Cooperative Jamming for Secure Communications in MIMO Relay Networks

Jing Huang, *Student Member, IEEE*, and A. Lee Swindlehurst, *Fellow, IEEE*

***Abstract*—Secure communications can be impeded by eavesdroppers in conventional relay systems. This paper proposes cooperative jamming strategies for two-hop relay networks where the eavesdropper can wiretap the relay channels in both hops. In these approaches, the normally inactive nodes in the relay network can be used as cooperative jamming sources to confuse the eavesdropper. Linear precoding schemes are investigated for two scenarios where single or multiple data streams are transmitted via a decode-and-forward (DF) relay, under the assumption that global channel state information (CSI) is available. For the case of single data stream transmission, we derive closed-form jamming beamformers and the corresponding optimal power allocation. Generalized singular value decomposition (GSVD)-based secure relaying schemes are proposed for the transmission of multiple data streams. The optimal power allocation is found for the GSVD relaying scheme via geometric programming. Based on this result, a GSVD-based cooperative jamming scheme is proposed that shows significant improvement in terms of secrecy rate compared to the approach without jamming. Furthermore, the case involving an eavesdropper with unknown CSI is also investigated in this paper. Simulation results show that the secrecy rate is dramatically increased when inactive nodes in the relay network participate in cooperative jamming.**

***Index Terms*—Interference, jamming, physical layer security, relay networks, secrecy, wiretap channel.**

I. Introduction

SECURITY is an important concern in wireless networks due to their vulnerability to eavesdropping. Traditionally, security is viewed as an issue addressed above the physical (PHY) layer, and all widely used cryptographic protocols are designed and implemented assuming the physical layer has already been established and provides an error-free link [1]. However, higher-layer key distribution and management may be difficult to implement and vulnerable to attack in complex environments such as *ad-hoc* or relay networks, in which transceivers may join or leave randomly [2], [3]. Therefore, there has recently been considerable interest in physical layer security, which explores the characteristics of the wireless channel to improve wireless transmission security.

The theoretical basis of this area was laid by Wyner, who introduced the wiretap channel and demonstrated that when the eavesdropper's channel is a degraded version of the channel of the legitimate receiver, the transmitter can send secret messages to the destination while keeping the eavesdropper from learning anything about the message [4]. The notion of secrecy capacity was introduced and defined as the maximum achievable transmission rate of confidential information from the source to its intended receiver. Later, Csiszár and Körner generalized Wyner's approach by considering the transmission of secret messages over broadcast channels [5]. Recently, considerable research has examined secrecy in wiretap channels with multiple antennas [6]–[14]. In particular, the secrecy capacity of the multiple-input multiple-output (MIMO) wiretap channel has been fully characterized in [10], [11]. With the additional degrees of freedom provided by multi-antenna systems, transmitters can generate artificial noise to degrade the channel condition of the eavesdropper while maintaining little interference to legitimate users [13]–[16].

As a natural extension, approaches for physical layer security have also been investigated in cooperative relaying networks [17]–[22]. In these cases, relays or even destinations can be used as helpers to provide jamming signals to confuse the eavesdropper. This approach is often referred to as cooperative jamming. In [20], a noise-forwarding strategy is introduced for a four-terminal relay-eavesdropper channel where the full-duplex relay sends codewords independent of the secret message to confuse the eavesdropper. A two-stage cooperative jamming protocol is investigated in [14], where multiple relay nodes act as an extension of the single-antenna source node. In this work, the "relays" only play the role of a helper and do not relay the information signals. In [21], three cooperative schemes are proposed for a single-antenna relay network, and the corresponding relay weights and power allocation strategy are derived to enhance the secrecy for the second hop. An optimal beamforming design for decode-and-forward (DF) relays is investigated in [22], but only the scenario where the eavesdropper wiretaps just the link between the relay and destination is considered.

Unlike the aforementioned work, this paper proposes cooperative jamming strategies for a half-duplex two-hop wireless MIMO relay system in which the eavesdropper can wiretap the channels during both transmission phases. Cases involving both single and multiple data stream transmissions are investigated. Due to the lack of "outer" helpers, the source, relay and destination must rely on themselves for jamming support. This approach guarantees that the eavesdropper is jammed whether it

Manuscript received October 31, 2010; revised February 08, 2011 and April 21, 2011; accepted June 19, 2011. Date of publication July 05, 2011; date of current version September 14, 2011. The associate editor coordinating the review of this manuscript and approving it for publication was Prof. Huaiyu Dai. This work was supported by the U.S. Army Research Office under the Multi-University Research Initiative (MURI) Grant W911NF-07-1-0318. The material in this paper was presented at the IEEE GLOBECOM 2010 and at ICASSP 2011.

The authors are with the Department of Electrical Engineering and Computer Science, University of California, Irvine, CA 92697 USA (e-mail: jing.huang@uci.edu; swindle@uci.edu).

Color versions of one or more of the figures in this paper are available online at http://ieeexplore.ieee.org.

Digital Object Identifier 10.1109/TSP.2011.2161295

is close to the source or the destination. In the proposed cooperative jamming strategies, the source and the destination nodes act as temporary helpers to transmit jamming signals during the transmission phases in which they are normally inactive. We define two types of cooperative jamming schemes, *full cooperative jamming* (FCJ) and *partial cooperative jamming* (PCJ), depending on whether or not both the transmitter and the temporary helper transmit jamming signals at the same time.

We focus on the design of linear precoding schemes throughout the paper, and begin with a simple scenario where the relay has only a single antenna. In this case, we investigate the joint design of the jamming beamformer and the power allocation for two optimization problems: (1) maximizing the secrecy rate with certain power constraints, and (2) minimizing the transmit power with a fixed target secrecy rate. Since a joint optimization of the beamformers and power allocation is in general intractable even if global CSI is available, we use a suboptimal zero-forcing constraint that the jamming and information signals lie in orthogonal subspaces when received by the legitimate nodes, and we derive closed-form expressions for the jamming beamformers. Based on these results, we find the optimal solution for the power allocation by utilizing the method of geometric programming (GP). Then we expand the scope to study the scenario where all nodes have multiple antennas, and multiple data streams are transmitted via the relay. A generalized singular value decomposition (GSVD)-based cooperative jamming scheme is proposed and the corresponding power allocation strategy is discussed. Unlike the single data stream case that uses a zero-forcing constraint, the cooperative GSVD-based jamming method will not in general produce jamming signals that are orthogonal to the desired signal.

Another important consideration is the availability of the eavesdropper's CSI. If the CSI of the eavesdropper is known, (for example, if the eavesdropper is another active user in the wireless network), the transmitter can optimize its beamformer to enhance the information transmission to intended nodes while suppressing or even eliminating the leakage to eavesdroppers. However, in some cases (e.g., passive eavesdroppers), it is impractical to assume known CSI for the eavesdroppers. Since the secrecy rate can not be optimized without knowledge of the eavesdropper's CSI, we will follow the approach of [15], [23]–[25], where the transmitter first allocates part of its resources to guarantee a fixed target rate, and then uses the remaining resources to jam the eavesdropper.

The organization of the paper is as follows. Section II describes the system model considered throughout the paper. In Section III, the cooperative jamming schemes, including the jamming beamformer design and power allocation, is investigated when the eavesdropper's CSI is known. Both single and multiple data stream transmissions are considered in this section. Secure relaying under the assumption of unknown eavesdropper's CSI is studied in Section IV. The performance of the proposed cooperative jamming schemes are discussed in Section V, and conclusions are drawn in Section VI.

The following notation is used in the paper: $\mathbb{E}\{\cdot\}$ denotes expectation, $(\cdot)^T$ the matrix transpose and $(\cdot)^H$ the Hermitian transpose. $\|\cdot\|$ represents the Euclidean norm, $|\cdot|$ is the absolute value, $[x]^+$ denotes $\max\{x, 0\}$, $\mathrm{tr}(\cdot)$ is the trace operator,

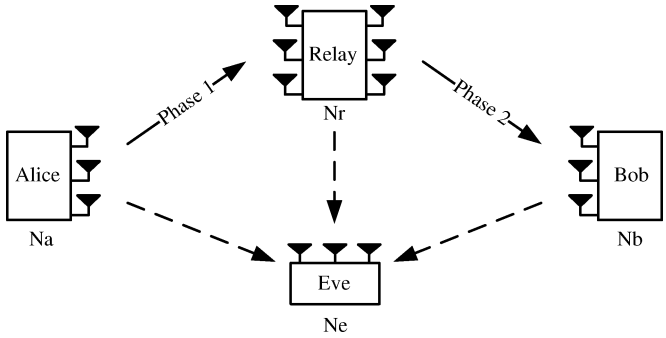

Fig. 1. Relay scenario.

$\mathcal{N}(\cdot)$ represents the null space, and $\mathbf{I}$ is an identity matrix of appropriate dimension.

II. System Model

We consider a two-phase four-terminal relay system composed of a source (Alice), a destination (Bob), a DF relay node and an eavesdropper (Eve), as shown in Fig. 1. The message from Alice is uniformly distributed over the message set $\mathcal{W} = \{1, \cdots, 2^{nR}\}$, where R denotes the source rate in bits per channel use. The confidential message is randomly mapped to a length-n source codeword $z_a^n \in \mathcal{Z}_a^n$ and the Relay encoder maps its received signal to codeword $z_r^n \in \mathcal{Z}_r^n$, where $\mathcal{Z}_a^n$ and $\mathcal{Z}_r^n$ are length-n input alphabets.

All nodes are assumed to be half-duplex, i.e., a two-hop time division multiple access system is considered. Alice transmits in the first phase while the relay listens, and relay transmits in the second phase. We assume there is no direct communication link between Alice and Bob, except perhaps for some low-rate control or channel state information, and thus Alice and Bob must rely on two-phase transmissions through the relay. This is a reasonable assumption in the type of scenarios where direct high-rate communication is too "expensive" in terms of the given power constraints, but low-rate control information can still be exchanged [19]. When Alice transmits a jamming signal, however, its impact on Bob's received signal must be taken into account. All nodes in general have multiple antennas. The number of antennas possessed by Alice, Bob, the Relay and Eve are denoted by N_a, N_b, N_r and N_e, respectively. In part of the paper, we will explicitly consider scenarios where the Relay has only a single antenna. We restrict attention to scenarios where all nodes (including the eavesdropper) employ linear precoding and receive beamforming.

A. Relay Transmission

In the first phase, Alice transmits the information signal to the Relay. Both the Relay and Eve will receive the signal as

$$\mathbf{y}_r = \mathbf{H}_{ar}\mathbf{T}_a\mathbf{z}_a + \mathbf{n}_r \tag{1}$$

$$\mathbf{y}_{e1} = \mathbf{H}_{ae}\mathbf{T}_a\mathbf{z}_a + \mathbf{n}_{e1} \tag{2}$$

where $\mathbf{z}_a$ is the information signal vector transmitted by Alice, $\mathbf{T}_a \in \mathbb{C}^{N_a \times k} (1 \le k \le s)$ is the transmit beamformer used by Alice, and we assume $m = rank\{\mathbf{H}_{ar}\}$, $n = rank\{\mathbf{H}_{rb}\}$, $s = \min(m, n)$ and k represents the number of data streams

to be transmitted. The terms $\mathbf{n}_r$ and $\mathbf{n}_{e1}$ represent naturally occurring noise at the Relay and Eve, respectively. For simplicity, we assume that the noise vectors at all nodes are Gaussian with covariance $\sigma^2\mathbf{I}$. In general, $\mathbf{H}_{ij}$ $(\mathbf{h}_{ij})$ represents the channel matrix from node i to j, with $i,j \in \{a,b,e,r\}$ denoting which of the four terminals is involved. These channel matrices are fixed over both hops. The signal received by Bob and Eve in the second transmission phase can be expressed as

$$\mathbf{y}_b = \mathbf{H}_{rb}\mathbf{T}_r\mathbf{z}_r + \mathbf{n}_b \tag{3}$$

$$\mathbf{y}_{e2} = \mathbf{H}_{re}\mathbf{T}_r\mathbf{z}_r + \mathbf{n}_{e2} \tag{4}$$

where $\mathbf{z}_r$ is the signal vector transmitted by the Relay, $\mathbf{T}_r \in \mathbb{C}^{N_r \times k}$ is the transmit beamformer used by the Relay, and $\mathbf{n}_b, \mathbf{n}_{e2}$ represent the noise vectors at Bob and Eve. There is a transmit power constraint P on both phases, i.e., $\mathbb{E}\{\mathbf{z}_a^H\mathbf{z}_a\} \leq P$ and $\mathbb{E}\{\mathbf{z}_r^H\mathbf{z}_r\} \leq P$. We assume a repetition-coding scheme, where $\mathbf{z}_r$ is simply a scaled version of $\mathbf{z}_a$. In particular, we assume $\mathbf{z}_a = \mathbf{D}_a\mathbf{z}$ and $\mathbf{z}_r = \mathbf{D}_r\mathbf{z}$, where $\mathbb{E}\{\mathbf{z}\mathbf{z}^H\} = \mathbf{I}$ and $\mathbf{D}_a, \mathbf{D}_r$ are diagonal power loading matrices that ensure the power constraints are met.

B. Cooperative Jamming

In the most general case, the signals transmitted by Alice in the first phase may contain both information and jamming signals, and Bob may also transmit jamming signals at the same time. Thus the signals received by the Relay and Eve in the first phase will be given by

$$\mathbf{y}_r = \mathbf{H}_{ar}\left(\mathbf{T}_a\mathbf{z}_a + \mathbf{T}'_a\mathbf{z}'_a\right) + \mathbf{H}_{br}\mathbf{T}'_b\mathbf{z}'_b + \mathbf{n}_r \tag{5}$$

$$\mathbf{y}_{e1} = \mathbf{H}_{ae}\left(\mathbf{T}_a\mathbf{z}_a + \mathbf{T}'_a\mathbf{z}'_a\right) + \mathbf{H}_{be}\mathbf{T}'_b\mathbf{z}'_b + \mathbf{n}_{e1} \tag{6}$$

where $\mathbf{z}'_a$ and $\mathbf{z}'_b$ are jamming signal vectors transmitted by Alice and Bob, respectively, and $\mathbf{T}'_a$ and $\mathbf{T}'_b$ are the corresponding transmit beamformers. In this paper, $\mathbf{T}'_a$ and $\mathbf{T}'_b$ could be chosen to project the jamming signals on the subspace orthogonal to the information signals, or they could allow a small amount of interference leakage to the legitimate receiver while producing more interference power at Eve, as will be discussed when the GSVD-based transmission strategy is used. We refer to the case where both $\mathbf{z}'_a \neq \mathbf{0}$ and $\mathbf{z}'_b \neq \mathbf{0}$ as *full cooperative jamming* (FCJ). If either of them is zero, we refer to it as *partial cooperative jamming* (PCJ). FCJ will not be considered in the scenario where Eve's CSI is known, since in this case splitting the power between data and jamming signals at Alice is known to be suboptimal. However, when Eve's CSI is known, we will still study the PCJ scheme where Bob uses part of the global transmit power to produce jamming signals. When Eve's CSI is not available, FCJ should be used, as will be discussed in Section IV.

In phase 2, the signals received by Bob and Eve are given by

$$\mathbf{y}_b = \mathbf{H}_{rb}\left(\mathbf{T}_r\mathbf{z}_r + \mathbf{T}'_r\mathbf{z}'_r\right) + \mathbf{H}_{ab}\mathbf{T}'_{a2}\mathbf{z}'_{a2} + \mathbf{n}_b \tag{7}$$

$$\mathbf{y}_{e2} = \mathbf{H}_{re}\left(\mathbf{T}_r\mathbf{z}_r + \mathbf{T}'_r\mathbf{z}'_r\right) + \mathbf{H}_{ae}\mathbf{T}'_{a2}\mathbf{z}'_{a2} + \mathbf{n}_{e2} \tag{8}$$

where $\mathbf{z}_r$ is the information signal vector of the Relay with transmit beamformer $\mathbf{T}_r$, $\mathbf{z}'_r$ and $\mathbf{z}'_{a2}$ are jamming signal vectors transmitted by the Relay and Alice, respectively, and $\mathbf{T}'_r$ and $\mathbf{T}'_{a2}$ are their corresponding transmit beamformers. Note that, although there is no direct link for the information signal, Bob still sees the jamming signal from Alice. For a global power constraint, we have

$$\mathbb{E}\left\{\mathbf{z}_a^H\mathbf{z}_a + \mathbf{z}_a'^H\mathbf{z}'_a + \mathbf{z}_b'^H\mathbf{z}'_b\right\} \leq P$$
$$\mathbb{E}\left\{\mathbf{z}_r^H\mathbf{z}_r + \mathbf{z}_r'^H\mathbf{z}'_r + \mathbf{z}_{a2}'^H\mathbf{z}'_{a2}\right\} \leq P.$$

We will also investigate scenarios with individual power constraints, i.e. $\mathbb{E}\{\mathbf{z}_a^H\mathbf{z}_a + \mathbf{z}_a'^H\mathbf{z}'_a\} \leq P_a$, $\mathbb{E}\{\mathbf{z}_b'^H\mathbf{z}'_b\} \leq P_b$, $\mathbb{E}\{\mathbf{z}_r^H\mathbf{z}_r + \mathbf{z}_r'^H\mathbf{z}'_r\} \leq P_r$, and $\mathbb{E}\{\mathbf{z}_{a2}'^H\mathbf{z}'_{a2}\} \leq P_a$.

C. Performance Metric

MIMO wiretap channels have been extensively analyzed in recent work, and the achievable secrecy rate has been shown to be [10], [11]

$$R_s = \max[I_d - I_e]^+ \tag{9}$$

where I_d is the mutual information from the source to the destination, I_e is the mutual information from the source to the eavesdropper, and the maximum is taken over all possible input covariance matrices. For the half-duplex two-hop relay channel, the achievable secrecy rate was found in [26] to satisfy the same expression as in (9), where amplify-and-forward, decode-and-forward, and compress-and-forward relaying modes were all investigated. Equation (9) was also used as a performance metric to evaluate cooperative jamming schemes for half-duplex relay networks in [21]. In general, to obtain the maximum secrecy rate, one must construct an optimal coding scheme, although potentially suboptimal Gaussian codebooks are assumed in [8], [21], [26]. In Section III, we will follow the convention adopted in [21], [26] and use (9) as our metric for evaluating the achievable secrecy rate, assuming Gaussian inputs. Note that (9) was shown to be valid for both independent and repetition codebooks [26], although we will only focus on repetition coding (e.g. [27] and [28]) at the relay since independent codebooks are expected to result in smaller secrecy rates when the encoding schemes and relay protocols are public information [26].

The discussion above applies to the cases where the eavesdropper's CSI is known or at least partially known (e.g. the case where only statistical channel knowledge is available and ergodic secrecy rate is studied [8], [29]). However, when the eavesdropper's CSI is completely unavailable, (9) may not represent an achievable secrecy rate. Some recent progress has been made on finding expressions for the achievable secrecy rate in certain scenarios where the eavesdropper's CSI is completely unknown [30], but the derivation of such an expression for the relay network considered here is still an open problem. Nonetheless, the difference in the mutual information between the desired receiver and the eavesdropper is still a valid metric for evaluating the relative security of competing physical layer approaches. While the transmission parameters cannot be chosen to optimize (9) when the eavesdropper's CSI is unknown, the approach of [15], [24], [25] can be followed in which attention is restricted to obtaining a certain desired QoS for the legitimate receiver, and then finding a robust strategy for using the remaining resources to jam potential eavesdroppers. This is the approach adopted in Section IV, with (9) as the performance metric.

III. Secure Relaying With Known ECSI

In this section, we assume that Eve's CSI (ECSI) is available to the relay network. We will begin with the simple case where the Relay is equipped with only a single antenna, then a more complicated scenario with a MIMO relay will be investigated.

A. Single Data Stream Relaying

We begin by assuming a single-antenna DF relay ($N_r = 1$), where only one data stream can be transmitted via the Relay. Under the PCJ approach, the signals received in each phase can be expressed as

$$y_r = \mathbf{h}_{ar}\mathbf{t}_a z_a + \mathbf{h}_{br}\mathbf{T}'_b\mathbf{z}'_b + n_r \tag{10}$$
$$\mathbf{y}_{e1} = \mathbf{H}_{ae}\mathbf{t}_a z_a + \mathbf{H}_{be}\mathbf{T}'_b\mathbf{z}'_b + \mathbf{n}_{e1} \tag{11}$$

and

$$\mathbf{y}_b = \mathbf{h}_{rb} z_r + \mathbf{H}_{ab}\mathbf{T}'_a\mathbf{z}'_a + \mathbf{n}_b \tag{12}$$
$$\mathbf{y}_{e2} = \mathbf{h}_{re} z_r + \mathbf{H}_{ae}\mathbf{T}'_a\mathbf{z}'_a + \mathbf{n}_{e2} \tag{13}$$

where $\mathbb{E}\{z_a^H z_a\} = p_a$, $\mathbb{E}\{\mathbf{z}_b'^H\mathbf{z}'_b\} = p_b$, $\mathbb{E}\{z_r^H z_r\} = p_r$, and $\mathbb{E}\{\mathbf{z}_a'^H\mathbf{z}'_a\} = p_{a2}$. This is the PCJ form of (5)–(8) with $\mathbf{z}'_a = \mathbf{0}$ and $\mathbf{z}'_r = \mathbf{0}$. Since $N_r = 1$ in this case, we can design $\mathbf{T}'_b$ such that the jamming signals are completely nulled at the Relay, i.e., $\mathbf{h}_{br}\mathbf{T}'_b = \mathbf{0}$. For the transmit beamformer $\mathbf{t}_a$ in the first phase, we choose the generalized eigenvector of the pencil $\left(\mathbf{I} + \frac{p_a}{\sigma^2}\mathbf{h}_{ar}^H\mathbf{h}_{ar}, \mathbf{I} + \frac{p_a}{\sigma^2}\mathbf{H}_{ae}^H\mathbf{H}_{ae}\right)$ with the largest generalized eigenvalue, which achieves the secrecy capacity for the single-hop MISO wiretap channel[13]. For the second phase, we design $\mathbf{T}'_a$ such that $\mathbf{H}_{ab}\mathbf{T}'_a$ is orthogonal to the one-dimensional signal subspace $\mathrm{span}\{\mathbf{h}_{rb}\}$, so that the jamming does not impact Bob's reception of the information signal.

1) Maximum Secrecy Rate With Power Constraints: Next, we will discuss the design of the jamming beamformers and power allocation for maximizing the secrecy rate under both global power constraints ($p_a + p_b \le P$ in the first phase and $p_r + p_{a2} \le P$ in the second phase) and individual power constraints. For a two-hop DF-based relay channel, the mutual information between Alice and Bob through the relay link can be written as [31]

$$I_d = \frac{1}{2}\min\left\{\log_2(1+\gamma_{ar}), \log_2(1+\gamma_{rb})\right\} \tag{14}$$

where $\frac{1}{2}$ appears because the relay transmission is divided into two stages, and γ_{ij} is the SINR at node j for the signal from node i. Eve receives data during both phases, and the mutual information is

$$I_e = \frac{1}{2}\min\left\{\log_2(1+\gamma_{ar}), \log_2(1+\gamma_{ae}+\gamma_{re})\right\}. \tag{15}$$

Thus, the secrecy rate can be expressed as

$$R_s = \begin{cases} \frac{1}{2}\log_2\frac{\min\{1+\gamma_{ar}, 1+\gamma_{rb}\}}{(1+\gamma_{ae}+\gamma_{re})}, & \gamma_{ae}+\gamma_{re} \le \gamma_{ar} < \gamma_{rb} \\ & \text{or } \gamma_{ar} \ge \max\{\gamma_{rb}, \gamma_{ae}+\gamma_{re}\} \\ 0, & \text{otherwise.} \end{cases} \tag{16}$$

Since the rate of the relay link is limited by the SINR of the inferior phase, for a single data stream the transmit power for Alice and the Relay should be adjusted such that $\gamma_{ar} = \gamma_{rb}$ for power efficiency. Thus $R_s = \frac{1}{2}\log_2\frac{(1+\gamma_{ar})}{(1+\gamma_{ae}+\gamma_{re})}$ will be used as the objective function in the remainder of this section, as a result of the power adjustment.

We assume Eve uses beamformers $\mathbf{w}_{e1}$ and $\mathbf{w}_{e2}$ to receive the signals from Alice and the Relay in the first and second phases, respectively

$$\mathbf{w}_{e1}^H\mathbf{y}_{e1} = \mathbf{w}_{e1}^H\left(\mathbf{H}_{ae}\mathbf{t}_a z_a + \mathbf{H}_{be}\mathbf{T}'_b\mathbf{z}'_b + \mathbf{n}_{e1}\right) \tag{17}$$
$$\mathbf{w}_{e2}^H\mathbf{y}_{e2} = \mathbf{w}_{e1}^H\left(\mathbf{h}_{re} z_r + \mathbf{H}_{ae}\mathbf{T}'_a\mathbf{z}'_a + \mathbf{n}_{e2}\right) \tag{18}$$

and we assume that Eve can compute the beamformers which yield the best SINR

$$\mathbf{w}_{e1} = \left(\mathbf{H}_{be}\mathbf{T}'_b\mathbf{Q}_{zb'}\mathbf{T}_b'^H\mathbf{H}_{be}^H + \sigma^2\mathbf{I}\right)^{-1}\mathbf{H}_{ae}\mathbf{t}_a \tag{19}$$
$$\mathbf{w}_{e2} = \left(\mathbf{H}_{ae}\mathbf{T}'_a\mathbf{Q}_{za'}\mathbf{T}_a'^H\mathbf{H}_{ae}^H + \sigma^2\mathbf{I}\right)^{-1}\mathbf{h}_{re} \tag{20}$$

where $\mathbf{Q}_{zb'} = \mathbb{E}\{\mathbf{z}'_b\mathbf{z}_b'^H\}$ and $\mathbf{Q}_{za'} = \mathbb{E}\{\mathbf{z}'_a\mathbf{z}_a'^H\}$. With the above assumptions, the secrecy rate can be written as

$$R_s = \frac{1}{2}\log_2\frac{(1+\gamma_{ar})}{(1+\gamma_{ae}+\gamma_{re})} \tag{21}$$

where

$$\gamma_{ar} = \frac{p_a}{\sigma^2}|\mathbf{h}_{ar}\mathbf{t}_a|^2 \tag{22}$$
$$\gamma_{ae} = p_a\mathbf{t}_a^H\mathbf{H}_{ae}^H\left(\mathbf{H}_{be}\mathbf{T}'_b\mathbf{Q}_{zb'}\mathbf{T}_b'^H\mathbf{H}_{be}^H + \sigma^2\mathbf{I}\right)^{-1}\mathbf{H}_{ae}\mathbf{t}_a \tag{23}$$
$$\gamma_{re} = p_r\mathbf{h}_{re}^H\left(\mathbf{H}_{ae}\mathbf{T}'_a\mathbf{Q}_{za'}\mathbf{T}_a'^H\mathbf{H}_{ae}^H + \sigma^2\mathbf{I}\right)^{-1}\mathbf{h}_{re} \tag{24}$$

and we aim to find the joint optimal solution for the jamming beamformers $\mathbf{T}'_a, \mathbf{T}'_b$, the covariance matrices $\mathbf{Q}_{zb'}, \mathbf{Q}_{za'}$, and the transmit power vector $\mathbf{p} = [p_a, p_r, p_{a2}, p_b]^T$ in order to maximize the secrecy rate R_s.

We will first consider optimizing the jamming beamformers and covariance matrices. For $\mathbf{T}'_b$ and $\mathbf{Q}_{zb'}$, the problem of minimizing the SINR at Eve γ_{ae} can be written as

$$\min_{\mathbf{Q}_{zb'}\succeq 0, \mathbf{T}'_b} \mathbf{t}_a^H\mathbf{H}_{ae}^H\left(\mathbf{H}_{be}\mathbf{T}'_b\mathbf{Q}_{zb'}\mathbf{T}_b'^H\mathbf{H}_{be}^H + \sigma^2\mathbf{I}\right)^{-1}\mathbf{H}_{ae}\mathbf{t}_a \tag{25a}$$
$$\text{s.t.} \quad \mathrm{tr}(\mathbf{Q}_{zb'}) \le p_b,\ \mathbf{h}_{br}\mathbf{T}'_b = \mathbf{0}. \tag{25b}$$

Although problem (25) can be formulated as a semidefinite program (SDP) that can be solved efficiently (see Appendix A), we can not directly obtain an analytical solution that is useful for optimizing the global power allocation. Therefore, we will make use of the following lemma, a proof of which is provided in Appendix B.

Lemma 1: The covariance matrix $\mathbf{Q}_{zb'}$ that minimizes (25a) is rank one.

According to Lemma 1, we know that a one-dimensional jamming signal is optimal for the case of single data stream transmission: $\mathbf{T}'_b = \mathbf{t}'_b$. Under the constraint that $\mathbf{h}_{br}\mathbf{t}'_b = 0$, and defining $\mathbf{G}_b^{\perp}$ as an orthonormal basis for $\mathcal{N}(\mathbf{h}_{br})$, the jamming beamformer from Bob can be written as $\mathbf{t}'_b = \mathbf{G}_b^{\perp}\mathbf{c}_b$, for some unit-length vector $\mathbf{c}_b$. Equation (23) becomes

$$\begin{aligned}\gamma_{ae} &= p_a\mathbf{t}_a^H\mathbf{H}_{ae}^H\left(p_b\mathbf{H}_{be}\mathbf{t}'_b\mathbf{t}_b'^H\mathbf{H}_{be}^H + \sigma^2\mathbf{I}\right)^{-1}\mathbf{H}_{ae}\mathbf{t}_a \\ &= \frac{p_a}{\sigma^2}\left(\mathbf{t}_a^H\mathbf{H}_{ae}^H\mathbf{H}_{ae}\mathbf{t}_a - \frac{\mathbf{t}_a^H\mathbf{H}_{ae}^H\mathbf{H}_{be}\mathbf{t}'_b\mathbf{t}_b'^H\mathbf{H}_{be}^H\mathbf{H}_{ae}\mathbf{t}_a}{\mathbf{t}_b'^H\left(\frac{\sigma^2}{p_b}\mathbf{I} + \mathbf{H}_{be}^H\mathbf{H}_{be}\right)\mathbf{t}'_b}\right)\end{aligned} \tag{26}$$

where the second equality holds due to the matrix inversion lemma [32]. The optimization problem is equivalent to maximizing the second term in (26), which can be formulated as

$$\max_{\mathbf{c}_b} \quad \frac{\mathbf{c}_b^H \mathbf{a}_b \mathbf{a}_b^H \mathbf{c}_b}{\mathbf{c}_b^H \left(\frac{\sigma^2}{p_b}\mathbf{I} + \mathbf{B}_b^H \mathbf{B}_b\right) \mathbf{c}_b} \quad \text{s.t.} \quad \mathbf{c}_b^H \mathbf{c}_b = 1 \tag{27}$$

where $\mathbf{a}_b = \mathbf{G}_b^{\perp H} \mathbf{H}_{be}^H \mathbf{H}_{ae} \mathbf{t}_a$ and $\mathbf{B}_b = \mathbf{H}_{be} \mathbf{G}_b^{\perp}$. The maximum value of the Rayleigh quotient in (27) is the largest generalized eigenvalue of the matrix pencil $\left(\mathbf{a}_b \mathbf{a}_b^H, \frac{\sigma^2}{p_b}\mathbf{I} + \mathbf{B}_b^H \mathbf{B}_b\right)$, and the vector that achieves it is the corresponding generalized eigenvector [33]. Since $\mathbf{a}_b \mathbf{a}_b^H$ is rank one, the solution can be written as

$$\mathbf{t}_b' = \mathbf{G}_b^{\perp} \frac{\left(\frac{\sigma^2}{p_b}\mathbf{I} + \mathbf{B}_b^H \mathbf{B}_b\right)^{-1} \mathbf{a}_b}{\left\| \left(\frac{\sigma^2}{p_b}\mathbf{I} + \mathbf{B}_b^H \mathbf{B}_b\right)^{-1} \mathbf{a}_b \right\|} \tag{28}$$

and γ_{ae} becomes

$$\gamma_{ae} = \frac{p_a}{\sigma^2} \left(\mathbf{t}_a^H \mathbf{H}_{ae}^H \mathbf{H}_{ae} \mathbf{t}_a - \mathbf{a}_b^H \left(\frac{\sigma^2}{p_b}\mathbf{I} + \mathbf{B}_b^H \mathbf{B}_b\right)^{-1} \mathbf{a}_b \right). \tag{29}$$

Similarly for the second phase, the SINR for Eve is rewritten as

$$\begin{aligned} \gamma_{re} &= p_r \mathbf{h}_{re}^H \left(p_{a2} \mathbf{H}_{ae} \mathbf{t}_a' \mathbf{t}_a'^H \mathbf{H}_{ae}^H + \sigma^2 \mathbf{I}\right)^{-1} \mathbf{h}_{re} \\ &= \frac{p_r}{\sigma^2} \left(\mathbf{h}_{re}^H \mathbf{h}_{re} - \frac{\mathbf{h}_{re}^H \mathbf{H}_{ae} \mathbf{t}_a' \mathbf{t}_a'^H \mathbf{H}_{ae}^H \mathbf{h}_{re}}{\mathbf{t}_a'^H \left(\frac{\sigma^2}{p_{a2}}\mathbf{I} + \mathbf{H}_{ae}^H \mathbf{H}_{ae}\right) \mathbf{t}_a'} \right). \end{aligned} \tag{30}$$

Using the same method as in (26)–(28), Alice's jamming beamformer is given by

$$\mathbf{t}_a' = \mathbf{G}_a^{\perp} \frac{\left(\frac{\sigma^2}{p_a}\mathbf{I} + \mathbf{B}_a^H \mathbf{B}_a\right)^{-1} \mathbf{a}_a}{\left\| \left(\frac{\sigma^2}{p_a}\mathbf{I} + \mathbf{B}_a^H \mathbf{B}_a\right)^{-1} \mathbf{a}_a \right\|} \tag{31}$$

where $\mathbf{G}_a^{\perp}$ is an orthonormal basis for $\mathcal{N}(\mathbf{h}_{rb}^H \mathbf{H}_{ab})$, $\mathbf{a}_a = \mathbf{G}_a^{\perp H} \mathbf{H}_{ae}^H \mathbf{h}_{re}$, $\mathbf{B}_a = \mathbf{H}_{ae} \mathbf{G}_a^{\perp}$, and γ_{re} becomes

$$\gamma_{re} = \frac{p_r}{\sigma^2} \left(\mathbf{h}_{re}^H \mathbf{h}_{re} - \mathbf{a}_a^H \left(\frac{\sigma^2}{p_a}\mathbf{I} + \mathbf{B}_a^H \mathbf{B}_a\right)^{-1} \mathbf{a}_a \right).$$

Next we find the power allocation that maximizes the secrecy rate. Note that the jamming beamformers are not independent of the jamming power, and thus we need to jointly optimize over both quantities. In general, (21) is not convex with respect to $\mathbf{p}$, so instead we maximize the following lower bound for R_s:

$$R_s(\mathbf{p}) \geq \frac{1}{2} \log_2 \frac{\gamma_{ar}}{(1 + \gamma_{ae} + \gamma_{re})} = \frac{1}{2} \log_2 \frac{|\mathbf{h}_{ar} \mathbf{t}_a|^2}{\sigma^2 g(\mathbf{p})} \tag{32}$$

where

$$g(\mathbf{p}) = p_a^{-1} + \tilde{p_b}^{-1} + p_a^{-1} p_r \tilde{p}_{a2}^{-1} \tag{33}$$

$$\tilde{p}_b^{-1} = \mathbf{t}_a^H \mathbf{H}_{ae}^H \mathbf{H}_{ae} \mathbf{t}_a - \mathbf{a}_b^H \left(\frac{\sigma^2}{p_b}\mathbf{I} + \mathbf{B}_b^H \mathbf{B}_b\right)^{-1} \mathbf{a}_b \tag{34}$$

$$\tilde{p}_{a2}^{-1} = \mathbf{h}_{re}^H \mathbf{h}_{re} - \mathbf{a}_a^H \left(\frac{\sigma^2}{p_a}\mathbf{I} + \mathbf{B}_a^H \mathbf{B}_a\right)^{-1} \mathbf{a}_a. \tag{35}$$

Over the range of practical transmit powers, $\tilde{p_b}$ and $\tilde{p}_{a2}$ can be accurately approximated as linear functions of p_b and p_{a2}, which we denote by $\tilde{p_b} = c_1 p_b + c_2$ and $\tilde{p}_{a2} = c_3 p_{a2} + c_4$. Note that according to (34), as p_b increases, the second term can only increase in size, which means $\tilde{p}_b^{-1}$ decreases, and hence $\tilde{p_b}$ increases, which implies that c_1 is positive. As p_b approaches zero, the second term approaches zero, but the first term is nonnegative, so that implies that $c_2 > 0$. Thus c_1 and c_2 are both positive constants. Similarly, we can see that c_3 and c_4 in (35) are also positive constants.

Using this approximation, the rate maximization problem under a global power constraint P becomes one of minimizing $g(\mathbf{p})$ in (32)

$$\begin{aligned} \min_{\mathbf{p}} \quad & p_a^{-1} + \tilde{p_b}^{-1} + p_a^{-1} p_r \tilde{p}_{a2}^{-1} && \text{(36a)} \\ \text{s.t.} \quad & p_a + c_1^{-1} \tilde{p_b} \leq P + c_1^{-1} c_2 && \text{(36b)} \\ & p_r + c_3^{-1} \tilde{p}_{a2} \leq P + c_3^{-1} c_4 && \text{(36c)} \\ & p_a |\mathbf{h}_{ar} \mathbf{t}_a|^2 = p_r |\mathbf{h}_{rb}|^2 && \text{(36d)} \end{aligned}$$

where (36b) and (36c) are derived from $p_a + p_b \leq P$ and $p_r + p_{a2} \leq P$, and (36d) is the optimal power adjustment for the two hops used to guarantee that $\gamma_{ar} = \gamma_{rb}$. The optimization problem stated above is in the standard form for Geometric Programming (GP) problems, with (36a), (36b), and (36c) as posynomial and (36d) as monomial constraints. GP problems are a class of nonlinear optimization problems that can be readily turned into convex optimization problems, and hence a global optimum can be efficiently computed [34]. If individual power constraints are employed, we can also use GP to solve the following similar optimization problem:

$$\begin{aligned} \min_{\mathbf{p}} \quad & p_a^{-1} + \tilde{p_b}^{-1} + p_a^{-1} p_r \tilde{p}_{a2}^{-1} && \text{(37a)} \\ \text{s.t.} \quad & p_a \leq P_a, \quad p_r \leq P_r && \text{(37b)} \\ & c_1^{-1} \tilde{p_b} \leq P_b + c_1^{-1} c_2 && \text{(37c)} \\ & c_3^{-1} \tilde{p}_{a2} \leq P_a + c_3^{-1} c_4 && \text{(37d)} \\ & p_a |\mathbf{h}_{ar} \mathbf{t}_a|^2 = p_r |\mathbf{h}_{rb}|^2. && \text{(37e)} \end{aligned}$$

Remark 1: As discussed in the beginning of this section, we choose the principal generalized eigenvector of the pencil $\left(\mathbf{I} + \frac{p_a}{\sigma^2} \mathbf{h}_{ar}^H \mathbf{h}_{ar}, \mathbf{I} + \frac{p_a}{\sigma^2} \mathbf{H}_{ae}^H \mathbf{H}_{ae}\right)$ as the information signal transmit beamformer $\mathbf{t}_a$. However, the allocated power p_a is unavailable before the optimization algorithm starts. Therefore, iterations will be needed for computing the beamformers, initialized with $p_a = P$, where P is the maximum transmit power. Based on our numerical experiments, the algorithm usually converges with very few iterations, and introduces little complexity to the overall algorithm.

Remark 2: For the case where $\mathbf{H}_{ae}$ does not have full column rank, i.e., $N_a > N_e$, an alternative would be to choose $\mathbf{t}_a$ to lie in the null space $\mathcal{N}(\mathbf{H}_{ae})$. This beamformer will in general be different from the one we propose, and will result in a solution where Eve will not receive any information signal in

the first phase and hence the jamming from Bob is not necessary. However, based on our numerical experiments, the solution we propose yields a larger secrecy rate. This is mainly due to the fact that although $\mathbf{t}_a$ may allow a small amount of information leakage from Alice to Eve, the rate improvement in the legitimate channel outweighs that of the wiretap channel, given the cooperative jamming support from Bob and the optimized power allocation.

2) Minimum Transmit Power With Fixed Secrecy Rate: The problem of minimizing the transmit power under a certain fixed secrecy rate is similar to the problems discussed above. We still choose jamming beamformers that lie in the subspace orthogonal to the intended channels. As before, for the first phase we will have $\mathbf{t}_b' = \rho_b \mathbf{G}_{\mathbf{b}}^{\perp} \mathbf{e}_b$, where ρ_b is a scalar that maintains the unit norm of $\mathbf{t}_b'$. We aim to minimize the norm of $\mathbf{e}_b$ under a fixed target secrecy rate R_0. According to (27) and (32), the problem can be formulated as

$$\min_{\mathbf{e}_b} \mathbf{e}_b^H \mathbf{e}_b \quad \text{s.t.} \ \frac{\mathbf{c}_b^H \mathbf{a}_b \mathbf{a}_b^H \mathbf{c}_b}{\mathbf{c}_b^H \left(\frac{\sigma^2}{p_b} \mathbf{I} + \mathbf{B}_b^H \mathbf{B}_b \right) \mathbf{c}_b} \geq f(R_0, \mathbf{t}_a') \quad (38)$$

where $f(R_0, \mathbf{t}_a')$ is a function of R_0 and $\mathbf{t}_a'$ independent of $\mathbf{t}_b'$. The solution is again seen to be the generalized eigenvector of the pencil $\left(\mathbf{a}_b \mathbf{a}_b^H, \frac{\sigma^2}{p_b} \mathbf{I} + \mathbf{B}_b^H \mathbf{B}_b \right)$ corresponding to the largest eigenvalue. Since it is a rank-one Hermitian matrix, $\mathbf{t}_b'$ has the same solution as shown in (28). Similarly, for the second phase, we also have the same beamformer as (31). Considering the transmit power of all the nodes, we can now formulate the optimization problem under the global transmit power constraint as

$$\min_{\mathbf{p}} \max(p_a + \tilde{p_b}, p_r + \tilde{p}_{a2}) \quad \text{s.t.} \ g(\mathbf{p}) \leq \frac{|\mathbf{h}_{ar} \mathbf{t}_a|^2}{2^{2R_0} \sigma^2} \quad (39)$$

where $g(\mathbf{p})$ is given in (32). This is also a GP problem. To minimize individual transmit powers, (39) should be rewritten as $\min_{\mathbf{p}} \max(p_a, \tilde{p_b}, p_r, \tilde{p}_{a2})$ instead.

B. Multiple Data Stream Relaying

Since ECSI is known to the relay network, Alice and the Relay can utilize certain beamformers to perform multiple data-stream relay transmission and reduce information leakage to Eve as well. The GSVD has been employed for the traditional MIMO wiretap channel [13], and it operates by dividing the channels from the transmitter to the intended receiver and the eavesdropper into a set of parallel subchannels.

Definition 1 (GSVD Transform): Given two matrices $\mathbf{H}_1 \in \mathbb{C}^{N_r \times N_a}$ and $\mathbf{H}_2 \in \mathbb{C}^{N_e \times N_a}$ and $k = rank\{[\mathbf{H}_1^H, \mathbf{H}_2^H]^H\}$, there exist unitary matrices $\mathbf{U} \in \mathbb{C}^{N_r \times N_r}$, $\mathbf{V} \in \mathbb{C}^{N_e \times N_e}$ and $\mathbf{\Psi} \in \mathbb{C}^{N_a \times N_a}$, and a non-singular upper-triangular matrix $\mathbf{R} \in \mathbb{C}^{k \times k}$ such that

$$\mathbf{U}^H \mathbf{H}_1 \mathbf{\Psi} = \mathbf{S}_1 [\mathbf{R}, \mathbf{0}_{k \times N_a - k}],$$
$$\mathbf{V}^H \mathbf{H}_2 \mathbf{\Psi} = \mathbf{S}_2 [\mathbf{R}, \mathbf{0}_{k \times N_a - k}]$$

where $\mathbf{S}_1 \in \mathbb{R}^{N_r \times k}$, $\mathbf{S}_2 \in \mathbb{R}^{N_e \times k}$ are nonnegative diagonal matrices with $\mathbf{S}_1^T \mathbf{S}_1 + \mathbf{S}_2^T \mathbf{S}_2 = \mathbf{I}_k$, the diagonal elements of $(\mathbf{S}_1^T \mathbf{S}_1)^{\frac{1}{2}}$ are ordered as $0 \leq s_{1,1} \leq \cdots \leq s_{1,k}$, and the diagonal elements of $(\mathbf{S}_2^T \mathbf{S}_2)^{\frac{1}{2}}$ are ordered as $s_{2,1} \geq \cdots \geq s_{2,k} \geq 0$.

It has been shown [7] that, for the standard Gaussian MIMO wiretap channel, using the GSVD-based beamformer

$$\mathbf{T} = \frac{\mathbf{\Psi}}{\|\mathbf{R}^{-1}\|} \begin{bmatrix} \mathbf{R}^{-1} \\ \mathbf{0}_{N_a - k \times k} \end{bmatrix}$$

to transmit the desired signals along dimensions where $s_{1,i} \geq s_{2,i}$ achieves the secrecy capacity in the high SNR regime with uniform power allocation. In this section, two transmission strategies based on the GSVD will be investigated for the two-hop relay channel. In the first strategy, each transmission phase is treated as a standard wiretap channel, and Alice and the Relay will use GSVD-based transmit beamformers in the first and the second phase, respectively, without any cooperative jamming from inactive nodes. In the second strategy, a cooperative jamming scheme is proposed in which Bob and Alice also transmit jamming signals based on the GSVD transform in a reverse manner.

1) Simple GSVD-Based Relaying: To begin, we consider the case where GSVD-based beamforming is used without jamming. According to Definition 1, the MIMO channels in phase 1 and phase 2 can be decomposed as

$$\mathbf{H}_{ar} = \mathbf{U}_a \mathbf{S}_{ar} [\mathbf{R}_a, \mathbf{0}_{s \times N_a - s}] \mathbf{\Psi}_a^H$$
$$\mathbf{H}_{ae} = \mathbf{V}_a \mathbf{S}_{ae} [\mathbf{R}_a, \mathbf{0}_{s \times N_a - s}] \mathbf{\Psi}_a^H$$

and

$$\mathbf{H}_{rb} = \mathbf{U}_r \mathbf{S}_{rb} [\mathbf{R}_r, \mathbf{0}_{s \times N_r - s}] \mathbf{\Psi}_r^H$$
$$\mathbf{H}_{re} = \mathbf{V}_r \mathbf{S}_{re} [\mathbf{R}_r, \mathbf{0}_{s \times N_r - s}] \mathbf{\Psi}_r^H$$

where $s = min(rank\{[\mathbf{H}_{ar}^H, \mathbf{H}_{ae}^H]^H\}, rank\{[\mathbf{H}_{rb}^H, \mathbf{H}_{re}^H]^H\})$, representing the maximum possible number of data streams. Alice and the Relay transmit signals with the following two beamformers, respectively

$$\mathbf{T}_a = \frac{\mathbf{\Psi}_a}{\|\mathbf{R}_a^{-1}\|} \begin{bmatrix} \mathbf{R}_a^{-1} \\ \mathbf{0}_{N_a - s \times s} \end{bmatrix}, \quad (40a)$$

$$\mathbf{T}_r = \frac{\mathbf{\Psi}_r}{\|\mathbf{R}_r^{-1}\|} \begin{bmatrix} \mathbf{R}_r^{-1} \\ \mathbf{0}_{N_r - s \times s} \end{bmatrix}. \quad (40b)$$

Proposition 1: When (40) is used for transmit beamforming, the secrecy rate under the simple GSVD-based relaying scheme can be expressed as

$$R_{\text{gsvd}} = \frac{1}{2} \log_2 \frac{\min \left\{ \prod_{i=1}^{s} \left(1 + \frac{p_{a,i} s_{ar,i}^2}{\sigma^2 \|\mathbf{R}_a^{-1}\|^2} \right), \prod_{i=1}^{s} \left(1 + \frac{p_{r,i} s_{rb,i}^2}{\sigma^2 \|\mathbf{R}_r^{-1}\|^2} \right) \right\}}{\prod_{i=1}^{s} \left(1 + \frac{p_{a,i} s_{ae,i}^2}{\sigma^2 \|\mathbf{R}_a^{-1}\|^2} + \frac{p_{r,i} s_{re,i}^2}{\sigma^2 \|\mathbf{R}_r^{-1}\|^2} \right)} \quad (41)$$

where $p_{a,i}$ and $p_{r,i}$ are the transmit power for the ith parallel channel from Alice and the Relay, respectively.

The proof of Proposition 1 is given in Appendix C. Next, we will investigate the power allocation for the above transmission scheme. Maximizing the rate in (41) is generally a nonconvex optimization problem. However, applying the *single condensation method* for GP [35], the posynomial in the numerator of (41)

can be accurately approximated as a monomial, and we can still solve this nonconvex problem through a *series* of GPs.

Lemma 2: Let

$$\prod_{i=1}^{s} f_i(p_{a,i}) = \prod_{i=1}^{s}\left(1+\frac{p_{a,i}s_{ar,i}^2}{\sigma^2\left\|\mathbf{R}_a^{-1}\right\|^2}\right). \tag{42}$$

We have

$$\begin{aligned}\prod_{i=1}^{s} f_i(p_{a,i}) &\geq \prod_{i=1}^{s}\widetilde{f}_i(p_{a,i})\\ &= \prod_{i=1}^{s}\left(\frac{1}{\alpha_{1,i}}\right)^{\alpha_{1,i}}\left(\frac{p_{a,i}s_{ar,i}^2}{\alpha_{2,i}\sigma^2\left\|\mathbf{R}_a^{-1}\right\|^2}\right)^{\alpha_{2,i}}\end{aligned} \tag{43}$$

where $\alpha_{1,i},\alpha_{2,i}\geq 0$. The inequality becomes an equality when $\alpha_{1,i},\alpha_{2,i}$ satisfy

$$\alpha_{1,i}=\frac{1}{f_i(p_{a,i})},\quad \alpha_{2,i}=\frac{p_{a,i}}{f_i(p_{a,i})}\frac{\partial f_i(p_{a,i})}{\partial p_{a,i}}, \tag{44}$$

in which case $\prod_{i=1}^{s}\widetilde{f}_i(p_{a,i})$ is the best local monomial approximation of $\prod_{i=1}^{s} f_i(p_{a,i})$ near $p_{a,i}$.

Proof: We can rewrite $\prod_{i=1}^{s} f_i(p_{a,i})$ as

$$\begin{aligned}&\prod_{i=1}^{s}\left(1+\frac{p_{a,i}s_{ar,i}^2}{\sigma^2\left\|\mathbf{R}_a^{-1}\right\|^2}\right)\\ &\quad=\prod_{i=1}^{s}\left(\alpha_{1,i}\frac{1}{\alpha_{1,i}}+\alpha_{2,i}\frac{p_{a,i}s_{ar,i}^2}{\alpha_{2,i}\sigma^2\left\|\mathbf{R}_a^{-1}\right\|^2}\right) &(45)\\ &\quad\geq\prod_{i=1}^{s}\left(\frac{1}{\alpha_{1,i}}\right)^{\alpha_{1,i}}\left(\frac{p_{a,i}s_{ar,i}^2}{\alpha_{2,i}\sigma^2\left\|\mathbf{R}_a^{-1}\right\|^2}\right)^{\alpha_{2,i}} &(46)\end{aligned}$$

where (46) holds according to the arithmetic-geometric mean inequality. Noting that $\alpha_{1,i}$ and $\alpha_{2,i}$ are both positive coefficients and $\alpha_{1,i}+\alpha_{2,i}=1$, $\forall i$, the proof of equality is straightforward by inserting (44) back into $\prod_{i=1}^{s}\widetilde{f}_i(p_{a,i})$. ∎

Similarly for the second phase, given the posynomial

$$\prod_{i=1}^{s} g_i(p_{r,i}) = \prod_{i=1}^{s}\left(1+\frac{p_{r,i}s_{rb,i}^2}{\sigma^2\left\|\mathbf{R}_r^{-1}\right\|^2}\right) \tag{47}$$

we have the approximation

$$\prod_{i=1}^{s}\widetilde{g}_i(p_{r,i}) = \prod_{i=1}^{s}\left(\frac{1}{\beta_{1,i}}\right)^{\beta_{1,i}}\left(\frac{p_{r,i}s_{rb,i}^2}{\beta_{2,i}\sigma^2\left\|\mathbf{R}_r^{-1}\right\|^2}\right)^{\beta_{2,i}} \tag{48}$$

where

$$\beta_{1,i}=\frac{1}{g_i(p_{r,i})},\quad \beta_{2,i}=\frac{p_{r,i}}{g_i(p_{r,i})}\frac{\partial g_i(p_{r,i})}{\partial p_{r,i}}. \tag{49}$$

The approach corresponding to these results is outlined in the following algorithm:

Algorithm 1: Single condensation method for power allocation

Initialize $p_{a,i}^{(0)}$ and $p_{r,i}^{(0)}$, $i=\{1,\cdots,s\}$.

For iteration k:

1) Evaluate posynomial $f_i(p_{a,i}^{(k-1)})$ and $g_i(p_{r,i}^{(k-1)})$, according to (42) and (47).
2) Compute $\alpha^{(k)}$ and $\beta^{(k)}$

$$\begin{cases}\alpha_{1,i}^{(k)}=\frac{1}{f_i\left(p_{a,i}^{(k-1)}\right)},\quad \beta_{1,i}^{(k)}=\frac{1}{g_i\left(p_{r,i}^{(k-1)}\right)}\\ \alpha_{2,i}^{(k)}=\frac{p_{a,i}^{(k-1)}}{f_i\left(p_{a,i}^{(k-1)}\right)}\frac{\partial f_i\left(p_{a,i}^{(k-1)}\right)}{\partial p_{a,i}^{(k-1)}}\\ \beta_{2,i}^{(k)}=\frac{p_{r,i}^{(k-1)}}{g_i\left(p_{r,i}^{(k-1)}\right)}\frac{\partial g_i\left(p_{r,i}^{(k-1)}\right)}{\partial p_{r,i}^{(k-1)}}.\end{cases} \tag{50}$$

3) Condense posynomials f_i and g_i into monomials $\widetilde{f}_i$ and $\widetilde{g}_i$, according to (43) and (48).
4) Solve the GP

$$\begin{aligned}\min_{\mathbf{p}}\ &\max\left\{\prod_{i=1}^{s}\widetilde{f}_i(p_{a,i})^{-1},\prod_{i=1}^{s}\widetilde{g}_i(p_{r,i})^{-1}\right\}\\ &\times\prod_{i=1}^{s}\left(1+\frac{p_{a,i}s_{ae,i}^2}{\sigma^2\left\|\mathbf{R}_a^{-1}\right\|^2}+\frac{p_{r,i}s_{re,i}^2}{\sigma^2\left\|\mathbf{R}_r^{-1}\right\|^2}\right) &(51a)\\ \text{s.t.}\quad &\sum_{i=1}^{s}p_{a,i}\leq P,\quad \sum_{i=1}^{s}p_{r,i}\leq P. &(51b)\end{aligned}$$

5) Apply the resulting $p_{a,i}^{(k)}$ and $p_{r,i}^{(k)}$ to step 1 and loop until convergence.

The GP problems in this successive optimization method can be solved using interior-point methods with polynomial-time complexity [36], and it has been proven in [35] that the solution obtained using successive approximations for the single condensation method will efficiently converge to a point satisfying the Karush-Kuhn-Tucker (KKT) conditions of the original problem. Note that (51a) is refered to as a *generalized posynomial* [36] since it is formed from posynomials using a maximum operation, and can be easily converted to the standard posynomial form as

$$\begin{aligned}\min_{\mathbf{p},\mu}\quad &\mu\prod_{i=1}^{s}\left(1+\frac{p_{a,i}s_{ae,i}^2}{\sigma^2\left\|\mathbf{R}_a^{-1}\right\|^2}+\frac{p_{r,i}s_{re,i}^2}{\sigma^2\left\|\mathbf{R}_r^{-1}\right\|^2}\right) &(52a)\\ \text{s.t.}\quad &\sum_{i=1}^{s}p_{a,i}\leq P,\quad \sum_{i=1}^{s}p_{r,i}\leq P &(52b)\\ &\prod_{i=1}^{s}\widetilde{f}_i(p_{a,i})^{-1}\mu^{-1}\leq 1\ \prod_{i=1}^{s}\widetilde{g}_i(p_{r,i})^{-1}\mu^{-1}\leq 1. &(52c)\end{aligned}$$

2) GSVD-Based PCJ: A GSVD-based, partial cooperative jamming scheme is proposed in this subsection. In this case, Alice and the Relay will still use the same transmit beamformers as in the case without cooperative jamming. Since Bob and Alice are normally inactive in phase 1 and phase 2 respectively, they can act as temporary helpers to help improve the secrecy rate. As before, however, the power used for jamming must

come from the total power budget of P in each hop. A GSVD-based beamformer for the jamming signal is used by Bob in the first phase, due to the assumption that ECSI is available. The GSVD is implemented in a reverse fashion, since Bob in phase 1 considers Eve as the intended receiver of the jamming and wants to avoid leaking interference signals to the Relay. Similarly in phase 2, Alice treats Eve as the intended receiver. The signal model for this scheme is given in Section II-B.

Performing the GSVD for the channels from Bob to Eve and the Relay according to Definition 1, we have

$$\begin{aligned}\mathbf{H}_{be} &= \mathbf{U}_b \mathbf{S}_{be} \left[\mathbf{R}_b, \mathbf{0}_{k_b \times N_r - k_b}\right] \mathbf{\Psi}_b^H \\ \mathbf{H}_{br} &= \mathbf{V}_b \mathbf{S}_{br} \left[\mathbf{R}_b, \mathbf{0}_{k_b \times N_r - k_b}\right] \mathbf{\Psi}_b^H \\ \mathbf{H}_{ae} &= \mathbf{U}_{a'} \mathbf{S}_{ae} \left[\mathbf{R}_{a'}, \mathbf{0}_{k_a \times N_a - k_a}\right] \mathbf{\Psi}_{a'}^H \\ \mathbf{H}_{ab} &= \mathbf{V}_{a'} \mathbf{S}_{ab} \left[\mathbf{R}_{a'}, \mathbf{0}_{k_a \times N_a - k_a}\right] \mathbf{\Psi}_{a'}^H\end{aligned}$$

where $k_b = rank\{[\mathbf{H}_{be}^H, \mathbf{H}_{br}^H]^H\}$. Bob and Alice use the following jamming beamformers to implement the reverse GSVD:

$$\begin{aligned}\mathbf{T}_b' &= \frac{\mathbf{\Psi}_b}{\left\|\mathbf{R}_b^{-1}\right\|} \begin{bmatrix} \mathbf{R}_b^{-1} \\ \mathbf{0}_{N_r - k_b \times k_b} \end{bmatrix} \\ \mathbf{T}_a' &= \frac{\mathbf{\Psi}_{a'}}{\left\|\mathbf{R}_{a'}^{-1}\right\|} \begin{bmatrix} \mathbf{R}_{a'}^{-1} \\ \mathbf{0}_{N_a - k_a \times k_a} \end{bmatrix}\end{aligned}$$

and, unlike the simple GSVD-based relaying scheme, there will be jamming energy present in the signals received by the Relay and Bob. For Eve, the received signal is given by

$$\mathbf{y}_e = \begin{bmatrix} \mathbf{H}_{ae}\mathbf{T}_a\mathbf{D}_a \\ \mathbf{H}_{re}\mathbf{T}_r\mathbf{D}_r \end{bmatrix} \mathbf{z} + \begin{bmatrix} \mathbf{H}_{be}\mathbf{T}_b'\mathbf{z}_b' + \mathbf{n}_{e1} \\ \mathbf{H}_{ae}\mathbf{T}_a'\mathbf{z}_a' + \mathbf{n}_{e2} \end{bmatrix} = \widetilde{\mathbf{H}}_e \mathbf{z} + \widetilde{\mathbf{n}}_e.$$

Employing the above jamming beamformers, the mutual information between Alice and Bob is

$$\begin{aligned} I_d = \min \Bigg\{ &\frac{1}{2}\log_2 \det\left(\mathbf{I} + \mathbf{H}_{ar}\mathbf{T}_a\mathbf{Q}_{za}\mathbf{T}_a^H\mathbf{H}_{ar}^H\mathbf{Q}_{\tilde{n}r}^{-1}\right), \\ &\frac{1}{2}\log_2 \det\left(\mathbf{I} + \mathbf{H}_{rb}\mathbf{T}_r\mathbf{Q}_{zr}\mathbf{T}_r^H\mathbf{H}_{rb}^H\mathbf{Q}_{\tilde{n}b}^{-1}\right) \Bigg\} \end{aligned} \quad (53)$$

where $\mathbb{E}(\mathbf{z}_a'\mathbf{z}_a'^H) = \mathbf{Q}_{za'}$ $\mathbb{E}(\mathbf{z}_b'\mathbf{z}_b'^H) = \mathbf{Q}_{zb'}$, and

$$\begin{aligned}\mathbf{Q}_{\tilde{n}r} &= \mathbb{E}\left[\left(\mathbf{H}_{br}\mathbf{T}_b'\mathbf{z}_b' + \mathbf{n}_r\right)\left(\mathbf{H}_{br}\mathbf{T}_b'\mathbf{z}_b' + \mathbf{n}_r\right)^H\right] \\ &= \mathbf{H}_{br}\mathbf{T}_b'\mathbf{Q}_{zb'}\mathbf{T}_b'^H\mathbf{H}_{br}^H + \sigma^2\mathbf{I}, \\ \mathbf{Q}_{\tilde{n}b} &= \mathbb{E}\left[\left(\mathbf{H}_{ab}\mathbf{T}_a'\mathbf{z}_a' + \mathbf{n}_b\right)\left(\mathbf{H}_{ab}\mathbf{T}_a'\mathbf{z}_a' + \mathbf{n}_b\right)^H\right] \\ &= \mathbf{H}_{ab}\mathbf{T}_a'\mathbf{Q}_{za'}\mathbf{T}_a'^H\mathbf{H}_{ab}^H + \sigma^2\mathbf{I}.\end{aligned}$$

The mutual information for Eve's link is

$$\begin{aligned} I_e = \min \Bigg\{ &\frac{1}{2}\log_2 \det\left(\mathbf{I} + \mathbf{H}_{ar}\mathbf{T}_a\mathbf{Q}_{za}\mathbf{T}_a^H\mathbf{H}_{ar}^H\mathbf{Q}_{\tilde{n}r}^{-1}\right), \\ &\frac{1}{2}\log_2 \det\left(\mathbf{I} + \widetilde{\mathbf{H}}_e\mathbf{Q}_z\widetilde{\mathbf{H}}_e^H\mathbf{Q}_{\tilde{n}e}^{-1}\right) \Bigg\} \end{aligned} \quad (54)$$

where

$$\begin{aligned}&\mathbf{Q}_{\tilde{n}e} \\ &= \begin{bmatrix} \mathbf{H}_{be}\mathbf{T}_b'\mathbf{Q}_{zb'}\mathbf{T}_b'^H\mathbf{H}_{be}^H + \sigma^2\mathbf{I} & \mathbf{0} \\ \mathbf{0} & \mathbf{H}_{ae}\mathbf{T}_a'\mathbf{Q}_{za'}\mathbf{T}_a'^H\mathbf{H}_{ae}^H + \sigma^2\mathbf{I} \end{bmatrix}.\end{aligned}$$

To maximize the secrecy rate, we then have the following optimization problem:

$$\begin{aligned} \max_{\mathbf{Q}_{za}, \mathbf{Q}_{zb'}, \mathbf{Q}_{zr}, \mathbf{Q}_{za'}} \quad & R_{gsvd}^{PCJ} \\ \text{s.t.} \quad & \mathrm{tr}(\mathbf{Q}_{za} + \mathbf{Q}_{zb'}) \le P, \quad \mathrm{tr}(\mathbf{Q}_{zr} + \mathbf{Q}_{za'}) \le P \end{aligned} \quad (55)$$

where $R_{gsvd}^{PCJ} = I_d - I_e$ and P is the global power constraint.

Remark 3: The secrecy rate in this case does not have a form similar to (41), and finding the optimal power allocation for this case is generally intractable. Therefore, we will use Newton's method initialized with the optimal point from the GSVD-based relaying algorithm. Though this may not find the global optimum, we can at least gain insight into this strategy. The global power constraints in (55) are set for fair comparison with the case without cooperative jamming.

IV. Secure Relaying With Unknown ECSI

In this section, we assume that ECSI is unknown to the relay network. Thus, Alice and the Relay can no longer use beamforming methods like those based on the GSVD to selectively transmit information away from and jamming signals towards the eavesdropper. However, cooperative jamming can still be used to improve the secrecy of the information in the two-hop network. As described below, the approach we take to achieve this goal is to first meet a fixed target rate for the relay link, and then allocate all remaining resources to wide-area jamming, while guaranteeing that the jamming signal has no impact on the desired information.

We propose a cooperative jamming strategy in which the signal space is divided into two orthogonal subspaces, an information subspace and a jamming subspace. Both PCJ and FCJ approaches can be applied in this scenario. For PCJ, any available jamming power will only be allocated to information transmitters, while Bob (phase 1) and Alice (phase 2) remain inactive. For FCJ, both the transmitter and the temporary helpers can perform cooperative jamming in the jamming subspace, which will allow the legitimate receivers to use beamforming to reject interference from this subspace. Note that when using FCJ, cooperative jamming requires the receiver to broadcast the jamming subspace so that the interference can be aligned at the desired receiver without a loss of information. Although Eve may also be aware of this subspace, she can not remove the jamming signal since she sees different channels from the transmitters and jammers.

In phase 1, assume $span\{\mathbf{H}_{ar}\} = span\{\eta_1, \eta_2, \ldots, \eta_k, \eta_{k+1}, \ldots, \eta_m\}$, where k is no greater than the maximum possible number of data streams, and $\eta_1, \eta_2 \ldots, \eta_m$ form an orthonormal basis. The information and jamming subspaces are defined to be $\mathcal{S}_1$ and $\mathcal{J}_1$, respectively, where $\mathcal{S}_1 = span\{\eta_1, \eta_2, \ldots, \eta_k\}$ and $\mathcal{J}_1 = \mathcal{S}_1^{\perp}$. Assuming the receive beamformer matrix at the Relay is $\mathbf{W}_r = [\eta_1, \eta_2, \ldots, \eta_k]$, the signal received by the Relay is

$$\begin{aligned}\widetilde{\mathbf{y}}_r &= \mathbf{W}_r^H\left[\mathbf{H}_{ar}\left(\mathbf{T}_a\mathbf{z}_a + \mathbf{T}_a'\mathbf{z}_a'\right) + \mathbf{H}_{br}\mathbf{T}_b'\mathbf{z}_b' + \mathbf{n}_r\right] \\ &= \widetilde{\mathbf{H}}_{ar}\mathbf{z}_a + \widetilde{\mathbf{n}}_r\end{aligned} \quad (56)$$

where $\widetilde{\mathbf{H}}_{ar} = \mathbf{W}_r^H \mathbf{H}_{ar} \mathbf{T}_a$, $\mathbf{z}_a$ is the information signal vector transmitted by Alice with covariance $\mathbf{Q}_{za}$, $\mathbf{z}'_a$, and $\mathbf{z}'_b$ are jamming signals transmitted by Alice and Bob, with covariance matrices $\mathbf{Q}_{z'a}$ and $\mathbf{Q}_{z'b}$, respectively. The transmit beamformers are chosen such that $\mathbf{H}_{ar}\mathbf{T}_a\mathbf{z}_a \in \mathcal{S}_1$, and $\mathbf{H}_{ar}\mathbf{T}'_a\mathbf{z}'_a \in \mathcal{J}_1$, $\mathbf{H}_{br}\mathbf{T}'_b\mathbf{z}'_b \in \mathcal{J}_1$. The signal received by Eve in phase 1 is

$$\begin{aligned}\mathbf{y}_{e1} &= \mathbf{H}_{ae}\left(\mathbf{T}_a\mathbf{z}_a + \mathbf{T}'_a\mathbf{z}'_a\right) + \mathbf{H}_{be}\mathbf{T}'_b\mathbf{z}'_b + \mathbf{n}_{e1} \\ &= \widetilde{\mathbf{H}}_{ae}\mathbf{z}_a + \widetilde{\mathbf{n}}_{e1} \end{aligned} \tag{57}$$

where $\widetilde{\mathbf{n}}_{e1} = \mathbf{H}_{ae}\mathbf{T}'_a\mathbf{z}'_a + \mathbf{H}_{be}\mathbf{T}'_b\mathbf{z}'_b + \mathbf{n}_{e1}$.

In phase 2, signal $\mathcal{S}_2$ and jamming $\mathcal{J}_2$ subspaces are chosen from $span\{\mathbf{H}_{rb}\}$, and similar to phase 1, the signals at Bob and Eve are

$$\begin{aligned}\widetilde{\mathbf{y}}_b &= \mathbf{W}_b^H\left[\mathbf{H}_{rb}\left(\mathbf{T}_r\mathbf{z}_r + \mathbf{T}'_r\mathbf{z}'_r\right) + \mathbf{H}_{ab}\mathbf{T}'_{a2}\mathbf{z}'_{a2} + \mathbf{n}_b\right] \\ &= \widetilde{\mathbf{H}}_{rb}\mathbf{z}_r + \widetilde{\mathbf{n}}_b \end{aligned} \tag{58}$$

$$\begin{aligned}\mathbf{y}_{e2} &= \mathbf{H}_{re}\left(\mathbf{T}_r\mathbf{z}_r + \mathbf{T}'_r\mathbf{z}'_r\right) + \mathbf{H}_{ae}\mathbf{T}'_{a2}\mathbf{z}'_{a2} + \mathbf{n}_{e2} \\ &= \widetilde{\mathbf{H}}_{re}\mathbf{z}_r + \widetilde{\mathbf{n}}_{e2} \end{aligned} \tag{59}$$

where $\widetilde{\mathbf{H}}_{rb} = \mathbf{W}_b^H\mathbf{H}_{rb}\mathbf{T}_r$, $\widetilde{\mathbf{H}}_{re} = \mathbf{H}_{re}\mathbf{T}_r$, and $\widetilde{\mathbf{n}}_{e2} = \mathbf{H}_{re}\mathbf{T}'_r\mathbf{z}'_r + \mathbf{H}_{ae}\mathbf{T}'_{a2}\mathbf{z}'_{a2} + \mathbf{n}_{e2}$, $\mathbf{z}_r$ is the information signal transmitted by the Relay with covariance $\mathbf{Q}_{zr}$, $\mathbf{z}'_{a2}$, and $\mathbf{z}'_r$ are jamming signals transmitted by Alice and the Relay, with covariance matrices $\mathbf{Q}_{z'a2}$ and $\mathbf{Q}_{z'r}$, respectively. As before, the beamformers $\mathbf{T}_r$ and $\mathbf{T}'_r$ force $\mathbf{H}_{rb}\mathbf{T}_r\mathbf{z}_r \in \mathcal{S}_2$, and $\mathbf{H}_{rb}\mathbf{T}'_r\mathbf{z}'_r \in \mathcal{J}_2$, $\mathbf{H}_{ab}\mathbf{T}'_{a2}\mathbf{z}'_{a2} \in \mathcal{J}_2$.

The cooperative scheme outlined in this section involves the allocation of power and the number of dimensions for the information and jamming subspaces. If the MIMO channel is rich enough, more dimensions allocated to the signal subspace increases the amount of power available for jamming, but leads to a smaller dimensional jamming subspace for both transmitters and cooperative jammers. More antennas for Eve usually requires a higher dimensional jamming subspace, especially when ECSI is unknown to the transmitters. One of the advantages of FCJ in this case is that in addition to the preassigned jamming subspace of dimension $N_a - k$ (for phase 1), the helpers provide jamming support in additional dimensions due to the fact they have different channels to Eve. Taking the transmission in phase 1 as an example, assuming k dimensions are assigned to the information subspace, the jamming subspace seen from Eve will be greater than $N_a - k$. In particular, $N_a - k \leq dim(span\{\mathbf{H}_{ae}\mathbf{T}'_a\} \cap span\{\mathbf{H}_{be}\mathbf{T}'_b\}) \leq 2(N_a - k)$.

Therefore, the tradeoff between power and allocation of the jamming subspace dimension needs to be considered. In this case, we propose to use an approach similar to that in [24] and minimize the product of the power allocated to the information signal and the dimension of the information subspace, $(p_a + p_r)k$, such that the fixed target rate for the relay transmission is achieved. We then allocate all the remaining dimensions and power for jamming. Since the ECSI is not known, the jamming power will be uniformly distributed among all available dimensions at the transmitters and cooperative jammers. Assuming the target rate for the relay transmission is R_t, we have the following FCJ algorithm:

Algorithm 2: FCJ with unknown ECSI

1) **Initialize** $svd(\mathbf{H}_{ar}) = \mathbf{U}_{ar}\mathbf{\Sigma}_{ar}\mathbf{V}_{ar}^H$ and $svd(\mathbf{H}_{rb}) = \mathbf{U}_{rb}\mathbf{\Sigma}_{rb}\mathbf{V}_{rb}^H$.
2) **While** $i \leq s$
   - Let $\mathbf{W}_r = \mathbf{U}_{ar}[:, 1:i]$, $\mathbf{W}_b = \mathbf{U}_{rb}[:, 1:i]$, $\mathbf{T}_a = \mathbf{V}_{ar}[:, 1:i]$, $\mathbf{T}_r = \mathbf{V}_{rb}[:, 1:i]$.
   - Let $\mathbf{T}'_a = \mathbf{V}_{ar}[:, i+1:N_a]$, $\mathbf{T}'_r = \mathbf{V}_{rb}[:, i+1:N_r]$.
   - Let $svd(\mathbf{W}_r^H\mathbf{H}_{br}) = \mathbf{U}_{br}\mathbf{\Sigma}_{br}\mathbf{V}_{br}^H$, $\mathbf{T}'_b = \mathbf{V}_{br}[:, i+1:N_b]$, and $svd(\mathbf{W}_b^H\mathbf{H}_{ab}) = \mathbf{U}_{ab}\mathbf{\Sigma}_{ab}\mathbf{V}_{ab}^H$, $\mathbf{T}'_{a2} = \mathbf{V}_{ab}[:, i+1:N_a]$.
   - Solve the following problem:

$$\begin{aligned} & p_a^{(i)} = \min\ \mathrm{tr}(\mathbf{Q}_{za}), \quad p_r^{(i)} = \min\ \mathrm{tr}(\mathbf{Q}_{zr}) \\ & \text{s.t. } \frac{1}{2}\log_2\det\left(\mathbf{I} + \frac{1}{\sigma^2}\widetilde{\mathbf{H}}_{ar}\mathbf{Q}_{za}\widetilde{\mathbf{H}}_{ar}^H\right) = R_t \\ & \quad \frac{1}{2}\log_2\det\left(\mathbf{I} + \frac{1}{\sigma^2}\widetilde{\mathbf{H}}_{rb}\mathbf{Q}_{zr}\widetilde{\mathbf{H}}_{rb}^H\right) = R_t \end{aligned}$$

     where the water filling algorithm is used to determine $\mathbf{Q}_{za}$ and $\mathbf{Q}_{zr}$.
3) Find $k = \arg\min_i[p_a^{(i)} + p_r^{(i)}] \cdot i$, and determine all beamformers for the resulting k.
4) Allocate $p_a^{(k)}$ to $\mathrm{diag}\{\mathbf{Q}_{za}\}$, and $p_r^{(k)}$ to $\mathrm{diag}\{\mathbf{Q}_{zr}\}$ using water filling.
5) Uniformly allocate $P - p_a^{(k)}$ to $diag\{\mathbf{Q}_{z'a}, \mathbf{Q}_{z'b}\}$, and $P - p_r^{(k)}$ to $diag\{\mathbf{Q}_{z'r}, \mathbf{Q}_{z'a2}\}$.

The PCJ algorithm in the unknown-ECSI case is similar to that for FCJ, except that jamming support will not be provided by Bob (in phase 1) and Alice (in phase 2), and thus the beamformers $\mathbf{T}'_b$ and $\mathbf{T}'_{a2}$ in step 2 will not be used. In step 5, when the necessary amount of power for information signals is assigned, all remaining jamming power will be used by Bob and Alice in phase 1 and phase 2, respectively; i.e., the power $P - p_a^{(k)}$ and $P - p_r^{(k)}$ will instead be assigned to $diag\{\mathbf{Q}_{z'a}\}$ and $diag\{\mathbf{Q}_{z'r}\}$. In either approach, the optimization problem in step 2 can be solved with a simple line search. If the minimum rate R_t cannot be achieved with the available power, the link is assumed to be in outage. In this algorithm, we assume that the Relay uses the same information dimension as Alice, as discussed in Section II. However, using different information dimensions for the two phases with a more complicated coding scheme may also be an interesting case to consider for future work.

V. Numerical Results

In the following simulations, the elements of all the channel matrices are assumed to be i.i.d. complex Gaussian. As shown in Fig. 2, Alice, Bob, the Relay and Eve are assumed to be located at $(-0.5, 0)$, $(0.5, 0)$, $(0, 0)$, $(d_x, -0.5)$ respectively, where distances are expressed in kilometers. We adopt a simple transmission model in which the standard deviation of each channel coefficient is inversely proportional to the distance between two nodes. We assume a path-loss coefficient of 3, and the same

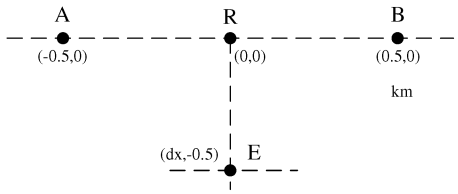

Fig. 2. Simulation scenario showing locations for Alice(A), Bob(B), Relay(R), and Eve(E).

background noise power $\sigma^2 = -60$ dBm at all nodes. All results are calculated based on an average of 3000 independent trials.

For the known-ECSI case discussed in Section III, we examine the performance of the following three schemes: PCJ for single data stream relaying (Section III-A), simple GSVD-relaying (Section III-B-1) and also GSVD-PCJ (Section III-B-2) for multiple data streams. For the unknown ECSI case discussed in Section IV, both the FCJ and PCJ approaches are simulated. For each of these schemes, we also examine the impact of both global and individual power constraints. For the case of individual power constraints, we assume the total transmit power to be evenly distributed to all transmit nodes. Furthermore, in order to examine the performance gain of the proposed cooperative jamming schemes and optimization algorithms, we also investigate cases using uniform power allocation, as well as cases involving conventional relay transmissions without jamming.

The secrecy rate as a function of transmit power is shown in Fig. 3 for a case with known ECSI, where Alice and Bob both have four antennas, and the Relay and Eve each has one. Eve is assumed to be located closer to the Relay at $(0, -0.5)$, which (as will be seen in the next example) is usually the worst-case assumption for the relay link. This will be the default assumption unless otherwise specified. Compared to traditional DF relaying, the PCJ schemes provide a significant improvement in terms of secrecy rate in the medium and high SNR regime. The benefit of having the flexibility associated with a global power constraint over fixed individual power constraints is clearly evident. Also, the performance gain of using geometric programming for power allocation is obvious, compared to the uniform power allocation scheme. We can also see that even the conventional relaying scheme is better than PCJ schemes with individual or uniform power allocation when the transmit power is low. This is because, with a less flexible power adjustment, a fraction of power that could have brought higher secrecy rate if used for data transmission is wasted on jamming signals. This illustrates the importance of an efficient power allocation if cooperative jamming support is applied.

Fig. 4 presents the impact of Eve's location on the transmit power fraction for both the information and jamming signals, assuming that the global transmit power is limited to 10 dBm. Unlike the settings in Fig. 3, Eve has four antennas in this scenario, which provides her with increased eavesdropping abilities. In this case, we plot the secrecy rate performance as Eve moves from $(-1, -0.5)$ to $(1, -0.5)$. The secrecy rate is smallest when Eve is at the midpoint $(0, -0.5)$, and increases in either direction away from $(0, -0.5)$. Note also that the fraction of the transmit

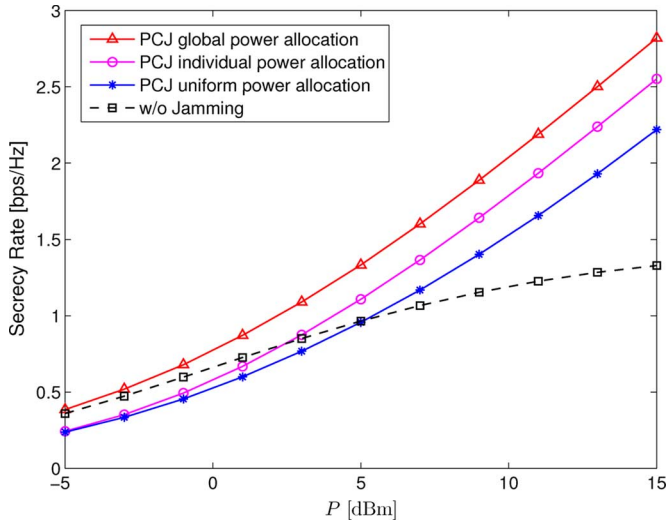

Fig. 3. Secrecy rate versus transmit power for $N_a = 4$, $N_b = 4$, $N_e = 1$, $N_r = 1$, and Eve located at $(0, -0.5)$.

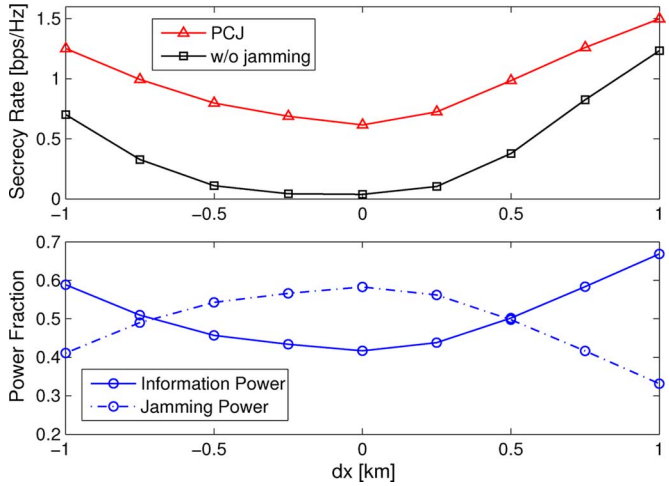

Fig. 4. Secrecy rate and transmit power fraction versus eavesdropper location for $N_a = 4$, $N_b = 4$, $N_e = 4$, $N_r = 1$, global power constraint $P = 10$ dBm, and Eve's location varies from $(-1, -0.5)$ to $(1, -0.5)$.

power devoted to jamming also decreases as Eve moves away from the midpoint. This behavior is due to the fact that, when Eve is closer to either Alice or Bob, most of her information about the desired signal comes from only one of the hops, due to the fact that the other hop is farther away and can be effectively jammed with minimal power by the transmitter she is closest to. This is the primary benefit of the cooperative jamming support provided by PCJ.

The performance of GSVD-based relaying without cooperative jamming and GSVD-based PCJ strategies, where the relay link transmits multiple data streams, is shown in Fig. 5. Here we see that cooperative jamming with global power allocation provides considerable gain in secrecy rate over other schemes. However, the use of individual power constraints significantly degrades the benefit of the jamming signals, although it still approaches and even surpasses the performance of GSVD-relaying with optimal power allocation when the transmit power is higher. In addition, we also see the benefit of Algorithm 1 for

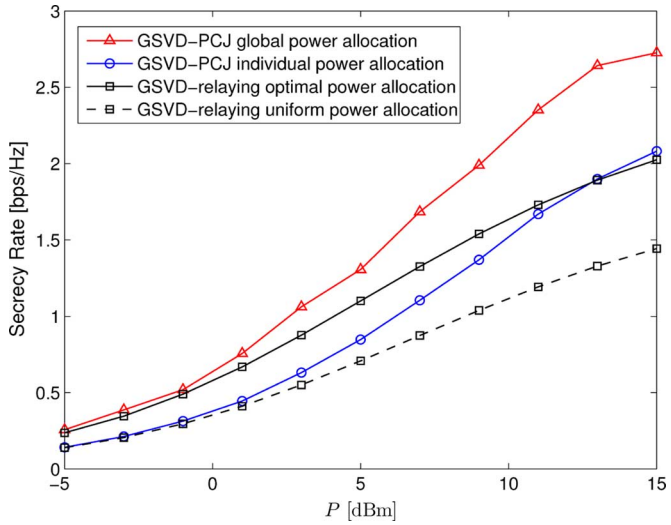

Fig. 5. Secrecy rate versus transmit power for $N_a = 4$, $N_b = 4$, $N_e = 4$, $N_r = 4$, and Eve located at $(0, -0.5)$.

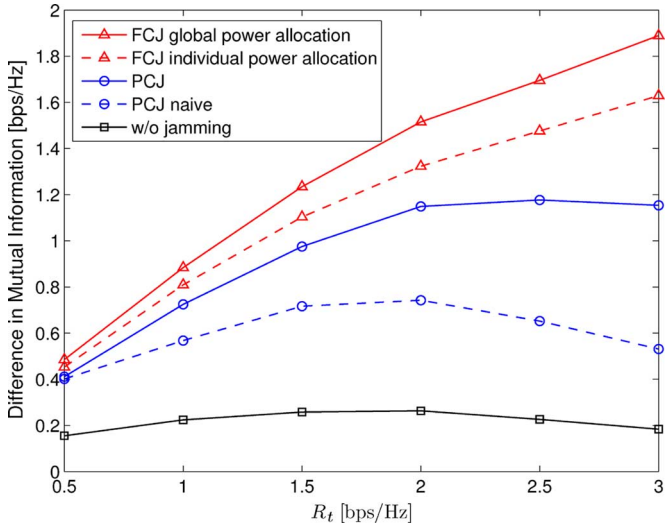

Fig. 6. Secrecy performance versus rate constraint for relay link when ECSI is unknown, $N_a = 4$, $N_b = 4$, $N_e = 4$, $N_r = 4$, Eve located at $(0, -0.5)$, $P = 15$ dBm.

power allocation in the GSVD-relaying scheme, compared with using simple uniform power allocations.

Finally we consider examples for the case where ECSI is not available. The transmit power P is set to be 15 dBm in these examples. In Fig. 6, all nodes are equipped with four antennas, and the secrecy performance is given as a function of the rate constraint at Bob. For purpose of comparison, a naive PCJ scheme that uses the criterion $\min(p_a + p_r)$ (instead of $\min(p_a + p_r)k$ as discussed in Section IV) is also simulated. It can be seen that if no jamming signals are used, there is little difference between the mutual information at Bob and that at Eve, and thus we expect the secrecy of the message to be low. Similar to Fig. 3, the individual power constraint will reduce the secrecy performance due to the inefficiency of the power assignment. We can see that FCJ achieves a big performance gain compared with PCJ as R_t increases, since FCJ leads to a higher dimensional jamming subspace than PCJ, although they transmit with the same jamming power. In addition, the performance of PCJ begins to level off and even drop for high R_t, since more power is allocated to information signals, and the protection from eavesdropping is reduced.

Fig. 7 provides a detailed look at how the number of eavesdropper antennas affects the performance of the different cooperative jamming schemes. In this case, we fix the target rate for relay transmission to be $R_t = 1$ bps/Hz. Alice, Bob, and the Relay are equipped with four antennas, and the number of Eve's antennas increases from one to eight. It can be seen that when Eve has only one antenna, little advantage is observed for FCJ since Eve only receives single-dimensional signals. However, as the capability of the eavesdropper increases (i.e., when Eve has more antennas), the relative gain of FCJ over PCJ increases, although the performance of all methods decreases.

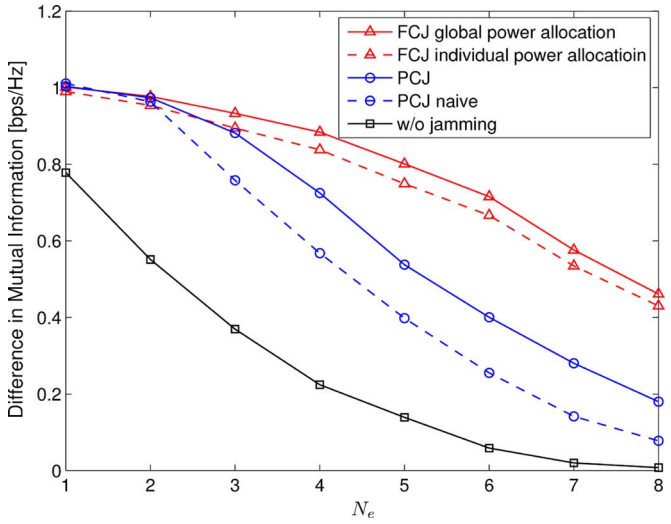

Fig. 7. Secrecy performance versus eavesdropper antenna number when ECSI is unknown, $N_a = 4$, $N_b = 4$, $N_r = 4$, Eve located at $(0, -0.5)$, fixed target rate $R_t = 1$ bps/Hz, $P = 15$ dBm.

VI. Conclusion

In this paper, we have proposed partial cooperative jamming (PCJ) and full cooperative jamming (FCJ) strategies for two-hop DF relay systems in the presence of an eavesdropper that can wiretap both transmission phases. Both single and multiple data stream transmission scenarios were considered. For single data stream relaying, the system design was conducted from the perspective of secrecy rate maximization and transmit power minimization. By adopting the zero-forcing constraint that the jamming signals be nulled out at the intended receivers, we obtained closed-form expressions for the jamming beamformers and the corresponding power allocation. For the case of multiple data stream transmission, we proposed a GSVD-based relaying scheme without jamming, as well as a GSVD-based PCJ scheme. The latter shows a significant performance improvement even though only a potentially suboptimal power allocation scheme is used. We also studied the secure relaying problem when the eavesdropper's CSI is unknown. Instead of maximizing the secrecy rate, a more reasonable relaying scheme with both PCJ and FCJ is proposed in which a target

QoS for the relay network is met, and only the remaining resources are used for jamming. These schemes are shown to provide large gains in terms of the difference in the mutual information between the desired receiver and the eavesdropper. In particular, FCJ is shown to be a better choice when the eavesdropper's CSI is unavailable since the ability to exploit additional jamming subspace dimensions is preferable when the transmitters possess no information about the eavesdropper.

APPENDIX A
SDP FOR PROBLEM (25)

Let $\tilde{\mathbf{Q}}_{zb'} = \mathbf{T}'_b\mathbf{Q}_{zb'}\mathbf{T}'^H_b$, where $\mathbf{T}'_b$ is normalized such that $\mathrm{tr}(\tilde{\mathbf{Q}}_{zb'}) = \mathrm{tr}(\mathbf{Q}_{zb'})$. Problem (25) is equivalent to

$$\min_{\tilde{\mathbf{Q}}_{zb'}\succeq 0,\mu\geq 0} \quad \mu \tag{60a}$$

$$\text{s.t.} \quad \mathbf{t}_a^H\mathbf{H}_{ae}^H\left(\mathbf{H}_{be}\tilde{\mathbf{Q}}_{zb'}\mathbf{H}_{be}^H+\sigma^2\mathbf{I}\right)^{-1}\mathbf{H}_{ae}\mathbf{t}_a \leq \mu \tag{60b}$$

$$\mathrm{tr}(\tilde{\mathbf{Q}}_{zb'}) \leq p_b. \tag{60c}$$

Using the Schur complement [32], constraint (60b) can be written as

$$\begin{bmatrix} \mu & \mathbf{H}_{ae}^H\mathbf{t}_a^H \\ \mathbf{H}_{ae}\mathbf{t}_a & \mathbf{H}_{be}\tilde{\mathbf{Q}}_{zb'}\mathbf{H}_{be}^H+\sigma^2\mathbf{I}\end{bmatrix}\succeq 0. \tag{61}$$

Combining (61) with the trace constraint and the semidefinite constraints on $\tilde{\mathbf{Q}}_{zb'}$, the equivalent problem becomes

$$\min \quad \mu \tag{62a}$$

$$\text{s.t.} \quad \mathrm{tr}(\tilde{\mathbf{Q}}_{zb'}) \leq p_b, \tilde{\mathbf{Q}}_{zb'}\succeq 0, \mu\geq 0, \mathbf{h}_{br}\tilde{\mathbf{Q}}_{zb'} = \mathbf{0} \tag{62b}$$

$$\begin{bmatrix} \mu & \mathbf{H}_{ae}^H\mathbf{t}_a^H \\ \mathbf{H}_{ae}\mathbf{t}_a & \mathbf{H}_{be}\tilde{\mathbf{Q}}_{zb'}\mathbf{H}_{be}^H+\sigma^2\mathbf{I}\end{bmatrix}\succeq 0. \tag{62c}$$

This is an SDP that consists of a linear objective function, a linear equality constraint, and a set of linear matrix inequalities (LMIs) [34], and thus can be solved efficiently, and $\mathbf{T}'_b$ can be obtained via the eigenvalue decomposition of $\tilde{\mathbf{Q}}_{zb'}$.

APPENDIX B
PROOF OF LEMMA 1

Given any jamming beamformer $\mathbf{T}'_b$, (25) becomes

$$\min_{\mathbf{Q}_{zb'}\succeq 0} \; f(\mathbf{Q}_{zb'}) \quad \text{s.t. } \mathrm{tr}(\mathbf{Q}_{zb'}) \leq p_b \tag{63}$$

where

$$f(\mathbf{Q}_{zb'}) = \mathbf{t}_a^H\mathbf{H}_{ae}^H\left(\mathbf{H}_{be}\mathbf{T}'_b\mathbf{Q}_{zb'}\mathbf{T}'^H_b\mathbf{H}_{be}^H+\sigma^2\mathbf{I}\right)^{-1}\mathbf{H}_{ae}\mathbf{t}_a$$

and the Lagrangian of (63) is

$$L(\mathbf{Q}_{zb'},\lambda,\mathbf{\Phi}) = f(\mathbf{Q}_{zb'}) + \lambda\left(\mathrm{tr}(\mathbf{Q}_{zb'})-p_b\right) - \mathrm{tr}(\mathbf{\Phi}\mathbf{Q}_{zb'}) \tag{64}$$

where $\lambda \geq 0$ is the Lagrange multiplier associated with the inequality constraint $\mathrm{tr}(\mathbf{Q}_{zb'}) \leq p_b$, and $\mathbf{\Phi}\succeq 0$ is the Lagrange multiplier associated with the inequality constraint $\mathbf{Q}_{zb'}\succeq 0$. Next, we can obtain the necessary conditions for the optimal $\mathbf{Q}_{zb'}$ by using the KKT conditions:

$$\mathrm{tr}(\mathbf{Q}_{zb'}) \leq p_b,\ \mathbf{Q}_{zb'}\succeq 0,\ \lambda\geq 0,\ \mathbf{\Phi}\succeq 0 \tag{65}$$

$$\mathrm{tr}(\mathbf{\Phi}\mathbf{Q}_{zb'}) = 0 \tag{66}$$

$$\lambda\left(\mathrm{tr}(\mathbf{Q}_{zb'})-p_b\right) = 0 \tag{67}$$

$$\mathbf{\Phi}-\mathbf{\Theta} = \lambda\mathbf{I} \tag{68}$$

where $\mathbf{\Theta}$ is obtained by differentiating $f(\mathbf{Q}_{zb'})$ with respect to $\mathbf{Q}_{zb'}$, and is given by

$$\mathbf{\Theta} = -\mathbf{H}_{be}^H\mathbf{T}'^H_b\left(\mathbf{H}_{be}\mathbf{T}'_b\mathbf{Q}_{zb'}\mathbf{T}'^H_b\mathbf{H}_{be}^H+\sigma^2\mathbf{I}\right)^{-1} \times\mathbf{H}_{ae}\mathbf{t}_a\mathbf{t}_a^H\mathbf{H}_{ae}^H\left(\mathbf{H}_{be}\mathbf{T}'_b\mathbf{Q}_{zb'}\mathbf{T}'^H_b\mathbf{H}_{be}^H+\sigma^2\mathbf{I}\right)^{-1}\mathbf{T}'_b\mathbf{H}_{be}.$$

Since $\mathbf{t}_a$ is a vector, it is obvious that $\mathbf{\Theta}$ is a rank-one negative semidefinite matrix.

For the case that $\lambda = 0$, according to (68), we have $\mathbf{\Theta} = \mathbf{\Phi}$. Since $\mathbf{\Theta}$ has a negative eigenvalue, $\mathbf{\Phi}$ will also have a negative eigenvalue, which contradicts the fact that $\mathbf{\Phi}$ is positive semidefinite. Thus λ can only be positive. For $\lambda > 0$, according to (68), we know that $\mathbf{\Phi}-\mathbf{\Theta}$ is a positive definite matrix. Therefore, $\mathbf{\Phi}$ has at least $N-1$ positive eigenvalues, i.e., $\mathrm{rank}(\mathbf{\Phi}) \geq N-1$, in order to keep $\mathbf{\Phi}-\mathbf{\Theta}\succ 0$.

Assuming $\lambda_i(\mathbf{\Phi})$ and $\lambda_i(\mathbf{Q}_{zb'})$, $i=\{1,2,\ldots,N\}$ are eigenvalues of $\mathbf{\Phi}$ and $\mathbf{Q}_{zb'}$, respectively, in nonincreasing order, and due to the fact that $\mathbf{\Phi}$ and $\mathbf{Q}_{zb'}$ are both positive semidefinite matrices, we know that $\mathrm{tr}(\mathbf{\Phi}\mathbf{Q}_{zb'}) \geq \sum_{i=1}^N \lambda_i(\mathbf{\Phi})\lambda_{N-i+1}(\mathbf{Q}_{zb'})$ [37]. Combining this observation with (66), we have

$$\sum_{i=1}^N \lambda_i(\mathbf{\Phi})\lambda_{N-i+1}(\mathbf{Q}_{zb'}) = 0. \tag{69}$$

Thus we can conclude that $rank(\mathbf{\Phi}) \neq N$, since otherwise all eigenvalues of $\mathbf{Q}_{zb'}$ are zero and no jamming signals are transmitted. Combining this conclusion and the observation that $rank(\mathbf{\Phi}) \geq N-1$, we can conclude that $rank(\mathbf{\Phi}) = N-1$. Therefore, according to (69), we have $\lambda_1(\mathbf{Q}_{zb'}) > 0$ and $\lambda_{i\neq 1}(\mathbf{Q}_{zb'}) = 0$, which indicates that $rank(\mathbf{Q}_{zb'}) = 1$, and the proof is complete.

APPENDIX C
PROOF OF PROPOSITION 1

According to the signal model given in Section II-A, the signals received by Eve during both phases can be combined together as

$$\mathbf{y}_e = \begin{bmatrix}\mathbf{H}_{ae}\mathbf{T}_a\mathbf{D}_a \\ \mathbf{H}_{re}\mathbf{T}_r\mathbf{D}_r\end{bmatrix}\mathbf{z} + \begin{bmatrix}\mathbf{n}_{e1}\\ \mathbf{n}_{e2}\end{bmatrix} = \widetilde{\mathbf{H}}_e\mathbf{z}+\widetilde{\mathbf{n}}_e \tag{70}$$

where $\mathbf{D}_k = \mathrm{diag}\{\sqrt{p_{k,i}}\}$ and $\mathbb{E}(\mathbf{z}\mathbf{z}^H) = \mathbf{Q}_z = \mathbf{I}$.

Using the transmit beamformers in (40), and denoting $\mathbb{E}(\mathbf{z}_a\mathbf{z}_a^H) = \mathbf{Q}_{za} = diag\{p_{a,1},\cdots,p_{a,s}\}$, $\mathbb{E}(\mathbf{z}_r\mathbf{z}_r^H) = \mathbf{Q}_{zr} = diag\{p_{r,1},\cdots,p_{r,s}\}$, the mutual information between Alice and Bob is

$$I_d = \min\left\{\frac{1}{2}\log_2\det\left(\mathbf{I}+\frac{1}{\sigma^2}\mathbf{H}_{ar}\mathbf{T}_a\mathbf{Q}_{za}\mathbf{T}_a^H\mathbf{H}_{ar}^H\right),\right. \left.\frac{1}{2}\log_2\det\left(\mathbf{I}+\frac{1}{\sigma^2}\mathbf{H}_{rb}\mathbf{T}_r\mathbf{Q}_{zr}\mathbf{T}_r^H\mathbf{H}_{rb}^H\right)\right\} \tag{71}$$

where

$$\frac{1}{2}\log_2\det\left(\mathbf{I}+\frac{1}{\sigma^2}\mathbf{H}_{ar}\mathbf{T}_a\mathbf{Q}_{za}\mathbf{T}_a^H\mathbf{H}_{ar}^H\right)$$
$$=\frac{1}{2}\log_2\det\left(\mathbf{I}+\frac{1}{\sigma^2}\mathbf{S}_{ar}\mathbf{Q}_{za}\mathbf{S}_{ar}^H\right)$$
$$=\frac{1}{2}\log_2\prod_{i=1}^{s}\left(1+\frac{p_{a,i}s_{ar,i}^2}{\sigma^2\left\|\mathbf{R}_a^{-1}\right\|^2}\right) \quad (72)$$

and

$$\frac{1}{2}\log_2\det\left(\mathbf{I}+\frac{1}{\sigma^2}\mathbf{H}_{rb}\mathbf{T}_r\mathbf{Q}_{zr}\mathbf{T}_r^H\mathbf{H}_{rb}^H\right)$$
$$=\frac{1}{2}\log_2\det\left(\mathbf{I}+\frac{1}{\sigma^2}\mathbf{S}_{rb}\mathbf{Q}_{zr}\mathbf{S}_{rb}^H\right)$$
$$=\frac{1}{2}\log_2\prod_{i=1}^{s}\left(1+\frac{p_{r,i}s_{rb,i}^2}{\sigma^2\left\|\mathbf{R}_r^{-1}\right\|^2}\right). \quad (73)$$

For Eve, we have

$$I_e=\min\left\{\frac{1}{2}\log_2\det\left(\mathbf{I}+\frac{1}{\sigma^2}\widetilde{\mathbf{H}}_{ar}\mathbf{Q}_{za}\widetilde{\mathbf{H}}_{ar}^H\right),\right.$$
$$\left.\frac{1}{2}\log_2\det\left(\mathbf{I}+\frac{1}{\sigma^2}\widetilde{\mathbf{H}}_{e}\mathbf{Q}_{z}\widetilde{\mathbf{H}}_{e}^H\right)\right\} \quad (74)$$

where

$$\frac{1}{2}\log_2\det\left(\mathbf{I}+\frac{1}{\sigma^2}\widetilde{\mathbf{H}}_{e}\mathbf{Q}_{z}\widetilde{\mathbf{H}}_{e}^H\right)$$
$$=\frac{1}{2}\log_2\det\left(\mathbf{I}+\frac{1}{\sigma^2}\widetilde{\mathbf{H}}_{e}^H\widetilde{\mathbf{H}}_{e}\right)$$
$$=\frac{1}{2}\log_2\det\left(\mathbf{I}+\frac{1}{\sigma^2}\left(\mathbf{D}_a^H\mathbf{S}_{ae}^H\mathbf{S}_{ae}\mathbf{D}_a+\mathbf{D}_r^H\mathbf{S}_{re}^H\mathbf{S}_{re}\mathbf{D}_r\right)\right)$$
$$=\frac{1}{2}\log_2\prod_{i=1}^{s}\left(1+\frac{p_{a,i}s_{ae,i}^2}{\sigma^2\left\|\mathbf{R}_a^{-1}\right\|^2}+\frac{p_{r,i}s_{re,i}^2}{\sigma^2\left\|\mathbf{R}_r^{-1}\right\|^2}\right) \quad (75)$$

and according to the same secrecy constraints in (16), the secrecy rate (41) can be obtained.

ACKNOWLEDGMENT

The authors would like to thank Dr. L. Dong for his helpful comments on an earlier draft of this work. They would also like to thank the anonymous reviewers for their insightful comments and suggestions.

REFERENCES

[1] 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.

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

[3] M. Debbah, "Mobile flexible networks: The challenges ahead," in *Proc. Int. Conf. Adv. Technol. Commun. (ATC)*, Oct. 2008, pp. 3–7.

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

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

[6] P. Parada and R. Blahut, "Secrecy capacity of SIMO and slow fading channels," in *Proc. Int. Symp. Inf. Theory (ISIT)*, Sep. 2005, pp. 2152–2155.

[7] 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.

[8] S. Shafiee and S. Ulukus, "Achievable rates in Gaussian MISO channels with secrecy constraints," in *Proc. IEEE Int. Symp. Inf. Theory (ISIT)*, Jun. 2007, pp. 2466–2470.

[9] R. Liu, R. Bustin, S. Shamai, and H. V. Poor, "An MMSE approach to the secrecy capacity of the MIMO Gaussian wiretap channel," in *Proc. IEEE Int. Symp. Inf. Theory (ISIT)*, Jun. 2009, pp. 2602–2606.

[10] F. Oggier and B. Hassibi, "The secrecy capacity of the MIMO wiretap channel," in *Proc. IEEE Int. Symp. Inf. Theory (ISIT)*, Jul. 2008, pp. 524–528.

[11] T. Liu and S. Shamai, "A note on the secrecy capacity of the multiple-antenna wiretap channel," *IEEE Trans. Inf. Theory*, vol. 55, no. 6, pp. 2547–2553, Jun. 2009.

[12] Z. Li, W. Trappe, and R. Yates, "Secret communication via multi-antenna transmission," in *Proc. 41st Ann. Conf. Inf. Sci. Syst. (CISS)*, Mar. 2007, pp. 905–910.

[13] A. Khisti, G. Wornell, A. Wiesel, and Y. Eldar, "On the Gaussian MIMO wiretap channel," in *Proc. IEEE Int. Symp. Inf. Theory (ISIT)*, Jun. 2007, pp. 2471–2475.

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

[15] A. L. Swindlehurst, "Fixed SINR solutions for the MIMO wiretap channel," in *Proc. IEEE Int. Conf. Acoust., Speech Signal Process. (ICASSP)*, Apr. 2009, pp. 2437–2440.

[16] J. Huang and A. L. Swindlehurst, "Robust secure transmission in MISO channels based on worst-case optimization," Apr. 2011 [Online]. Available: http://arxiv.org/abs/1104.3161

[17] Y. Oohama, "Capacity theorems for relay channels with confidential messages," in *Proc. IEEE Int. Symp. Inf. Theory (ISIT)*, Jun. 2007, pp. 926–930.

[18] E. Tekin and A. Yener, "The general Gaussian multiple-access and two-way wiretap channels: Achievable rates and cooperative jamming," *IEEE Trans. Inf. Theory*, vol. 54, no. 6, pp. 2735–2751, Jun. 2008.

[19] X. He and A. Yener, "Two-hop secure communication using an untrusted relay," *EURASIP J. Wireless Commun. Netw.*, vol. 2009, pp. 1–13, 2009.

[20] L. Lai and H. El Gamal, "The relay-eavesdropper channel: Cooperation for secrecy," *IEEE Trans. Inf. Theory*, vol. 54, no. 9, pp. 4005–4019, Sep. 2008.

[21] 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.

[22] J. Zhang and M. C. Gursoy, "Collaborative relay beamforming for secrecy," in *Proc. IEEE Int Commun. Conf (ICC)*, May 2010, pp. 1–5.

[23] J. Wang and A. L. Swindlehurst, "Cooperative jamming in MIMO ad-hoc networks," in *Proc. 43rd Asilomar Conf. Signals, Syst. Comput.*, Nov. 2009, pp. 1719–1723.

[24] A. Mukherjee and A. L. Swindlehurst, "Fixed-rate power allocation strategies for enhanced secrecy in MIMO wiretap channels," in *Proc. 10th IEEE Int. Workshop on Signal Process. Adv. Wireless Commun. (SPAWC)*, Jun. 2009, pp. 344–348.

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

[26] M. Yuksel and E. Erkip, "Secure communication with a relay helping the wire-tapper," in *Proc. IEEE Inf. Theory Workshop (ITW)*, Sep. 2007, pp. 595–600.

[27] J. N. Laneman and G. W. Wornell, "Distributed space-time-coded protocols for exploiting cooperative diversity in wireless networks," *IEEE Trans. Inf. Theory*, vol. 49, no. 10, pp. 2415–2425, Oct. 2003.

[28] K. Azarian, H. El Gamal, and P. Schniter, "On the achievable diversity-multiplexing tradeoff in half-duplex cooperative channels," *IEEE Trans. Inf. Theory*, vol. 51, no. 12, pp. 4152–4172, Dec. 2005.

[29] J. Li and A. P. Petropulu, "On ergodic secrecy rate for Gaussian MISO wiretap channels," *IEEE Trans. Wireless Commun.*, vol. 10, no. 4, pp. 1176–1187, Apr. 2011.

[30] X. He and A. Yener, "MIMO wiretap channels with arbitrarily varying eavesdropper channel states," Jul. 2010 [Online]. Available: http://arxiv.org/abs/1007.4801
[31] J. N. Laneman, D. N. C. Tse, and G. W. Wornell, "Cooperative diversity in wireless networks: Efficient protocols and outage behavior," *IEEE Trans. Inf. Theory*, vol. 50, no. 12, pp. 3062–3080, Dec. 2004.
[32] G. H. Golub and C. F. Van Loan, *Matrix Computations*. Baltimore, MD: The Johns Hopkins Univ. Press, 1996.
[33] 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.
[34] S. P. Boyd and L. Vandenberghe, *Convex Optimization*. Cambridge, U.K.: Cambridge Univ. Press, 2004.
[35] M. Chiang, C. W. Tan, D. P. Palomar, D. O'Neill, and D. Julian, "Power control by geometric programming," *IEEE Trans. Wireless Commun.*, vol. 6, no. 7, pp. 2640–2651, Jul. 2007.
[36] S. Boyd, S. J. Kim, L. Vandenberghe, and A. Hassibi, "A tutorial on geometric programming," *Optimiz. Eng.*, vol. 8, no. 1, pp. 67–127, Apr. 2007.
[37] A. W. Marshall and I. Olkin, *Inequalities: Theory of Majorization and Its Applications*. New York: Academic, 1979.

Jing Huang (S'10) received the B.S. degree in communication engineering from Jilin University, Changchun, China, in 2006, and the M.S. degree in communications and information systems from Beijing University of Posts and Telecommunications, Beijing, China, in 2009.

He is currently working toward the Ph.D. degree at the Department of Electrical Engineering and Computer Science, University of California, Irvine. His research interests include cooperative communications, applied signal processing, and resource allocation in wireless networks.

A. Lee Swindlehurst (S'83–M'84–SM'99–F'04) received the B.S. (*summa cum laude*) and M.S. degrees in electrical engineering from Brigham Young University, Provo, UT, in 1985 and 1986, respectively, and the Ph.D. degree in electrical engineering from Stanford University, Stanford, CA, in 1991.

From 1986 to 1990, he was with ESL, Inc., Sunnyvale, CA, where he was involved in the design of algorithms and architectures for several radar and sonar signal processing systems. He was on the faculty of the Department of Electrical and Computer Engineering, Brigham Young University, from 1990 to 2007, where he was a Full Professor and served as Department Chair from 2003 to 2006. During 1996–1997, he held a joint appointment as a visiting scholar at both Uppsala University, Uppsala, Sweden, and at the Royal Institute of Technology, Stockholm, Sweden. From 2006 to 2007, he was on leave working as Vice President of Research for ArrayComm LLC, San Jose, CA. He is currently a Professor of Electrical Engineering and Computer Science at the University of California at Irvine. His research interests include sensor array signal processing for radar and wireless communications, detection and estimation theory, and system identification. He has more than 200 publications in these areas.

Dr. Swindlehurst is a past Secretary of the IEEE Signal Processing Society, past Editor-in-Chief of the IEEE JOURNAL OF SELECTED TOPICS IN SIGNAL PROCESSING, and past member of the Editorial Boards for the EURASIP *Journal on Wireless Communications and Networking*, IEEE *Signal Processing Magazine*, and the IEEE TRANSACTIONS ON SIGNAL PROCESSING. He is a recipient of several paper awards: the 2000 IEEE W. R. G. Baker Prize Paper Award, the 2006 and 2010 IEEE Signal Processing Society's Best Paper Award, the 2006 IEEE Communications Society Stephen O. Rice Prize in the Field of Communication Theory, and is coauthor of a paper that received the IEEE Signal Processing Society Young Author Best Paper Award in 2001.