

$$\begin{aligned} P_2\left|\mathbf{h}_{e2}^H\mathbf{w}_c\right|^2 &= \frac{P_2\left|\mathbf{h}_{e2}^H\Pi^{\perp}_{\mathbf{H}_{12}^H}\mathbf{h}_{e2}\right|^2}{\left\|\Pi^{\perp}_{\mathbf{H}_{12}^H}\mathbf{h}_{e2}\right\|^2} \\ &= \frac{P_2\left(\mathbf{h}_{e2}^H\Pi^{\perp}_{\mathbf{H}_{12}^H}\mathbf{h}_{e2}\right)^2}{\mathbf{h}_{e2}^H\left(\Pi^{\perp}_{\mathbf{H}_{12}^H}\right)^H\Pi^{\perp}_{\mathbf{H}_{12}^H}\mathbf{h}_{e2}} \\ &= P_2\mathbf{h}_{e2}^H\left(\mathbf{N}_c\mathbf{N}_c^H\right)\mathbf{h}_{e2}. \end{aligned}$$

Here, the third equation follows from the fact that for any orthogonal projection matrix $\mathbf{P}$, we have

$$\mathbf{P}^H = \mathbf{P} = \mathbf{P}^2.$$

In addition, given $\mathbf{w}_m$ in (26) is utilized to generate AN, the interference created by Charlie in the modified CJ scheme can be calculated as

$$\begin{aligned} P_2\left|\mathbf{h}_{e2}^H\mathbf{w}_m\right|^2 &= \frac{P_2\left|\mathbf{h}_{e2}^H\Pi^{\perp}_{\mathbf{H}_{12}^H\mathbf{u}_c}\mathbf{h}_{e2}\right|^2}{\left\|\Pi^{\perp}_{\mathbf{H}_{12}^H\mathbf{u}_c}\mathbf{h}_{e2}\right\|^2} \\ &= P_2\mathbf{h}_{e2}^H\left(\mathbf{N}_m\mathbf{N}_m^H\right)\mathbf{h}_{e2}. \end{aligned}$$

Then, the difference between the above two interferences can be calculated as

$$\begin{aligned} &P_2\left|\mathbf{h}_{e2}^H\mathbf{w}_m\right|^2 - P_2\left|\mathbf{h}_{e2}^H\mathbf{w}_c\right|^2 \\ &\quad = P_2\mathbf{h}_{e2}^H\left(\mathbf{N}_m\mathbf{N}_m^H - \mathbf{N}_c\mathbf{N}_c^H\right)\mathbf{h}_{e2}. \end{aligned} \quad (58)$$

To compare these two interferences, we need the following lemma.

Lemma 1: $\mathbf{N}_m\mathbf{N}_m^H - \mathbf{N}_c\mathbf{N}_c^H$ in (58) is a PSD matrix.

Proof: Since null $(\mathbf{H}_{12}) \subseteq$ null $\left(\mathbf{u}_c^H\mathbf{H}_{12}\right)$, there must exist a matrix $\mathbf{A}$ such that $\mathbf{N}_m\mathbf{A} = \mathbf{N}_c$. Accordingly, we can infer that

$$\begin{aligned} &\mathbf{N}_m\mathbf{N}_m^H\left(\mathbf{N}_c\mathbf{N}_c^H\right)\mathbf{N}_m\mathbf{N}_m^H \\ &\quad = \mathbf{N}_m\mathbf{N}_m^H\left(\mathbf{N}_m\mathbf{A}\mathbf{A}^H\mathbf{N}_m^H\right)\mathbf{N}_m\mathbf{N}_m^H \\ &\quad = \mathbf{N}_m\mathbf{A}\mathbf{A}^H\mathbf{N}_m^H \\ &\quad = \mathbf{N}_c\mathbf{N}_c^H. \end{aligned} \quad (59)$$

Furthermore, from (59), we have

$$\begin{aligned} &\mathbf{N}_m\mathbf{N}_m^H - \mathbf{N}_c\mathbf{N}_c^H \\ &\quad = \mathbf{N}_m\mathbf{N}_m^H - \mathbf{N}_m\mathbf{N}_m^H\left(\mathbf{N}_c\mathbf{N}_c^H\right)\mathbf{N}_m\mathbf{N}_m^H \\ &\quad = \left(\mathbf{N}_m\mathbf{N}_m^H\right)\left(\mathbf{I} - \mathbf{N}_c\mathbf{N}_c^H\right)\left(\mathbf{N}_m\mathbf{N}_m^H\right)^H. \end{aligned}$$

It can be demonstrated that both $\mathbf{N}_m\mathbf{N}_m^H$ and $\mathbf{I}-\mathbf{N}_c\mathbf{N}_c^H$ are orthogonal projection matrices, and thus are PSD. Accordingly, the matrix $\mathbf{N}_m\mathbf{N}_m^H-\mathbf{N}_c\mathbf{N}_c^H$ is PSD. ■

According to (58) and **Lemma 1**, we can conclude that $P_2\left|\mathbf{h}_{e2}^H\mathbf{w}_m\right|^2 \geq P_2\left|\mathbf{h}_{e2}^H\mathbf{w}_c\right|^2$. Specifically, the equality holds only when the following condition are satisfied.

$$\begin{aligned}
&P_2\left|\mathbf{h}_{e2}^H\mathbf{w}_m\right|^2 = P_2\left|\mathbf{h}_{e2}^H\mathbf{w}_c\right|^2\\
&\Longleftrightarrow\ \mathbf{h}_{e2}^H\left(\mathbf{N}_m\mathbf{N}_m^H-\mathbf{N}_c\mathbf{N}_c^H\right)\mathbf{h}_{e2}=0\\
&\Longleftrightarrow\ \left(\mathbf{N}_m\mathbf{N}_m^H-\mathbf{N}_c\mathbf{N}_c^H\right)^{\frac{1}{2}}\mathbf{h}_{e2}=\mathbf{0}\\
&\Longleftrightarrow\ \mathbf{h}_{e2}\in\text{null}\left(\mathbf{N}_m\mathbf{N}_m^H-\mathbf{N}_c\mathbf{N}_c^H\right)^{\frac{1}{2}}
\end{aligned}$$

However, The probability of this occurrence is very small, given that all channels are assumed to be independently distributed. Therefore, compared with the CJ scheme, the modified scenario almost surely creates more interferences, i.e., $P_2\left|\mathbf{h}_{e2}^H\mathbf{w}_m\right|^2 > P_2\left|\mathbf{h}_{e2}^H\mathbf{w}_c\right|^2$.

2) Second step: Similar to the derivation of (21), we can conclude that

$$\mu_{\max}(\mathbf{Z}_1)=\mu_{\max}(\mathbf{Z}_2)$$

where $\mathbf{Z}_2=\left(\mathbf{I}+\frac{P_1\mathbf{h}_{e1}\mathbf{h}_{e1}^H}{1+P_2\left|\mathbf{h}_{e2}^H\mathbf{w}_c\right|^2}\right)^{-1}\left(\mathbf{I}+P_1\mathbf{H}_{11}^H\mathbf{u}_c\mathbf{u}_c^H\mathbf{H}_{11}\right)$, and $\mathbf{Z}_1$ is given in (24).

For simplicity, we define new matrices

$$\mathbf{A}_1=\left(\mathbf{I}+\frac{P_1\mathbf{h}_{e1}\mathbf{h}_{e1}^H}{1+P_2\left|\mathbf{h}_{e2}^H\mathbf{w}_c\right|^2}\right)^{-1}, \tag{60}$$

$$\mathbf{A}_2=\left(\mathbf{I}+\frac{P_1\mathbf{h}_{e1}\mathbf{h}_{e1}^H}{1+P_2\left|\mathbf{h}_{e2}^H\mathbf{w}_m\right|^2}\right)^{-1}, \tag{61}$$

$$\mathbf{B}=\mathbf{I}+P_1\mathbf{H}_{11}^H\mathbf{u}_c\mathbf{u}_c^H\mathbf{H}_{11}.$$

It can be shown that $\mathbf{A}_1$, $\mathbf{A}_2$, and $\mathbf{B}$ are all positive definite (PD) matrices. Therefore, both $\mathbf{B}^{\frac{1}{2}}\mathbf{A}_1\mathbf{B}^{\frac{1}{2}}$ and $\mathbf{B}^{\frac{1}{2}}\mathbf{A}_2\mathbf{B}^{\frac{1}{2}}$ are PD matrices. In addition, the secrecy rate expressions in (25) and (29) can be rewritten as

$$\begin{aligned}
R_{s1}&=\left[\log_2\left(\mu_{\max}(\mathbf{Z}_1)\right)\right]^+\\
&=\left[\log_2\left(\mu_{\max}(\mathbf{Z}_2)\right)\right]^+\\
&=\left[\log_2\left(\mu_{\max}(\mathbf{A}_1\mathbf{B})\right)\right]^+, \qquad (62)\\
R_s&=\left[\log_2\left(\mu_{\max}(\mathbf{Z})\right)\right]^+\\
&=\left[\log_2\left(\mu_{\max}(\mathbf{A}_2\mathbf{B})\right)\right]^+. \qquad (63)
\end{aligned}$$

To compare R_{s1} in (62) with R_s in (63), we need the following two lemmas.

Lemma 2: Given both $\mathbf{C}$ and $\mathbf{D}$ are PD matrices, then we have $\mathbf{CD}$ is similar to $\mathbf{D}^{\frac{1}{2}}\mathbf{CD}^{\frac{1}{2}}$, and all eigenvalues of $\mathbf{CD}$ are positive.

Proof: Since $\mathbf{C}\succ\mathbf{0}$ and $\mathbf{D}\succ\mathbf{0}$, we can verify that $\mathbf{D}^{\frac{1}{2}}\succ\mathbf{0}$, $\mathbf{D}^{-\frac{1}{2}}\succ\mathbf{0}$, and $\mathbf{D}^{\frac{1}{2}}\mathbf{CD}^{\frac{1}{2}}\succ\mathbf{0}$. Besides, the matrix $\mathbf{CD}$ can be rewritten as

$$\mathbf{CD}=\mathbf{D}^{-\frac{1}{2}}\left(\mathbf{D}^{\frac{1}{2}}\mathbf{CD}^{\frac{1}{2}}\right)\mathbf{D}^{\frac{1}{2}}.$$

Accordingly, we can conclude that $\mathbf{CD}$ is similar to $\mathbf{D}^{\frac{1}{2}}\mathbf{CD}^{\frac{1}{2}}$. Then all eigenvalues of $\mathbf{CD}$ and $\mathbf{D}^{\frac{1}{2}}\mathbf{CD}^{\frac{1}{2}}$ are equal. Since $\mathbf{D}^{\frac{1}{2}}\mathbf{CD}^{\frac{1}{2}}\succ\mathbf{0}$, all eigenvalues of $\mathbf{D}^{\frac{1}{2}}\mathbf{CD}^{\frac{1}{2}}$ are positive. This completes the proof of **Lemma 2**. ■

Lemma 3: Given $\mathbf{E}\succ\mathbf{F}\succ\mathbf{0}$, then we have $\mu_{\max}(\mathbf{E})>\mu_{\max}(\mathbf{F})>0$.

Proof: The derivation is as follows.

$$\begin{aligned}
&\mathbf{E}\succ\mathbf{F}\succ\mathbf{0}\\
&\Longrightarrow\ \frac{\mathbf{x}^H(\mathbf{E}-\mathbf{F})\mathbf{x}}{\mathbf{x}^H\mathbf{x}}>0, \quad \forall\mathbf{x}\neq\mathbf{0}\\
&\Longrightarrow\ \frac{\mathbf{x}^H\mathbf{E}\mathbf{x}}{\mathbf{x}^H\mathbf{x}}>\frac{\mathbf{x}^H\mathbf{F}\mathbf{x}}{\mathbf{x}^H\mathbf{x}}>0, \quad \forall\mathbf{x}\neq\mathbf{0}\\
&\Longrightarrow\ \max\frac{\mathbf{x}^H\mathbf{E}\mathbf{x}}{\mathbf{x}^H\mathbf{x}}>\max\frac{\mathbf{y}^H\mathbf{E}\mathbf{y}}{\mathbf{y}^H\mathbf{y}}>0,\ \forall\mathbf{x}\neq0,\ \mathbf{y}\neq0\\
&\Longrightarrow\ \mu_{\max}(\mathbf{E})>\mu_{\max}(\mathbf{F})>0.
\end{aligned}$$

This completes the proof of **Lemma 3**. ■

By **Lemma 2**, we can conclude that

$$\begin{aligned}
\mu_{\max}(\mathbf{A}_1\mathbf{B})&=\mu_{\max}\left(\mathbf{B}^{\frac{1}{2}}\mathbf{A}_1\mathbf{B}^{\frac{1}{2}}\right)>0,\\
\mu_{\max}(\mathbf{A}_2\mathbf{B})&=\mu_{\max}\left(\mathbf{B}^{\frac{1}{2}}\mathbf{A}_2\mathbf{B}^{\frac{1}{2}}\right)>0.
\end{aligned}$$

According to (60)-(61), it can be shown that

$$\begin{aligned}
&\mathbf{A}_1^{-1}-\mathbf{A}_2^{-1}\\
&=\left(\frac{1}{1+P_2\left|\mathbf{h}_{e2}^H\mathbf{w}_c\right|^2}-\frac{1}{1+P_2\left|\mathbf{h}_{e2}^H\mathbf{w}_m\right|^2}\right)P_1\mathbf{h}_{e1}\mathbf{h}_{e1}^H.
\end{aligned}$$

Since $P_2\left|\mathbf{h}_{e2}^H\mathbf{w}_m\right|^2 > P_2\left|\mathbf{h}_{e2}^H\mathbf{w}_c\right|^2$, we can conclude that $\mathbf{A}_1^{-1}\succeq\mathbf{A}_2^{-1}\succ\mathbf{0}$. Hence, we have $\mathbf{A}_2\succeq\mathbf{A}_1\succ\mathbf{0}$. Furthermore, we can obtain

$$\mathbf{B}^{\frac{1}{2}}\mathbf{A}_2\mathbf{B}^{\frac{1}{2}}\succeq\mathbf{B}^{\frac{1}{2}}\mathbf{A}_1\mathbf{B}^{\frac{1}{2}}\succ\mathbf{0}.$$

Then, according to **Lemma 2** and **Lemma 3**, we can conclude that

$$\begin{aligned}
&\mu_{\max}\left(\mathbf{B}^{\frac{1}{2}}\mathbf{A}_2\mathbf{B}^{\frac{1}{2}}\right)\geq\mu_{\max}\left(\mathbf{B}^{\frac{1}{2}}\mathbf{A}_1\mathbf{B}^{\frac{1}{2}}\right)>0\\
&\Longleftrightarrow\ \mu_{\max}(\mathbf{A}_2\mathbf{B})\geq\mu_{\max}(\mathbf{A}_1\mathbf{B})>0\\
&\Longleftrightarrow\ \mu_{\max}(\mathbf{Z})\geq\mu_{\max}(\mathbf{Z}_2)=\mu_{\max}(\mathbf{Z}_1)>0
\end{aligned}$$

Finally, from (62)-(63), we can conclude that

$$\begin{cases}
R_s\geq R_{s1}>0, & \text{if } \mu_{\max}(\mathbf{Z}_1)>1\\
R_s>R_{s1}=0, & \text{if } \mu_{\max}(\mathbf{Z}_1)\leq1<\mu_{\max}(\mathbf{Z})\\
R_s=R_{s1}=0, & \text{if } \mu_{\max}(\mathbf{Z})\leq1
\end{cases}$$

This completes the proof of **Proposition 3**. ■

ACKNOWLEDGMENT

The authors would like to thank Mr. Zhen-Qing He for many fruitful discussions and comments on the draft of this paper. They would also like to thank the anonymous reviewers for their excellent suggestions.

REFERENCES

[1] J. Su, Z. Sheng, G. Wen, and V. C. M. Leung, "A time efficient tag identification algorithm using dual prefix probe scheme (DPPS)," *IEEE Signal Process. Lett.*, vol. 23, no. 3, pp. 386–389, Mar. 2016.

[2] N. Yang, L. Wang, G. Geraci, M. Elkashlan, J. Yuan, and M. Di Renzo, "Safeguarding 5G wireless communication networks using physical layer security," *IEEE Commun. Mag.*, vol. 53, no. 4, pp. 20–27, Apr. 2015.

[3] B. Schneier, "Cryptographic design vulnerabilities," *Computer*, vol. 31, no. 9, pp. 29–33, Sep. 1998.

[4] A. Barenghi, L. Breveglieri, I. Koren, and D. Naccache, "Fault injection attacks on cryptographic devices: Theory, practice, and countermeasures," *Proc. IEEE*, vol. 100, no. 11, pp. 3056–3076, Nov. 2012.

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

[6] H. Wen, *Physical Layer Approaches for Securing Wireless Communication Systems*. New York, NY, USA: Springer-Verlag, Feb. 2013.

[7] X. Zhou, L. Song, and Y. Zhang, *Physical Layer Security in Wireless Communications*. Boca Raton, FL, USA: CRC Press, 2013.

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

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

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

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

[12] Y.-W. P. Hong, P.-C. Lan, and C.-C. J. Kuo, "Enhancing physical-layer secrecy in multiantenna wireless systems: An overview of signal processing approaches," *IEEE Signal Process. Mag.*, vol. 30, no. 5, pp. 29–40, Sep. 2013.

[13] H. Wen *et al.*, "A cross-layer secure communication model based on discrete fractional Fourier transform (DFRFT)" *IEEE Trans. Emerg. Topics Comput.*, vol. 3, no. 1, pp. 119–126, Mar. 2015.

[14] H. Wen, P.-H. Ho, and B. Wu, "Achieving secure communications over wiretap channels via security codes from resilient functions," *IEEE Wireless Commun. Lett.*, vol. 3, no. 3, pp. 273–276, Jun. 2014.

[15] 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, Jul. 2010.

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

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

[18] H.-M. Wang, T.-X. Zheng, and X.-G. Xia, "Secure MISO wiretap channels with multiantenna passive eavesdropper: Artificial noise vs. artificial fast fading," *IEEE Trans. Wireless Commun.*, vol. 14, no. 1, pp. 94–106, Jan. 2015.

[19] P.-H. Lin, S.-H. Lai, S.-C. Lin, and H.-J. Su, "On secrecy rate of the generalized artificial-noise assisted secure beamforming for wiretap channels," *IEEE J. Sel. Areas Commun.*, vol. 31, no. 9, pp. 1728–1740, Sep. 2013.

[20] X. Zhang, X. Zhou, and M. R. McKay, "On the design of artificial-noise-aided secure multi-antenna transmission in slow fading channels," *IEEE Trans. Veh. Technol.*, vol. 62, no. 5, pp. 2170–2181, Jun. 2013.

[21] B. Wang, P. Mu, and Z. Li, "Secrecy rate maximization with artificial-noise-aided beamforming for MISO wiretap channels under secrecy outage constraint," *IEEE Commun. Lett.*, vol. 19, no. 1, pp. 18–21, Jan. 2015.

[22] J. Tang *et al.*, "Associating MIMO beamforming with security codes to achieve unconditional communication security," *IET Commun.*, vol. 10, no. 12, pp. 1522–1531, Aug. 2016.

[23] T.-X. Zheng, H.-M. Wang, J. Yuan, D. Towsley, and M. H. Lee, "Multi-antenna transmission with artificial noise against randomly distributed eavesdroppers," *IEEE Trans. Commun.*, vol. 63, no. 11, pp. 4347–4362, Nov. 2015.

[24] T.-X. Zheng and H.-M. Wang, "Optimal power allocation for artificial noise under imperfect CSI against spatially random eavesdroppers," *IEEE Trans. Veh. Technol.*, 2016, doi: 10.1109/TVT.2015.2513003.

[25] R. Bassily *et al.*, "Cooperative security at the physical layer: A summary of recent advances," *IEEE Signal Process. Mag.*, vol. 30, no. 5, pp. 16–28, Sep. 2013.

[26] L. J. Rodriguez, N. H. Tran, T. Q. Duong, T. Le-Ngoc, M. Elkashlan, and S. Shetty, "Physical layer security in wireless cooperative relay networks: State of the art and beyond," *IEEE Commun. Mag.*, vol. 53, no. 12, pp. 32–39, Dec. 2015.

[27] H.-M. Wang and X.-G. Xia, "Enhancing wireless secrecy via cooperation: Signal design and optimization," *IEEE Commun. Mag.*, vol. 53, no. 12, pp. 47–53, Dec. 2015.

[28] L. Dong, Z. Han, A. P. Petropulu, and H. V. Poor, "Improving wireless physical layer security via cooperating relays," *IEEE Trans. Signal Process.*, vol. 58, no. 3, pp. 1875–1888, Mar. 2010.

[29] H.-M. Wang, M. Luo, X.-G. Xia, and Q. Yin, "Joint cooperative beamforming and jamming to secure AF relay systems with individual power constraint and no eavesdropper's CSI," *IEEE Signal Process. Lett.*, vol. 20, no. 1, pp. 39–42, Jan. 2013.

[30] D. Wang, B. Bai, W. Chen, and Z. Han, "Secure green communication for amplify-and-forward relaying with eavesdroppers," in *Proc. IEEE ICC*, Jun. 2015, pp. 4468–4473.

[31] T. X. Zheng, H. M. Wang, F. Liu, and M. H. Lee, "Outage constrained secrecy throughput maximization for DF relay networks," *IEEE Trans. Commun.*, vol. 63, no. 5, pp. 1741–1755, May 2015.

[32] C. Wang, H.-M. Wang, and X.-G. Xia, "Hybrid opportunistic relaying and jamming with power allocation for secure cooperative networks," *IEEE Trans. Wireless Commun.*, vol. 14, no. 2, pp. 589–605, Feb. 2015.

[33] H. Deng, H. M. Wang, W. Guo, and W. Wang, "Secrecy transmission with a helper: To relay or to jam," *IEEE Trans. Inf. Forensics Security*, vol. 10, no. 2, pp. 293–307, Feb. 2015.

[34] J. H. Lee and W. Choi, "Multiuser diversity for secrecy communications using opportunistic jammer selection: Secure DoF and jammer scaling law," *IEEE Trans. Signal Process.*, vol. 62, no. 4, pp. 828–839, Feb. 2014.

[35] P. Mu, X. Hu, B. Wang, and Z. Li, "Secrecy rate maximization with uncoordinated cooperative jamming by single-antenna helpers under secrecy outage probability constraint," *IEEE Commun. Lett.*, vol. 19, no. 12, pp. 2174–2177, Dec. 2015.

[36] C. Wang, H. M. Wang, X. G. Xia, and C. Liu, "Uncoordinated jammer selection for securing SIMOME wiretap channels: A stochastic geometry approach," *IEEE Trans. Wireless Commun.*, vol. 14, no. 5, pp. 2596–2612, May 2015.

[37] Z. Chu, K. Cumanan, Z. Ding, M. Johnston, and S. Le Goff, "Secrecy rate optimizations for a MIMO secrecy channel with a cooperative jammer," *IEEE Trans. Veh. Technol.*, vol. 64, no. 5, pp. 1833–1847, May 2015.

[38] L. Hu, B. Wu, J. Tang, F. Pan, and H. Wen, "Outage constrained secrecy rate maximization using artificial-noise aided beamforming and cooperative jamming," in *Proc. IEEE ICC*, May 2016, pp. 1–5.

[39] H.-M. Wang, Q. Yin, and X.-G. Xia, "Distributed beamforming for physical-layer security of two-way relay networks," *IEEE Trans. Signal Process.*, vol. 60, no. 7, pp. 3532–3545, Jul. 2012.

[40] H.-M. Wang, M. Luo, Q. Yin, and X.-G. Xia, "Hybrid cooperative beamforming and jamming for physical-layer security of two-way relay networks," *IEEE Trans. Inf. Forensics Security*, vol. 8, no. 12, pp. 2007–2020, Dec. 2013.

[41] X. Chen and Y. Zhang, "Mode selection in MU-MIMO downlink networks: A physical-layer security perspective," *IEEE Syst. J.*, 2015, doi: 10.1109/JSYST.2015.2413843.

[42] B. He, N. Yang, X. Zhou, and J. Yuan, "Base station cooperation for confidential broadcasting in multi-cell networks," *IEEE Trans. Wireless Commun.*, vol. 14, no. 10, pp. 5287–5299, Oct. 2015.

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

[44] 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.

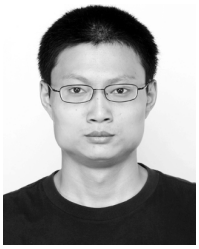
[45] A. Mukherjee and A. L. Swindlehurst, "Detecting passive eavesdroppers in the MIMO wiretap channel," in *Proc. IEEE ICASSP*, Mar. 2012, pp. 2809–2812.

[46] M. Bloch, J. Barros, M. R. D. Rodrigues, and S. W. McLaughlin, "Wireless information-theoretic security," *IEEE Trans. Inf. Theory*, vol. 54, no. 6, pp. 2515–2534, Jun. 2008.

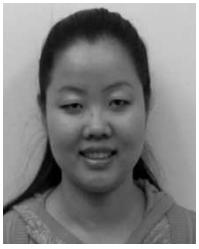
[47] R. Mochaourab and E. A. Jorswieck, "Optimal beamforming in interference networks with perfect local channel information," *IEEE Trans. Signal Process.*, vol. 59, no. 3, pp. 1128–1141, Mar. 2011.

[48] 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.

[49] G. H. Golub and C. F. Van Loan, *Matrix Computations*. Baltimore, MD, USA: The Johns Hopkins Univ. Press, 2012.



LIN HU is currently pursuing the registered Ph.D. degree with the National Key Lab of Communications, University of Electronic Science and Technology of China, Chengdu, China. His research interests include physical layer security of wireless communications, convex optimization for signal processing, and cooperative communication systems.



HONG WEN was born in Chengdu, China. She received the M.Sc. degree in electrical engineering from the Sichuan Union University of Sichuan, China, in 1997, and the Ph.D. degree from the Communication and Computer Engineering Department, Southwest Jiaotong University, Chengdu. She was an Associate Professor with the National Key Laboratory of Science and Technology on Communications, UESTC, China. From 2008 to 2009, she was a Visiting Scholar and a Post-Doctoral Fellow with the ECE Department, University of Waterloo. She holds the professor position with UESTC, China. Her major interests focus on wireless communication systems.

BIN WU (S'04–M'07) received the Ph.D. degree in electrical and electronic engineering from the University of Hong Kong, Hong Kong, in 2007. He was a Post-Doctoral Research Fellow with the Department of Electrical and Computer Engineering, University of Waterloo, Waterloo, ON, Canada, from 2007 to 2012. He is currently a Professor with the School of Computer Science and Technology, Tianjin University, Tianjin, China. His research interests include computer systems and networking, IP, optical and wireless communications and networking, and network survivability and security issues.

JIE TANG was born in Chengdu, China. He is currently pursuing the Ph.D. degree in communication and information system with the National Key Laboratory of Science and Technology on Communications, Chengdu. His current main interests lie in wireless communication system and information security.

FEI PAN was born in Yaan, China. She received the bachelor's degree from Northwest University, China, in 2011. She is currently pursuing the Ph.D. degree in communication and information system with the National Key Laboratory of Science and Technology on Communications, University of Electronic Science and Technology of China, Chengdu. Her current main interests lie in wireless communication systems security.