Secure Beamforming for Full-duplex MIMO Two-way Communication via Untrusted Relaying

Shuangrui Zhao*, Jia Liu†, *Member, IEEE*, Xiaochen Li*,‡, *Student Member, IEEE*,
Yulong Shen*, *Member, IEEE* and Xiaohong Jiang‡, *Senior Member, IEEE*
*School of Computer Science and Technology, Xidian University, China
†Center for Cybersecurity Research and Development, National Institute of Informatics, Japan
‡School of Systems Information Science, Future University Hakodate, Japan
Email: srzhao@stu.xidian.edu.cn, jliu@nii.ac.jp, xiaochenli@ieee.org,
ylshen@mail.xidian.edu.cn, jiang@fun.ac.jp

***Abstract*—Full-duplex (FD) technique is very promising to support enormous data for 5G networks since it can greatly improve the spectrum efficiency. However, the secrecy performance of FD communication systems still remains largely unknown. As an initial step towards this end, this paper studies the physical layer security-based beamforming design in a FD two-way amplify-and-forward relay system, where two source nodes exchange messages with the assistance of an untrusted relay. The untrusted relay is willing to forward the messages and may also work as an eavesdropper to intercept the confidential messages. Our objective is to optimize the source and relay beamformers for maximizing the secrecy sum rate of the two-way communications with imperfect self-interference cancellation. For a specific system configuration, we first derive the expression of secrecy sum rate. By utilizing signal alignment technique and gradient method, we then propose two iterative algorithms to find the optimal source and relay beamforming matrices, respectively. Simulation results demonstrate that when the number of antennas at the relay is appropriate and the interference-to-noise ratio is in a low region the proposed FD scheme significantly improves the secrecy sum rate over conventional schemes.**

***Index Terms*—Physical layer security, full-duplex, beamforming, two-way relay channel.**

I. Introduction

The two-way relay channel (TWRC), as one of the basic elements in decentralized/centralized wireless networks, has gained lots of attention due to its higher spectral efficiency than one-way relaying channel. In two-way relay channel, two source nodes exchange signals via a relay node. The communication takes two phases by employing the principle of physical layer network coding. In the first phase, two source nodes simultaneously send their signals to the relay node. In the second phase, the relay node broadcasts the mixed signal received in the first phase to the two source nodes [1]–[5]. The TWRC is generally assumed to be half-duplex so that each source can cancel the self-interference from its received signal to help decode the desired message from the other source node.

Full-duplex (FD) technique is expected to be a promising solution to support enormous data for 5G networks since it can achieve higher spectral efficiency than conventional half-duplex operation [6]–[9], and thus has attracted considerable attentions from both academic and industrial communities. In FD TWRC, each node can simultaneously transmit and receive signals on the same frequency band. Due to the concurrent transmission and reception, the main challenge of FD TWRC is high self-interference. Different schemes have been investigated in [10]–[12] to suppress self-interference in MIMO FD two-way relay systems. In [10], beamforming for relay and power allocation at sources to maximize the achievable sum rate was studied. To suppress self-interference, a zero forcing constraint and an iterative algorithm was proposed. In [11], to balance the residual self-interference suppression and the desired signal in a two-way FD amplify-and-forward relay system, beamforming matrix at relay under a power constraint was designed based on minimum mean square error method. A joint Alamouti-based rank-two beamforming and artificial noise design for secrecy sum rate maximization in a FD two-way relay system were studied in [12].

In the aforementioned works, all relay nodes are assumed to be friendly and help to keep the confidential messages from eavesdropping. However, from a perspective of cooperative security, confidential messages of the source may be eavesdropped by an untrusted relay. Although the untrusted relay nodes may intentionally be as eavesdroppers, they are still helpful for communication. It has been point out in [13] that, seeking help from the untrusted relay, a higher secrecy rate can be achieved than just treating the untrusted relay as an eavesdropper. This is a very interesting issue to consider an untrusted relay in FD two-way relay system. To the best of our knowledge, research on secure beamforming in MIMO FD two-way untrusted relay systems is missing.

In this paper, we investigate the secure beamforming design problem in MIMO FD two-way relay communication systems where two FD sources exchange confidential messages via a FD untrusted relay. Our objective is to design the beamforming matrices to maximize the achievable secrecy sum rate. We first study the transmission scheme and present the achievable secrecy sum rate of MIMO FD TWRC under a general beamforming configuration. We then formulate the secure source

(Corresponding author: Yulong Shen)

978-1-5386-3920-7/17/$31.00 ©2017 IEEE

and relay beamforming design problems and find solutions of the source and relay beamforming, respectively. Finally, we compare the proposed FD two-way untrusted relaying with two conventional schemes. Numerical results show that when the number of antennas at the relay is appropriate and the interference-to-noise ratio is in a low region the proposed FD scheme significantly improves the secrecy sum rates over conventional schemes.

The rest of the paper is organized as follows. Section II describes the system model. Secure beamformers for FD two-way relay schemes are presented in Section III. Simulation results are presented in Section IV. We conclude this paper in Section V.

Notations: Scalars, vectors and matrices are denoted by lower-case, lower-case bold-face and upper-case bold-face letters, respectively. The trace, inverse, Frobenius norm, conjugate and Hermite of matrix $\mathbf{A}$ are denoted by $\mathrm{Tr}(\mathbf{A})$, $\mathbf{A}^{-1}$, $||\mathbf{A}||$, $\mathbf{A}^*$ and $\mathbf{A}^H$, respectively. $||\mathbf{q}||$ denotes the norm of the vector. $\boldsymbol{\psi}_{max}(\mathbf{A})$ is the eigenvector of $\mathbf{A}$ corresponding to the largest eigenvalue. $\boldsymbol{\psi}_{max}(\mathbf{A}, \mathbf{B})$ is the generalized eigenvector of $(\mathbf{A}, \mathbf{B})$ corresponding to the largest generalized eigenvalue. The identity matrix is denoted by $\mathbf{I}$.

II. System Model

Consider a FD amplify-and-forward two-way relay system consisting of two source nodes S_1 and S_2 and one untrusted relay node R, as shown in Fig. 1. The relay may intentionally eavesdrop the signal but does not make any malicious attack. Each node in the network operates in FD mode. We use N_1, N_2 and N_R to denote the number of antennas at S_1, S_2 and R, respectively. In the tth time slot, let $\mathbf{H}_1^{(t)} \in \mathbb{C}^{N_R \times N_1}$ and $\mathbf{H}_2^{(t)} \in \mathbb{C}^{N_R \times N_2}$ denote the channel matrices from S_1 and S_2 to R, respectively. $\mathbf{G}_1^{(t)} \in \mathbb{C}^{N_1 \times N_R}$ and $\mathbf{G}_2^{(t)} \in \mathbb{C}^{N_2 \times N_R}$ denote the channel matrices from R to S_1 and S_2, respectively. We assume that each node knows its own transmitted signal vectors and perfect channel state information (CSI) between two nodes. In addition, $\mathbf{H}_{11}^{(t)} \in \mathbb{C}^{N_1 \times N_1}$, $\mathbf{H}_{22}^{(t)} \in \mathbb{C}^{N_2 \times N_2}$ and $\mathbf{H}_{RR}^{(t)} \in \mathbb{C}^{N_R \times N_R}$ denote loopback channel matrices at the corresponding nodes. We assume that each node have imperfect CSI on its loopback channel due to channel estimation errors. The loopback channel is modeled as $\mathbf{H}_{ii}^{(t)} = \hat{\mathbf{H}}_{ii}^{(t)} + \boldsymbol{\Delta}_{ii}^{(t)}$ for $i \in \{1, 2, R\}$, where $\hat{\mathbf{H}}_{ii}^{(t)}$ denote the estimation of loopback channel matrices, $\boldsymbol{\Delta}_{ii}^{(t)}$ denote the channel estimation error matrices. After applying the self-interference cancellation scheme, each node cannot perfectly cancel their loopback self-interference. For simplicity, we consider a single data stream for each source node, in time slot t, the transmitted signal at source i is denoted as $s_i^{(t)}$ with covariance $\mathbb{E}(|s_i^{(t)}|^2 = 1)$, and the associated source beamforming vectors are denoted as $\mathbf{q}_i^{(t)} \in \mathbb{C}^{N_i \times 1}$, for $i \in \{1, 2\}$. Meanwhile, we consider the untrusted relay as a beamformer. This case is available in real life. For example, if the sources and the untrusted relay belong to heterogenous network, the nodes will have different security clearances and different levels of access to the information. The zero-mean white Gaussian noise signals at S_1, S_2 and the relay are denoted as $\mathbf{n}_1^{(t)}$, $\mathbf{n}_2^{(t)}$ and $\mathbf{n}_R^{(t)}$ with $\mathbb{E}[\mathbf{n}_1^{(t)} \mathbf{n}_1^{(t)H}] = \sigma_1^2 \mathbf{I}$, $\mathbb{E}[\mathbf{n}_2^{(t)} \mathbf{n}_2^{(t)H}] = \sigma_2^2 \mathbf{I}$ and $\mathbb{E}[\mathbf{n}_R^{(t)} \mathbf{n}_R^{(t)H}] = \sigma_R^2 \mathbf{I}$, respectively.

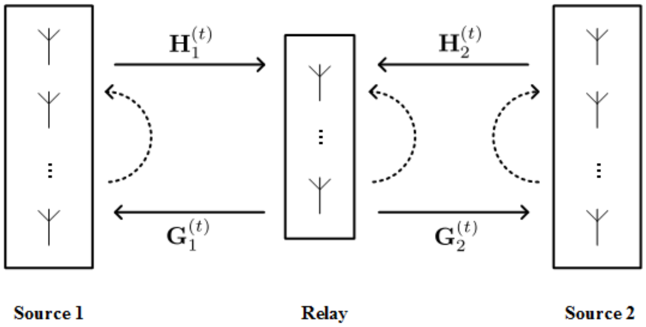


Fig. 1. Full-duplex two-way AF relay system in time slot t.

In time slot 0, the two sources simultaneously transmit signals to the untrusted relay, because the relay does not have any signal before data transmission, the relay does not operate transmission in this time slot. The received signal at the relay can be expressed as

$$\mathbf{y}_R^{(0)} = \mathbf{H}_1^{(0)} \mathbf{q}_1^{(0)} s_1^{(0)} + \mathbf{H}_2^{(0)} \mathbf{q}_2^{(0)} s_2^{(0)} + \mathbf{n}_R^{(0)}. \tag{1}$$

In time slot 1, the untrusted relay amplifies the received signal by multiplying with a relay beamforming matrix $\mathbf{F}^{(1)} \in \mathbb{C}^{N_R \times N_R}$, and then retransmits signal to both S_1 and S_2. At the same time, the two sources nodes transmit their next signals to the relay, FD operation substantially starts from this time slot. The received signals at S_1, S_2 and relay with imperfect loopback self-interference cancellation are respectively given by

$$\begin{aligned} \mathbf{y}_1^{(1)} &= \mathbf{G}_1^{(1)} \mathbf{F}^{(1)} \mathbf{H}_2^{(0)} \mathbf{q}_2^{(0)} s_2^{(0)} + \mathbf{G}_1^{(1)} \mathbf{F}^{(1)} \mathbf{n}_R^{(0)} \\ &\quad + \boldsymbol{\Delta}_{11}^{(1)} \mathbf{q}_1^{(1)} s_1^{(1)} + \mathbf{n}_1^{(1)}, \end{aligned} \tag{2}$$

$$\begin{aligned} \mathbf{y}_2^{(1)} &= \mathbf{G}_2^{(1)} \mathbf{F}^{(1)} \mathbf{H}_1^{(0)} \mathbf{q}_1^{(0)} s_1^{(0)} + \mathbf{G}_2^{(1)} \mathbf{F}^{(1)} \mathbf{n}_R^{(0)} \\ &\quad + \boldsymbol{\Delta}_{22}^{(1)} \mathbf{q}_2^{(1)} s_2^{(1)} + \mathbf{n}_2^{(1)}, \end{aligned} \tag{3}$$

$$\begin{aligned} \mathbf{y}_R^{(1)} &= \mathbf{H}_1^{(1)} \mathbf{q}_1^{(1)} s_1^{(1)} + \mathbf{H}_2^{(1)} \mathbf{q}_2^{(1)} s_2^{(1)} + \mathbf{n}_R^{(1)} + \boldsymbol{\Delta}_{RR}^{(1)} \\ &\quad \mathbf{F}^{(1)} (\mathbf{H}_1^{(0)} \mathbf{q}_1^{(0)} s_1^{(0)} + \mathbf{H}_2^{(0)} \mathbf{q}_2^{(0)} s_2^{(0)} + \mathbf{n}_R^{(0)}). \end{aligned} \tag{4}$$

In this manner, the received signal at untrusted relay in time slot $t-1$ $(t \geq 2)$ is given by

$$\begin{aligned} \mathbf{y}_R^{(t-1)} &= \mathbf{H}_1^{(t-1)} \mathbf{q}_1^{(t-1)} s_1^{(t-1)} + \mathbf{H}_2^{(t-1)} \mathbf{q}_2^{(t-1)} s_2^{(t-1)} \\ &\quad + \mathbf{n}_R^{(t-1)} + \mathbf{W}^{(t-1)}, \end{aligned} \tag{5}$$

where

$$\begin{aligned} \mathbf{W}^{(t-1)} &= \sum_{i=0}^{t-2} \{ \prod_{j=1}^{t-1-j} (\boldsymbol{\Delta}_{RR}^{(t-j)} \mathbf{F}^{(t-j)}) (\mathbf{H}_1^{(i)} \mathbf{q}_1^{(i)} s_1^{(i)} \\ &\quad + \mathbf{H}_2^{(i)} \mathbf{q}_2^{(i)} s_2^{(i)} + \mathbf{n}_R^{(i)}) \}. \end{aligned} \tag{6}$$

In time slot t, the relay broadcasts the received signal, thus, the received signal at source node k are given by

$$\begin{aligned}\mathbf{y}_k^{(t)} &= \mathbf{G}_k^{(t)}\mathbf{F}^{(t)}\mathbf{H}_{\bar{k}}^{(t-1)}\mathbf{q}_{\bar{k}}^{(t-1)}s_{\bar{k}}^{(t-1)} + \mathbf{G}_k^{(t)}\mathbf{F}^{(t)}\mathbf{n}_R^{(t-1)} \\ &\quad + \mathbf{G}_k^{(t)}\mathbf{F}^{(t)}\mathbf{W}^{(t-1)} + \boldsymbol{\Delta}_{kk}^{(t)}\mathbf{q}_k^{(t)}s_k^{(t)} + \mathbf{n}_k^{(t)},\end{aligned} \tag{7}$$

where $k, \bar{k} \in \{1, 2\}$, $k \neq \bar{k}$ and $\mathbf{F}^{(t)} \in \mathbb{C}^{N_R \times N_R}$ is the relay beamforming matrix at time slot t.

The untrusted relay wants to decode the two messages s_1 and s_2 in time slot t-1, the upper bound of the untrusted relay information rate is

$$\begin{aligned}R_e^{(t-1)} &= \log_2(1 + \mathbf{q}_1^{(t-1)^H}\mathbf{H}_1^{(t-1)^H}\mathbf{T}_R^{(t-1)^{-1}}\mathbf{H}_1^{(t-1)}\mathbf{q}_1^{(t-1)} \\ &\quad + \mathbf{q}_2^{(t-1)^H}\mathbf{H}_2^{(t-1)^H}\mathbf{T}_R^{(t-1)^{-1}}\mathbf{H}_2^{(t-1)}\mathbf{q}_2^{(t-1)}),\end{aligned} \tag{8}$$

where

$$\mathbf{T}_R^{(t-1)} = \mathbf{W}^{(t-1)}\mathbf{W}^{(t-1)^H} + \sigma_R^2\mathbf{I}. \tag{9}$$

Considering imperfect loopback self-interference cancelation, the achievable information rate from node k to $\bar{k}$ ($k, \bar{k} \in \{1, 2\}$, $k \neq \bar{k}$) in time slot t can be expressed as

$$\begin{aligned}R_{\bar{k}}^{(t)} &= \log_2(1 + \mathbf{q}_k^{(t-1)^H}\mathbf{H}_k^{(t-1)^H}\mathbf{F}^{(t)^H}\mathbf{G}_{\bar{k}}^{(t)^H}\mathbf{T}_{\bar{k}}^{(t)^{-1}} \\ &\quad \mathbf{G}_{\bar{k}}^{(t)}\mathbf{F}^{(t)}\mathbf{H}_k^{(t-1)}\mathbf{q}_k^{(t-1)}),\end{aligned} \tag{10}$$

where

$$\begin{aligned}\mathbf{T}_{\bar{k}}^{(t)} &= \mathbf{G}_{\bar{k}}^{(t)}\mathbf{F}^{(t)}\mathbf{F}^{(t)^H}\mathbf{G}_{\bar{k}}^{(t)^H} + \mathbf{G}_{\bar{k}}^{(t)}\mathbf{F}^{(t)}\mathbf{W}^{(t-1)} \\ &\quad \mathbf{W}^{(t-1)^H}\mathbf{F}^{(t)^H}\mathbf{G}_{\bar{k}}^{(t)^H} + \boldsymbol{\Delta}_{kk}^{(t)}\mathbf{q}_k^{(t)}\mathbf{q}_k^{(t)^H}\boldsymbol{\Delta}_{kk}^{(t)^H} \\ &\quad + \sigma_k^2\mathbf{I}.\end{aligned} \tag{11}$$

According to [5], by combining (8) and (10), the achievable secrecy sum rate of the FD two-way relay system is thus given by

$$R_s^{(t)} = \mathbb{E}[R_k^{(t)} + R_{\bar{k}}^{(t)} - R_e^{(t-1)}]^+. \tag{12}$$

III. BEAMFORMING DESIGN

In the considered model, the two sources simultaneously transmit their signals to relay in time slot t-1, the untrusted relay broadcasts its received signal in time slot t. The CSI is different between time slot t-1 and time slot t. There are two problems in message transmission process, on one hand, we should protect the confidential messages from leaking to the untrusted relay nodes in time slot t-1, on the other hand, we should maximize the achievable secrecy rate in time slot t. The objective of this section is to solve the aforementioned two problems by designing the source beamforming matrices $\mathbf{q}_1^{(t-1)}$, $\mathbf{q}_2^{(t-1)}$ and relay beamforming matrix $\mathbf{F}^{(t)}$. We propose algorithms for the design of source beamforming and relay beamforming, respectively.

A. Source beamforming vector in time slot t-1

We first introduce the signal alignment technique before presenting the problem formulations of source beamforming design. The signal alignment technique was proposed in [14] to achieve the degrees of freedom of the MIMO Y channel which is generalized two-way relay channel with three users. The key idea of this technique is to align the two signal vectors transmitted from two users at the receiver of the relay to jointly perform detection and encoding for network coding. The two source beamforming vectors are chosen to make the two received signals in relay node align in the same direction. The signal vectors after aligning are helpful to keep confidential messages from eavesdropping.

In time slot t-1, the upper bound of the untrusted relay information rate is (8). According to signal alignment technique, to maximize the secrecy information rate in time slot t-1 the problem of source beamforming matrices design in this time slot is formulated as (13) shown at the bottom of the page.

We optimize the source beamforming vectors $\mathbf{q}_1^{(t-1)}$ and $\mathbf{q}_2^{(t-1)}$ in an alternating manner. Given $\mathbf{q}_{\bar{k}}^{(t-1)}$, we can rewrite the objective function (13a) as a particular Rayleigh quotient problem, according to [15], the optimum of the Rayleigh quotient problem is attained by the eigenvector corresponding to the largest generalized eigenvalue. Thus, the optimal beamforming $\mathbf{q}_k^{(t-1)}$ of (13) is the generalized eigenvector of the pair $(\mathbf{I} + P_k^{(t-1)}\mathbf{H}_k^{(t-1)^H}\mathbf{H}_k^{(t-1)}, \mathbf{I} + (\mathbf{q}_{\bar{k}}^{(t-1)^H}\mathbf{H}_{\bar{k}}^{(t-1)^H}\mathbf{H}_{\bar{k}}^{(t-1)}\mathbf{q}_{\bar{k}}^{(t-1)})\mathbf{I} + P_k^{(t-1)}\mathbf{H}_k^{(t-1)^H}\mathbf{H}_k^{(t-1)})$ corresponding to the largest generalized eigenvalue. We obtain (14) shown at the bottom of the page. Here we omit the details. Formally, we present the method in Algorithm 1. Note that the algorithm always converges because the source power is limited and the (13a) is non-decreasing in every iteration.

$$\begin{aligned}\max_{\mathbf{A}} \quad & \log_2(1 + \mathbf{q}_1^{(t-1)^H}\mathbf{H}_1^{(t-1)^H}\mathbf{H}_1^{(t-1)}\mathbf{q}_1^{(t-1)}) + \log_2(1 + \mathbf{q}_2^{(t-1)^H}\mathbf{H}_2^{(t-1)^H}\mathbf{H}_2^{(t-1)}\mathbf{q}_2^{(t-1)}) \\ & - \log_2(1 + \mathbf{q}_1^{(t-1)^H}\mathbf{H}_1^{(t-1)^H}\mathbf{H}_1^{(t-1)}\mathbf{q}_1^{(t-1)} + \mathbf{q}_2^{(t-1)^H}\mathbf{H}_2^{(t-1)^H}\mathbf{H}_2^{(t-1)}\mathbf{q}_2^{(t-1)})\end{aligned} \tag{13a}$$

$$\text{s.t.} \quad ||\mathbf{q}_k^{(t-1)}|| \leq P_k^{(t-1)} \tag{13b}$$

$$\mathbf{q}_k^{(t-1)} = \frac{\sqrt{P_k^{(t-1)}}\boldsymbol{\psi}_{max}(\mathbf{I} + P_k^{(t-1)}\mathbf{H}_k^{(t-1)^H}\mathbf{H}_k^{(t-1)}, \mathbf{I} + (\mathbf{q}_{\bar{k}}^{(t-1)^H}\mathbf{H}_{\bar{k}}^{(t-1)^H}\mathbf{H}_{\bar{k}}^{(t-1)}\mathbf{q}_{\bar{k}}^{(t-1)})\mathbf{I} + P_k^{(t-1)}\mathbf{H}_k^{(t-1)^H}\mathbf{H}_k^{(t-1)})}{||\boldsymbol{\psi}_{max}(\mathbf{I} + P_k^{(t-1)}\mathbf{H}_k^{(t-1)^H}\mathbf{H}_k^{(t-1)}, \mathbf{I} + (\mathbf{q}_{\bar{k}}^{(t-1)^H}\mathbf{H}_{\bar{k}}^{(t-1)^H}\mathbf{H}_{\bar{k}}^{(t-1)}\mathbf{q}_{\bar{k}}^{(t-1)})\mathbf{I} + P_k^{(t-1)}\mathbf{H}_k^{(t-1)^H}\mathbf{H}_k^{(t-1)})||} \tag{14}$$

Algorithm 1 algorithm for source beamforming design

```
1:Initialize $\mathbf{q}_1^{(t-1)}$ and $\mathbf{q}_2^{(t-1)}$.
2:Repeat
  (a) Optimize $\mathbf{q}_1^{(t-1)}$ given $\mathbf{q}_2^{(t-1)}$ according to (14).
  (b) Optimize $\mathbf{q}_2^{(t-1)}$ given $\mathbf{q}_1^{(t-1)}$ according to (14) by swapping $\mathbf{q}_1^{(t-1)}$ and $\mathbf{q}_2^{(t-1)}$.
3:Until the (13a) does not increase.
```

B. Relay beamforming vector in time slot t

Note that the relay beamforming matrix $\mathbf{F}^{(t)}$ only influences the information rate $R_1^{(t)}$ and $R_2^{(t)}$. Therefore, the optimal $\mathbf{F}^{(t)}$ that maximizes the secrecy sum rate (12) is the same as that maximizes the information sum rate $R_1^{(t)} + R_2^{(t)}$. Due to the rank-one precoding at each source node, we have the equivalent channel $\mathbf{H}_k^{(t-1)}\mathbf{q}_k^{(t-1)}$ from source node k to relay.

In time slot t, the optimal relay beamforming matrix $\mathbf{F}^{(t)}$ that maximizes the secrecy sum rate has the following structure:

$$\mathbf{F}^{(t)} = \mathbf{V}^{(t)}\mathbf{A}^{(t)}{\mathbf{U}^{(t)}}^H, \tag{15}$$

where $\mathbf{A}^{(t)}$ is an unknown matrix, $\mathbf{V}^{(t)}$ and $\mathbf{U}^{(t)}$ are orthonormal matrices depend on the following two QR decompositions:

$$\begin{bmatrix}{\mathbf{G}_1^{(t)}}^H & {\mathbf{G}_2^{(t)}}^H\end{bmatrix} = \mathbf{V}^{(t)}\mathbf{G_0}, \tag{16}$$

$$\begin{bmatrix}\mathbf{H}_1^{(t-1)}\mathbf{q}_1^{(t-1)} & \mathbf{H}_2^{(t-1)}\mathbf{q}_2^{(t-1)}\end{bmatrix} = \mathbf{U}^{(t)}\mathbf{H_0}. \tag{17}$$

where $\mathbf{G_0}$ and $\mathbf{H_0}$ are upper triangle matrices.

It is seen from (15) that number of unknown elements in $\mathbf{F}^{(t)}$ is reduced from N_R^2 to $2\min\{N_R, N_1 + N_2\}$. (15) greatly reduces the computational complexity of the relay beamforming design. Given $\mathbf{q}_1^{(t-1)}$ and $\mathbf{q}_2^{(t-1)}$, we can use the gradient method to search $\mathbf{A}^{(t)}$. The problem of relay beamforming matrices design in time slot t is formulated as (18) shown at the bottom of the page. The logarithmic barrier function $J(\mathbf{A}^{(t)}, \lambda)$ is defined as (19) and the gradient of $J(\mathbf{A}^{(t)}, \lambda)$ with respect to $\mathbf{A}^{(t)}$ is formulated as (20), respectively. With this gradient, we can use gradient descent method to search $\mathbf{A}^{(t)}$. We present the method in Algorithm 2.

Algorithm 2 algorithm for relay beamforming design

```
1:Initialize $\mathbf{A}^{(t)}$.
2:Repeat
  Optimize $\mathbf{A}^{(t)}$ given $\mathbf{q}_1^{(t-1)}$ and $\mathbf{q}_2^{(t-1)}$ based on gradient method.
3:Until the achievable secrecy sum rate does not increase.
```

IV. SIMULATION RESULTS

In this section, the performance of the proposed scheme is validated by simulation results. In the simulation, all the channel matrices $\mathbf{H}_1^{(t)}$, $\mathbf{H}_2^{(t)}$, $\mathbf{G}_1^{(t)}$, $\mathbf{G}_2^{(t)}$ are independent and identically distributed complex Gaussian random variables with zero mean and unit variance. The channel estimation error matrices $\mathbf{\Delta}_{ii}^{(t)}$ for $i \in \{1, 2, R\}$ are independent and identically distributed complex Gaussian random variables

$$\min_{\mathbf{A}} \quad -R_s^{(t)} \tag{18a}$$

$$\begin{aligned}\text{s.t.} \quad & \mathrm{Tr}(\mathbf{A}^{(t)}{\mathbf{U}^{(t)}}^H\mathbf{H}_1^{(t-1)}\mathbf{q}_1^{(t-1)}{\mathbf{q}_1^{(t-1)}}^H{\mathbf{H}_1^{(t-1)}}^H\mathbf{U}^{(t)}{\mathbf{A}^{(t)}}^H + \mathbf{A}^{(t)}{\mathbf{U}^{(t)}}^H\mathbf{H}_2^{(t-1)}\mathbf{q}_2^{(t-1)}{\mathbf{q}_2^{(t-1)}}^H \\ & {\mathbf{H}_2^{(t-1)}}^H\mathbf{U}^{(t)}{\mathbf{A}^{(t)}}^H + \mathbf{A}^{(t)}{\mathbf{U}^{(t)}}^H\mathbf{W}^{(t-1)}{\mathbf{W}^{(t-1)}}^H\mathbf{U}^{(t)}{\mathbf{A}^{(t)}}^H + \mathbf{A}^{(t)}{\mathbf{A}^{(t)}}^H) \leq P_R^{(t)}\end{aligned} \tag{18b}$$

$$\begin{aligned}J(\mathbf{A}^{(t)}, \lambda) = & -R_s^{(t)} - \lambda\ \ln\Big(P_R^{(t)} - \mathrm{Tr}(\mathbf{A}^{(t)}{\mathbf{U}^{(t)}}^H\mathbf{H}_1^{(t-1)}\mathbf{q}_1^{(t-1)}{\mathbf{q}_1^{(t-1)}}^H{\mathbf{H}_1^{(t-1)}}^H\mathbf{U}^{(t)}{\mathbf{A}^{(t)}}^H + \mathbf{A}^{(t)}{\mathbf{U}^{(t)}}^H\mathbf{H}_2^{(t-1)}\mathbf{q}_2^{(t-1)} \\ & {\mathbf{q}_2^{(t-1)}}^H{\mathbf{H}_2^{(t-1)}}^H\mathbf{U}^{(t)}{\mathbf{A}^{(t)}}^H + \mathbf{A}^{(t)}{\mathbf{U}^{(t)}}^H\mathbf{W}^{(t-1)}{\mathbf{W}^{(t-1)}}^H\mathbf{U}^{(t)}{\mathbf{A}^{(t)}}^H + \mathbf{A}^{(t)}{\mathbf{A}^{(t)}}^H)\Big)\end{aligned} \tag{19}$$

$$\frac{\partial J(\mathbf{A}^{(t)}, \lambda)}{\partial {\mathbf{A}^{(t)}}^*} = -\sum_{k\in\{1,2\}} \log_2 e \frac{J_1\mathbf{U}^{(t)} - J_1J_2\mathbf{U}^{(t)} - J_1J_2\mathbf{W}^{(t-1)}{\mathbf{W}^{(t-1)}}^H\mathbf{U}^{(t)}}{J_3} + \frac{\lambda(J_4 + J_5)}{P_R^{(t)} - \mathrm{Tr}\Big((J_4 + J_5){\mathbf{A}^{(t)}}^H\Big)} \tag{20}$$

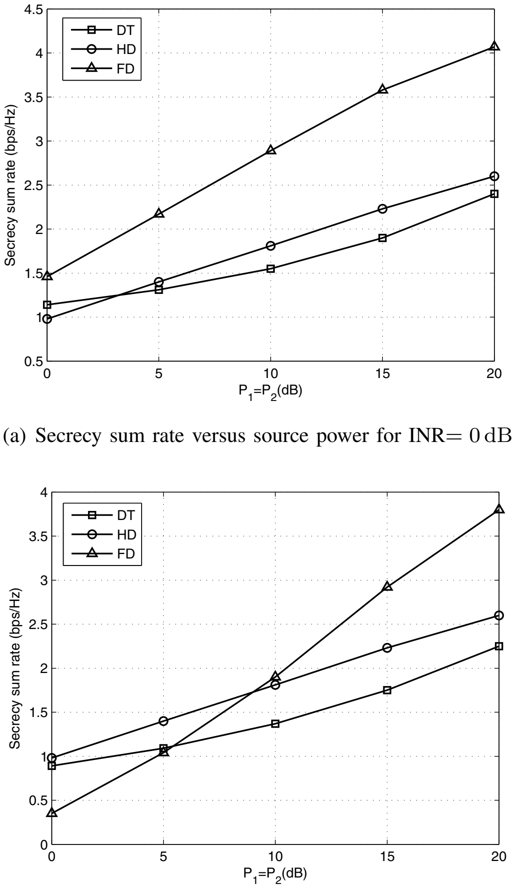
$$J_1 = {\mathbf{V}^{(t)}}^H{\mathbf{G}_{\overline{k}}^{(t)}}^H{\mathbf{T}_{\overline{k}}^{(t)}}^{-1}\mathbf{G}_{\overline{k}}^{(t)}\mathbf{F}^{(t)}\mathbf{H}_k^{(t-1)}\mathbf{q}_k^{(t-1)}{\mathbf{q}_k^{(t-1)}}^H{\mathbf{H}_k^{(t-1)}}^H \tag{21}$$

$$J_2 = {\mathbf{F}^{(t)}}^H{\mathbf{G}_{\overline{k}}^{(t)}}^H{\mathbf{T}_{\overline{k}}^{(t)}}^{-1}\mathbf{G}_{\overline{k}}^{(t)}\mathbf{F}^{(t)} \tag{22}$$

$$J_3 = 2(1 + {\mathbf{q}_k^{(t-1)}}^H{\mathbf{H}_k^{(t-1)}}^H{\mathbf{F}^{(t)}}^H{\mathbf{G}_{\overline{k}}^{(t)}}^H{\mathbf{T}_{\overline{k}}^{(t)}}^{-1}\mathbf{G}_{\overline{k}}^{(t)}\mathbf{F}^{(t)}\mathbf{H}_k^{(t-1)}\mathbf{q}_k^{(t-1)}) \tag{23}$$

$$J_4 = \mathbf{A}^{(t)}{\mathbf{U}^{(t)}}^H\mathbf{W}^{(t-1)}{\mathbf{W}^{(t-1)}}^H\mathbf{U}^{(t)} + \mathbf{A}^{(t)} \tag{24}$$

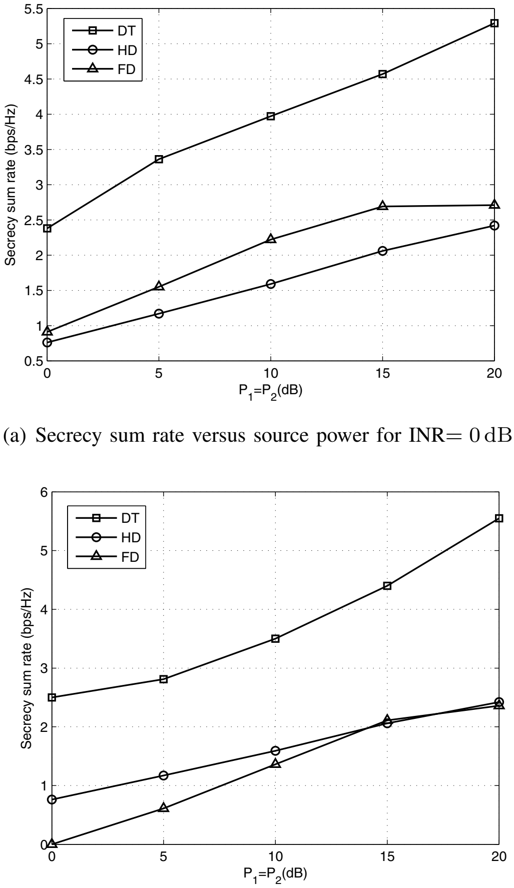
$$J_5 = \mathbf{A}^{(t)}{\mathbf{U}^{(t)}}^H\mathbf{H}_1^{(t-1)}\mathbf{q}_1^{(t-1)}{\mathbf{q}_1^{(t-1)}}^H{\mathbf{H}_1^{(t-1)}}^H\mathbf{U}^{(t)} + \mathbf{A}^{(t)}{\mathbf{U}^{(t)}}^H\mathbf{H}_2^{(t-1)}\mathbf{q}_2^{(t-1)}{\mathbf{q}_2^{(t-1)}}^H{\mathbf{H}_2^{(t-1)}}^H\mathbf{U}^{(t)} \tag{25}$$



(a) Secrecy sum rate versus source power for INR$=0\,\mathrm{dB}$.

(b) Secrecy sum rate versus source power for INR$=5\,\mathrm{dB}$.

Fig. 2. Comparison of three schemes when $N_1=2$, $N_2=2$, $N_R=3$ and $P_R=60\,\mathrm{dB}$.



(a) Secrecy sum rate versus source power for INR$=0\,\mathrm{dB}$.

(b) Secrecy sum rate versus source power for INR$=5\,\mathrm{dB}$.

Fig. 3. Comparison of three schemes when $N_1=3$, $N_2=3$, $N_R=2$ and $P_R=40\,\mathrm{dB}$.

with zero mean and variance σ_{ii}^2. For simplicity, the variances of Gaussian noise at each node are set to be as $\sigma_1^2=\sigma_2^2=\sigma_R^2=\sigma_n^2$, the variances of channel estimation error are set to be as $\sigma_{11}^2=\sigma_{22}^2=\sigma_{RR}^2=\sigma_e^2$. Interference-to-noise ratio (INR) is defined as σ_e^2/σ_n^2. We assume that the power of each node is constant all the time and set to be as P_1, P_2, P_R, respectively. We present the secrecy sum rate comparison of our proposed full-duplex secure beamforming scheme, direct transmission (DT) beamforming scheme and conventional half-duplex scheme. The conventional half-duplex (HD) scheme takes two-phases and doesn't suffer from self-interference. Unlike the proposed scheme and the conventional half-duplex scheme, the direct transmission scheme treats the untrusted relay as an eavesdropper.

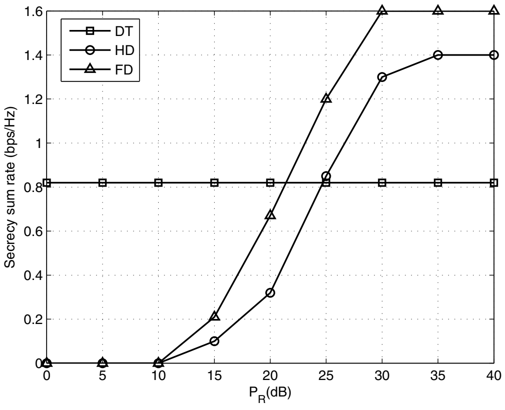


Fig. 4. Comparison of the schemes with varying relay power when $N_1=2$, $N_2=2$, $N_R=3$, INR$=0\,\mathrm{dB}$ and $P_1=P_2=15\,\mathrm{dB}$.

Fig. 2 shows the secrecy sum rate of three schemes versus source power for different INR values when $N_1=2$, $N_2=2$, $N_R=3$ and $P_R=60\,\mathrm{dB}$. As source power increases, the secrecy sum rate of three schemes increases. When INR$=0\,\mathrm{dB}$, we find that the proposed scheme is the best and the direct transmission scheme is better than the half-duplex scheme. When INR$=5\,\mathrm{dB}$, the proposed scheme is much better than the other two schemes when source power is high. From Fig. 2, we find that we can seek cooperation with the untrusted relay when the number of antennas at the relay is appropriate. It will achieve a higher secrecy sum rate than just treat the untrusted relay as pure eavesdropper.

Fig. 3 shows the secrecy sum rate of three schemes versus source power for different INR values when $N_1 = 3$, $N_2 = 3$, $N_R = 2$ and $P_R = 40\,\mathrm{dB}$. We can see that the maximum secrecy sum rate of direct transmission scheme tends to infinity with the increase of the source powers. In this case, the proposed scheme is better than half-duplex scheme when INR$=\ 0\,\mathrm{dB}$. Compared to Fig. 2, we note that reducing the number of antennas at the relay obviously increase the performance of direct transmission scheme. When the number of antenna the untrusted relay is too small, we'd better treat the untrusted relay as an eavesdropper.

Fig. 4 shows the secrecy sum rate of three schemes with varying relay power when $N_1 = 2$, $N_2 = 2$, $N_R = 3$, INR$=$ $0\,\mathrm{dB}$ and $P_1 = P_2 = 15\,\mathrm{dB}$. Note that the relay acts as an eavesdropper and does not make any help. Therefore, the secrecy sum rate of direct transmission scheme constant with the relay power increases. For proposed FD scheme, as the relay power increases, the secrecy sum rate rises from zero up to 1.6 bps/HZ. When the relay power is high, the proposed scheme is better than the other two schemes. From Fig. 4, we can see the importance of relaying power for the proposed scheme and half-duplex scheme.

V. Conclusion

This paper investigated secure beamforming design in a MIMO FD two-way amplify-and-forward relay system where the two source nodes exchange messages via an untrusted relay. We analyzed the secrecy sum rate of the system. For efficiently preventing the untrusted relay from eavesdropping confidential messages, we proposed two algorithms to design the secure source and relay beamforming matrices at each time slot. Simulation results demonstrate that the proposed FD scheme can improve the secrecy rate when the number of antennas at the relay is appropriate and the INR is in a low region.

Acknowledgment

This work was supported in part by the Natural Science Foundation of China (NSFC) under Grant U1536202, Grant 61373173, and Grant 61571352; in part by the Project of Cyber Security Establishment with Inter-University Cooperation; and in part by the Secom Science and Technology Foundation.

References

[1] B. Rankov and A. Wittneben, "Achievable rate regions for the two-way relay channel," in *2006 IEEE International Symposium on Information Theory*, July 2006.

[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 Journal on Selected Areas in Communications*, vol. 27, no. 5, pp. 699–712, June 2009.

[3] Q. Li, S. H. Ting, A. Pandharipande, and Y. Han, "Adaptive two-way relaying and outage analysis," *IEEE Transactions on Wireless Communications*, vol. 8, no. 6, pp. 3288–3299, June 2009.

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

[5] J. Mo, M. Tao, Y. Liu, and R. Wang, "Secure beamforming for MIMO two-way communications with an untrusted relay," *IEEE Transactions on Signal Processing*, vol. 62, no. 9, pp. 2185–2199, May 2014.

[6] D. W. Bliss, P. A. Parker, and A. R. Margetts, "Simultaneous transmission and reception for improved wireless network performance," in *2007 IEEE/SP 14th Workshop on Statistical Signal Processing*, Aug 2007.

[7] Z. Zhang, X. Chai, K. Long, A. V. Vasilakos, and L. Hanzo, "Full duplex techniques for 5G networks: self-interference cancellation, protocol design, and relay selection," *IEEE Communications Magazine*, vol. 53, no. 5, pp. 128–137, 2015.

[8] N. H. Mahmood, G. Berardinelli, F. M. Tavares, and P. Mogensen, "On the potential of full duplex communication in 5G small cell networks," in *IEEE 81st Vehicular Technology Conference (VTC Spring)*, 2015, pp. 1–5.

[9] X. Zhang, W. Cheng, and H. Zhang, "Full-duplex transmission in PHY and MAC layers for 5G mobile wireless networks," *IEEE Wireless Communications Magazine*, vol. 22, no. 5, pp. 112–121, 2015.

[10] G. Zheng, "Joint beamforming optimization and power control for full-duplex MIMO two-way relay channel," *IEEE Transactions on Signal Processing*, vol. 63, no. 3, pp. 555–566, Feb 2015.

[11] Y. Shim, W. Choi, and H. Park, "Beamforming design for full-duplex two-way amplify-and-forward MIMO relay," *IEEE Transactions on Wireless Communications*, vol. 15, no. 10, pp. 6705–6715, Oct 2016.

[12] Q. Li, W. K. Ma, and D. Han, "Sum secrecy rate maximization for full-duplex two-way relay networks using alamouti-based rank-two beamforming," *IEEE Journal of Selected Topics in Signal Processing*, vol. 10, no. 8, pp. 1359–1374, Dec 2016.

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

[14] N. Lee, J. B. Lim, and J. Chun, "Degrees of freedom of the MIMO Y channel: Signal space alignment for network coding," *IEEE Transactions on Information Theory*, vol. 56, no. 7, pp. 3332–3342, July 2010.

[15] A. Khisti and G. W. Wornell, "Secure transmission with multiple antennas I: The MISOME wiretap channel," *IEEE Transactions on Information Theory*, vol. 56, no. 7, pp. 3088–3104, July 2010.