Secure Beamforming for MIMO Two-Way Communications With an Untrusted Relay

Jianhua Mo, *Student Member, IEEE*, Meixia Tao, *Senior Member, IEEE*, Yuan Liu, *Member, IEEE*, and Rui Wang

***Abstract*—This paper studies the secure beamforming design in a multiple-antenna three-node system where two source nodes exchange messages with the help of an untrusted relay node. The relay acts as both an essential signal forwarder and a potential eavesdropper. Both two-phase and three-phase two-way relay strategies are considered. Our goal is to jointly optimize the source and relay beamformers for maximizing the secrecy sum rate of the two-way communications. We first derive the optimal relay beamformer structures. Then, iterative algorithms are proposed to find source and relay beamformers jointly based on alternating optimization. Furthermore, we conduct asymptotic analysis on the maximum secrecy sum-rate. Our analysis shows that when all transmit powers approach infinity, the two-phase two-way relay scheme achieves the maximum secrecy sum rate if the source beamformers are designed such that the received signals at the relay align in the same direction. This reveals an important advantage of signal alignment technique in against eavesdropping. It is also shown that if the source powers approach zero, the three-phase scheme performs the best while the two-phase scheme is even worse than direct transmission. Simulation results have verified the efficiency of the proposed secure beamforming algorithms as well as the analytical findings.**

***Index Terms*—Physical layer security, signal alignment, two-way relaying, untrusted relay.**

I. Introduction

A. Motivation

COOPERATIVE relaying has been shown effective for power reduction, coverage extension and throughput enhancement in wireless communications. Recently, with the advance of wireless information-theoretic security at the physical layer, a new dimension for designing relaying strategies arises. In specific, from a perspective of physical-layer security, a relay can be friendly and may help to keep the confidential message from being eavesdropped by others, while an untrusted relay may intentionally eavesdrop the signal when relaying. The case of untrusted relay exists in real life. For example, the relays and sources belong to different network in today's heterogenous network, where the nodes have different security clearances and thus different levels of access to the information. It is therefore important to find out whether the untrusted relay is still beneficial compared with direct transmission and if so what is the new relay strategy.

The goal of this work is to study the physical layer security in two-way relay systems where the relay is untrusted and each node is equipped with multiple antennas. Compared with traditional one-way relaying, the problem in two-way relaying is more interesting. This is because by applying physical layer network coding, the relay only needs to decode the network-coded message rather than each individual message and hence the network coding procedure itself also brings certain security. Three questions will be addressed in this work. First, under what conditions, should we treat the two-way untrusted relay as a passive eavesdropper or seek help from it? This is a challenging problem because different power constraints and antennas configurations may result in different answers. Second, if help is necessary, how to jointly optimize the source and relay beamformers? Typically this would be a non-convex problem and very difficult to solve. Thirdly, would physical layer network coding, originally known for throughput enhancement in two-way relay systems, bring new insights to the new performance metric of information security?

B. Related Work

We first review the existing works on beamforming design in MIMO two-way relay systems without taking secrecy into account. Then we review the related works on secure communications in relay systems.

1) Beamforming in MIMO Two-Way Relay Systems: When the source nodes are each equipped with a single antenna, the work [2] studied the optimal relay beamforming structure and proposed an iterative algorithm to find the capacity region. When both source and relay have multiple antennas, the work [3] obtained an optimal relay precoding structure and proposed an alternating optimization method to design the source and relay precoding jointly. Based on the mean-square-error (MSE) criterion, the authors in [4] proposed an iterative algorithm for the joint source and relay precoding design.

Manuscript received August 01, 2013; revised November 25, 2013 and January 31, 2014; accepted February 11, 2014. Date of publication February 20, 2014; date of current version April 01, 2014. The associate editor coordinating the review of this manuscript and approving it for publication was Prof. Y.-W. Peter Hong. This work is supported by the NSF of China under grants 61322102 and 61221001, and by the Program for New Century Excellent Talents in University (NCET) under grant NCET-11-0331. The material in this paper was partly presented at the IEEE Wireless Communications and Networking Conference, Shanghai, China, April 2013 [1]. (*Corresponding Author: M. Tao.*)

J. Mo was with the Department of Electronic Engineering, Shanghai Jiao Tong University, Shanghai, China. He is now with Wireless Networking and Communications Group, The University of Texas at Austin, Austin, TX 78712 USA (e-mail: jhmo@utexas.edu).

M. Tao is with the Department of Electronic Engineering, Shanghai Jiao Tong University, Shanghai 200240, China (e-mail: mxtao@sjtu.edu.cn or mxtao@ieee.org).

Y. Liu was with the Department of Electronic Engineering, Shanghai Jiao Tong University, Shanghai 200240, China. He is now with the School of Electronic and Information Engineering, South China University of Technology, China (e-mail: eeyliu@scut.edu.cn).

R. Wang was with the Department of Electronic Engineering, Shanghai Jiao Tong University, Shanghai, China. He is now with the Institute of Network Coding, The Chinese University of Hong Kong, Hong Kong (e-mail: ruiwang@ie.cuhk.edu.hk).

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.2014.2307276

2) Secure Communications With Trusted Relay: A trusted relay is treated as a legitimate user in secure communications and can help to counter external eavesdroppers and enhance the secrecy of the networks. Most of the existing works have focused on the secure communication with traditional one-way relaying (e.g., [5]–[11]). Only a few attempts have been made very recently to study two-way relay secret communication [12]–[17]. Specifically, [12] and [13] investigated the relay and jammer selection problem in the two-way relay networks. The authors in [14] studied beamforming design in MIMO two-way relaying for maximizing secrecy sum rate which is proven to be achievable in [18]. In [15] and [16], the authors analyzed the two-way relay networks with multiple single-antenna relays. The relay and jammer selection, power allocation, and distributed beamforming were considered jointly to maximize the secrecy sum rate. Besides, several secret key agreement in two-way relay systems was studied in [17].

3) Secure Communications With Untrusted Relay: Untrusted relay channels with confidential messages was first studied in [19], where an achievable secrecy rate was obtained. A destination-based jamming (DBJ) technique was proposed in [20] and [21] without source-destination link. The performance of DBJ in fading channel and multi-relay scenarios was analyzed in [22]. When the source-destination link exists, authors in [23] discussed whether cooperating with the untrusted relay is better than treating it as a passive eavesdropper. A Stackelberg game between the two sources and external friendly jammers in a two-way relay system was formulated as a power control problem in [24]. In [25], the authors considered MIMO one-way amplify-and-forward (AF) relay systems and jointly deigned the source and relay beamforming using alternating optimization. The work [26] examined the secrecy outage probability in one-way non-regenerative relay systems.

From these existing literature, it is found that secure communication problem in MIMO two-way untrusted relay systems has not been considered yet.

C. Contribution

In this paper, we investigate physical layer security in MIMO two-way relay systems, where the two sources exchange confidential information with each other through an untrusted relay. The relay acts as both an essential helper and a potential eavesdropper, but does not make any malicious attack. In our previous work [1], the two-phase two-way relay scheme was considered. In this extension, we study both two-phase and three-phase two-way relay schemes. In particular, we formulate the joint secure source and relay beamforming design problems for both schemes. The objective is to maximize the secrecy sum rate of the bidirectional links subject to the source and relay power constraints. Furthermore, we conduct asymptotic analysis on the maximum secrecy sum rate of the different two-way relay schemes in comparison with direct transmission.

The main contributions and results of this paper are summarized as follows:

- The optimal structure of the relay beamforminger with fixed source beamformers is derived. With this structure, the number of unknowns in the relay beamformer is significantly reduced and thus the joint source and relay beamformer design can be simplified.
- Iterative algorithms based on alternating optimization are proposed to find a solution of the joint source and relay beamformers. These algorithms are convergent but cannot ensure global optimality due to the nonconvexity of the optimization problems.
- Via asymptotic analysis, we show that when the powers of the source and relay nodes approach infinity, the two-phase scheme achieves the maximum secrecy rate if the transceiver beamformers are designed such that the received signals at the relay align in the same direction. This reveals an important advantage of *signal alignment* techniques in against eavesdropping. It gives a new perspective to achieve the physical layer security, and also lowers the source antenna number requirement for ensuring security.
- It is also shown via asymptotic analysis that when the power of the relay goes to infinity and that of the two sources approach zeros, the three-phase two-way relay scheme performs the best while the two-phase performs even worse than direct transmission.

D. Organization and Notations

The rest of the paper is organized as follows. Section II describes the system model and problem formulations. The optimal secure beamformers for two- and three-phase two-way relay schemes are presented in Section III. Asymptotical results are detailed in Section IV. Comprehensive simulation results are given in Section V. Finally, we conclude this paper in Section VI.

Notations: Scalars, vectors and matrices are denoted by lower-case, lower-case bold-face and upper-case bold-face letters, respectively. $[x]^+$ denotes $\max(0, x)$. $\mathrm{Tr}(\mathbf{A})$, $\mathbf{A}^{-1}$, $\mathrm{Rank}(\mathbf{A})$, $\|\mathbf{A}\|_F$, $\mathbf{A}^*$ and $\mathbf{A}^H$ denote the trace, inverse, rank, Frobenius norm, conjugate and Hermite of matrix $\mathbf{A}$, respectively. $\mathrm{span}(\mathbf{A})$ represents the column space (range space) of $\mathbf{A}$ and $\dim(\mathbf{A})$ denotes the dimension of $\mathbf{A}$. The projection matrix onto the null space of $\mathbf{A}$ is denoted by $\mathbf{A}^{\mathcal{N}}$. $\|\mathbf{q}\|$ denotes the norm of the vector $\mathbf{q}$. $\sigma_{\max}(\mathbf{A})$ is the largest singular value of $\mathbf{A}$. $\lambda_{\max}(\mathbf{A})$ is the largest eigenvalue of $\mathbf{A}$ and $\boldsymbol{\psi}_{\max}(\mathbf{A})$ is the eigenvector of $\mathbf{A}$ corresponding to the largest eigenvalue. $\lambda_{\max}(\mathbf{A}, \mathbf{B})$ is the largest generalized eigenvalue of the matrices $\mathbf{A}$ and $\mathbf{B}$. $\boldsymbol{\psi}_{\max}(\mathbf{A}, \mathbf{B})$ is the generalized eigenvector of $(\mathbf{A}, \mathbf{B})$ corresponding to the largest generalized eigenvalue. We use P_i^{DT}, P_i^{2P} and P_i^{3P} to represent the transmit power of node $i \in \{A, B, R\}$ in two-way direct transmission, two-phase two-way relaying and three-phase two-way relaying, respectively. Throughout this paper, the noise power at all nodes is normalized to 1.

II. System Model and Problem Formulation

We consider a two-way relay system as shown in Fig. 1, where two source nodes A and B exchange information with

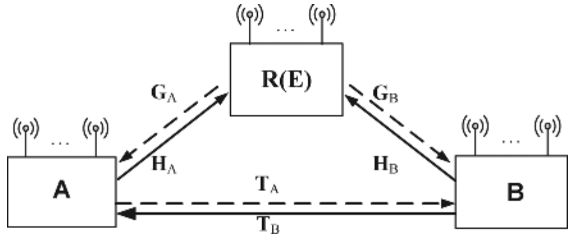


Fig. 1. MIMO two-way relay model.

each other with the assistance of a relay node R. The relay acts as both an essential helper and a potential eavesdropper but does not make any malicious attack. Note that the decode-and-forward (DF) relay strategy is not applicable here since the relay is untrusted and not expected to decode the received signal from the source nodes. As such, we assume the relay adopts AF strategy, which also has low complexity. The number of antennas at nodes A, B and R are denoted as N_A, N_B and N_R, respectively. As shown in Fig. 1, $\mathbf{T}_A \in \mathbb{C}^{N_B \times N_A}$, $\mathbf{T}_B \in \mathbb{C}^{N_A \times N_B}$, $\mathbf{H}_A \in \mathbb{C}^{N_R \times N_A}$, $\mathbf{G}_A \in \mathbb{C}^{N_A \times N_R}$, $\mathbf{H}_B \in \mathbb{C}^{N_R \times N_B}$, $\mathbf{G}_B \in \mathbb{C}^{N_B \times N_R}$ denote the channel matrices of link $A \to B$, $B \to A$, $A \to R$, $R \to A$, $B \to R$ and $R \to B$, respectively. If the system operates in time division duplex (TDD) mode and channel reciprocity holds, then we have $\mathbf{T}_A = \mathbf{T}_B^T$, $\mathbf{H}_A = \mathbf{G}_A^T$, and $\mathbf{H}_B = \mathbf{G}_B^T$. For simplicity, we only consider single data stream for each source node in this paper. Denote the transmitted symbol at the source i as $s_i \in \mathbb{C}$ with $\mathbb{E}(|s_i|^2) = 1$, and the associated beamforming vector as $\mathbf{q}_i \in \mathbb{C}^{N_i \times 1}$, for $i \in \{A, B\}$.

Different two-way relay schemes have been studied in the literature [27], [28]. In this paper, we focus on two well-known ones, two-phase and three-phase two-way relay schemes. For the purpose of comparison, the two-way direct transmission is also considered as given in Appendix A, wherein the relay node is treated as a pure eavesdropper [25], [29].

A. Two-Phase Two-Way Relay Scheme

In the first phase, the two source nodes A and B simultaneously transmit signals to the relay node R. In the second phase, the relay node amplifies its received signal by multiplying with a precoding matrix, denoted as $\mathbf{F}$, and then broadcasts it to both A and B.

Assuming perfect self-interference cancellation at each source node receiver, the achievable information rate from node i, $i \in \{A, B\}$ to node $\bar{i}, \bar{i} \neq i$, can be expressed as

$$\mathcal{R}_{i\bar{i}}^{2P} = \frac{1}{2}\log_2\left(1 + \mathbf{q}_i^H \mathbf{H}_i^H \mathbf{F}^H \mathbf{G}_{\bar{i}}^H \mathbf{K}_{\bar{i}}^{-1} \mathbf{G}_{\bar{i}} \mathbf{F} \mathbf{H}_i \mathbf{q}_i\right), \quad (1)$$

where

$$\mathbf{K}_{\bar{i}} = \mathbf{G}_{\bar{i}} \mathbf{F} \mathbf{F}^H \mathbf{G}_{\bar{i}}^H + \mathbf{I}. \quad (2)$$

If the untrusted relay wants to eavesdrop the signals from both source nodes, it may try to fully decode the two messages s_A and s_B. Therefore, the achievable information rate at the untrusted relay can be expressed as the maximum sum-rate of a classic two-user MIMO multiple-access channel, given by

$$\begin{aligned}\mathcal{R}_R^{2P} &= \frac{1}{2}\log_2\left|\mathbf{I} + [\mathbf{H}_A\mathbf{q}_A \quad \mathbf{H}_B\mathbf{q}_B]\begin{bmatrix}\mathbf{q}_A^H\mathbf{H}_A^H \\ \mathbf{q}_B^H\mathbf{H}_B^H\end{bmatrix}\right| \\ &\overset{(a)}{=} \frac{1}{2}\log_2\left|\mathbf{I} + \begin{bmatrix}\mathbf{q}_A^H\mathbf{H}_A^H \\ \mathbf{q}_B^H\mathbf{H}_B^H\end{bmatrix}[\mathbf{H}_A\mathbf{q}_A \quad \mathbf{H}_B\mathbf{q}_B]\right| \\ &= \frac{1}{2}\log_2\Big(1 + \|\mathbf{H}_A\mathbf{q}_A\|^2 + \|\mathbf{H}_B\mathbf{q}_B\|^2 \\ &\quad + \|\mathbf{H}_A\mathbf{q}_A\|^2\|\mathbf{H}_B\mathbf{q}_B\|^2 - \|\mathbf{q}_B^H\mathbf{H}_B^H\mathbf{H}_A\mathbf{q}_A\|^2\Big), \quad (3)\end{aligned}$$

where (a) is from the identity $|\mathbf{I} + \mathbf{AB}| = |\mathbf{I} + \mathbf{BA}|$.

The achievable secrecy sum rate[18] of the two source nodes is thus given by,

$$\mathcal{R}_s^{2P} = \left[\mathcal{R}_{AB}^{2P} + \mathcal{R}_{BA}^{2P} - \mathcal{R}_R^{2P}\right]^+. \quad (4)$$

Our goal is to maximize the secrecy sum rate by jointly optimizing the relay and source beamformers $\mathbf{F}$, $\mathbf{q}_A$ and $\mathbf{q}_B$. The problem can be formulated as

$$\begin{aligned}&\max_{\{\mathbf{F}, \mathbf{q}_A, \mathbf{q}_B\}} \ \mathcal{R}_s^{2P} && (5a)\\ &\text{s. t.} \ \ \|\mathbf{q}_i\|^2 \leq P_i^{2P}, \ \ i \in \{A, B\}, && (5b)\\ &\qquad \mathrm{Tr}\big(\mathbf{F}\mathbf{H}_A\mathbf{q}_A\mathbf{q}_A^H\mathbf{H}_A^H\mathbf{F}^H + \mathbf{F}\mathbf{H}_B\mathbf{q}_B\mathbf{q}_B^H\mathbf{H}_B^H\mathbf{F}^H \\ &\qquad + \mathbf{F}\mathbf{F}^H\big) \leq P_R^{2P}. && (5c)\end{aligned}$$

where (5b) is the source power constraints and (5c) is the relay power constraint.

B. Three-Phase Two-Way Relay Scheme

In the first phase, source node A transmits, while relay R and source node B listen. In the second phase, source node B transmits, while R and A listen. In the third phase, the relay node R amplifies its received signals by multiplying them with matrices $\mathbf{F}_A$ and $\mathbf{F}_B$ respectively, and then broadcast the combined signals.

By combining the received signals from the second and third phases and cancelling the self-interference, the information rate from B to A can be expressed as,

$$\begin{aligned}\mathcal{R}_{BA}^{3P} = \frac{1}{3}\log_2\Big(1 &+ \mathbf{q}_B^H\mathbf{T}_B^H\mathbf{T}_B\mathbf{q}_B + \mathbf{q}_B^H\mathbf{H}_B^H\mathbf{F}_B^H\mathbf{G}_A^H \\ &\cdot\left(\mathbf{G}_A\left(\mathbf{F}_A\mathbf{F}_A^H + \mathbf{F}_B\mathbf{F}_B^H\right)\mathbf{G}_A^H + \mathbf{I}\right)^{-1}\mathbf{G}_A\mathbf{F}_B\mathbf{H}_B\mathbf{q}_B\Big). \quad (6)\end{aligned}$$

Likewise, the information rate from A to B, denoted as $\mathcal{R}_{AB}^{3P}$, can be obtained.

The information sum rate leaked to the untrusted relay is,

$$\begin{aligned}\mathcal{R}_R^{3P} = \frac{1}{3}\log_2&\left(1 + \mathbf{q}_A^H\mathbf{H}_A^H\mathbf{H}_A\mathbf{q}_A\right) \\ &+ \frac{1}{3}\log_2\left(1 + \mathbf{q}_B^H\mathbf{H}_B^H\mathbf{H}_B\mathbf{q}_B\right). \quad (7)\end{aligned}$$

Thus, the secrecy sum rate is given by

$$\mathcal{R}_s^{3P} = [\mathcal{R}_{BA}^{3P} + \mathcal{R}_{AB}^{3P} - \mathcal{R}_R^{3P}]^+. \quad (8)$$

We can formulate the secrecy sum rate maximization problem for three-phase two-way relay scheme as

$$\max_{\{\mathbf{F}_A, \mathbf{F}_B, \mathbf{q}_A, \mathbf{q}_B\}} \mathcal{R}_s^{3P} \tag{9a}$$

$$\text{s.t.} \quad \|\mathbf{q}_i\|^2 \le P_i^{3P}, \ i \in \{A, B\}, \tag{9b}$$

$$\mathrm{Tr}\Big(\mathbf{F}_A\mathbf{H}_A\mathbf{q}_A\mathbf{q}_A^H\mathbf{H}_A^H\mathbf{F}_A^H + \mathbf{F}_B\mathbf{H}_B\mathbf{q}_B\mathbf{q}_B^H\mathbf{H}_B^H\mathbf{F}_B^H + \mathbf{F}_A\mathbf{F}_A^H + \mathbf{F}_B\mathbf{F}_B^H\Big) \le P_R^{3P}, \tag{9c}$$

where (9c) is the relay power constraint.

In the above two schemes, we assume that one of the source nodes, say A is responsible for the joint design of source and relay beamformers. After finishing the design, A sends the corresponding designed beamformer to B and the relay. Then, the two source nodes and the untrusted relay will use their beamformers to process the transmit signals.

III. Secure Beamfomring Designs

After introducing the problem formulations in (5) and (9) for the two-phase and three-phase two-way relay schemes, respectively, we now present algorithms to design these secure beamformers in this section. Note the optimization problems (5) and (9) are non-convex since the objective functions, i.e., the secrecy sum rate, are not convex functions of the variables $\mathbf{q}_A$, $\mathbf{q}_B$ and $\mathbf{F}$. We first obtain the optimal structure of the secure relay beamforming matrix. Then we present an iterative algorithm to find a local optimal solution for the joint secure source and relay beamformers.

A. Secure Beamforming in Two-Phase Two-Way Relay Scheme

Define the following two QR decompositions:

$$[\,\mathbf{G}_A^H \quad \mathbf{G}_B^H\,] = \mathbf{V}\mathbf{R}_1^{2P}, \tag{10}$$

$$[\,\mathbf{H}_A\mathbf{q}_A \quad \mathbf{H}_B\mathbf{q}_B\,] = \mathbf{U}\mathbf{R}_2^{2P}, \tag{11}$$

where $\mathbf{V} \in \mathbb{C}^{N_R \times \min\{N_A+N_B, N_R\}}$, $\mathbf{U} \in \mathbb{C}^{N_R \times 2}$ are orthonormal matrices and $\mathbf{R}_1^{2P}$, $\mathbf{R}_2^{2P}$ are upper triangle matrices.

Lemma 1: In the two-phase two-way relay scheme, the optimal relay beamforming matrix $\mathbf{F} \in \mathbb{C}^{N_R \times N_R}$ *that maximizes the secrecy sum rate has the following structure:*

$$\mathbf{F} = \mathbf{V}\mathbf{A}\mathbf{U}^H, \tag{12}$$

where $\mathbf{A} \in \mathbb{C}^{\min\{N_A+N_B, N_R\} \times 2}$ *is an unknown matrix.*

Proof: Note that the relay beamforming matrix $\mathbf{F}$ only influences the information rate $\mathcal{R}_{AB}^{2P}$ and $\mathcal{R}_{BA}^{2P}$. Therefore, the optimal $\mathbf{F}$ that maximizes the secrecy sum rate is the same as the $\mathbf{F}$ that maximizes the information sum rate $\mathcal{R}_{AB}^{2P} + \mathcal{R}_{BA}^{2P}$. Due to the rank-one precoding at each source node, we have the equivalent channel $\mathbf{H}_i\mathbf{q}_i$ from source node i to relay. Therefore, applying the results in [3], we readily have Lemma 1. ■

Note that Lemma 1 is similar to those in [2] and [3]. This indicates that the optimal relay beamforming structure in the two-phase two-way relay system remains the same regardless of the trust in the relay. It is also seen from this Lemma that the number of unknowns in $\mathbf{F}$ is reduced from N_R^2 to $2\min\{N_R, N_A + N_B\}$. This greatly reduces the computational complexity of the relay beamforming design as will be clear shortly.

We note that it is not easy to find the optimal solution to the problem (5). Even after substituting the optimal structure of $\mathbf{F}$ (12) into (4), the problem is still nonconvex since the secrecy sum rate is not a convex function of $\mathbf{q}_A$, $\mathbf{q}_B$ and $\mathbf{A}$. Therefore, we optimize the source beamforming vectors $\mathbf{q}_A$, $\mathbf{q}_{\mathbf{B}}$ and the unknown matrix $\mathbf{A}$ in the relay beamforming matrix $\mathbf{F}$ in an alternating manner. Given $\mathbf{q}_A$ and $\mathbf{q}_B$, we use the gradient method shown in Appendix B to search $\mathbf{A}$. Given $\mathbf{F}$ and $\mathbf{q}_i$, we can find the optimal $\mathbf{q}_{\bar{i}}$, where the optimization method is shown in Appendix C. Formally, we present the method in Algorithm 1. Here, the initial points of the complex vectors $\mathbf{q}_A$ and $\mathbf{q}_B$ can be randomly generated as long as they satisfy the given power constraint.

Algorithm 1: Iterative algorithm for secure beamforming in two-phase two-way relay scheme

```
1: Initialize $\mathbf{A}$, $\mathbf{q}_A$ and $\mathbf{q}_B$.
2: Repeat
     (a) Optimize $\mathbf{A}$ given $\mathbf{q}_A$ and $\mathbf{q}_B$ based on gradient
         method given in Appendix B;
     (b) Optimize $\mathbf{q}_B$ given $\mathbf{A}$ and $\mathbf{q}_A$ according to
         Appendix C;
     (c) Optimize $\mathbf{q}_A$ given $\mathbf{A}$ and $\mathbf{q}_B$ according to
         Appendix C by swapping $A$ and $B$;
3: Until the secrecy sum rate does not increase.
```

Note that the algorithm always converges because the secrecy sum rate is finite and non-decreasing in every iteration. Simulation results will show that Algorithm 1 converges in a few iterations. In Steps 2(b) and 2(c), the optimal source beamforming vectors are found by the semi-definite relaxation (SDR), which has polynomial complexity, see [30] for example. In Step 2(a), the relay beamforming matrix is optimized by the gradient method, the complexity of which is proportional to the size of matrix $\mathbf{A}$, thanks to Lemma 1.

B. Secure Beamforming in Three-Phase Two-Way Relay Scheme

Similar to the two-phase case, we define the following QR decomposition:

$$[\,\mathbf{G}_A^H \quad \mathbf{G}_B^H\,] = \mathbf{V}\mathbf{R}^{3P}, \tag{13}$$

where $\mathbf{V} \in \mathbb{C}^{N_R \times \min\{N_A+N_B, N_R\}}$ is an orthonormal matrix and $\mathbf{R}^{3P} \in \mathbb{C}^{\min\{N_A+N_B, N_R\} \times (N_A+N_B)}$ is an upper triangle matrix. Then we give the optimal structure of the relay beamforming matrices $\mathbf{F}_A$ and $\mathbf{F}_B$ in the following lemma.

Lemma 2: In the three-phase two-way relay scheme, the optimal relay beamforming matrices $\mathbf{F}_A$, $\mathbf{F}_B$ *that maximize the secrecy sum rate have the following structure:*

$$\mathbf{F}_A = \mathbf{V}\mathbf{a}_A\frac{(\mathbf{H}_A\mathbf{q}_A)^H}{\|\mathbf{H}_A\mathbf{q}_A\|}, \ \mathbf{F}_B = \mathbf{V}\mathbf{a}_B\frac{(\mathbf{H}_B\mathbf{q}_B)^H}{\|\mathbf{H}_B\mathbf{q}_B\|}, \tag{14}$$

where $\mathbf{a}_A \in \mathbb{C}^{\min\{N_A+N_B, N_R\} \times 1}$, $\mathbf{a}_B \in \mathbb{C}^{\min\{N_A+N_B, N_R\} \times 1}$ *are unknown vectors.*

Proof: See Appendix D. ■

Lemma 2 simplifies the design of two beamforming matrices $\{\mathbf{F}_i\}$ to the design of two beamforming vectors $\{\mathbf{a}_i\}$. Thus, the number of unknowns is reduced to $2\min\{N_R, N_A+N_B\}$. Note that the number of unknowns in the relay beamforming matrices is the same for two- and three-phase schemes.

Using Lemma 2, we can develop a similar iterative algorithm as Algorithm 1 to obtain a solution of problem (9), where $\mathbf{q}_A$, $\mathbf{q}_B$, $\mathbf{a}_A$ and $\mathbf{a}_B$ are alternatively optimized until the secrecy sum rate does not increase. The algorithm, denoted as Algorithm 2, has same complexity as Algorithm 1. Due to space limit, the details of Algorithm 2 is omitted.

Note that neither Algorithm 1 nor Algorithm 2 can ensure global optimality due to the nonconvexity of problems (5) and (9). However, letting the transmit power on each node approach zero or infinity, we can derive interesting intuitions which lead to the asymptotically optimal solution for secure beamforming. In the next section, we present such asymptotic analysis.

IV. Asymptotic Analysis

The goal of this section is to find the asymptotical optimal secure beamforming design when the relay power P_R approaches infinity. We first present the analysis when the two source powers are also infinite in Section IV-A, followed by the analysis when the two source powers approach zero in Section IV-B. Finally, we briefly discuss the case where the relay power P_R approaches zero. For comparison purpose, the asymptotic result for the direct transmission is presented in this section as well.

A. The Case of High Relay and Source Powers

Proposition 1 (2P): When $P_R \to \infty$, $P_A \to \infty$ and $P_B \to \infty$, the maximum secrecy sum rate of the two-phase two-way relay scheme is:

1) *If $N_A + N_B > N_R$,*

$$\mathcal{R}_{\max}^{2P} = \max_{(\mathbf{q}_A,\mathbf{q}_B)} \frac{1}{2}\log_2 \frac{\|\mathbf{H}_A\mathbf{q}_A\|^2\|\mathbf{H}_B\mathbf{q}_B\|^2}{\|\mathbf{H}_A\mathbf{q}_A\|^2+\|\mathbf{H}_B\mathbf{q}_B\|^2}, \tag{15}$$

where the optimal source beamformers satisfy

$$\beta\mathbf{H}_A\mathbf{q}_A = \mathbf{H}_B\mathbf{q}_B \tag{16}$$

with β being an arbitrary real number, and the maximization is over all $(\mathbf{q}_A, \mathbf{q}_B)$ that meet the condition (16) as well as the peak power constraints $\|\mathbf{q}_A\|^2 \le P_A$ and $\|\mathbf{q}_B\|^2 \le P_B$.

2) *If $N_A + N_B \le N_R$,*

$$\mathcal{R}_{\max}^{2P} = \frac{1}{2}\log_2 \frac{1}{1-\left(\sigma_{\max}(\mathbf{U}_A^H\mathbf{U}_B)\right)^2}, \tag{17}$$

and the corresponding optimal source beamformers are,

$$\mathbf{q}_A = \mathbf{R}_A^{-1}\boldsymbol{\psi}_{\max}\left(\mathbf{U}_A^H\mathbf{U}_B\mathbf{U}_B^H\mathbf{U}_A\right), \tag{18}$$
$$\mathbf{q}_B = \mathbf{R}_B^{-1}\boldsymbol{\psi}_{\max}\left(\mathbf{U}_B^H\mathbf{U}_A\mathbf{U}_A^H\mathbf{U}_B\right), \tag{19}$$

where $\mathbf{U}_A \in \mathbb{C}^{N_R\times\min\{N_A,N_R\}}$ and $\mathbf{U}_B \in \mathbb{C}^{N_R\times\min\{N_B,N_R\}}$ are obtained from the QR decomposition of $\mathbf{H}_A$ and $\mathbf{H}_B$, respectively, i.e.,

$$\mathbf{H}_i = \mathbf{U}_i\mathbf{R}_i, \quad i \in \{A, B\}, \tag{20}$$

where $\mathbf{R}_i \in \mathbb{C}^{\min\{N_R,N_i\}\times N_i}$ are upper triangle matrices.

Proof: We first prove the following fact:

When $P_R \to \infty$, the information rate from i to $\bar{i}$ in two-phase two-way relay scheme is

$$\lim_{P_R\to\infty} R_{i\bar{i}}^{2P} = \frac{1}{2}\log_2\left(1+\mathbf{q}_i^H\mathbf{H}_i^H\mathbf{H}_i\mathbf{q}_i\right), \tag{21}$$

To prove (21), we first plug in the optimal structure of $\mathbf{F}$ to (1) and let $\mathbf{F} = t\mathbf{V}\mathbf{A}\mathbf{U}^H$ where t is a real number. When $P_R \to \infty$, we just let $t \to \infty$. Thus,

$$\begin{aligned}
&\mathbf{q}_i^H\mathbf{H}_i^H\mathbf{F}^H\mathbf{G}_{\bar{i}}^H\mathbf{K}_{\bar{i}}^{-1}\mathbf{G}_{\bar{i}}\mathbf{F}\mathbf{H}_i\mathbf{q}_i\\
&=\mathbf{q}_i^H\mathbf{H}_i^H t\mathbf{U}\mathbf{A}^H\mathbf{V}^H\mathbf{G}_{\bar{i}}^H\left(t^2\mathbf{G}_{\bar{i}}\mathbf{V}\mathbf{A}\mathbf{A}^H\mathbf{V}^H\mathbf{G}_{\bar{i}}^H+\mathbf{I}\right)^{-1}\\
&\quad\cdot\mathbf{G}_{\bar{i}}t\mathbf{V}\mathbf{A}\mathbf{U}^H\mathbf{H}_i\mathbf{q}_i\\
&\overset{(a)}{=}\mathbf{q}_i^H\mathbf{H}_i^H\mathbf{U}\left(\mathbf{I}-\left(\mathbf{I}+t^2\mathbf{A}^H\mathbf{V}^H\mathbf{G}_{\bar{i}}^H\mathbf{G}_{\bar{i}}\mathbf{V}\mathbf{A}\right)^{-1}\right)\mathbf{U}^H\mathbf{H}_i\mathbf{q}_i\\
&=\mathbf{q}_i^H\mathbf{H}_i^H\mathbf{U}\mathbf{U}^H\mathbf{H}_i\mathbf{q}_i-\mathbf{q}_i^H\mathbf{H}_i^H\mathbf{U}\left(\mathbf{I}+t^2\mathbf{A}^H\mathbf{V}^H\mathbf{G}_{\bar{i}}^H\mathbf{G}_{\bar{i}}\mathbf{V}\mathbf{A}\right)^{-1}\\
&\quad\cdot\mathbf{U}^H\mathbf{H}_i\mathbf{q}_i\\
&\overset{(b)}{=}\mathbf{q}_i^H\mathbf{H}_i^H\mathbf{H}_i\mathbf{q}_i-\mathbf{q}_i^H\mathbf{H}_i^H\mathbf{U}\left(\mathbf{I}+t^2\mathbf{A}^H\mathbf{V}^H\mathbf{G}_{\bar{i}}^H\mathbf{G}_{\bar{i}}\mathbf{V}\mathbf{A}\right)^{-1}\\
&\quad\cdot\mathbf{U}^H\mathbf{H}_i\mathbf{q}_i
\end{aligned}$$

where (a) is from the matrix inverse lemma and (b) is from QR decomposition (11). Since nodes A, B and R all have multiple antennas, we have $\mathrm{Rank}\left(\mathbf{G}_{\bar{i}}\right) \ge 2$ with probability one as every element of $\mathbf{G}_{\bar{i}}$ is drawn from continuous distribution. Therefore, it is always possible to find $\mathbf{A}$ such that $\left(\mathbf{A}^H\mathbf{V}^H\mathbf{G}_{\bar{i}}^H\mathbf{G}_{\bar{i}}\mathbf{V}\mathbf{A}\right) \in \mathbb{C}^{2\times 2}$ is positive definite. Hence, the eigenvalue of $\left(\mathbf{I}+t^2\mathbf{A}^H\mathbf{V}^H\mathbf{G}_{\bar{i}}^H\mathbf{G}_{\bar{i}}\mathbf{V}\mathbf{A}\right)$ approaches positive infinity when $t \to \infty$. As a result, the term $\mathbf{q}_i^H\mathbf{H}_i^H\mathbf{U}\left(\mathbf{I}+t^2\mathbf{A}^H\mathbf{V}^H\mathbf{G}_{\bar{i}}^H\mathbf{G}_{\bar{i}}\mathbf{V}\mathbf{A}\right)^{-1}\mathbf{U}^H\mathbf{H}_i\mathbf{q}_i$ approaches zero and we obtain that when $P_R \to \infty$, $R_{i\bar{i}}^{2P} \ge \frac{1}{2}\log_2\left(1+\mathbf{q}_i^H\mathbf{H}_i^H\mathbf{H}_i\mathbf{q}_i\right)$. In addition, it is easy to see that $\lim_{P_R\to\infty} R_{i\bar{i}}^{2P} \le \frac{1}{2}\log_2\left(1+\mathbf{q}_i^H\mathbf{H}_i^H\mathbf{H}_i\mathbf{q}_i\right)$. Therefore, we obtain (21).

Substituting (3) and (21) into (4), we obtain the achievable sum-rate as

$$\lim_{P_R\to\infty}\mathcal{R}_s^{2P} = \frac{1}{2}\log_2\frac{1}{1-f(\mathbf{q}_A,\mathbf{q}_B)} \tag{22}$$

where

$$f(\mathbf{q}_A,\mathbf{q}_B) \triangleq \frac{\left|\mathbf{q}_A^H\mathbf{H}_A^H\mathbf{H}_B\mathbf{q}_B\right|^2}{\left(1+\|\mathbf{H}_B\mathbf{q}_B\|^2\right)\left(1+\|\mathbf{H}_A\mathbf{q}_A\|^2\right)}. \tag{23}$$

From (22), we see that to maximize $\lim_{P_R\to\infty}\mathcal{R}_s^{2P}$, we should maximize $f(\mathbf{q}_A,\mathbf{q}_B)$. An upper bound of $f(\mathbf{q}_A,\mathbf{q}_B)$ is,

$$f(\mathbf{q}_A,\mathbf{q}_B) < \frac{\left|\mathbf{q}_A^H\mathbf{H}_A^H\mathbf{H}_B\mathbf{q}_B\right|^2}{\|\mathbf{H}_B\mathbf{q}_B\|^2\|\mathbf{H}_A\mathbf{q}_A\|^2} \le 1, \tag{24}$$

and this upper bound can be approached when $P_A \to \infty$ and $P_B \to \infty$, i.e.,

$$\begin{aligned}
\bar{f}(\mathbf{q}_A,\mathbf{q}_B) &\triangleq \lim_{P_A\to\infty,P_B\to\infty} f(\mathbf{q}_A,\mathbf{q}_B)\\
&= \frac{\left|\mathbf{q}_A^H\mathbf{H}_A^H\mathbf{H}_B\mathbf{q}_B\right|^2}{\|\mathbf{H}_B\mathbf{q}_B\|^2\|\mathbf{H}_A\mathbf{q}_A\|^2}.
\end{aligned} \tag{25}$$

Therefore, the problem is transformed to maximizing $\bar{f}(\mathbf{q}_A, \mathbf{q}_B)$, which is to find two vectors with the minimum angle between the column spaces of $\mathbf{U}_A$ and $\mathbf{U}_B$.

For the case $N_A + N_B > N_R$, with probability one, we can find $\mathbf{q}_A$ and $\mathbf{q}_B$ satisfying the alignment condition given in (16). In this case, $\bar{f}(\mathbf{q}_A, \mathbf{q}_B)$ can take its maximum value of 1 in (24)[1]. Therefore, substituting the condition (16) into (22), we obtain

$$\begin{aligned}\lim_{P_R\to\infty} \mathcal{R}_s^{2P} &= \frac{1}{2}\log_2 \frac{1}{1-f(\mathbf{q}_A,\mathbf{q}_B)} \\ &= \frac{1}{2}\log_2 \frac{\left(1+\|\mathbf{H}_A\mathbf{q}_A\|^2\right)\left(1+\|\mathbf{H}_B\mathbf{q}_B\|^2\right)}{1+\|\mathbf{H}_A\mathbf{q}_A\|^2+|\mathbf{H}_B\mathbf{q}_B|^2} \\ &\approx \frac{1}{2}\log_2 \frac{\|\mathbf{H}_A\mathbf{q}_A\|^2\|\mathbf{H}_B\mathbf{q}_B\|^2}{\|\mathbf{H}_A\mathbf{q}_A\|^2+\|\mathbf{H}_B\mathbf{q}_B\|^2} \\ &\quad \text{if } P_A\to\infty, P_B\to\infty.\end{aligned}$$

At last, we maximize over all the possible alignment directions and obtain the first part of Proposition 1.

On the other hand, if $N_A + N_B \le N_R$, we have,

$$\begin{aligned}&\left|\mathbf{q}_B^H\mathbf{H}_B^H\mathbf{H}_A\mathbf{q}_A\right| \\ &\overset{(a)}{=} \left|\mathbf{q}_B^H\mathbf{R}_B^H\mathbf{U}_B^H\mathbf{U}_A\mathbf{R}_A\mathbf{q}_A\right| \\ &\overset{(b)}{\le} \sigma_{\max}\left(\mathbf{U}_B^H\mathbf{U}_A\right)\|\mathbf{R}_A\mathbf{q}_A\|\,\|\mathbf{R}_B\mathbf{q}_B\| \\ &\overset{(c)}{=} \sigma_{\max}\left(\mathbf{U}_B^H\mathbf{U}_A\right)\|\mathbf{U}_A\mathbf{R}_A\mathbf{q}_A\|\,\|\mathbf{U}_B\mathbf{R}_B\mathbf{q}_B\| \\ &\overset{(d)}{=} \sigma_{\max}\left(\mathbf{U}_B^H\mathbf{U}_A\right)\|\mathbf{H}_A\mathbf{q}_A\|\,\|\mathbf{H}_B\mathbf{q}_B\| \end{aligned} \tag{26}$$

where (a) and (d) are from (20), (b) is from the singular value decomposition of $\mathbf{U}_B^H\mathbf{U}_A$ and the equality can be achieved by letting $\mathbf{q}_A = \mathbf{R}_A^{-1}\boldsymbol{\psi}_{\max}\left(\mathbf{U}_A^H\mathbf{U}_B\mathbf{U}_B^H\mathbf{U}_A\right)$ and $\mathbf{q}_B = \mathbf{R}_B^{-1}\boldsymbol{\psi}_{\max}\left(\mathbf{U}_B^H\mathbf{U}_A\mathbf{U}_A^H\mathbf{U}_B\right)$ where the upper triangle matrices $\mathbf{R}_i \in \mathbb{C}^{N_i\times N_i}$ are invertible, and (c) is from $\mathbf{q}_i^H\mathbf{R}_i^H\mathbf{R}_i\mathbf{q}_i = \mathbf{q}_i^H\mathbf{R}_i^H\mathbf{U}_i^H\mathbf{U}_i\mathbf{R}_i\mathbf{q}_i$. Substituting (26) back to (22), we obtain the second part of Proposition 1.

Notice that we always have $\sigma_{\max}\left(\mathbf{U}_B^H\mathbf{U}_A\right) < 1$ when $N_A + N_B \le N_R$. The proof is as follows. First, as $\left|\mathbf{q}_B^H\mathbf{H}_B^H\mathbf{H}_A\mathbf{q}_A\right| \le \|\mathbf{H}_A\mathbf{q}_A\|\,\|\mathbf{H}_B\mathbf{q}_B\|$ and the fact that the equality in (b) of (26) can be achieved, we know that $\sigma_{\max}\left(\mathbf{U}_B^H\mathbf{U}_A\right) \le 1$. Second, if $\sigma_{\max}\left(\mathbf{U}_B^H\mathbf{U}_A\right) = 1$, there is an intersection subspace between the spaces $\text{span}(\mathbf{H}_A)$ and $\text{span}(\mathbf{H}_B)$ such that $\beta\mathbf{H}_A\mathbf{q}_A = \mathbf{H}_B\mathbf{q}_B$ where β is a real number. However, according to *dimension theorem*[32] and because the entries of the channel matrices are generated from continuous distribution, we have

$$\begin{aligned}&\dim(\text{span}(\mathbf{H}_A)\cap\text{span}(\mathbf{H}_B)) \\ &\quad = \dim(\text{span}(\mathbf{H}_A)) + \dim(\text{span}(\mathbf{H}_B)) \\ &\qquad - \dim(\text{span}([\mathbf{H}_A, \mathbf{H}_B])) \\ &\quad = N_A + N_B - (N_A + N_B) \\ &\quad = 0.\end{aligned}$$

Consequently, there is no intersection subspace and we have $\sigma_{\max}\left(\mathbf{U}_B^H\mathbf{H}_A\right) < 1$.

Thus, the proof of Proposition 1 is completed. ■

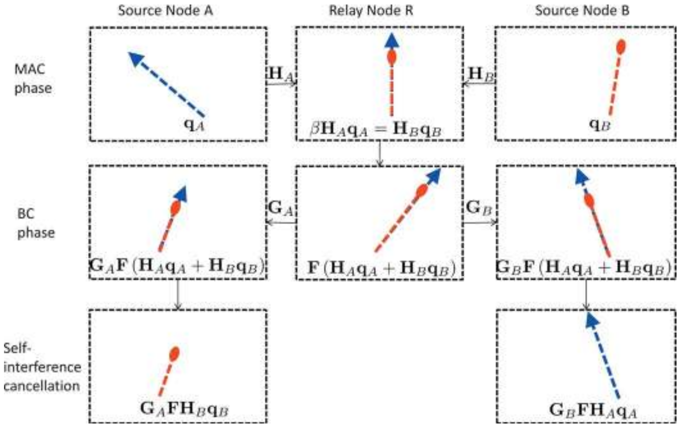

Source Node A
Relay Node R
Source Node B
MAC phase
BC phase
Self-interference cancellation
$\mathbf{H}_A$
$\mathbf{H}_B$
$\mathbf{G}_A$
$\mathbf{G}_B$
$\mathbf{q}_A$
$\beta\mathbf{H}_A\mathbf{q}_A = \mathbf{H}_B\mathbf{q}_B$
$\mathbf{q}_B$
$\mathbf{G}_A\mathbf{F}(\mathbf{H}_A\mathbf{q}_A + \mathbf{H}_B\mathbf{q}_B)$
$\mathbf{F}(\mathbf{H}_A\mathbf{q}_A + \mathbf{H}_B\mathbf{q}_B)$
$\mathbf{G}_B\mathbf{F}(\mathbf{H}_A\mathbf{q}_A + \mathbf{H}_B\mathbf{q}_B)$
$\mathbf{G}_A\mathbf{F}\mathbf{H}_B\mathbf{q}_B$
$\mathbf{G}_B\mathbf{F}\mathbf{H}_A\mathbf{q}_A$

Fig. 2. The signal vectors of the two-phase two-way relaying scheme.

Proposition 1 is essentially similar to the so-called signal alignment. In [31], this technique was first proposed to achieve the degrees of freedom of the MIMO Y channel which is a generalized two-way relay channel with three users. The key idea of the signal alignment is to align the two desired signal vectors coming from two users at the receiver of the relay to jointly perform detection and encoding for network coding. Specifically, if $N_A + N_B > N_R$, there is intersection subspace between the column spaces of $\mathbf{H}_i$ with probability one and thus there exists $\beta \in \mathbb{R}$ such that (16) holds. As illustrated in Fig. 2, the secure beamformers at the two source nodes are chosen such that the two received signals align in the same direction at the relay node. Intuitively, aligning the signal vectors at the relay node will hinder the relay node decode the source messages and make the system more secure. After self-interference cancellation, the two source nodes can obtain the desired signal. The maximum secrecy sum rate goes to infinity as the source powers approach infinity. On the other hand, if $N_A+N_B \le N_R$, there is no intersection subspace with probability one and there is a ceiling for the maximum secrecy sum rate. Specifically, $\mathbf{U}_i$ is the orthonormal basis of the column space of $\mathbf{H}_i$. Thus, $\arccos\left(\sigma_{\max}\left(\mathbf{U}_A^H\mathbf{U}_B\right)\right)$, is the minimum angle between any two vectors from the respect two column spaces. Actually, it is called the minimum principal angle of these two subspaces [33], [34].

Proposition 2 (3P): When $P_R \to \infty$, $P_A \to \infty$ and $P_B \to \infty$, the maximum secrecy sum rate of the three-phase two-way relay scheme is,

$$\mathcal{R}_{\max}^{3P} \approx \sum_{i\in\{A,B\}} \Theta_i, \tag{27}$$

where

$$\Theta_i \in \left[\frac{1}{3}\left[\log_2\left(\frac{1}{2} + \lambda_{\max}\left(\mathbf{T}_i^H\mathbf{T}_i, \mathbf{H}_i^H\mathbf{H}_i\right)\right)\right]^+, \right. \\ \left. \frac{1}{3}\left[\log_2\left(1 + \lambda_{\max}\left(\mathbf{T}_i^H\mathbf{T}_i, \mathbf{H}_i^H\mathbf{H}_i\right)\right)\right]^+\right],$$

if $N_i \le N_R$ and

$$\Theta_i = \frac{1}{3}\left[\log_2\left(\frac{3}{2}P_i\right) + \log_2\left(\lambda_{\max}\left(\mathbf{H}_i^{\mathcal{N}}\mathbf{T}_i^H\mathbf{T}_i\mathbf{H}_i^{\mathcal{N}}\right)\right)\right],$$

if $N_i > N_R$.

[1] A simple algorithm to find $\mathbf{q}_A$ and $\mathbf{q}_B$ was shown in [31, Lemma 1].

Proof: See Appendix E. ■

Proposition 2 shows that the secrecy sum-rate of the three-phase scheme will reach a constant if the untrusted relay has more antennas than the two source nodes.

Proposition 3 (DT): When $P_A \to \infty$ and $P_B \to \infty$, the maximum secrecy sum rate of the two-way direct transmission scheme is

$$\mathcal{R}_{\max}^{DT} \approx \sum_{i\in\{A,B\}} \Omega_i, \tag{28}$$

where

$$\Omega_i = \begin{cases} \frac{1}{2}\left[\log_2 \lambda_{\max}\left(\mathbf{T}_i^H\mathbf{T}_i, \mathbf{H}_i^H\mathbf{H}_i\right)\right]^+, & \text{if } N_i \le N_R \\ \frac{1}{2}\left[\log_2 P_i + \log_2 \lambda_{\max}\left(\mathbf{H}_i^{\mathcal{N}}\mathbf{T}_i^H\mathbf{T}_i\mathbf{H}_i^{\mathcal{N}}\right)\right], & \text{if } N_i > N_R \end{cases},$$

and the optimal beamforming $\mathbf{q}_i^{DT}$ is given in (38).

Proof: This proposition is based on [25, Lemma 7]. Here, we assume that the entries of the channel matrices are generated from continuous distribution. As a result, $\mathrm{Rank}(\mathbf{H}^{m\times n}) \ge \min\{m,n\}$ with probability one. In addition, the condition $\mathbf{H}_i^{\mathcal{N}}\mathbf{T}_i^H \ne \mathbf{0}$ in [25, Lemma 7] is also satisfied with probability one. ■

As shown in Proposition 3, the secrecy sum-rate of the direct transmission scheme will also reach a constant if untrusted relay has more antennas than the source nodes. This is similar to the three-phase case.

From Propositions 1, 2, and 3, we find that the asymptotic comparison among these three schemes depend not only on the antenna numbers N_A, N_B, N_R but also on specific channel realizations. In the following, we only present the comparison results in two cases.

Corollary 1: When $P_R \to \infty$, and $N_A \le N_R$, $N_B \le N_R$, $N_A + N_B > N_R$, the maximum of secrecy sum rate of the two-phase two-way relay scheme keeps increasing when the two source powers P_A and P_B increase while the maximum secrecy sum rates of two-way direct transmission and three-phase scheme both approach constants. Thus, we have

$$\mathcal{R}_{\max}^{2P} \ge \max\left\{\mathcal{R}_{\max}^{DT}, \mathcal{R}_{\max}^{3P}\right\}. \tag{29}$$

Proof: It can be easily verified from Propositions 1, 2 and 3. ■

Remark 1: As shown in [25], [29] for two-way direct transmission, in the infinite power case, the infinite maximum secrecy sum rate needs $N_A > N_R$ or $N_B > N_R$. Proposition 1 reveals that with the signal alignment techniques at the untrusted relay, the infinite maximum secrecy sum rate only needs $N_A + N_B > N_R$, which lowers the requirement of the numbers of antennas at the two sources. The result clearly demonstrates the benefits of signal alignment for physical layer security, which is the unique feature in two-way relaying.

Corollary 2: When $P_R \to \infty$, $P_A \to \infty$, $P_B \to \infty$ and $N_A > N_R$, $N_B > N_R$,

$$\mathcal{R}_{\max}^{DT} \ge \mathcal{R}_{\max}^{3P}. \tag{30}$$

Proof: When $N_i > N_R$, we have

$$\mathcal{R}_{\max}^{DT} = \sum_{i\in\{A,B\}} \frac{1}{2}\left[\log_2 P_i + \mathcal{O}\left(\log_2 P_i\right)\right] \tag{31}$$

$$\mathcal{R}_{\max}^{3P} = \sum_{i\in\{A,B\}} \frac{1}{3}\left[\log_2 P_i + \mathcal{O}\left(\log_2 P_i\right)\right] \tag{32}$$

where the order notation $\mathcal{O}(P)$ means that $\mathcal{O}(P)/P \to 0$ as $P \to \infty$. Thus, the Corollary 2 follows. ■

From this Corollary we see that when the number of antennas at each source node is larger than the number of antennas at the relay node, direct transmission performs better than the three-phase two-way relaying at high SNR.

B. The Case of High Relay Power and Low Source Powers

Proposition 4 (2P): When $P_R \to \infty$, $P_A \to 0$ and $P_B \to 0$, the optimal source beamforming vectors of the two-phase two-way relay scheme are

$$\mathbf{q}_A = \frac{\sqrt{P_A}\boldsymbol{\psi}_{\max}\left(\mathbf{H}_A^H\mathbf{H}_B\mathbf{H}_B^H\mathbf{H}_A\right)}{\left\|\boldsymbol{\psi}_{\max}\left(\mathbf{H}_A^H\mathbf{H}_B\mathbf{H}_B^H\mathbf{H}_A\right)\right\|}, \tag{33}$$

$$\mathbf{q}_B = \frac{\sqrt{P_B}\boldsymbol{\psi}_{\max}\left(\mathbf{H}_B^H\mathbf{H}_A\mathbf{H}_A^H\mathbf{H}_B\right)}{\left\|\boldsymbol{\psi}_{\max}\left(\mathbf{H}_B^H\mathbf{H}_A\mathbf{H}_A^H\mathbf{H}_B\right)\right\|}, \tag{34}$$

and the maximum secrecy sum rate is

$$\mathcal{R}_{\max}^{2P} \approx \frac{1}{2\ln 2} P_A P_B \lambda_{\max}\left(\mathbf{H}_A^H\mathbf{H}_B\mathbf{H}_B^H\mathbf{H}_A\right). \tag{35}$$

Proof: See Appendix F. ■

Note that $\mathbf{q}_A$ and $\mathbf{q}_B$ are determined by the concatenated channel $\mathbf{H}_A^H\mathbf{H}_B$.

Proposition 5 (3P): When $P_R \to \infty$, $P_A \to 0$ and $P_B \to 0$, the maximum secrecy sum rate of the three-phase two-way relay scheme satisfies

$$\frac{1}{2\ln 2}\sum_{i\in\{A,B\}}\left[P_i\lambda_{\max}\left(\mathbf{T}_i^H\mathbf{T}_i - \frac{1}{2}\mathbf{H}_i^H\mathbf{H}_i\right)\right]^+ \le \mathcal{R}_{\max}^{3P} \le \frac{1}{2\ln 2}\sum_{i\in\{A,B\}} P_i\lambda_{\max}\left(\mathbf{T}_i^H\mathbf{T}_i\right).$$

Proof: Substituting the upper bound and lower bound of $\lim_{P_R\to\infty}\mathcal{R}_{i\bar{i}}^{3C}$ given in (47) into (8), and letting $P_A \to 0$ and $P_B \to 0$, we can easily prove Proposition 5. ■

Proposition 6 (DT): When $P_A \to 0$ and $P_B \to 0$, the maximum secrecy sum rate of the two-way direct transmission scheme is,

$$\mathcal{R}_{\max}^{DT} \approx \frac{1}{2\ln 2}\sum_{i\in\{A,B\}}\left[P_i\lambda_{\max}\left(\mathbf{T}_i^H\mathbf{T}_i - \mathbf{H}_i^H\mathbf{H}_i\right)\right]^+$$

and the optimal beamforming $\mathbf{q}_i^{DT}$ are given in (38).

Proof: It is easily obtained from (39) or [25, Lemma 6]. ■

We find that different from the two-phase scheme, the secrecy sum rates of the direct transmission and the three-phase scheme are closely related to the term $\mathbf{T}_i^H\mathbf{T}_i - \alpha\mathbf{H}_i^H\mathbf{H}_i$ ($\alpha = 0, 1, \frac{1}{2}$).

TABLE I
THE COMPARISON OF THE THREE SCHEMES IN TERMS OF THE MAXIMUM SECRECY SUM RATE. (IN THE TABLE, WE USE 'DT', '2P', '3P' TO DENOTE THE THREE SCHEMES. AND, A $>$ B MEANS THAT SCHEME A IS BETTER THAN SCHEME B)

Conditions			Comparison
$P_R \to \infty$	$P_A \to 0$, $P_B \to 0$		3P $>$ DT $>$ 2P (Corollary 3)
	$P_A \to \infty$, $P_B \to \infty$	$N_A + N_B > N_R$, $N_A \leq N_R$, $N_B \leq N_R$	2P $>$ DT and 2P $>$ 3P (Corollary 1)
		$N_A > N_R$, $N_B > N_R$	DT $>$ 3P (Corollary 2)
		Other cases	Channel dependent
$P_R \to 0$			DT $>$ 3P $>$ 2P (Corollary 4)

Corollary 3: When $P_R \to \infty$, $P_A \to 0$ and $P_B \to 0$, we have

$$\mathcal{R}_{\max}^{3P} \geq \mathcal{R}_{\max}^{DT} \geq \mathcal{R}_{\max}^{2P}.$$

Proof: This corollary can be easily obtained from Propositions 4, 5 and 6. Since $\mathbf{H}_i^H \mathbf{H}_i$ are positive semidefinite matrices, $\lambda_{\max}\left(\mathbf{T}_i^H \mathbf{T}_i - \frac{1}{2}\mathbf{H}_i^H \mathbf{H}_i\right) \geq \lambda_{\max}\left(\mathbf{T}_i^H \mathbf{T}_i - \mathbf{H}_i^H \mathbf{H}_i\right)$. Therefore, the three-phase two-way relay scheme is better than direct transmission scheme. In addition, $\mathcal{R}_{\max}^{2P}$ approaches zero faster than the other two schemes. ■

Corollary 3 clearly suggests that when the two source powers are extremely low, it is the best to apply the three-phase two-way relay scheme for secure transmission.

C. The Case of Low Relay Power

In this subsection, we present the asymptotic secrecy sum rate when relay power approaches zero.

First, we briefly show when the relay power $P_R \to 0$, the maximum secrecy sum rate of the two-phase two-way relay scheme $\mathcal{R}_{\max}^{2P}$ approaches zero. As the relay power approaches zero, the information rate through the relay link goes to zero, which means that $\mathcal{R}_{AB}^{2P} + \mathcal{R}_{BA}^{2P}$ approaches zero. On the other hand, the information rate leaked to untrusted relay $\mathcal{R}_R^{2P}$ is not related to the relay power and does not approach zero. Therefore, the secrecy sum rate is zero when $P_R \to 0$.

Corollary 4: When the relay power $P_R \to 0$,

$$\mathcal{R}_{\max}^{DT} \geq \mathcal{R}_{\max}^{3P} \geq \mathcal{R}_{\max}^{2P}. \tag{36}$$

Proof: See Appendix G. ■

Corollary 4 shows that the direct transmission is the best when the relay power is low. In the relay system without secrecy constraint, the similar conclusion holds [35].

D. Summary and Discussion

We can now summarize the main comparison results in Table I. By Table I, we can choose the best transmission scheme under different scenarios. For example, we can see that the two-phase scheme is only optimal in the high SNR regime and when the two source nodes in together have more antennas than the untrusted relay node. In addition, the three-phase scheme is optimal when the source nodes are power limited.

Note that besides the three schemes we considered in this work, four-phase one-way relay scheme is also possible for secure bi-directional transmission. In this four-phase scheme, the conventional one-way relaying is used twice for communications as $A \to R \to B$ and $B \to R \to A$. It can be shown that this four-phase scheme is the best when $P_R \to \infty$, $P_A \to 0$ and $P_B \to 0$. For the other cases, either this scheme is suboptimal or the comparison depends on the channel realization.

V. SIMULATION RESULTS AND DISCUSSIONS

In this section, we show some simulation results to validate the design and analysis in the previous two sections. In the simulation, we assume that the channel reciprocity holds, i.e., $\mathbf{H}_A = \mathbf{G}_A^T$, $\mathbf{H}_B = \mathbf{G}_B^T$ and $\mathbf{T}_A = \mathbf{T}_B^T$. We first use the following example deterministic channel coefficients (every entry of the matrices is generated from $\mathcal{CN}(0,1)$ distribution) as an example, then demonstrate the fading channel case. See the equation at the bottom of the page.

$$\bar{\mathbf{H}}_A = \begin{bmatrix} 0.2686 - 0.0965i & 0.1305 - 1.2373i & 0.6027 + 0.8313i \\ 0.9510 + 0.8678i & -0.4450 + 0.2224i & -0.4630 + 0.3531i \\ 0.4050 - 0.7642i & -0.6673 - 0.7447i & -0.0039 + 1.0646i \\ -0.9971 + 0.2578i & -1.5888 - 0.9503i & -0.4514 - 0.2944i \\ -1.1448 + 0.1069i & -0.5209 - 0.0569i & 0.1598 + 0.0048i \end{bmatrix}$$

$$\bar{\mathbf{H}}_B = \begin{bmatrix} 0.3612 + 0.7099i & -0.0464 - 1.1249i & 0.6175 - 1.6643i \\ 0.6236 - 0.3490i & 0.2193 + 0.8722i & -0.8481 - 0.1791i \\ -0.4814 - 0.3466i & 0.2838 + 0.3014i & -0.3683 + 1.6906i \\ -0.2929 + 1.5306i & -0.2643 + 0.8701i & -1.6770 + 0.0192i \\ -0.0722 + 0.1413i & 0.1504 + 0.9271i & 0.9011 - 0.3934i \end{bmatrix}$$

$$\bar{\mathbf{T}}_A = \begin{bmatrix} 0.0538 + 1.3647i & 1.1100 - 0.5711i & -0.5226 - 0.0653i \\ 0.9241 - 0.9370i & -0.5684 - 1.1719i & -0.3993 - 0.6427i \\ -0.0592 - 1.2997i & -0.9250 + 0.1194i & 0.1469 + 0.4010i \end{bmatrix}$$

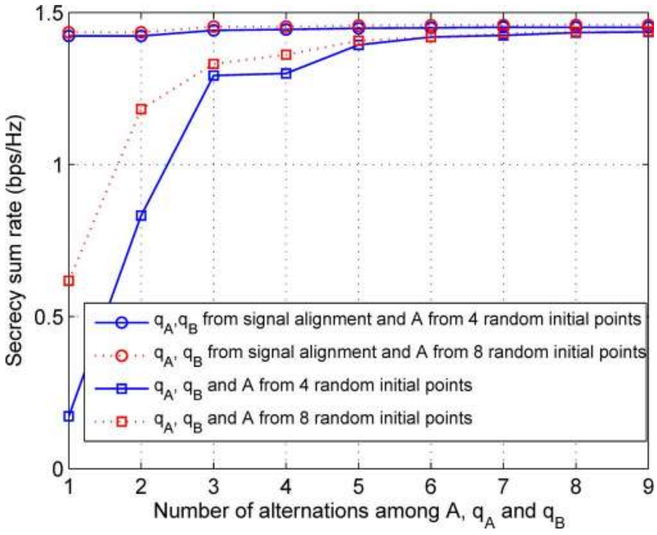


Fig. 3. Convergence behavior comparison of different initialization methods for Algorithm 1. $N_A = N_B = 2$, $N_R = 3$, $P_R = 30$ dB and $P_A = P_B = 10$ dB.

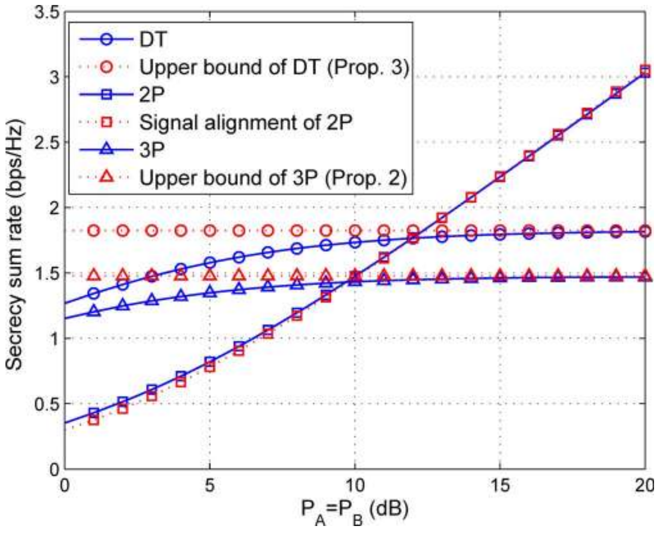


Fig. 4. Comparison of the three schemes in high power regimes when $N_A = 2$, $N_R = 3$, $N_B = 2$ and $P_R = 40$ dB.

If the channel matrix we need is smaller than the dimension of the above matrices, we simply choose the left upper part of the corresponding matrix. For instance, if $N_A = 2$, $N_R = 3$, we choose $\mathbf{H}_A = \bar{\mathbf{H}}_A(1:3, 1:2)$.

Note that Algorithms 1 and 2 are not guaranteed to find the optimal solution and the convergent point may be far from the optimal solution. A method to cope with this problem is to randomly generate multiple initializations and choose the one with the best performance. Fig. 3 illustrates the convergence behavior of Algorithm 1 with different initializations. It is seen that when the initial vectors $\mathbf{q}_A$ and $\mathbf{q}_B$ are chosen based on the signal alignment technique, the algorithm converges faster than the case of random generated vectors. Thus, in the rest of our simulation, we choose the asymptotic optimal beamforming vectors shown in Section IV as the initial points of $\mathbf{q}_A$ and $\mathbf{q}_B$.

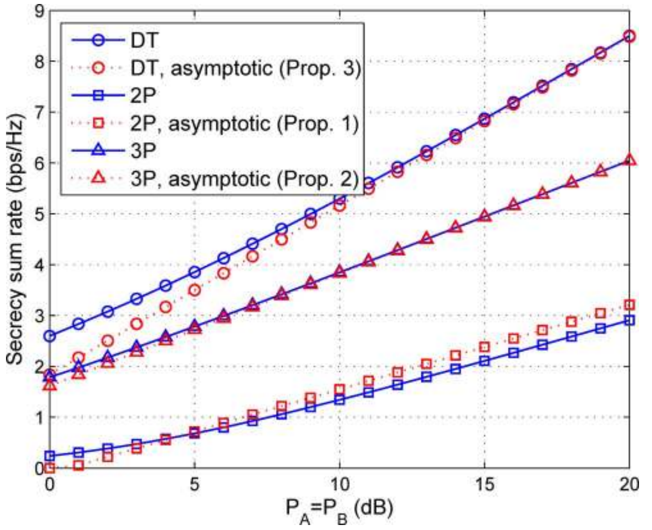


Fig. 5. Comparison of the three schemes in high power regimes when $N_A = 3$, $N_R = 2$, $N_B = 3$ and $P_R = 40$ dB.

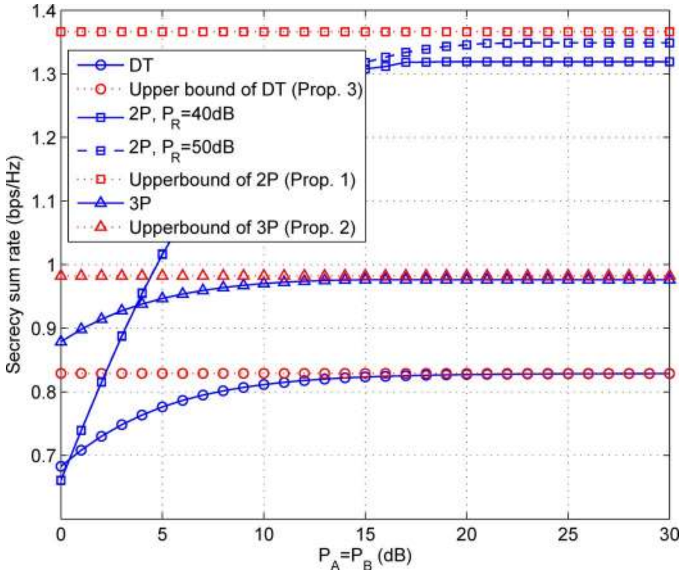


Fig. 6. Comparison of the three schemes in high power regimes when $N_A = 2$, $N_R = 5$, $N_B = 2$ and $P_R = 40$ dB.

A. High Relay Power and High Source Powers

Figs. 4–6 compare the secrecy sum rates obtained by different schemes. Here the relay power is fixed at $P_R = 40$ dB, but the source powers are changing. The results for the two-phase and three-phase two-way relay schemes are obtained using the Algorithm 1 and 2 proposed in Section III. For the direct transmission, we use the closed-form expression (39) given in Appendix A. Here we also implement a heuristic algorithm using the signal alignment technique. In this algorithm, the source beamformers $\mathbf{q}_A$ and $\mathbf{q}_B$ are chosen to satisfy the alignment condition (16). Then the relay beamformer is optimized based on the same gradient method used in Algorithm 1. Since there is no iteration, this heuristic method has much lower complexity than Algorithm 1.

1) Case 1) $N_A = 2$, $N_R = 3$, $N_B = 2$: This is an example of the case when $N_A < N_R$, $N_B < N_R$ and $N_A + N_B > N_R$. We see from Fig. 4 that the maximum secrecy sum rate of two-phase scheme goes to infinity with the increase of the source powers, while that of the other two schemes approach to two upper bounds. Under this channel setup, the upper bound of the direct transmission scheme is about 1.82 bps/Hz and that of three-phase scheme is 1.48 bps/Hz. Fig. 4 clearly verifies the importance of signal alignment for security as analyzed in Corollary 1.

2) Case 2) $N_A = 3$, $N_R = 2$, $N_B = 3$: This is an example of the case when $N_A > N_R$ and $N_B > N_R$. As shown in Fig. 5, the maximum secrecy sum rate for these schemes all approach to infinity as the powers increase. We find that the direct transmission scheme is the best. This agrees with our analysis in Corollary 2 . Actually, as shown in (31) and (32), the degrees of freedom of the direct transmission scheme is one and the degrees of freedom of the three-phase scheme is $\frac{2}{3}$. In this case, although the signal alignment of the two-phase scheme is feasible, the direct transmission scheme is better than the two-phase scheme.

3) Case 3) $N_A = 2$, $N_R = 5$, $N_B = 2$: This is the scenario when $N_A + N_B \leq N_R$. Under this condition, all the schemes have upper bounds for their secrecy sum rates. The comparison results are shown in Fig. 6. It is shown that the two-phase scheme is the best. We also plot the curve for two-phase scheme when $P_R = 50$ dB. The curve can approach the upper bound more closely than the curve when $P_R = 40$ dB. This implies that to approach the upper bound given in (17), we need the powers of all the three nodes go to infinity and the relay power should be much larger than the source powers. In this case, although the signal alignment of the two-phase scheme cannot be achieved, the two-phase scheme is better than the direct transmission scheme.

From Figs. 4 and 6, we can see that increasing the number of antennas at the relay reduces the performance. This is in contrast to the relay system without secrecy constraints, where with more antennas at the relay, the performance will be better.

B. High Relay Power and Low Source Powers

Fig. 7 shows the performance of three schemes when $P_R = 40$ dB and the source powers are low. We find that the two-phase scheme is much worse than the other schemes and three-phase scheme is better than the direct transmission scheme, which verifies Corollary 3. By careful observation, we see that $R^{2P}_{\max}$ decreases to zero as twice faster as $R^{DT}_{\max}$ and $R^{3P}_{\max}$ when the source powers tend to zero. Moreover, we also find that the asymptotical results are quite accurate when the source powers are low.

C. Low Relay Power

In Fig. 8, we compare the three schemes when the relay power is as low as -20 dB. We find that the maximum secrecy sum rate of two-phase scheme is close to zero and direct transmission is better than three-phase scheme, which verifies Corollary 4. The reason is that the only link $A \leftrightarrows R \leftrightarrows B$ of the two-phase scheme is very weak while there are strong direct links in the other two schemes with high source powers.

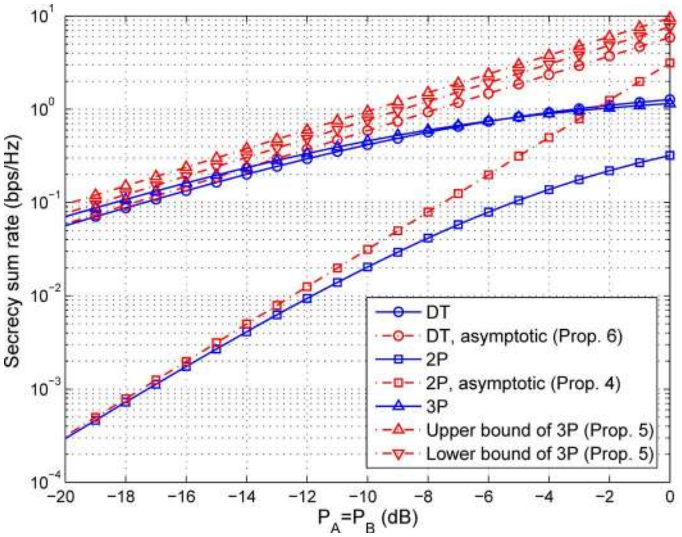


Fig. 7. Comparison of the three schemes with high relay power when $N_A = 2$, $N_R = 3$, $N_B = 2$ and $P_R = 40$ dB.

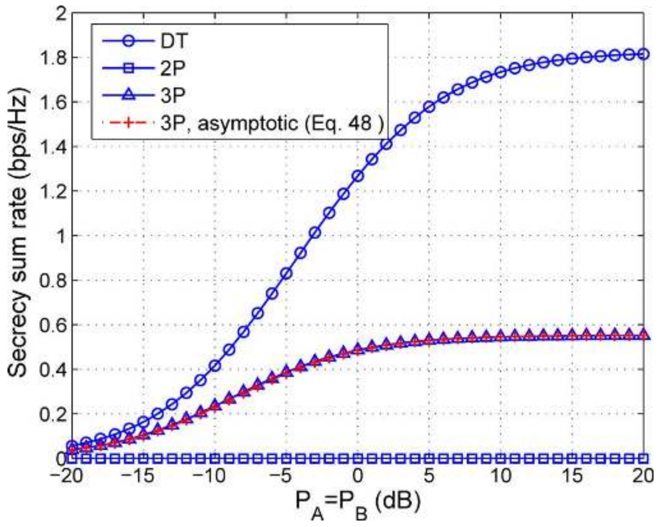


Fig. 8. Comparison of the three schemes with low relay power. $N_A = 2$, $N_R = 3$, $N_B = 2$ and $P_R = -20$ dB.

D. Fading Channels

In this subsection, we provide some simulation results averaged over fading channels. We generated 1000 independent channel realizations (every entry of the matrices is generated from $\mathcal{CN}(0, 1)$ distribution) and obtain average secrecy sum rate. For the two-phase and three-phase scheme, the simulation results are obtained by Algorithms 1 and 2.

In Fig. 9, we compare the average secrecy sum rates of the three schemes with varying relay power. The source powers are fixed at 15 dB and $N_A = N_B = 2$, $N_R = 3$. The average rate of the three-phase scheme increases with the relay power and has similar performance with direct transmission at high relay power. For the two-phase scheme, as the relay power increases, the average rate rises from zero up to 2.2 bps/Hz. We can see that

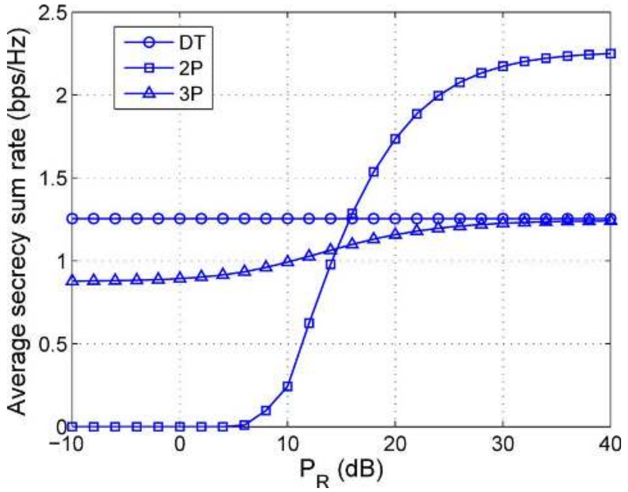


Fig. 9. Comparison of the three schemes with varying relay power, $P_A = P_B = 15\ \mathrm{dB}, N_A = 2, N_R = 3, N_R = 2$.

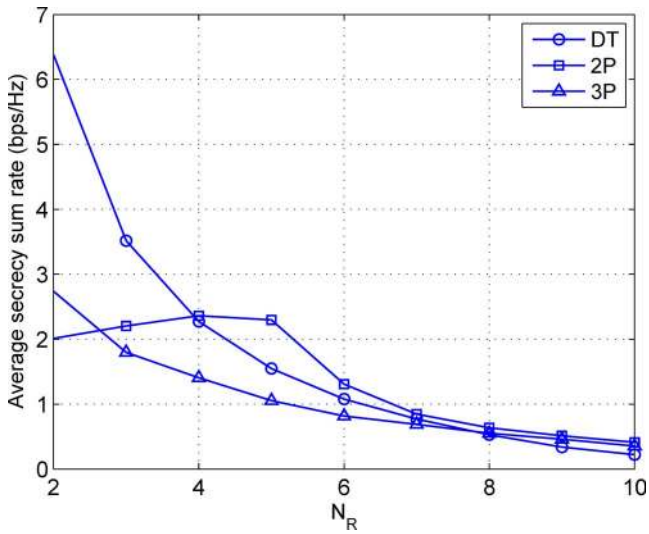


Fig. 10. Comparison of the three schemes with varying relay antenna number, $P_A = P_B = 15\ \mathrm{dB}, P_R = 25\ \mathrm{dB}, N_A = 3, N_B = 3$.

the two-phase scheme is much better than the other two schemes when relay power is high. The reason is that signal alignment can be achieved when P_R is large as $N_A + N_B > N_R$.

In Fig. 10, we plot the average secrecy sum rate versus the relay antenna number. The source nodes A and B both have three antennas. The relay power is 25 dB and the source powers are 15 dB. From the figure, we see that the average rate of the direct transmission scheme monotonically decreases with N_R. This is because the untrusted relay can overhear more information as N_R increases. For the two-phase transmission scheme, the average rate achieves the largest value when $N_R = 4$. The reason is that when N_R is too small, the relay does not have enough abilities to help the two-way transmission and when N_R is too large, the relay will be more powerful to decode the received signals. For the three-phase scheme, the average rate also decreases with N_R in this case.

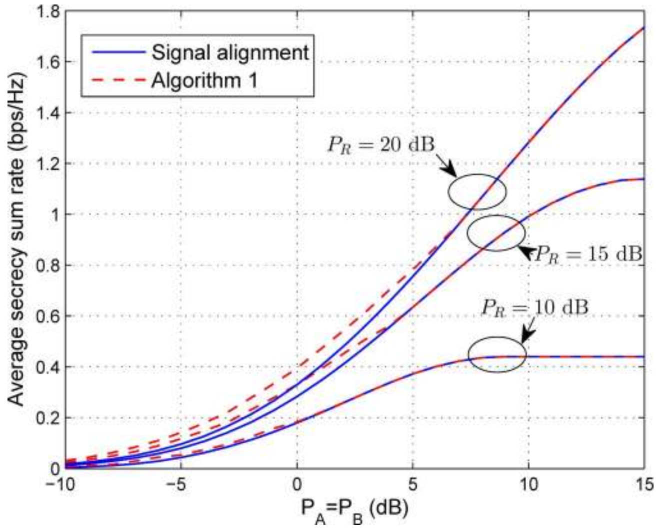


Fig. 11. Comparison between signal alignment and Algorithm 1 for the two-phase two-way relay scheme, $N_A = 2, N_R = 3$ and $N_B = 2$.

Finally, in Fig. 11, we illustrate the performance of the signal alignment technique in comparison with the Algorithm 1 for the two-phase two-way relay scheme at finite SNR regions. It is seen that at $P_R = 10\ \mathrm{dB}$, the signal alignment technique performs almost the same as Algorithm 1 when $P_A = P_B > 0\ \mathrm{dB}$. Similarly, at $P_R = 15\ \mathrm{dB\ and}\ 20\ \mathrm{dB}$, the two curves are almost the same when $P_A = P_B > 5\ \mathrm{dB\ and}\ 7\ \mathrm{dB}$, respectively. Therefore, we can conclude that the signal alignment technique generally performs quite good compared with Algorithm 1 as long as the source and relay powers are not so small.

VI. Conclusion

In this paper, we investigated a MIMO two-way AF relay system where the two source nodes exchange confidential information with an untrusted relay. For both two-phase and three-phase two-way relay schemes, we proposed efficient algorithms to jointly design the secure source and relay beamformers iteratively. Furthermore, we analyzed the asymptotical performance of the secure beamforming schemes in low and high power regimes of the sources and relay. Simulation results validate our asymptotical analysis.

From these results, we can conclude that the conventional two-way direct transmission is preferred when the relay power goes to zero. When the relay power approaches infinity and source powers approach zero, the three-phase two-way relay scheme performs best. Moreover, when all powers go to infinity, the two-phase two-way relay scheme has the best performance if signal alignment techniques are used, which also lowers the requirement of numbers of antennas at the source nodes for security.

Appendix A
Secure Beamforming of Two-Way Direct Transmission Scheme

For the two-way direct transmission scheme, the transmission consists of two phases. In the first phase, A transmits while B and R listen. During the second phase, B transmits while A and

R listens. An achievable secrecy sum rate of this two-way direct transmission scheme given by [29] is,

$$\mathcal{R}_s^{DT} = \sum_{i\in\{A,B\}} \frac{1}{2}\left[\log_2 \frac{1+\mathbf{q}_i^H\mathbf{T}_i^H\mathbf{T}_i\mathbf{q}_i}{1+\mathbf{q}_i^H\mathbf{H}_i^H\mathbf{H}_i\mathbf{q}_i}\right]^+. \tag{37}$$

We want to maximize the secrecy sum rate $\mathcal{R}_s^{DT}$ subject to the source power constraints. According to [29], [36] and [25], the optimal beamforming $\mathbf{q}_i^{DT}$ of the two-way direct transmission scheme is given by

$$\mathbf{q}_i^{DT} = \frac{\sqrt{P_i^{DT}}\boldsymbol{\psi}_{\max}(\mathbf{I}+P_i^{DT}\mathbf{T}_i^H\mathbf{T}_i, \mathbf{I}+P_i^{DT}\mathbf{H}_i^H\mathbf{H}_i)}{\|\boldsymbol{\psi}_{\max}(\mathbf{I}+P_i^{DT}\mathbf{T}_i^H\mathbf{T}_i, \mathbf{I}+P_i^{DT}\mathbf{H}_i^H\mathbf{H}_i)\|}, \quad i\in\{A,B\}, \tag{38}$$

and the maximum secrecy sum rate is given by

$$\begin{aligned}&\mathcal{R}_{\max}^{DT}(P_A^{DT}, P_B^{DT})\\ &= \sum_{i\in\{A,B\}} \frac{1}{2}\left[\log_2 \lambda_{\max}\left(\mathbf{I}+P_i\mathbf{T}_i^H\mathbf{T}_i, \mathbf{I}+P_i\mathbf{H}_i^H\mathbf{H}_i\right)\right]^+. \end{aligned}\tag{39}$$

Appendix B
Search A Using Gradient Method

Substituting (12) into (5), we obtain a subproblem of optimizing $\mathbf{A}$ given $\mathbf{q}_A$ and $\mathbf{q}_B$ as follows,

$$\min_{\mathbf{A}} \quad -\mathcal{R}_s^{2P} \tag{40a}$$

$$\text{s. t.} \quad \mathrm{Tr}\big(\mathbf{A}\mathbf{U}^H\mathbf{H}_A\mathbf{q}_A\mathbf{q}_A^H\mathbf{H}_A^H\mathbf{U}\mathbf{A}^H \tag{40b}$$

$$+\mathbf{A}\mathbf{U}^H\mathbf{H}_B\mathbf{q}_B\mathbf{q}_B^H\mathbf{H}_B^H\mathbf{U}\mathbf{A}^H+\mathbf{A}\mathbf{A}^H\big)\le P_R^{2P}. \tag{40c}$$

We use the logarithmic barrier method to incorporate the constraint into the objective function. The logarithmic barrier function associated with (40) is,

$$\begin{aligned}B(\mathbf{A},\mu) = &-\mathcal{R}_s^{2P} - \mu\ln\Big(P_R^{2P}\\ &-\mathrm{Tr}\big(\mathbf{A}\mathbf{U}^H\mathbf{H}_A\mathbf{q}_A\mathbf{q}_A^H\mathbf{H}_A^H\mathbf{U}\mathbf{A}^H\\ &+\mathbf{A}\mathbf{U}^H\mathbf{H}_B\mathbf{q}_B\mathbf{q}_B^H\mathbf{H}_B^H\mathbf{U}\mathbf{A}^H+\mathbf{A}\mathbf{A}^H\big)\Big)\end{aligned} \tag{41}$$

where $\mu > 0$ is the barrier parameter.

The gradient of $B(\mathbf{A},\mu)$ with respect to $\mathbf{A}$ is given by (42) shown at the bottom of the page. With this gradient, we use gradient descent method to search $\mathbf{A}$.

Appendix C
Search Optimal $\mathbf{q}_B$ Given $\mathbf{F}$ and $\mathbf{q}_A$ in Two-Phase Two-Way Relay Scheme

First, we rewrite (5) in the homogenized form with respect to $\mathbf{q}_B$, as (43) shown at the bottom of the page. Then, we can follow the same procedure in [37, Section III-B] or [25, Appendix A] to find the optimal $\mathbf{q}_B$. The basic idea is to first relax (43) into a fractional semi-definite programming (SDP) problem, which is then transformed to a SDP problem using Charnes-Cooper variable transformation. At last, the rank-one matrix decomposition theorem [38, Theorem 2.3] is used. Here we omit the details.

Appendix D
Proof of Lemma 2

First, we consider the case where $N_R > N_A + N_B$. Without loss of generality, we can express $\mathbf{F}_i$ as

$$\mathbf{F}_i = [\mathbf{V} \quad \mathbf{V}^\perp]\begin{bmatrix}\mathbf{a}_i & \mathbf{B}_i\\ \mathbf{c}_i & \mathbf{D}_i\end{bmatrix}\begin{bmatrix}\mathbf{U}_i^H\\ \mathbf{U}_i^{\perp H}\end{bmatrix} \tag{44}$$

$$\begin{aligned}\frac{\partial B(\mathbf{A},\mu)}{\partial \mathbf{A}^*} = &-\sum_{i\in\{A,B\}} \log_2 e\frac{\mathbf{V}^H\mathbf{G}_i^H\mathbf{K}_i^{-1}\mathbf{G}_i\mathbf{F}\mathbf{H}_{\bar{i}}\mathbf{q}_{\bar{i}}\mathbf{q}_{\bar{i}}^H\mathbf{H}_{\bar{i}}^H\mathbf{U} - \mathbf{V}^H\mathbf{G}_i^H\mathbf{K}_i^{-1}\mathbf{G}_i\mathbf{F}\mathbf{H}_{\bar{i}}\mathbf{q}_{\bar{i}}\mathbf{q}_{\bar{i}}^H\mathbf{H}_{\bar{i}}^H\mathbf{F}^H\mathbf{G}_i^H\mathbf{K}_i^{-1}\mathbf{G}_i\mathbf{F}\mathbf{U}}{2\big(1+\mathbf{q}_{\bar{i}}^H\mathbf{H}_{\bar{i}}^H\mathbf{F}^H\mathbf{G}_i^H\mathbf{K}_i^{-1}\mathbf{G}_i\mathbf{F}\mathbf{H}_{\bar{i}}\mathbf{q}_{\bar{i}}\big)}\\ &+\mu\frac{\mathbf{A}\mathbf{U}^H\mathbf{H}_A\mathbf{q}_A\mathbf{q}_A^H\mathbf{H}_A^H\mathbf{U}+\mathbf{A}\mathbf{U}^H\mathbf{H}_B\mathbf{q}_B\mathbf{q}_B^H\mathbf{H}_B^H\mathbf{U}+\mathbf{A}}{P_R^{2P}-\mathrm{Tr}\big(\mathbf{A}\mathbf{U}^H\mathbf{H}_A\mathbf{q}_A\mathbf{q}_A^H\mathbf{H}_A^H\mathbf{U}\mathbf{A}^H+\mathbf{A}\mathbf{U}^H\mathbf{H}_B\mathbf{q}_B\mathbf{q}_B^H\mathbf{H}_B^H\mathbf{U}\mathbf{A}^H+\mathbf{A}\mathbf{A}^H\big)}\end{aligned} \tag{42}$$

$$\max_{\mathbf{q}_B,t} \quad \frac{\mathrm{Tr}\left\{\begin{bmatrix}\mathbf{H}_B^H\mathbf{F}^H\mathbf{G}_A^H\mathbf{K}_A^{-1}\mathbf{G}_A\mathbf{F}\mathbf{H}_B & \mathbf{0}\\ \mathbf{0} & 1\end{bmatrix}\begin{bmatrix}\mathbf{q}_B\mathbf{q}_B^H & \mathbf{q}_Bt^*\\ \mathbf{q}_B^Ht & |t|^2\end{bmatrix}\right\}}{\mathrm{Tr}\left\{\begin{bmatrix}\mathbf{H}_B^H\left(\left(1+\|\mathbf{H}_A\mathbf{q}_A\|^2\right)\mathbf{I}-\mathbf{H}_A\mathbf{q}_A\mathbf{q}_A^H\mathbf{H}_A^H\right)\mathbf{H}_B & \mathbf{0}\\ \mathbf{0} & 1+\|\mathbf{H}_A\mathbf{q}_A\|^2\end{bmatrix}\begin{bmatrix}\mathbf{q}_B\mathbf{q}_B^H & \mathbf{q}_Bt^*\\ \mathbf{q}_B^Ht & |t|^2\end{bmatrix}\right\}} \tag{43a}$$

$$s.t. \quad \mathrm{Tr}\left\{\begin{bmatrix}\mathbf{I} & \mathbf{0}\\ \mathbf{0} & 0\end{bmatrix}\begin{bmatrix}\mathbf{q}_B\mathbf{q}_B^H & \mathbf{q}_Bt^*\\ \mathbf{q}_B^Ht & |t|^2\end{bmatrix}\right\} \le P_B, \tag{43b}$$

$$\mathrm{Tr}\left\{\begin{bmatrix}\mathbf{H}_B^H\mathbf{F}^H\mathbf{F}\mathbf{H}_B & \mathbf{0}\\ \mathbf{0} & 0\end{bmatrix}\begin{bmatrix}\mathbf{q}_B\mathbf{q}_B^H & \mathbf{q}_Bt^*\\ \mathbf{q}_B^Ht & |t|^2\end{bmatrix}\right\} \le P_r - \mathrm{Tr}\left\{\mathbf{F}\mathbf{F}^H\right\} - \mathrm{Tr}\left\{\mathbf{F}\mathbf{H}_A\mathbf{q}_A\mathbf{q}_A^H\mathbf{H}_A^H\mathbf{F}^H\right\}, \tag{43c}$$

$$\mathrm{Tr}\left\{\begin{bmatrix}\mathbf{0} & \mathbf{0}\\ \mathbf{0} & 1\end{bmatrix}\begin{bmatrix}\mathbf{q}_B\mathbf{q}_B^H & \mathbf{q}_Bt^*\\ \mathbf{q}_B^Ht & |t|^2\end{bmatrix}\right\} = 1. \tag{43d}$$

where $\mathbf{V}$ is from (13), $\mathbf{V}^{\perp} \in \mathbb{C}^{N_R \times (N_R - N_A - N_B)}$ such that $\left[\mathbf{V} \quad \mathbf{V}^{\perp}\right]$ is unitary , $\mathbf{U}_i$ is $\frac{\mathbf{H}_i \mathbf{q}_i}{\|\mathbf{H}_i \mathbf{q}_i\|}$, $\mathbf{U}_i^{\perp} \in \mathbb{C}^{N_R \times (N_R - 1)}$ such that $\left[\mathbf{U}_i \quad \mathbf{U}_i^{\perp}\right]$ is unitary, and $\mathbf{a}_i \in \mathbb{C}^{(N_A+N_B)\times 1}$, $\mathbf{c}_i \in \mathbb{C}^{(N_R-N_A-N_B)\times 1}$, $\mathbf{B}_i \in \mathbb{C}^{(N_A+N_B)\times(N_R-1)}$, $\mathbf{D}_i \in \mathbb{C}^{(N_R-N_A-N_B)\times(N_R-1)}$. Therefore, we obtain (45) shown at the bottom of the page. Therein, (a) is from the above property of $\mathbf{F}_i$ (44), (b) is from that $\sum_{i\in\{A,B\}} \mathbf{G}_A \mathbf{V} \mathbf{B}_i \mathbf{B}_i^H \mathbf{V} \mathbf{G}_A^H$ is positive semidefinite matrix. We see that the information rate from B to A $\mathcal{R}_{BA}^{3P} = \log_2(1 + \mathbf{q}_B^H \mathbf{H}_B^H \mathbf{H}_B \mathbf{q}_B + x_{BA})$ is not related to $\mathbf{c}_i$ and $\mathbf{D}_i$ and achieves a upper bound when $\mathbf{B}_i = \mathbf{0}$. Similarly, the information rate from A to B, $\mathcal{R}_{AB}^{3P}$, is also not related to $\mathbf{c}_i$ and $\mathbf{D}_i$ and achieves a upper bound when $\mathbf{B}_i = \mathbf{0}$. In addition, the power consumed by the relay is

$$\begin{aligned}
&\operatorname{Tr}\big(\mathbf{F}_A \mathbf{H}_A \mathbf{q}_A \mathbf{q}_A^H \mathbf{H}_A^H \mathbf{F}_A^H + \mathbf{F}_B \mathbf{H}_B \mathbf{q}_B \mathbf{q}_B^H \mathbf{H}_B^H \mathbf{F}_B^H \\
&\quad + \mathbf{F}_A \mathbf{F}_A^H + \mathbf{F}_B \mathbf{F}_B^H\big) \\
&= \sum_{i\in\{A,B\}} \|\mathbf{H}_i \mathbf{q}_i\|^2 \left(\|\mathbf{a}_i\|^2 + \|\mathbf{c}_i\|^2\right) \\
&\quad + \sum_{i\in\{A,B\}} \left(\|\mathbf{a}_i\|^2 + \|\mathbf{B}_i\|_F^2 + \|\mathbf{c}_i\|^2 + \|\mathbf{D}_i\|_F^2\right)
\end{aligned}$$

We find that the relay power is increased when $\mathbf{B}_i, \mathbf{c}_i, \mathbf{D}_i$ is not zero. Therefore, it leads to $\mathbf{B}_i = \mathbf{0}$, $\mathbf{c}_i = \mathbf{0}$ and $\mathbf{D}_i = \mathbf{0}$.

When $N_R \leq N_A + N_B$, we can express $\mathbf{F}_i$ as

$$\mathbf{F}_i = \mathbf{V}\left[\mathbf{a}_i \quad \mathbf{B}_i\right] \begin{bmatrix} \mathbf{U}_i^H \\ \mathbf{U}_i^{\perp H} \end{bmatrix} \tag{46}$$

where $\mathbf{V}$ is from (13), $\mathbf{U}_i$ is $\frac{\mathbf{H}_i \mathbf{q}_i}{\|\mathbf{H}_i \mathbf{q}_i\|}$, $\mathbf{U}_i^{\perp} \in \mathbb{C}^{N_R \times (N_R-1)}$ such that $\left[\mathbf{U}_i \quad \mathbf{U}_i^{\perp}\right]$ is unitary, and $\mathbf{a}_i \in \mathbb{C}^{N_R \times 1}$, $\mathbf{B}_i \in \mathbb{C}^{N_R \times (N_R-1)}$. Similar as the above case, we can prove that the optimal $\mathbf{B}_i = \mathbf{0}$.

Appendix E
Proof of Proposition 2

Substituting the optimal relay beamforming structure (14) into (6), we obtain the third term in (6) as follows,

$$\begin{aligned}
&\mathbf{q}_B^H \mathbf{H}_B^H \mathbf{F}_B^H \mathbf{G}_A^H \left(\mathbf{G}_A \left(\mathbf{F}_A \mathbf{F}_A^H + \mathbf{F}_B \mathbf{F}_B^H\right) \mathbf{G}_A^H + \mathbf{I}\right)^{-1} \\
&\quad \cdot \mathbf{G}_A \mathbf{F}_B \mathbf{H}_B \mathbf{q}_B \\
&= \|\mathbf{H}_B \mathbf{q}_B\|^2 \mathbf{a}_B^H \mathbf{V}^H \mathbf{G}_A^H \\
&\quad \cdot \left(\sum_{i\in\{A,B\}} \mathbf{G}_A \mathbf{V} \mathbf{a}_i \mathbf{a}_i^H \mathbf{V}^H \mathbf{G}_A^H + \mathbf{I}\right)^{-1} \mathbf{G}_A \mathbf{V} \mathbf{a}_B \\
&\overset{(a)}{\leq} \|\mathbf{H}_B \mathbf{q}_B\|^2 \mathbf{a}_B^H \mathbf{V}^H \mathbf{G}_A^H \left(\mathbf{G}_A \mathbf{V} \mathbf{a}_B \mathbf{a}_B^H \mathbf{V}^H \mathbf{G}_A^H + \mathbf{I}\right)^{-1} \mathbf{G}_A \mathbf{V} \mathbf{a}_B \\
&\overset{(b)}{=} \|\mathbf{H}_B \mathbf{q}_B\|^2 \mathbf{a}_B^H \mathbf{V}^H \mathbf{G}_A^H \\
&\quad \cdot \Big(\mathbf{I} - \mathbf{G}_A \mathbf{V} \mathbf{a}_B (\mathbf{a}_B^H \mathbf{V}^H \mathbf{G}_A^H \mathbf{G}_A \mathbf{V} \mathbf{a}_B + 1)^{-1} \\
&\quad \cdot \mathbf{a}_B^H \mathbf{V}^H \mathbf{G}_A^H\Big) \mathbf{G}_A \mathbf{V} \mathbf{a}_B \\
&= \|\mathbf{H}_B \mathbf{q}_B\|^2 \frac{\|\mathbf{G}_A \mathbf{V} \mathbf{a}_B\|^2}{1 + \|\mathbf{G}_A \mathbf{V} \mathbf{a}_B\|^2} \\
&\leq \|\mathbf{H}_B \mathbf{q}_B\|^2
\end{aligned}$$

where (a) is from that $\mathbf{G}_A \mathbf{V} \mathbf{a}_1 \mathbf{a}_1^H \mathbf{V}^H \mathbf{G}_A^H$ is positive semidefinite, (b) is from the matrix inverse lemma.

The above third term in (6) also has a lower bound by simply letting $\mathbf{a}_A = \mathbf{a}_B = \bar{\mathbf{a}}$,

$$\begin{aligned}
&\mathbf{q}_B^H \mathbf{H}_B^H \mathbf{F}_B^H \mathbf{G}_A^H \left(\mathbf{G}_A \left(\mathbf{F}_A \mathbf{F}_A^H + \mathbf{F}_B \mathbf{F}_B^H\right) \mathbf{G}_A^H + \mathbf{I}\right)^{-1} \\
&\quad \cdot \mathbf{G}_A \mathbf{F}_B \mathbf{H}_B \mathbf{q}_B \\
&= \|\mathbf{H}_B \mathbf{q}_B\|^2 \mathbf{a}^H \mathbf{V}^H \mathbf{G}_A^H \left(2\mathbf{G}_A \mathbf{V} \mathbf{a} \mathbf{a}^H \mathbf{V}^H \mathbf{G}_A^H + \mathbf{I}\right)^{-1} \mathbf{G}_A \mathbf{V} \mathbf{a} \\
&= \frac{1}{2}\|\mathbf{H}_B \mathbf{q}_B\|^2 \left(1 - \left(1 + 2\mathbf{a}^H \mathbf{V}^H \mathbf{G}_A^H \mathbf{G}_A \mathbf{V} \mathbf{a}\right)^{-1}\right) \\
&= \frac{1}{2}\|\mathbf{H}_B \mathbf{q}_B\|^2 \frac{2\|\mathbf{G}_A \mathbf{V} \mathbf{a}\|^2}{1 + 2\|\mathbf{G}_A \mathbf{V} \mathbf{a}\|^2} \\
&\to \frac{1}{2}\|\mathbf{H}_B \mathbf{q}_B\|^2 \quad \text{as} \quad P_R \to \infty
\end{aligned}$$

Therefore, we have

$$\begin{aligned}
&\frac{1}{3}\log_2\left(1 + \mathbf{q}_i^H \mathbf{T}_i^H \mathbf{T}_i \mathbf{q}_i + \frac{1}{2}\mathbf{q}_i^H \mathbf{H}_i^H \mathbf{H}_i \mathbf{q}_i\right) \\
&\quad \leq \lim_{P_R \to \infty} \mathcal{R}_{i\bar{i}}^{3P} \\
&\quad \leq \frac{1}{3}\log_2\left(1 + \mathbf{q}_i^H \mathbf{T}_i^H \mathbf{T}_i \mathbf{q}_i + \mathbf{q}_i^H \mathbf{H}_i^H \mathbf{H}_i \mathbf{q}_i\right)
\end{aligned} \tag{47}$$

To prove Proposition 2, we first substitute the upper bound and lower bound into (8). The rest of the proof is similar to the proof of [25, Lemma 7]. In addition, the condition that the entries of channel matrices are generated from continuous distribution are used in the proof.

$$\begin{aligned}
x_{BA} &\triangleq \mathbf{q}_B^H \mathbf{H}_B^H \mathbf{F}_B^H \mathbf{G}_A^H \left(\mathbf{G}_A \left(\mathbf{F}_A \mathbf{F}_A^H + \mathbf{F}_B \mathbf{F}_B^H\right) \mathbf{G}_A^H + \mathbf{I}\right)^{-1} \mathbf{G}_A \mathbf{F}_B \mathbf{H}_B \mathbf{q}_B \\
&\overset{(a)}{=} \|\mathbf{H}_B \mathbf{q}_B\|^2 \mathbf{a}_B^H \mathbf{V}^H \mathbf{G}_A^H \left(\sum_{i\in\{A,B\}} \mathbf{G}_A \mathbf{V} \mathbf{a}_i \mathbf{a}_i^H \mathbf{V}^H \mathbf{G}_A^H + \sum_{i\in\{A,B\}} \mathbf{G}_A \mathbf{V} \mathbf{B}_i \mathbf{B}_i^H \mathbf{V}^H \mathbf{G}_A^H + \mathbf{I}\right)^{-1} \mathbf{G}_A \mathbf{V} \mathbf{a}_B \\
&\overset{(b)}{\leq} \|\mathbf{H}_B \mathbf{q}_B\|^2 \mathbf{a}_B^H \mathbf{V}^H \mathbf{G}_A^H \left(\sum_{i\in\{A,B\}} \mathbf{G}_A \mathbf{V} \mathbf{a}_i \mathbf{a}_i^H \mathbf{V}^H \mathbf{G}_A^H + \mathbf{I}\right)^{-1} \mathbf{G}_A \mathbf{V} \mathbf{a}_B
\end{aligned} \tag{45}$$

APPENDIX F
PROOF OF PROPOSITION 4

Plugging the condition $P_A \rightarrow 0$, $P_B \rightarrow 0$ into (22), we have

$$\begin{aligned}
&\lim_{P_R\rightarrow\infty} \mathcal{R}_s^{2P}\\
&= \frac{1}{2}\log_2 \frac{1}{1-\frac{\mathbf{q}_B^H\mathbf{H}_B^H\mathbf{H}_A\mathbf{q}_A\mathbf{q}_A^H\mathbf{H}_A^H\mathbf{H}_B\mathbf{q}_B}{\left(1+\mathbf{q}_B^H\mathbf{H}_B^H\mathbf{H}_B\mathbf{q}_B\right)\left(1+\mathbf{q}_A^H\mathbf{H}_A^H\mathbf{H}_A\mathbf{q}_A\right)}}\\
&= -\frac{1}{2}\log_2\left(1-\frac{\mathbf{q}_B^H\mathbf{H}_B^H\mathbf{H}_A\mathbf{q}_A\mathbf{q}_A^H\mathbf{H}_A^H\mathbf{H}_B\mathbf{q}_B}{\left(1+\mathbf{q}_B^H\mathbf{H}_B^H\mathbf{H}_B\mathbf{q}_B\right)\left(1+\mathbf{q}_A^H\mathbf{H}_A^H\mathbf{H}_A\mathbf{q}_A\right)}\right)\\
&\approx -\frac{1}{2}\log_2\left(1-\mathbf{q}_B^H\mathbf{H}_B^H\mathbf{H}_A\mathbf{q}_A\mathbf{q}_A^H\mathbf{H}_A^H\mathbf{H}_B\mathbf{q}_B\right)\\
&\approx \frac{1}{2\ln 2}\left\|\mathbf{q}_B^H\mathbf{H}_B^H\mathbf{H}_A\mathbf{q}_A\right\|^2.
\end{aligned}$$

To maximize $\|\mathbf{q}_B^H\mathbf{H}_B^H\mathbf{H}_A\mathbf{q}_A\|^2$, we obtain Proposition 4.

APPENDIX G
PROOF OF COROLLARY 4

For fair comparison, we set $P_i = P_i^{DT} = P_i^{2P} = \frac{2}{3}P_i^{3P}$, $i \in \{A, B\}$ and $P_R = P_R^{2P} = \frac{2}{3}P_R^{3P}$. When the relay power $P_R \rightarrow 0$, there are only direct links between the two source nodes for the three-phase scheme. Thus, the maximum secrecy sum rate of the three-phase two-way relay scheme $\mathcal{R}_{\max}^{3P}$ is

$$\begin{aligned}
&\mathcal{R}_{\max}^{3P}\\
&\approx \max_{\mathbf{q}_A,\mathbf{q}_B}\frac{1}{3}\sum_{i\in\{A,B\}}\left[\log_2\frac{1+\mathbf{q}_i^H\mathbf{T}_i^H\mathbf{T}_i\mathbf{q}_i}{1+\mathbf{q}_i^H\mathbf{H}_i^H\mathbf{H}_i\mathbf{q}_i}\right]^+\\
&= \frac{1}{3}\sum_{i\in\{A,B\}}\left[\log_2\left(\lambda_{\max}\left(\mathbf{I}+P_i^{3P}\mathbf{T}_i^H\mathbf{T}_i, \mathbf{I}+P_i^{3P}\mathbf{H}_i^H\mathbf{H}_i\right)\right)\right]^+\\
&= \frac{1}{3}\sum_{i\in\{A,B\}}\left[\log_2\left(\lambda_{\max}\left(\mathbf{I}+\frac{3}{2}P_i\mathbf{T}_i^H\mathbf{T}_i, \mathbf{I}+\frac{3}{2}P_i\mathbf{H}_i^H\mathbf{H}_i\right)\right)\right]^+.
\end{aligned} \tag{48}$$

In addition, we have

$$\begin{aligned}
&\lambda_{\max}\left(\mathbf{I}+\frac{3}{2}P_i\mathbf{T}_i^H\mathbf{T}_i, \mathbf{I}+\frac{3}{2}P_i\mathbf{H}_i^H\mathbf{H}_i\right)\\
&\overset{(a)}{=} \lambda_{\max}\left(\frac{3}{2}P_i\mathbf{T}_i^H\mathbf{T}_i-\frac{3}{2}P_i\mathbf{H}_i^H\mathbf{H}_i, \mathbf{I}+\frac{3}{2}P_i\mathbf{H}_i^H\mathbf{H}_i\right)+1\\
&= \max_{\boldsymbol{\psi}}\frac{\boldsymbol{\psi}^H\left(\frac{3}{2}P_i\mathbf{T}_i^H\mathbf{T}_i-\frac{3}{2}P_i\mathbf{H}_i^H\mathbf{H}_i\right)\boldsymbol{\psi}}{\boldsymbol{\psi}^H\left(\mathbf{I}+\frac{3}{2}P_i\mathbf{H}_i^H\mathbf{H}_i\right)\boldsymbol{\psi}}+1\\
&\le \max_{\boldsymbol{\psi}}\frac{3}{2}\frac{\boldsymbol{\psi}^H\left(P_i\mathbf{T}_i^H\mathbf{T}_i-P_i\mathbf{H}_i^H\mathbf{H}_i\right)\boldsymbol{\psi}}{\boldsymbol{\psi}^H\left(\mathbf{I}+P_i\mathbf{H}_i^H\mathbf{H}_i\right)\boldsymbol{\psi}}+1\\
&= \frac{3}{2}\lambda_{\max}\left(P_i\mathbf{T}_i^H\mathbf{T}_i-P_i\mathbf{H}_i^H\mathbf{H}_i, \mathbf{I}+P_i\mathbf{H}_i^H\mathbf{H}_i\right)+1\\
&\overset{(b)}{\le} \left(\lambda_{\max}\left(P_i\mathbf{T}_i^H\mathbf{T}_i-P_i\mathbf{H}_i^H\mathbf{H}_i, \mathbf{I}+P_i\mathbf{H}_i^H\mathbf{H}_i\right)+1\right)^{\frac{3}{2}}\\
&\overset{(c)}{=} \left(\lambda_{\max}\left(\mathbf{I}+P_i\mathbf{T}_i^H\mathbf{T}_i, \mathbf{I}+P_i\mathbf{H}_i^H\mathbf{H}_i\right)\right)^{\frac{3}{2}},
\end{aligned}$$

where (a) and (c) are from $\lambda_{\max}(\mathbf{A},\mathbf{B}) = \lambda_{\max}(\mathbf{A}-\mathbf{B},\mathbf{B})+1$, (b) is from $\frac{3}{2}x+1 \le (x+1)^{\frac{3}{2}}$ when x is a nonnegative real number.

Therefore, we obtain $\mathcal{R}_{\max}^{DT} \ge \mathcal{R}_{\max}^{3P}$ when $P_R \rightarrow 0$. Together with $\mathcal{R}_{\max}^{2P} \rightarrow 0$ when $P_R \rightarrow 0$, we obtain Proposition 4.

ACKNOWLEDGMENT

Prof. Y. Huang at Hong Kong Baptist University provided suggestions and codes for matrix rank-one decomposition used in Algorithms 1 and 2. The authors gratefully acknowledge this inspiration and support. We also thank the Associate Editor and anonymous reviewers for providing invaluable feedback.

REFERENCES

[1] J. Mo, M. Tao, Y. Liu, B. Xia, and X. Ma, "Secure beamforming for MIMO two-way transmission with an untrusted relay," in *Proc. IEEE Wireless Commun. Netw. Conf. (WCNC)*, 2013, pp. 4180–4185.

[2] R. Zhang, Y.-C. Liang, C. C. Chai, and S. Cui, "Optimal beamforming for two-way multi-antenna relay channel with analogue network coding," *IEEE J. Sel. Areas Commun.*, vol. 27, no. 5, pp. 699–712, 2009.

[3] S. Xu and Y. Hua, "Optimal design of spatial source-and-relay matrices for a non-regenerative two-way MIMO relay system," *IEEE Trans. Wireless Commun.*, vol. 10, no. 5, pp. 1645–1655, May 2011.

[4] R. Wang and M. Tao, "Joint source and relay precoding designs for MIMO two-way relaying based on MSE criterion," *IEEE Trans. Signal Process.*, vol. 60, no. 3, pp. 1352–1365, Mar. 2012.

[5] 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.

[6] C. Jeong and I.-M. Kim, "Optimal power allocation for secure multicarrier relay systems," *IEEE Trans. Signal Process.*, vol. 59, no. 11, pp. 5428–5442, Nov. 2011.

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

[8] I. Krikidis, J. Thompson, and S. Mclaughlin, "Relay selection for secure cooperative networks with jamming," *IEEE Trans. Wireless Commun.*, vol. 8, no. 10, pp. 5003–5011, Oct. 2009.

[9] D. Ng, E. Lo, and R. Schober, "Secure resource allocation and scheduling for OFDMA decode-and-forward relay networks," *IEEE Trans. Wireless Commun.*, vol. 10, no. 10, pp. 3528–3540, Oct. 2011.

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

[11] J. Mo, M. Tao, and Y. Liu, "Relay placement for physical layer security: A secure connection perspective," *IEEE Commun. Lett.*, vol. 16, no. 6, pp. 878–881, Jun. 2012.

[12] J. Chen, R. Zhang, L. Song, Z. Han, and B. Jiao, "Joint relay and jammer selection for secure two-way relay networks," *IEEE Trans. Inf. Forensics Security*, vol. 7, no. 1, pp. 310–320, Feb. 2012.

[13] 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.

[14] A. Mukherjee and A. L. Swindlehurst, "Securing multi-antenna two-way relay channels with analog network coding against eavesdroppers," in *Proc. IEEE 11th Int Signal Process. Adv. Wireless Commun. (SPAWC) Workshop*, 2010, pp. 1–5.

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

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

[17] T. Shimizu, H. Iwai, and H. Sasaoka, "Physical-layer secret key agreement in two-way wireless relaying systems," *IEEE Trans. Inf. Forensics Security*, vol. 6, no. 3, pp. 650–660, Sep. 2011.

[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] Y. Oohama, "Coding for relay channels with confidential messages," in *Proc. Inf. Theory Workshop*, 2001, pp. 87–89.

[20] X. He and A. Yener, "Two-hop secure communication using an untrusted relay: A case for cooperative jamming," in *Proc. IEEE Global Telecommun. Conf.*, Dec. 4, 2008, pp. 1–5.

[21] X. He and A. Yener, "Two-hop secure communication using an untrusted relay," *EURASIP J. Wirel. Commun. Netw.*, vol. 2009, pp. 9:1–9:10, May 2009.

[22] L. Sun, T. Zhang, Y. Li, and H. Niu, "Performance study of two-hop amplify-and-forward systems with untrustworthy relay nodes," *IEEE Trans. Veh. Technol.*, vol. 61, no. 8, pp. 3801–3807, 2012.

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

[24] R. Zhang, L. Song, Z. Han, and B. Jiao, "Physical layer security for two-way untrusted relaying with friendly jammers," *IEEE Trans. Veh. Technol.*, vol. 61, no. 8, pp. 3693–3704, Oct. 2012.

[25] C. Jeong, I.-M. Kim, and D. I. 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.

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

[27] B. Rankov and A. Wittneben, "Spectral efficient protocols for half-duplex fading relay channels," *IEEE J. Sel. Areas Commun.*, vol. 25, no. 2, pp. 379–389, Feb. 2007.

[28] S. J. Kim, P. Mitran, and V. Tarokh, "Performance bounds for bidirectional coded cooperation protocols," *IEEE Trans. Inf. Theory*, vol. 54, no. 11, pp. 5253–5241, Aug. 2008.

[29] A. Khisti and G. Wornell, "Secure transmission with multiple antennas I: The MISOME wiretap channel," *IEEE Trans. Inf. Theory*, vol. 56, no. 7, pp. 3088–3104, Jul. 2010.

[30] Z.-Q. Luo, W.-K. Ma, A.-C. So, Y. Ye, and S. Zhang, "Semidefinite relaxation of quadratic optimization problems," *IEEE Signal Process. Mag.*, vol. 27, no. 3, pp. 20–34, 2010.

[31] N. Lee, J.-B. Lim, and J. Chun, "Degrees of freedom of the MIMO y channel: Signal space alignment for network coding," *IEEE Trans. Inf. Theory*, vol. 56, no. 7, pp. 3332–3342, Jul. 2010.

[32] G. Strang*, Linear Algebra and Its Applications*, 4th ed. Pacific Grove, CA, USA: Brooks/Cole, 2006.

[33] G. H. Golub and C. F. Van Loan*, Matrix computations*. Baltimore, MD, USA: John Hopkins Univ. Press, 2012.

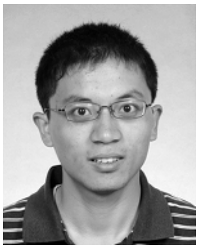
[34] A. Bjorck and G. H. Golub, "Numerical methods for computing angles between linear subspaces," *Math. Comput.*, vol. 27, no. 123, pp. 579–594, 1973.

[35] M. Chen and A. Yener, "Power allocation for F/TDMA multiuser two-way relay networks," *IEEE Trans. Wireless Commun.*, vol. 9, no. 2, pp. 546–551, 2010.

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

[37] A. De Maio, Y. Huang, D. Palomar, S. Zhang, and A. Farina, "Fractional QCQP with applications in ML steering direction estimation for radar detection," *IEEE Trans. Signal Process.*, vol. 59, no. 1, pp. 172–185, 2011.

[38] W. Ai, Y. Huang, and S. Zhang, "New results on hermitian matrix rank-one decomposition," *Math. Programm.*, vol. 128, no. 1-2, pp. 253–283, 2011.



Jianhua Mo (S'12) received his BS and MS degree in Electronic Engineering from Shanghai Jiao Tong University in 2010 and 2013 respectively. He also received MS degree in Electrical and Computer Engineering from Georgia Institute of Technology. He is currently a PhD student in Wireless Networking and Communications Group, The University of Texas at Austin. His research interest includes physical layer security and millimeter wave communications.

Meixia Tao (S'00–M'04–SM'10) received the B.S. degree in electronic engineering from Fudan University, Shanghai, China, in 1999, and the Ph.D. degree in electrical and electronic engineering from Hong Kong University of Science and Technology in 2003. She is currently a Professor with the Department of Electronic Engineering, Shanghai Jiao Tong University, China. Prior to that, she was a Member of Professional Staff at Hong Kong Applied Science and Technology Research Institute during 2003–2004, and a Teaching Fellow then an Assistant Professor at the Department of Electrical and Computer Engineering, National University of Singapore from 2004 to 2007. Her current research interests include physical layer network coding, wireless resource allocation, MIMO techniques, and physical layer security.

Dr. Tao is an Editor for the IEEE TRANSACTIONS ON COMMUNICATIONS and the IEEE WIRELESS COMMUNICATIONS LETTERS. She was on the Editorial Board of the IEEE TRANSACTIONS ON WIRELESS COMMUNICATIONS from 2007 to 2011 and the IEEE COMMUNICATIONS LETTERS from 2009 to 2012. She also served as Guest Editor for IEEE COMMUNICATIONS MAGAZINE with feature topic on LTE-Advanced and 4G Wireless Communications in 2012, and Guest Editor for EURISAP J WCN with special issue on Physical Layer Network Coding for Wireless Cooperative Networks in 2010.

Dr. Tao is the recipient of the IEEE Heinrich Hertz Award for Best Communications Letters in 2013, the IEEE ComSoc Asia-Pacific Outstanding Young Researcher Award in 2009, and the International Conference on Wireless Communications and Signal Processing (WCSP) Best Paper Award in 2012.

Yuan Liu (S'11–M'13) received the B.S. degree from Hunan University of Science and Technology, Xiangtan, China, in 2006, the M.S. degree from Guangdong University of Technology, Guangzhou, China, in 2009, and the Ph.D. degree from Shanghai Jiao Tong University, China, in 2013, all in electronic engineering. Since 2013 fall, he has been with South China University of Technology as an Assistant Professor. His current research interests include green communications, heterogeneous networks, resource allocation and networking, and physical layer security.

Rui Wang received the B.S. degree from Anhui Normal University, Wuhu, China, in 2006, the M.S. degree from Shanghai University, Shanghai, China, in 2009, and the Ph.D degree from Shanghai Jiao Tong University, Shanghai, China, in 2013, all in electronic engineering. Currently he is a post-doc in the Institute of Network Coding, The Chinese University of Hong Kong, Hong Kong. His research interests include digital image processing, cognitive radio and signal processing for wireless cooperative communication.