Joint Transmit Design and Node Selection for One-Way and Two-Way Untrusted Relay Channels

Jing Huang and A. Lee Swindlehurst
Center for Pervasive Communications and Computing
University of California, Irvine, CA 92697
Email: {jing.huang; swindle}@uci.edu

***Abstract*—We investigate a relay network where the source and destination select one relay out of a group of untrusted relay nodes to establish a reliable and confidential connection. We assume there is no direct link between them, and the users have to employ an untrusted relay while simultaneously protecting the confidential data from it. We study joint transmit design and node selection strategies for both one-way relaying with the help of cooperative jamming from the destination, and two-way relaying. We first derive optimal algorithms through numerical methods for secrecy rate maximization, and then we propose closed-form suboptimal solutions with reduced complexity. Simulation results show that unlike the conventional relay channels, when untrusted relays are used, one-way relaying with cooperative jamming is more efficient than the two-way relaying scheme in terms of secrecy rate.**

I. Introduction

Secrecy concerns have recently been raised in cooperative relaying networks with an external eavesdropper in both one-way and two-way relay channels [1]–[5]. However, even if external eavesdroppers are absent, the relays may belong to a heterogeneous network without the same security clearance as the end users and thus are *untrusted*. For this scenario, [6] showed that using an untrusted compress-and-forward relay node to relay information can achieve a higher secrecy rate than just treating the relay as an eavesdropper. The joint source/relay beamforming design problem for an untrusted MIMO relay channel was studied in [7], and the secrecy outage probability for untrusted amplify-and-forward (AF) relay channels was investigated in [8]. [9] considered secrecy rate maximization problem in untrusted two-way relaying channels with friendly jammers.

This paper studies a relay network where the source and destination can activate and utilize one out of a group of untrusted AF relays to establish a communication link. We assume there is no direct link between the end users, so they must rely on the untrusted relay in order to obtain a reliable and private connection; the users must be able to benefit from the untrusted relay while keeping the message secret from it. We further assume the end users have multiple antennas and each relay is equipped with a single antenna. We consider both the one-way relaying case with the help of cooperative jamming from the destination, and the two-way relaying case where the users can take the advantage of forcing the untrusted relay to use multi-user decoding. We derive optimal algorithms for the design of the transmit covariance matrices and selection of the relay node that maximize the secrecy rate via semidefinite programming (SDP) combined with line search methods. Then we propose suboptimal strategies with lower complexity that only use maximum ratio combining (MRC) transmit beamformers. Among our findings, we demonstrate that under secrecy constraints, one-way relaying in general achieves a higher secrecy rate than two-way relaying which normally provides higher throughput in conventional relay networks. However, when the power budget at the legitimate transmitter is much smaller than that at the receiver, two-way relaying is preferred.

The remainder of this work is organized as follows. The mathematical model of the relaying protocols is introduced in Section II. The joint transmit design and node selection algorithms for one-way and two-way relaying are derived in Sections III and IV, respectively. Selected numerical results are shown in Section V, and we conclude in Section VI.

This work was supported by the U.S. Army Research Office MURI grant W911NF-07-1-0318, and by the National Sciene Foundation under grant CCF-1117983.

II. Mathematical Model

We consider a half-duplex two-hop relaying system composed of a source (Alice), a destination (Bob), and a total of K AF relays, as seen in Fig. 1. Alice and Bob have N_a and N_b antennas respectively, and each relay is equipped with a single antenna. We assume the relays are untrusted in the sense that once activated they are able to wiretap information from legitimate transmitters while also forwarding messages. The channels are assumed to be quasi-static, *i.e.*, constant during the two hops. We also assume that there is no direct link between Alice and Bob, so that reliable communication can only be achieved via the untrusted relays. We assume a single relay selection policy, which prevents the untrusted relays from cooperatively decoding the private messages. Therefore, in each transmission Alice and Bob will select and activate only one relay in the network, and perform either one-way or two-way relaying.

A. One-Way Relaying with Cooperative Jamming

When employing an untrusted AF relay in one-way mode, either a direct link between Alice and Bob or cooperative jamming should be used to obtain a positive secrecy rate [8]. Therefore, we consider one-way relaying with cooperative

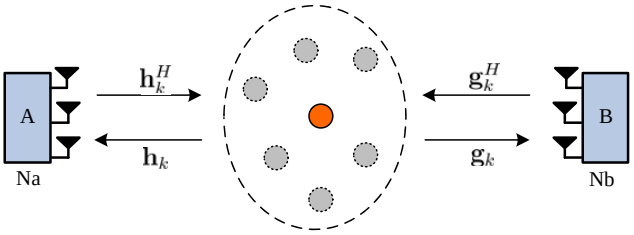

Fig. 1. Illustration of system model

jamming by the receiver in this work. During the first phase, Alice and Bob transmit information and jamming signals respectively, and the selected relay k receives

$$y_k = \mathbf{h}_k^H \mathbf{x}_A + \mathbf{g}_k^H \mathbf{x}_B + n_k, \tag{1}$$

where $\mathbf{x}_A$ and $\mathbf{x}_B$ are the data and noise-like jamming signal vectors transmitted by Alice and Bob respectively. The covariance matrices of $\mathbf{x}_A$ and $\mathbf{x}_B$ are denoted by $\mathbf{Q}_A = \mathbb{E}\{\mathbf{x}_A \mathbf{x}_A^H\}$ and $\mathbf{Q}_B = \mathbb{E}\{\mathbf{x}_B \mathbf{x}_B^H\}$ with power constraints $\text{tr}(\mathbf{Q}_A) \leq P_A$, $\text{tr}(\mathbf{Q}_B) \leq P_B$. The $N_a \times 1$ and $N_b \times 1$ channel vectors from Alice and Bob to relay k are denoted by $\{\mathbf{h}_k, \mathbf{g}_k\}$, respectively. The term n_k represents naturally occurring noise at the relay. For simplicity, we assume that the noise at all nodes is zero-mean circular complex Gaussian with variance N_0.

During the second phase, the kth relay normalizes its received signal y_k and transmits a scaled version $x_k = \frac{1}{\sigma_k} y_k$ to Bob where

$$\sigma_k = \sqrt{(\mathbf{h}_k^H \mathbf{Q}_A \mathbf{h}_k + \mathbf{g}_k^H \mathbf{Q}_B \mathbf{g}_k + N_0)/P_R} \tag{2}$$

and each relay is assumed to have the same power budget P_R. The received signal at Bob via the kth relay is then given by

$$\mathbf{y}_{Bk} = \frac{1}{\sigma_k} \mathbf{g}_k \mathbf{h}_k^H \mathbf{x}_A + \frac{1}{\sigma_k} \mathbf{g}_k \mathbf{g}_k^H \mathbf{x}_B + \frac{1}{\sigma_k} \mathbf{g}_k n_k + \mathbf{n}_B \tag{3}$$

where the intentional interference term can be removed by Bob since $\mathbf{x}_B$ is known to him.

B. Two-Way Relaying

For two-way relaying, both Alice and Bob transmit data signals to the activated relay in the first phase, and the signal received at the relay is similar to (1) with the difference that $\mathbf{x}_B$ is also a data signal vector. In this relaying mode, the advantage of the legitimate receivers over the untrusted relay is that the relay needs to perform multi-user decoding (if she can) and Alice and Bob only need to decode single user data. Thus, a positive secrecy rate is possible even without artificial noise support or a direct link transmission.

During the second phase, the relay will forward a scaled version of the received signal to both Alice and Bob. The received signal at Bob is given by (3), and Alice receives

$$\mathbf{y}_{Ak} = \frac{1}{\sigma_k} \mathbf{h}_k \mathbf{g}_k^H \mathbf{x}_B + \frac{1}{\sigma_k} \mathbf{h}_k \mathbf{h}_k^H \mathbf{x}_A + \frac{1}{\sigma_k} \mathbf{h}_k n_k + \mathbf{n}_A \tag{4}$$

where the self-generated signal $\mathbf{x}_A$ can be removed by Alice.

III. Transmit Design for One-Way Relaying

In this section, we investigate the joint optimization of transmit covariance matrices at Alice and Bob, and the relay selection to maximize the secrecy rate. We will first give an optimal algorithm based on convex optimization, and then we will propose a MRC-based solution with lower computation complexity.

A. Optimal Transmit Design and Node Selection

With the help of a selected untrusted relay, the achievable secrecy rate for one-way relaying is given by

$$R_s^{OW} = [I_B^{OW} - I_R^{OW}]^+ \tag{5}$$

where $[x]^+ \triangleq \max\{0, x\}$, I_B^{OW} and I_R^{OW} represent the mutual information between Alice and Bob, and between Alice and the relay respectively.

Assuming Bob uses the minimum mean square error (MMSE) receiver, the mutual information expressions are then given by

$$I_B^{OW} = \frac{1}{2} \log \det[\mathbf{I} + \mathbf{g}_k \mathbf{h}_k^H \mathbf{Q}_A \mathbf{h}_k \mathbf{g}_k^H (N_0 \mathbf{g}_k \mathbf{g}_k^H + \sigma_k^2 N_0 I)^{-1}], \tag{6}$$

$$I_R^{OW} = \frac{1}{2} \log \left(1 + \frac{\mathbf{h}_k^H \mathbf{Q}_A \mathbf{h}_k}{\mathbf{g}_k^H \mathbf{Q}_B \mathbf{g}_k + N_0}\right), \tag{7}$$

and the optimization problem can be expressed as

$$\max_k \max_{\mathbf{Q}_A, \mathbf{Q}_B} \quad R_s^{OW} \tag{8a}$$

$$s.t. \quad \text{tr}(\mathbf{Q}_A) \leq P_A, \ \text{tr}(\mathbf{Q}_B) \leq P_B \tag{8b}$$

$$\mathbf{Q}_A \succeq 0, \ \mathbf{Q}_B \succeq 0. \tag{8c}$$

According to (2) and (5), and using the fact that $\det(\mathbf{I} + \mathbf{AB}) = \det(\mathbf{I} + \mathbf{BA})$, with some mathematical manipulations problem (8) can be rewritten as

$$\max_k \max_{\alpha_k, \gamma_k, \mathbf{Q}_A, \mathbf{Q}_B} \quad \frac{1 + \alpha_k}{1 + \gamma_k} \tag{9a}$$

$$s.t. \quad \text{tr}(\mathbf{Q}_A) \leq P_A, \ \text{tr}(\mathbf{Q}_B) \leq P_B \tag{9b}$$

$$\text{tr}(\mathbf{Q}_A \mathbf{\Phi}_k) \geq \alpha_k \tag{9c}$$

$$\mathbf{h}_k^H \mathbf{Q}_A \mathbf{h}_k \leq \gamma_k (\mathbf{g}_k^H \mathbf{Q}_B \mathbf{g}_k + N_0) \tag{9d}$$

$$\mathbf{Q}_A \succeq 0, \ \mathbf{Q}_B \succeq 0, \tag{9e}$$

where

$$\mathbf{\Phi}_k = \mathbf{h}_k \mathbf{g}_k^H (N_0 \mathbf{g}_k \mathbf{g}_k^H + \sigma_k^2 N_0 I)^{-1} \mathbf{g}_k \mathbf{h}_k^H. \tag{10}$$

We observe that in (9), the objective is quasi-linear and all the constraints are linear matrix inequalities (LMIs) except for (9d). If we fix the value of γ_k, the above problem becomes a semidefinite program (SDP) and the solutions for α_k, $\mathbf{Q}_A$ and $\mathbf{Q}_B$ can be efficiently found using, for example, the interior method [10]. Therefore, we can solve Problem (9) through SDP combined with an outer line search over the non-negative scalar γ_k. The detailed procedure is listed in Algorithm 1 as follows.

Algorithm 1

1) **for** the kth relay,
   initialize $\gamma_k = \frac{(P_A/N_a)||\mathbf{h}_k||^2}{(P_B/N_b)||\mathbf{g}_k||^2+N_0}$, and
   $\sigma_k^2 = \left(\frac{P_A}{N_a}||\mathbf{h}_k||^2 + \frac{P_B}{N_b}||\mathbf{g}_k||^2 + N_0\right)/P_R$.
2) solve the following problem via SDP

$$\begin{aligned}\max_{\alpha_k,\mathbf{Q}_A,\mathbf{Q}_B} \quad & \alpha_k \\ s.t. \quad & \text{tr}(\mathbf{Q}_A) \le P_A,\ \text{tr}(\mathbf{Q}_B) \le P_B \\ & \text{tr}(\mathbf{Q}_A\mathbf{\Phi}_k) \ge \alpha_k \\ & \mathbf{h}_k^H\mathbf{Q}_A\mathbf{h}_k \le \gamma_k(\mathbf{g}_k^H\mathbf{Q}_B\mathbf{g}_k + N_0) \\ & \mathbf{Q}_A \succeq 0,\ \mathbf{Q}_B \succeq 0,\end{aligned}$$

   and update σ_k^2 with $\mathbf{Q}_A$, $\mathbf{Q}_B$ according to (2) and loop until convergence.
3) perform a line search over γ_k and repeat step (2) until $\frac{1+\alpha_k}{1+\gamma_k}$ is maximized.
4) select the best relay $k^* = \arg\max_k \left(\frac{1+\alpha_k}{1+\gamma_k}\right)$.

The algorithm is initialized by using the uniform power allocation $\mathbf{Q}_A = \frac{P_A}{N_a}\mathbf{I}$ and $\mathbf{Q}_B = \frac{P_B}{N_b}\mathbf{I}$. It is worth noting that since it is optimal to use the full transmit power of the relay, the alternating optimization procedure [11] used for σ_k^2 and the covariance matrices $\mathbf{Q}_{A/B}$ in step (2) is guaranteed to converge. Also note that one can apply the derivative-free line search method [12] for step (3).

B. MRC-based Transmit Design and Node Selection

The above optimal method requires SDP and a line search for each relay and thus has relatively high complexity. Thus in this section we will propose a simple strategy that only employs MRC transmit beamformers for both Alice and Bob, since each relay is equipped with a single antenna. The performance of this scheme will be evaluated in Section V.

By using the MRC transmit beamformers for both Alice and Bob, we have

$$\mathbf{x}_A = \frac{\mathbf{h}_k}{||\mathbf{h}_k||}x_A, \tag{11}$$

$$\mathbf{x}_B = \frac{\mathbf{g}_k}{||\mathbf{g}_k||}x_B, \tag{12}$$

where $\mathbb{E}\{x_A x_A^H\} \le P_A$ and $\mathbb{E}\{x_B x_B^H\} \le P_B$.

Therefore, for high SNRs, the secrecy rate can be approximated as

$$\tilde{R}_s^{OW} = \frac{1}{2}\log\left[\frac{\mathbf{h}_k^H\mathbf{Q}_A\mathbf{h}_k\mathbf{g}_k^H(N_0\mathbf{g}_k\mathbf{g}_k^H + \sigma_k^2N_0I)^{-1}\mathbf{g}_k}{\mathbf{h}_k^H\mathbf{Q}_A\mathbf{h}_k/\left(\mathbf{g}_k^H\mathbf{Q}_B\mathbf{g}_k + N_0\right)}\right] \tag{13}$$

where $\mathbf{Q}_A = \frac{P_A}{||\mathbf{h}_k||^2}\mathbf{h}_k\mathbf{h}_k^H$, $\mathbf{Q}_B = \frac{P_B}{||\mathbf{g}_k||^2}\mathbf{g}_k\mathbf{g}_k^H$, and a simple selection policy that maximizes $\tilde{R}_s^{OW}$ is given by

$$\begin{aligned}k^* &= \arg\max_k \left\{\tilde{R}_s^{OW}\right\} \\ &= \arg\max_k \left\{\mathbf{g}_k^H(N_0\mathbf{g}_k\mathbf{g}_k^H + \sigma_k^2N_0I)^{-1}\mathbf{g}_k\left(P_B||\mathbf{g}_k||^2 + N_0\right)\right\} \\ &\overset{a}{=} \arg\max_k \left\{\frac{||\mathbf{g}_k||^2\left(P_B||\mathbf{g}_k||^2 + N_0\right)}{||\mathbf{g}_k||^2 + (P_A||\mathbf{h}_k||^2 + P_B||\mathbf{g}_k||^2 + N_0)/P_R}\right\}\end{aligned} \tag{14}$$

where equality (a) is obtained using the matrix inversion lemma. From the relay selection criterion in (14), we observe that when $\mathbf{g}_k$ is fixed, in the first phase the users will select a relay with relatively weak $\mathbf{h}_k$, since the first-phase transmission has equivalent contribution to the legitimate receiver and the untrusted relay, while the second phase jamming signal only degrades the decoding ability at the relay.

IV. Transmit Design for Two-Way Relaying

Two-way relaying can increase the transmission efficiency and sum rate in conventional relay networks. However, in terms of secrecy rate, the advantage of two-way relay may not hold when an untrusted relay is involved. In this section, we study joint optimization of the transmit covariance matrices and the node selection policy.

A. Optimal Transmit Design and Node Selection

For the two-way relaying case, we will use the secrecy sum rate as an optimization criterion. Considering the secrecy constraint, the sum rate is given by [3]

$$R_s^{TW} = [I_A^{TW} + I_B^{TW} - I_R^{TW}]^+. \tag{15}$$

Similar to the one-way relaying case, according to the signal model in Section II-B, we have

$$I_A^{TW} = \frac{1}{2}\log\det[\mathbf{I} + \mathbf{h}_k\mathbf{g}_k^H\mathbf{Q}_B\mathbf{g}_k\mathbf{h}_k^H(N_0\mathbf{h}_k\mathbf{h}_k^H + \sigma_k^2N_0I)^{-1}],$$

$$I_B^{TW} = \frac{1}{2}\log\det[\mathbf{I} + \mathbf{g}_k\mathbf{h}_k^H\mathbf{Q}_A\mathbf{h}_k\mathbf{g}_k^H(N_0\mathbf{g}_k\mathbf{g}_k^H + \sigma_k^2N_0I)^{-1}].$$

We assume that the untrusted relay is able to conduct multi-user (successive) decoding. Hence we have

$$I_R^{TW} = \frac{1}{2}\log\left(1 + \frac{\mathbf{h}_k^H\mathbf{Q}_A\mathbf{h}_k + \mathbf{g}_k^H\mathbf{Q}_B\mathbf{g}_k}{N_0}\right). \tag{16}$$

Comparing (16) to (7), we can observe that the relay's wiretapping ability in the two-way relay case is significantly increased, although the transmission efficiency for public messages is also improved. According to (2) and (15), and using the fact that $\det(\mathbf{I}+\mathbf{AB}) = \det(\mathbf{I}+\mathbf{BA})$, the secrecy sum rate maximization problem can be expressed as

$$\max_k \max_{\alpha_k,\beta_k,\mathbf{Q}_A,\mathbf{Q}_B} \frac{(1+\alpha_k)(1+\beta_k)}{\sigma_k^2\frac{P_R}{N_0}} \tag{17a}$$

$$s.t.\ \text{tr}(\mathbf{Q}_A) \le P_A,\ \text{tr}(\mathbf{Q}_B) \le P_B \tag{17b}$$

$$\text{tr}(\mathbf{Q}_A\mathbf{\Phi}_k) \ge \alpha_k,\ \text{tr}(\mathbf{Q}_B\mathbf{\Psi}_k) \ge \beta_k \tag{17c}$$

$$\mathbf{h}_k^H\mathbf{Q}_A\mathbf{h}_k + \mathbf{g}_k^H\mathbf{Q}_B\mathbf{g}_k + N_0 = \sigma_k^2P_R \tag{17d}$$

$$\mathbf{Q}_A \succeq 0,\ \mathbf{Q}_B \succeq 0, \tag{17e}$$

where

$$\mathbf{\Phi}_k = \mathbf{h}_k\mathbf{g}_k^H(N_0\mathbf{g}_k\mathbf{g}_k^H + \sigma_k^2N_0I)^{-1}\mathbf{g}_k\mathbf{h}_k^H, \tag{18}$$

$$\mathbf{\Psi}_k = \mathbf{g}_k\mathbf{h}_k^H(N_0\mathbf{h}_k\mathbf{h}_k^H + \sigma_k^2N_0I)^{-1}\mathbf{h}_k\mathbf{g}_k^H. \tag{19}$$

Similar to Problem (9), all the expressions in (17) are linear except for (17a). Thus we can solve the above problem via SDP combined with a line search over the non-negative scalar β_k, as described in Algorithm 2. Similar to Algorithm 1, this algorithm is also initialized by uniform transmit power allocation and the alternating optimization procedure used for σ_k^2 and $\mathbf{Q}_{A/B}$ will converge since it is always optimal to use all the available transmit power of the relay in this case.

Algorithm 2

1) **for** the kth relay,
initialize $\beta_k = \frac{P_B}{N_b}||\mathbf{g}_k||^2\mathbf{h}_k^H(N_0\mathbf{h}_k\mathbf{h}_k^H + \sigma_k^2 N_0 I)^{-1}\mathbf{h}_k$, and $\sigma_k^2 = \left(\frac{P_A}{N_a}||\mathbf{h}_k||^2 + \frac{P_B}{N_b}||\mathbf{g}_k||^2 + N_0\right)/P_R$.
2) solve the following problem via SDP

$$\begin{aligned}\max_{\alpha_k,\mathbf{Q}_A,\mathbf{Q}_B} \quad & \alpha_k \\ s.t. \quad & \text{tr}(\mathbf{Q}_A) \le P_A,\ \text{tr}(\mathbf{Q}_B) \le P_B \\ & \text{tr}(\mathbf{Q}_A\mathbf{\Phi}_k) \ge \alpha_k,\ \text{tr}(\mathbf{Q}_B\mathbf{\Psi}_k) \ge \beta_k \\ & \mathbf{h}_k^H\mathbf{Q}_A\mathbf{h}_k + \mathbf{g}_k^H\mathbf{Q}_B\mathbf{g}_k + N_0 = \sigma_k^2 P_R \\ & \mathbf{Q}_A \succeq 0,\ \mathbf{Q}_B \succeq 0,\end{aligned}$$

and update σ_k^2 with $\mathbf{Q}_A$, $\mathbf{Q}_B$ according to (2) and loop until convergence.
3) perform a line search over β_k and repeat step (2) until $\frac{(1+\alpha_k)(1+\beta_k)}{\sigma_k^2\frac{P_R}{N_0}}$ is maximized.
4) select the best relay $k^* = \arg\max_k \left(\frac{(1+\alpha_k)(1+\beta_k)}{\sigma_k^2\frac{P_R}{N_0}}\right)$.

B. MRC-based Transmit Design and Node Selection

To simplify Algorithm 2, in this section we use the MRC transmit beamformers for both Alice and Bob during the first phase, *i.e.* $\mathbf{x}_A = \frac{\mathbf{h}_k}{||\mathbf{h}_k||}x_A$ and $\mathbf{x}_B = \frac{\mathbf{g}_k}{||\mathbf{g}_k||}x_B$, where $\mathbb{E}\{x_A x_A^H\} \le P_A$ and $\mathbb{E}\{x_B x_B^H\} \le P_B$. Therefore, for high SNRs, the secrecy sum rate in (15) can be approximated as

$$\begin{aligned}\tilde{R}_s^{TW} &= \frac{1}{2}\log\left[\frac{\mathbf{h}_k^H\mathbf{Q}_A\mathbf{h}_k\mathbf{g}_k^H\mathbf{Q}_B\mathbf{g}_k}{\sigma_k^2\frac{P_R}{N_0}}\right. \\ &\left.\times\mathbf{g}_k^H(N_0\mathbf{g}_k\mathbf{g}_k^H + \sigma_k^2N_0I)^{-1}\mathbf{g}_k\mathbf{h}_k^H(N_0\mathbf{h}_k\mathbf{h}_k^H + \sigma_k^2N_0I)^{-1}\mathbf{h}_k\right] \\ &\overset{a}{=} \log\left[\frac{P_AP_BN_0}{P_R}\frac{||\mathbf{h}_k||^4||\mathbf{g}_k||^4}{\sigma_k^2(\sigma_k^2+||\mathbf{h}_k||^2)(\sigma_k^2+||\mathbf{g}_k||^2)}\right] \qquad (20)\end{aligned}$$

where equality (a) again uses the matrix inversion lemma. Therefore, a corresponding selection policy that maximizes $\tilde{R}_s^{TW}$ is then given by

$$\begin{aligned}k^* &= \arg\max_k\left\{\tilde{R}_s^{TW}\right\} \\ &= \arg\max_k\left\{\frac{||\mathbf{h}_k||^4||\mathbf{g}_k||^4}{\sigma_k^2(\sigma_k^2+||\mathbf{h}_k||^2)(\sigma_k^2+||\mathbf{g}_k||^2)}\right\}. \qquad (21)\end{aligned}$$

We see that unlike the selection policy in (14) for one-way relaying, this criterion has the same weight for both first and second phase relay links. It is also worth noting that the suboptimal schemes proposed in Section IV-B and here use unit-rank transmit covariance matrices for all transmitters. This will potentially degrade the throughput performance. Also, there is no power allocation in these suboptimal algorithms and all nodes simply transmit at full power. Although using full power at the relay is optimal, it is not necessarily the case for Alice and Bob, especially when either of them acts as a cooperative jammer during the first phase. This will also decrease the secrecy rate compared to the proposed optimal methods.

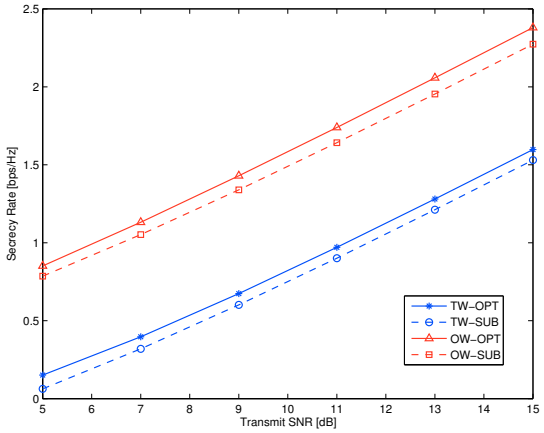

Fig. 2. Secrecy rates versus transmit SNRs γ_A (γ_B,γ_R), with antenna numbers at Alice and Bob $N_a = N_b = 4$, and relay number $K = 4$.

V. Numerical Results

In this section, we present numerical examples of the secrecy performance for the investigated transmission schemes: one-way optimal (OW-OPT), one-way suboptimal (OW-SUB), two-way optimal (TW-OPT) and two-way suboptimal (TW-SUB). We assume that both Alice and Bob have four antennas, *i.e.* $N_a = N_b = 4$ for all examples. The entries of all the channel vectors are assumed to be i.i.d. zero-mean, unit variance, complex Gaussian random variables. We perform Monte Carlo experiments with 1000 independent trials to obtain the average results. We denote the transmit SNRs at Alice, Bob and the relay as $\gamma_A = P_A/N_0$, $\gamma_B = P_B/N_0$ and $\gamma_R = P_R/N_0$ respectively.

Fig. 2 depicts the secrecy rate as a function of transmit SNRs at all nodes. There are four relays ($K = 4$) in the network. It is interesting to see that, unlike the conventional relay channels, the secrecy rate of one-way relaying is almost twice that of two-way relaying. This is because the untrusted relay is able to perform multi-user decoding and is more powerful in terms of wiretapping than the relays in one-way transmission mode. This indicates that while two-way relaying achieves better user fairness, it typically is not as efficient as one-way relaying in terms of secrecy rate. However, later we will also show a case where two-way relaying outperforms one-way relaying. We also observe that the performance of the proposed suboptimal schemes is very close to their optimal counterparts. As discussed in Section IV-B, the gaps come from the rank constraint and the naive power consumption in the suboptimal schemes.

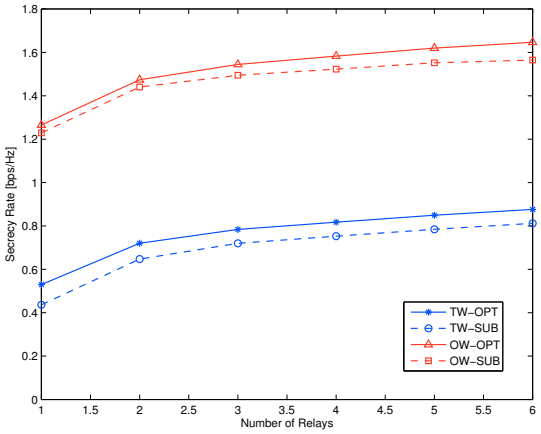

Fig. 3. Secrecy rates versus relay number K, $\gamma_A = \gamma_B = \gamma_R = 10$dB, with antenna numbers at Alice and Bob $N_a = N_b = 4$.

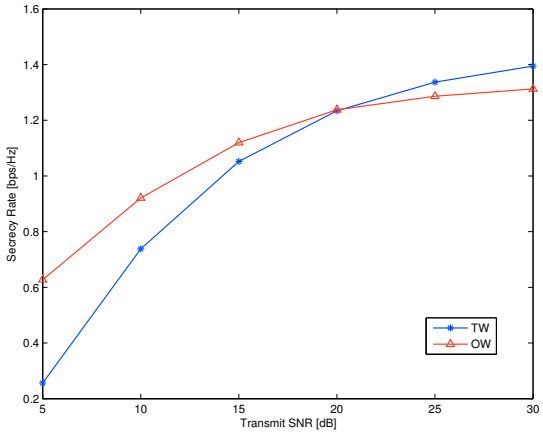

Fig. 4. Secrecy rates versus transmit SNRs γ_B and γ_R, with $\gamma_A = 0$dB, antenna numbers at Alice and Bob $N_a = N_b = 4$, and relay number $K = 4$.

Fig. 3 depicts the impact of the number of relays K on the secrecy rate. The transmit SNRs at all nodes are set to be 10dB in this example, and K ranges from one to six. The figure shows that the secrecy performance improves with increasing K due to the diversity gain obtained from relay selection. It also shows that the gain improves significantly when K goes from one to two relays, and gradually flattens out for larger K.

Fig. 4 shows the performance as a function of γ_B and γ_R ranging from 5 to 30dB. In this figure we fix the transmit power of Alice (*i.e.*, the transmit power of the data signal in the one-way relaying case), and only increase the power of Bob and the relay. It is shown that when γ_B and γ_R are relatively high compared to γ_A (greater than 20dB in this case), the secrecy rate of two-way relaying exceeds that of one-way relaying and the gain continues growing from that point. This is because in one-way relaying, the jamming power becomes less useful if the signal power allocated to data is too small, while in two-way relaying, increasing the data signal power at Bob will keep contributing to the secrecy rate. This example indicates that when the legitimate receiver in a one-way relaying network has a much higher power budget than the transmitter, one-way relaying with cooperative jamming is not the best choice.

VI. Conclusions

This paper studied joint transmit design and relay node selection for a relay network with a group of untrusted relay nodes. Both one-way relaying with cooperative jamming and two-way relaying schemes were investigated. We derived optimal algorithms for secrecy rate maximization via SDP combined with a line search. Corresponding closed-form MRC-based suboptimal solutions were then proposed with reduced complexity. Numerical results reveal that one-way relaying with secrecy constraints usually achieves a higher secrecy rate than two-way relaying, and the performance of the proposed suboptimal solutions is very close to that of the optimal ones. Since two-way relaying outperforms one-way relaying in some cases as shown in the simulations, future work on this topic should investigate the combination of two-way relaying and cooperative jamming.

References

[1] 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.

[2] J. Huang and A. L. Swindlehurst, "Cooperative jamming for secure communications in MIMO relay networks," *IEEE Trans. Signal Process.*, vol. 59, no. 10, pp. 4871–4884, Oct. 2011.

[3] 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.

[4] A. Mukherjee and A. Swindlehurst, "Securing multi-antenna two-way relay channels with analog network coding against eavesdroppers," in *Proc. 11th IEEE SPAWC*, Jun. 2010, pp. 1–5.

[5] Z. Ding, M. Xu, J. Lu, and F. Liu, "Improving wireless security for bidirectional communication scenarios," *IEEE Trans. Veh. Technol.*, vol. 61, no. 6, pp. 2842–2848, Jul. 2012.

[6] X. He and A. Yener, "Cooperation with an untrusted relay: A secrecy perspective," *IEEE Trans. Inf. Theory*, vol. 56, no. 8, pp. 3807–3827, Jul. 2010.

[7] C. Jeong, I. Kim, and D. Kim, "Joint secure beamforming design at the source and the relay for an amplify-and-forward MIMO untrusted relay system," *IEEE Trans. Signal Process.*, vol. 60, no. 1, pp. 310–325, Jan. 2012.

[8] J. Huang, A. Mukherjee, and A. L. Swindlehurst, "Secure communication via an untrusted non-regenerative relay in fading channels," *IEEE Trans. Signal Process.*, vol. 61, no. 10, pp. 2536–2550, May 2013.

[9] R. Zhang, L. Song, Z. Han, B. Jiao, and M. Debbah, "Physical layer security for two way relay communications with friendly jammers," in *Proc. IEEE GLOBECOM*, Dec. 2010, pp. 1–6.

[10] S. P. Boyd and L. Vandenberghe, *Convex Optimization*. Cambridge University Press, 2004.

[11] I. Csiszár and G. Tusnády, "Information geometry and alternating minimization procedures," *Statistics and decisions*, no. 1, pp. 205–237, 1984.

[12] R. P. Brent, *Algorithms for Minimization Without Derivatives*. Prentice-Hall, Englewood Cliffs, 1973.