Secure Beamforming with Artificial Noise for Two-way Relay Networks

Dandan Li[1], Ke Xiong[2,1], Guanyao Du[1] and Zhengding Qiu[1]
[1] School of Computer and Information Technology, Beijing Jiaotong University
Beijing, China, 100044
[e-mail: dandanli.iis@gmail.com, 08112076@bjtu.edu.cn, zdqiu@bjtu.edu.cn]
[2] State Key Laboratory of Rail Traffic Control and Safety,
Beijing Jiaotong University, Beijing, China,100044
[e-mail: kxiong@bjtu.edu.cn]
*Corresponding author: Ke Xiong

Received July 19, 2012; revised March 7, 2013; revised April 25, 2013; accepted May 22, 2013; published June 26, 2013

Abstract

This paper studies the problem of secure information exchange between two sources via multiple relays in the presence of an eavesdropper. To this end, we propose a relay beamforming scheme, i.e., relay beamforming with artificial noise (RBwA), where the relay beamforming vector and the artificial noise vector are jointly designed to maintain the received signal-to-interference-ratio (SINR) at the two sources over a predefined Quality of Service (QoS) threshold while limiting the received SINR at the eavesdropper under a predefined secure threshold. For comparsion, the relay beamforming without artificial noise (RBoA) is also considered. We formulate two optimization problems for the two schemes, where our goal is to seek the optimal beamforming vector to minimize the total power consumed by relay nodes such that the secrecy of the information exchange between the two sources can be protected. Since both optimization problems are nonconvex, we solve them by semidefinite program (SDP) relaxation theory. Simulation results show that, via beamforming design, physical layer secrecy of two-way relay networks can be greatly improved and our proposed RBwA outperforms the RBoA in terms of both low power consumption and low infeasibility rate.

Keywords: relay beamforming, artificial noise, two-way relay, physical layer secrecy, optimal design

This work was supported by the State Key Laboratory of Rail Traffic Control and Safety under Grant No. RCS2012ZT008, Beijing Jiaotong University, by the National Nature Science Foundation of China under Grants No. 61201203 and also by the Fundamental Research Funds for the Central Universities under Grant No. 2012JBM030.

http://dx.doi.org/10.3837/tiis.2013.06.004

1. Introduction

Because of the broadcast nature of wireless medium, secrecy, especially the secure transmission in the presence of eavesdroppers, has become a fundamental problem in wireless networks. Up to now, there are two main strategies to improve the secrecy of communication systems. One is the data encryption strategy at the network layer/application layer of networks, and the other is the signal encryption strategy at the physical layer. In this paper, we focus on the encryption at the physical layer, which is also referred to as the physical layer secrecy. As for physical layer secrecy, it can be traced back to Wyner's work in [1], which provided some theoretical results of establishing security communications.

Recently, physical layer secrecy has attracted growing attentions, especially for multi-antenna systems [2][3]. With multi-antenna, the eavesdropper's interception can be degraded by the spatial degree of freedom achieved by beamforming techniques. However, due to energy or size limitations of mobile devices, equpping multiple antennas may not always be available in practical systems. Fortunately, through the cooperation among multiple single-antenna nodes, a virtual multi-antenna system can be constructed. By doing so, the system with multiple single-antenna nodes are also able to enjoy the benefits of multiple-antenna architecture. Some works recently have reported the secrecy with relay beamforming design, e.g., see [4][5][6]. In [4] and [5], the secrecy enhancement for two-hop relay networks were discussed, where Amplify-and-Forward (AF) and Decode-and-Forward (DF) relaying protocols deployed at relay nodes. In [6], the secure relay beamforming design was investigated, where jamming approach was applied for two-hop relay systems.

However, so far, most of existing works on secure relay beamforming have only been done for one-way relay networks, see e.g., [4][5][6]. To the best of our knowledge, only the work in [7] studied the secure relay beamforming design for two-way relay networks. Thus, in this paper, we also fucus on the the secure relay beamforming design for two-way relay networks.

Compared with the works in [7], the main differences of our work can be listed as follows: *Firstly*, the authors in [7] aimed to achieve the maximum secrecy sum rate by relay beamforming vector design under total power constraint, while our goal is to optimally design relay beamforming vectors to minimize the total transmission power consumed by all relay nodes while satisfying the secrecy requirement of the system. *Secondly*, with the assumption that the eavesdropper's Channel State Information (CSI) is known at the transmitters, the authors in [7] designed the relay beamforming vector in the null space of the eavesdropper's channel to eliminate the information leakage to the eavesdropper. In their design, they thought that the information can not be overheard by the eavesdropper only when no useful signal is received at the eavesdropper. In our opinion, these assumptions may be too strict for secure transmissions, because when the eavesdropper can not correctly decode the overheared information the transmission also can be considered to be secure. To keep the eavesdropper not correctly decoding the overheared, it only requires the received Signal-to-Interference-Noise (SINR) at the eavesdropper below a certain threshold. With this consideration, in this paper, we design the relay beamforming vector under such a security constraint, i.e., the received SINR at each source is kept higher than a predefined Quality-of Service (QoS) threshold while the received SINR at the eavesdropper is kept lower than a predefined secrecy threshold. *Thirdly*, like most existing works on artificial noise based beamforming design, in [7], it assumed that no eavesdropper's CSI is known by transmitters. Under such assumption, in their work, the artificial noise was just kept isotropic and its

spatiality was not fully utilized. Very recently, some works have began to utilize the spatiality of artificial noise, e.g., see [8][9], and showed that one may utilize the eavesdropper's CSI to steer the artificial noise towards eavesdropper's direction for more efficient secure beamforming design. Hence, in our work, we utilize the eavesdropper's CSI and jointly design the optimized artificial noise vector and the beamforming vector to achieve the minimal total power consumption of the relay nodes.

The rest of this paper are organized as follows. Section II describes the system model and then present two relay beamforming methods, i.e., Relay Beamforming without Arificial noise (RBoA) and Relay Beamforming with Arificial noise (RBwA). Section III formulates the optimization problems for both RBoA and RBwA, where our goal is to design energy-minimized relay beamforming vectors such that the received SINR of each source is kept higher than a predefined QoS threshold while the received SINR of the eavesdropper is kept lower than a predefined security threshold. Since the formulated problems are nonconvex, in Section III, we solve them by using semidefinite program (SDP) relaxation theory. In Section IV, we present some simulation results to demonstrate the effectiveness of our proposed schemes and show that RBwA outperforms RBoA in terms of both low power consumption and low infeasibility rate. Finally, Section V summarizes this paper.

2. System Model

Consider a two-way relay system as shown in **Fig. 1**, where two sources, A and B, exchange their information via K relay nodes in the presence of an eavesdropper E. It is assumed that all nodes are equipped with single antenna and all channel matrices of the links are known to the transceivers. We assume that the eavesdroppers' CSI can be obtained when the eavesdroppers are active in the network [10], and this is applicable particularly in networks combining multicast and unicast transmissions, where terminals play dual roles as legitimate receivers for some signals and eavesdroppers for others. Furthermore, half-duplex constraint is cosidered, so that two phases, i.e., the Multiple Access (MA) phase and the Broadcast (BC) phase, are involved to complete a round of information exchange between A and B. In the MA phase, A and B send their signal to the K relays simultaneously, and in the BC phase, each relay amplifies the received signals and then broadcasts them to A and B simultaneously. Since A and B know their own transmitted signals, the self-interference is able to be canceled and the desired information can be extracted from the received mixed signals. However, since the eavesdropper E resides in the system, the information exchange between A and B may be overheard by E in both the MA phase and BC phase, resulting in the insecurity of the two-way relay transmissions.

We assume that there is no direct link between A and B. Therefore, to keep the secrecy of the two-way relay transmission, the relay nodes should: 1) help the information exchange between A and B, and 2) prevent the information leakage to the eavesdropper to enhance security. In order to meet these two goals simulatenously, we adopt the received SINR as a measurement of QoS and secrecy, where the received SINR at each source node should be kept higher than a predefined threshold to keep the QoS of the information exchange between the two sources, and the received SINR at E should be limited below a predefined security threshold to avoid the information overhearing by the eavesdropper.

Let $\mathbf{h}_{\mathrm{R}}=[h_{\mathrm{R}_1},h_{\mathrm{R}_2},...h_{\mathrm{R}_K}]$ and $\mathbf{f}_{\mathrm{R}}=[f_{\mathrm{R}_1},f_{\mathrm{R}_2},...f_{\mathrm{R}_K}]$ and $\mathbf{g}_{\mathrm{R}}=[g_{\mathrm{R}_1},g_{\mathrm{R}_2},...g_{\mathrm{R}_K}]$ denote the quasi-stationary flat-fading channel coefficient vectors between A and the relay nodes, between B and the relay nodes and between E and the relay nodes, respectively. Denote the channel coefficients between A and E and B and E with h_{E} and f_{E}, respectively. To keep the

secrecy for the two-way relay transmissions, we propose two beamforming schemes, i.e., RBoA and RBwA as decribed in the following two subsections.

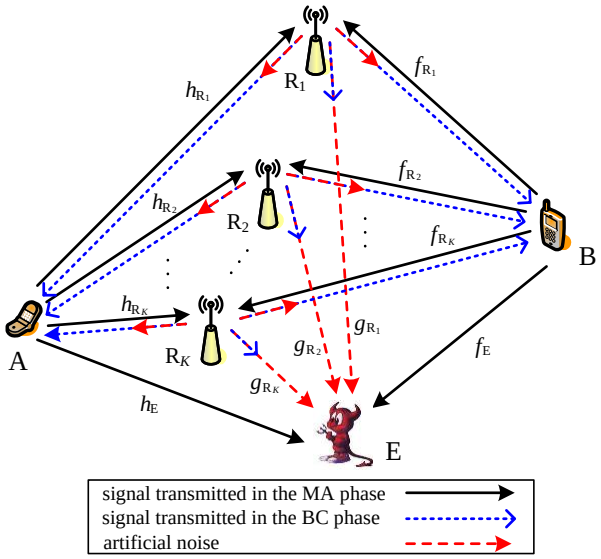


Fig. 1. System model and the illustration of secure relay beamforming with artificial noise

2.1. RBoA

In this subsection, we describe the RBoA scheme. In the MA phase, A and B send their information to the K relays, simultaneously. Thus, the received signals at the relays and at E can be respectively given by

$$\mathbf{y}_{\mathrm{R}} = \sqrt{P_{\mathrm{A}}}\mathbf{h}_{\mathrm{R}} x_{\mathrm{A}} + \sqrt{P_{\mathrm{B}}}\mathbf{f}_{\mathrm{R}} x_{\mathrm{B}} + \mathbf{n}_{\mathrm{R}} \ , \tag{1}$$

$$y_{\mathrm{E_{MA}}} = \sqrt{P_{\mathrm{A}}} h_{\mathrm{E}} x_{\mathrm{A}} + \sqrt{P_{\mathrm{B}}} f_{\mathrm{E}} x_{\mathrm{B}} + n_{\mathrm{E_{MA}}} \ , \tag{2}$$

where $\mathbf{y}_{\mathrm{R}}$ is a $K\times 1$ complex vector of the received signal at the K relays and y_{E} is the received signal at E in the MA phase. Let P_{A} and P_{B} denote the transmit power of A and B, respectively. $\mathbf{n}_{\mathrm{R}}$ is a $K\times 1$ complex vector of Additive White Gaussian Noise (AWGN) at the relays and $n_{\mathrm{E_{MA}}}$ is the AWGN at E in the MA phase.

In the BC phase, the i-th relay amplifies the received signal by a complex beamforming weight w_i. Thus, the processed signal vector at the relay nodes can be written as

$$\mathbf{x}_{\mathrm{R}}^{(\mathrm{RBoA})} = \mathbf{\Omega}\mathbf{y}_{\mathrm{R}} \, , \tag{3}$$

where $\mathbf{x}_{\mathrm{R}}^{(RBoA)}$ is a $K\times 1$ complex vector and $\mathbf{\Omega} = \mathrm{diag}([w_1, w_2, \ldots w_K])$. After this, the K relays broadcast the processed signals to A and B, simultaneously. So, the signals received at A, B and E can be expressed as

$$y_{\mathrm{A}}^{(\mathrm{RBoA})} = \mathbf{h}_{\mathrm{R}}^T \mathbf{x}^{(\mathrm{RBoA})} + n_{\mathrm{A}} = \mathbf{h}_{\mathrm{R}}^T \mathbf{\Omega}\mathbf{y}_{\mathrm{R}} + n_{\mathrm{A}} = \underbrace{\sqrt{P_{\mathrm{A}}}\mathbf{h}_{\mathrm{R}}^T \mathbf{\Omega}\mathbf{h}_{\mathrm{R}} x_{\mathrm{A}}}_{\text{self-interference}} + \underbrace{\sqrt{P_{\mathrm{B}}}\mathbf{h}_{\mathrm{R}}^T \mathbf{\Omega}\mathbf{f}_{\mathrm{R}} x_{\mathrm{B}}}_{\text{desired signal}} + \underbrace{\mathbf{h}_{\mathrm{R}}^T \mathbf{\Omega}\mathbf{n}_{\mathrm{R}} + n_{\mathrm{A}}}_{\text{noise}} \, , \tag{4}$$

$$y_{\mathrm{B}}^{(\mathrm{RBoA})} = \mathbf{f}_{\mathrm{R}}^T \mathbf{x}^{(\mathrm{RBoA})} + n_{\mathrm{B}} = \mathbf{f}_{\mathrm{R}}^T \mathbf{\Omega}\mathbf{y}_{\mathrm{R}} + n_{\mathrm{B}} = \underbrace{\sqrt{P_{\mathrm{A}}}\mathbf{f}_{\mathrm{R}}^T \mathbf{\Omega}\mathbf{h}_{\mathrm{R}} x_{\mathrm{A}}}_{\text{desired signal}} + \underbrace{\sqrt{P_{\mathrm{B}}}\mathbf{f}_{\mathrm{R}}^T \mathbf{\Omega}\mathbf{f}_{\mathrm{R}} x_{\mathrm{B}}}_{\text{self-interference}} + \underbrace{\mathbf{f}_{\mathrm{R}}^T \mathbf{\Omega}\mathbf{n}_{\mathrm{R}} + n_{\mathrm{B}}}_{\text{noise}} \, , \tag{5}$$

$$y_{\mathrm{E_{BC}}}^{(\mathrm{RBoA})} = \mathbf{g}_{\mathrm{R}}^T \mathbf{x}^{(\mathrm{RBoA})} + n_{\mathrm{E_{BC}}} = \mathbf{g}_{\mathrm{R}}^T \mathbf{\Omega}\mathbf{y}_{\mathrm{R}} + n_{\mathrm{E_{BC}}} = \sqrt{P_{\mathrm{A}}}\mathbf{g}_{\mathrm{R}}^T \mathbf{\Omega}\mathbf{h}_{\mathrm{R}} x_{\mathrm{A}} + \sqrt{P_{\mathrm{B}}}\mathbf{g}_{\mathrm{R}}^T \mathbf{\Omega}\mathbf{f}_{\mathrm{R}} x_{\mathrm{B}} + \underbrace{\mathbf{g}_{\mathrm{R}}^T \mathbf{\Omega}\mathbf{n}_{\mathrm{R}} + n_{\mathrm{E_{BC}}}}_{\text{noise}} \, , \tag{6}$$

where n_{A}, n_{B} and $n_{\mathrm{E_{BC}}}$ are the noise received at A, B and E, respectively.

Since A and B know their own transmitted signals, i.e., x_{A} and x_{B}, respectively, they can

cancel the self-interference. Thus, in terms of (4) and (5), the end-to-end received SINR at A and B can be respectively given by

$$\mathrm{SINR}_{\mathrm{A}}^{(\mathrm{RBoA})}=\frac{P_{\mathrm{B}}\mathbf{w}^{H}\mathbf{G}_{\mathrm{AB}}\mathbf{w}}{\sigma^{2}\mathbf{w}^{\mathbf{H}}\mathbf{D}_{\mathrm{A}}\mathbf{w}+\sigma^{2}}\ , \tag{7}$$

$$\mathrm{SINR}_{\mathrm{B}}^{(\mathrm{RBoA})}=\frac{P_{\mathrm{A}}\mathbf{w}^{H}\mathbf{G}_{\mathrm{AB}}\mathbf{w}}{\sigma^{2}\mathbf{w}^{\mathbf{H}}\mathbf{D}_{\mathrm{B}}\mathbf{w}+\sigma^{2}}, \tag{8}$$

where $\mathbf{G}_{\mathrm{AB}}=\mathrm{diag}(\mathbf{h}_{\mathrm{R}})\mathbf{f}_{\mathrm{R}}(\mathrm{diag}(\mathbf{h}_{\mathrm{R}})\mathbf{f}_{\mathrm{R}})^{H}$, $\mathbf{D}_{\mathrm{A}}=\mathrm{diag}(\mathbf{h}_{\mathrm{R}})(\mathrm{diag}(\mathbf{h}_{\mathrm{R}}))^{H}$, $\mathbf{D}_{\mathrm{B}}=\mathrm{diag}(\mathbf{f}_{\mathrm{R}})(\mathrm{diag}(\mathbf{f}_{\mathrm{R}}))^{H}$ and $\mathbf{w}=[w_1,w_2,...w_K]^{H}$.

For E, it collects the signals in both phases, we assume that the Maximal Ratio Combining (MRC) is used at E to extract the desired signals. Therefore, the received SINR for the signals transmitted from A and B at E can be given by

$$\mathrm{SINR}_{\mathrm{E_A}}^{(\mathrm{RBoA})}=\frac{P_{\mathrm{A}}\mid h_{\mathrm{E}}\mid^{2}}{P_{\mathrm{B}}\mid f_{\mathrm{E}}\mid^{2}+\sigma^{2}}+\frac{P_{\mathrm{A}}\mathbf{w}^{H}\mathbf{G}_{\mathrm{AE}}\mathbf{w}}{P_{\mathrm{B}}\mathbf{w}^{H}\mathbf{G}_{\mathrm{BE}}\mathbf{w}+\sigma^{2}\mathbf{w}^{H}\mathbf{D}_{\mathrm{E}}\mathbf{w}+\sigma^{2}}, \tag{9}$$

$$\mathrm{SINR}_{\mathrm{E_B}}^{(\mathrm{RBoA})}=\frac{P_{\mathrm{B}}\mid f_{\mathrm{E}}\mid^{2}}{P_{\mathrm{A}}\mid h_{\mathrm{E}}\mid^{2}+\sigma^{2}}+\frac{P_{\mathrm{B}}\mathbf{w}^{H}\mathbf{G}_{\mathrm{BE}}\mathbf{w}}{P_{\mathrm{A}}\mathbf{w}^{H}\mathbf{G}_{\mathrm{AE}}\mathbf{w}+\sigma^{2}\mathbf{w}^{H}\mathbf{D}_{\mathrm{E}}\mathbf{w}+\sigma^{2}}, \tag{10}$$

respectively, where $\mathbf{G}_{\mathrm{AE}}=\mathrm{diag}(\mathbf{h}_{\mathrm{R}})\mathbf{g}_{\mathrm{R}}(\mathrm{diag}(\mathbf{h}_{\mathrm{R}})\mathbf{g}_{\mathrm{R}})^{H}$, $\mathbf{G}_{\mathrm{BE}}=\mathrm{diag}(\mathbf{f}_{\mathrm{R}})\mathbf{g}_{\mathrm{R}}(\mathrm{diag}(\mathbf{f}_{\mathrm{R}})\mathbf{g}_{\mathrm{R}})^{H}$ and $\mathbf{D}_{\mathrm{E}}=\mathrm{diag}(\mathbf{g}_{\mathrm{R}})(\mathrm{diag}(\mathbf{g}_{\mathrm{R}}))^{H}$. Actually, the first terms in (9) and (10) are the received SINRs for the signals transmitted from A and from B to E in the MA phase, respectively, and the second terms in (9) and (10) are the received SINRs for the signals transmitted from A and from B to E in the BC phase, respectively.

2.2. RBwA

In this section, we introduce the proposed RBwA. The process in the MA phase of RBwA is the same with that of RBoA, so we do not repeat the description of it again. In the BC phase of RBwA, the so-called artificial noise scheme [8] is adopted, where the relay nodes transmit artificial noise (interference) to mask the concurrent transmission of information bearing signal to the eavesdroppers. Thus, the transmit signal vector $\mathbf{x}$ at relay nodes can be expressed as

$$\mathbf{x}_{\mathrm{R}}^{(\mathrm{RBwA})}=\mathbf{\Omega}\mathbf{y}_{\mathrm{R}}+\varepsilon, \tag{11}$$

where ε is the $K\times 1$ artificial noise vector and it follows the zeros-mean complex Gaussian distribution with covariance matrix $\mathbf{\Sigma}\pm 0$. Thus, the signal received at A, B and E can be expressed as

$$y_{\mathrm{A}}^{(\mathrm{RBwA})}=\mathbf{h}_{\mathrm{R}}^{T}\mathbf{x}^{(\mathrm{RBwA})}+n_{\mathrm{A}}=\underbrace{\sqrt{P_{\mathrm{A}}}\mathbf{h}_{\mathrm{R}}^{T}\mathbf{\Omega}\mathbf{h}_{\mathrm{R}}x_{\mathrm{A}}}_{\text{self-interference}}+\underbrace{\sqrt{P_{\mathrm{B}}}\mathbf{h}_{\mathrm{R}}^{T}\mathbf{\Omega}\mathbf{f}_{\mathrm{R}}x_{\mathrm{B}}}_{\text{desired signal}}+\underbrace{\mathbf{h}_{\mathrm{R}}^{T}\mathbf{\Omega}\mathbf{n}_{\mathrm{R}}+n_{\mathrm{A}}}_{\text{noise}}+\underbrace{\mathbf{h}_{\mathrm{R}}^{T}\varepsilon}_{\text{artificial noise}}\ , \tag{12}$$

$$y_{\mathrm{B}}^{(\mathrm{RBwA})}=\mathbf{f}_{\mathrm{R}}^{T}\mathbf{x}^{(\mathrm{RBwA})}+n_{\mathrm{B}}=\underbrace{\sqrt{P_{\mathrm{A}}}\mathbf{f}_{\mathrm{R}}^{T}\mathbf{\Omega}\mathbf{h}_{\mathrm{R}}x_{\mathrm{A}}}_{\text{desired signal}}+\underbrace{\sqrt{P_{\mathrm{B}}}\mathbf{f}_{\mathrm{R}}^{T}\mathbf{\Omega}\mathbf{f}_{\mathrm{R}}x_{\mathrm{B}}}_{\text{self-interference}}+\underbrace{\mathbf{f}_{\mathrm{R}}^{T}\mathbf{\Omega}\mathbf{n}_{\mathrm{R}}+n_{\mathrm{B}}}_{\text{noise}}+\underbrace{\mathbf{f}_{\mathrm{R}}^{T}\varepsilon}_{\text{artificial noise}}\ , \tag{13}$$

$$y_{\mathrm{E_{BC}}}^{(\mathrm{RBwA})}=\mathbf{g}_{\mathrm{R}}^{T}\mathbf{x}^{(\mathrm{RBwA})}+n_{\mathrm{E_{BC}}}=\sqrt{P_{\mathrm{A}}}\mathbf{g}_{\mathrm{R}}^{T}\mathbf{\Omega}\mathbf{h}_{\mathrm{R}}x_{\mathrm{A}}+\sqrt{P_{\mathrm{B}}}\mathbf{g}_{\mathrm{R}}^{T}\mathbf{\Omega}\mathbf{f}_{\mathrm{R}}x_{\mathrm{B}}+\underbrace{\mathbf{g}_{\mathrm{R}}^{T}\mathbf{\Omega}\mathbf{n}_{\mathrm{R}}+n_{\mathrm{E_{BC}}}}_{\text{noise}}+\underbrace{\mathbf{g}_{\mathrm{R}}^{T}\varepsilon}_{\text{artificial noise}}\ , \tag{14}$$

respectively. In terms of (12) and (13), the end-to-end received SINRs at A and B can be given by

$$\mathrm{SINR}_{\mathrm{A}}^{(\mathrm{RBwA})}=\frac{P_{\mathrm{B}}\mathbf{w}^{H}\mathbf{G}_{\mathrm{AB}}\mathbf{w}}{\sigma^{2}\mathbf{w}^{\mathbf{H}}\mathbf{D}_{\mathrm{A}}\mathbf{w}+\mathrm{tr}(\mathbf{H}_{\mathrm{A}}\mathbf{\Sigma})+\sigma^{2}}, \tag{15}$$

$$\mathrm{SINR}_{\mathrm{B}}^{(\mathrm{RBwA})}=\frac{P_{\mathrm{A}}\mathbf{w}^{H}\mathbf{G}_{\mathrm{AB}}\mathbf{w}}{\sigma^{2}\mathbf{w}^{\mathbf{H}}\mathbf{D}_{\mathrm{B}}\mathbf{w}+\mathrm{tr}(\mathbf{H}_{\mathrm{B}}\boldsymbol{\Sigma})+\sigma^{2}}, \tag{16}$$

where $\mathbf{H}_{\mathrm{A}}=\mathbf{h}_{\mathrm{R}}\mathbf{h}_{\mathrm{R}}^{H}$, $\mathbf{H}_{\mathrm{B}}=\mathbf{f}_{\mathrm{R}}\mathbf{f}_{\mathrm{R}}^{H}$. With MRC method, the received SINR at E for the signal transmitted from A and B can be respectively written as

$$\mathrm{SINR}_{\mathrm{E_A}}^{(\mathrm{RBwA})}=\frac{P_{\mathrm{A}}\mid h_{\mathrm{E}}\mid^{2}}{P_{\mathrm{B}}\mid f_{\mathrm{E}}\mid^{2}+\sigma^{2}}+\frac{P_{\mathrm{A}}\mathbf{w}^{H}\mathbf{G}_{\mathrm{AE}}\mathbf{w}}{P_{\mathrm{B}}\mathbf{w}^{H}\mathbf{G}_{\mathrm{BE}}\mathbf{w}+\sigma^{2}\mathbf{w}^{H}\mathbf{D}_{\mathrm{E}}\mathbf{w}+\mathrm{tr}(\mathbf{F}_{\mathrm{E}}\boldsymbol{\Sigma})+\sigma^{2}}, \tag{17}$$

$$\mathrm{SINR}_{\mathrm{E_B}}^{(\mathrm{RBwA})}=\frac{P_{\mathrm{B}}\mid f_{\mathrm{E}}\mid^{2}}{P_{\mathrm{A}}\mid h_{\mathrm{E}}\mid^{2}+\sigma^{2}}+\frac{P_{\mathrm{B}}\mathbf{w}^{H}\mathbf{G}_{\mathrm{BE}}\mathbf{w}}{P_{\mathrm{A}}\mathbf{w}^{H}\mathbf{G}_{\mathrm{AE}}\mathbf{w}+\sigma^{2}\mathbf{w}^{H}\mathbf{D}_{\mathrm{E}}\mathbf{w}+\mathrm{tr}(\mathbf{F}_{\mathrm{E}}\boldsymbol{\Sigma})+\sigma^{2}}, \tag{18}$$

where $\mathbf{F}_{\mathrm{E}}=\mathbf{g}_{\mathrm{R}}\mathbf{g}_{\mathrm{R}}^{H}$.

Based on the description above, in next section, we will find the optimal $\mathbf{w}$ for RBoA and the joint optimal $\mathbf{w}$ and $\boldsymbol{\Sigma}$ for RBwA, respectively.

3. Optimization Design for RBoA and RBwA.

In this section, we design the optimal beamforming vector $\mathbf{w}$ for RBoA and the jointly optimized beamforming vector $\mathbf{w}$ and artificial noise vector $\boldsymbol{\Sigma}$ for RBwA to minimize the total transmit powers of all relay nodes. To meet the security requirement of the system, two constraints are considered. Firstly, the received SINR at both A and B should be higher than predefined QoS thresholds, i.e., γ_{A} and γ_{B}, respectively. Secondly, the received SINR at E should be kept below the predefined secure thresholds, i.e., $\gamma_{\mathrm{E_A}}$ and $\gamma_{\mathrm{E_B}}$, respectively. Then, a uniform optimization framework for the two schemes, RBoA and RBwA, can be mathematically given by

$$\begin{aligned}\min_{\mathbf{w}}\quad & P_{\mathrm{R}}\\ \text{s.t.}\quad & \mathrm{SINR}_{\mathrm{A}}\geq\gamma_{\mathrm{A}},\mathrm{SINR}_{\mathrm{B}}\geq\gamma_{\mathrm{B}}\\ & \mathrm{SINR}_{\mathrm{E_A}}\leq\gamma_{\mathrm{E_A}},\mathrm{SINR}_{\mathrm{E_B}}\leq\gamma_{\mathrm{E_B}}\end{aligned}. \tag{19}$$

3.1. Optimal Design for RBoA

In RBoA, $P_{\mathrm{R}}=P_{\mathrm{R}}^{(\mathrm{RBoA})}=E\{\mathbf{x}_{\mathrm{R}}^{(\mathrm{RBoA})}(\mathbf{x}_{\mathrm{R}}^{(\mathrm{RBoA})})^{H}\}=P_{\mathrm{A}}\mathbf{w}^{H}\mathbf{D}_{\mathrm{A}}\mathbf{w}+P_{\mathrm{B}}\mathbf{w}^{H}\mathbf{D}_{\mathrm{B}}\mathbf{w}+\sigma^{2}\mathbf{w}^{H}\mathbf{w}$, and $\mathrm{SINR}_{\mathrm{A}}$, $\mathrm{SINR}_{\mathrm{B}}$, $\mathrm{SINR}_{\mathrm{E_A}}$ and $\mathrm{SINR}_{\mathrm{E_B}}$ can be found in (7), (8), (9), (10), respectively. Let $\eta_{\mathrm{E_A}}=P_{\mathrm{A}}\mid h_{\mathrm{E}}\mid^{2}/(P_{\mathrm{B}}\mid f_{\mathrm{E}}\mid^{2}+\sigma^{2})$ and $\eta_{\mathrm{E_B}}=P_{\mathrm{B}}\mid f_{\mathrm{E}}\mid^{2}/(P_{\mathrm{A}}\mid h_{\mathrm{E}}\mid^{2}+\sigma^{2})$. According to the problem in (19), we have that

$$\begin{aligned}\min_{\mathbf{w}}\quad & P_{\mathrm{A}}\mathbf{w}^{H}\mathbf{D}_{\mathrm{A}}\mathbf{w}+P_{\mathrm{B}}\mathbf{w}^{H}\mathbf{D}_{\mathrm{B}}\mathbf{w}+\sigma^{2}\mathbf{w}^{H}\mathbf{w}\\ \text{s.t.}\quad & \frac{P_{\mathrm{B}}\mathbf{w}^{H}\mathbf{G}_{\mathrm{AB}}\mathbf{w}}{\sigma^{2}\mathbf{w}^{H}\mathbf{D}_{\mathrm{A}}\mathbf{w}+\sigma^{2}}\geq\gamma_{\mathrm{A}}\\ & \frac{P_{\mathrm{A}}\mathbf{w}^{H}\mathbf{G}_{\mathrm{AB}}\mathbf{w}}{\sigma^{2}\mathbf{w}^{H}\mathbf{D}_{\mathrm{B}}\mathbf{w}+\sigma^{2}}\geq\gamma_{\mathrm{B}}\\ & \frac{P_{\mathrm{A}}\mathbf{w}^{H}\mathbf{G}_{\mathrm{AE}}\mathbf{w}}{P_{\mathrm{B}}\mathbf{w}^{H}\mathbf{G}_{\mathrm{BE}}\mathbf{w}+\sigma^{2}\mathbf{w}^{H}\mathbf{D}_{\mathrm{E}}\mathbf{w}+\sigma^{2}}\leq\gamma_{\mathrm{E_A}}-\eta_{\mathrm{E_A}}\\ & \frac{P_{\mathrm{A}}\mathbf{w}^{H}\mathbf{G}_{\mathrm{AE}}\mathbf{w}}{P_{\mathrm{B}}\mathbf{w}^{H}\mathbf{G}_{\mathrm{BE}}\mathbf{w}+\sigma^{2}\mathbf{w}^{H}\mathbf{D}_{\mathrm{E}}\mathbf{w}+\sigma^{2}}\leq\gamma_{\mathrm{E_A}}-\eta_{\mathrm{E_A}}\end{aligned}. \tag{20}$$

In fact, $\eta_{\mathrm{E_A}}$ and $\eta_{\mathrm{E_B}}$ are the received SINRs for the transmission from A to E and from B to E in the MA phase, respectively. Note that SINR must be nonnegative, so when $\eta_{\mathrm{E_A}} > \gamma_{\mathrm{E_A}}$, the problem will have no solution. The case $\eta_{\mathrm{E_A}} > \gamma_{\mathrm{E_A}}$ actually implies that only by the overhearing in the MA phase, E can decode the signal transmitted from B. This also applies to the case $\eta_{\mathrm{E_B}} > \gamma_{\mathrm{E_B}}$. Therefore, in this paper, we just focus on the case $\eta_{\mathrm{E_A}} \le \gamma_{\mathrm{E_A}}$ and $\eta_{\mathrm{E_B}} \le \gamma_{\mathrm{E_B}}$.

Since the problem of (20) is nonconvex, we handle it using SDP relaxation theory. By introducing a new variable $\mathbf{W} = \mathbf{w}\mathbf{w}^H$, the problem of (20) can be transformed into

$$\min_{\mathbf{W}} \; P_{\mathrm{A}}\mathrm{tr}(\mathbf{D}_{\mathrm{A}}\mathbf{W}) + P_{\mathrm{B}}\mathrm{tr}(\mathbf{D}_{\mathrm{B}}\mathbf{W}) + \sigma^2\mathrm{tr}(\mathbf{W}) \tag{21a}$$

$$\text{s.t. } \sigma^2\gamma_{\mathrm{A}}\mathrm{tr}(\mathbf{D}_{\mathrm{A}}\mathbf{W}) - P_{\mathrm{B}}\mathrm{tr}(\mathbf{G}_{\mathrm{AB}}\mathbf{W}) + \sigma^2\gamma_{\mathrm{A}} \le 0 \tag{21b}$$

$$\sigma^2\gamma_{\mathrm{B}}\mathrm{tr}(\mathbf{D}_{\mathrm{B}}\mathbf{W}) - P_{\mathrm{A}}\mathrm{tr}(\mathbf{G}_{\mathrm{AB}}\mathbf{W}) + \sigma^2\gamma_{\mathrm{B}} \le 0 \tag{21c}$$

$$P_{\mathrm{A}}\mathrm{tr}(\mathbf{G}_{\mathrm{AE}}\mathbf{W}) - \sigma^2(\gamma_{\mathrm{E_A}} - \eta_{\mathrm{E_A}})\mathrm{tr}(\mathbf{D}_{\mathrm{E}}\mathbf{W}) - (\sigma^2 + P_{\mathrm{B}}\mathrm{tr}(\mathbf{G}_{\mathrm{BE}}\mathbf{W}))(\gamma_{\mathrm{E_A}} - \eta_{\mathrm{E_A}}) \le 0 \tag{21d}$$

$$P_{\mathrm{B}}\mathrm{tr}(\mathbf{G}_{\mathrm{BE}}\mathbf{W}) - \sigma^2(\gamma_{\mathrm{E_B}} - \eta_{\mathrm{E_B}})\mathrm{tr}(\mathbf{D}_{\mathrm{E}}\mathbf{W}) - (\sigma^2 + P_{\mathrm{A}}\mathrm{tr}(\mathbf{G}_{\mathrm{AE}}\mathbf{W}))(\gamma_{\mathrm{E_B}} - \eta_{\mathrm{E_B}}) \le 0 \tag{21e}$$

$$\mathbf{W} \pm 0 \tag{21f}$$

$$\mathrm{rank}(\mathbf{W}) = 1 \tag{21g}$$

From problem (21), it can be observed that the resulting objective function is linear, and all constraints are convex sets except the rank-one constraint. Following the SDP relaxation theory, if we drop the rank-one constraint, we have that

$$\begin{aligned} \min_{\mathbf{W}} \quad & P_{\mathrm{A}}\mathrm{tr}(\mathbf{D}_{\mathrm{A}}\mathbf{W}) + P_{\mathrm{B}}\mathrm{tr}(\mathbf{D}_{\mathrm{B}}\mathbf{W}) + \sigma^2\mathrm{tr}(\mathbf{W}) \\ \text{s.t.} \quad & \text{(21b),(21c),(21d),(21e),(21f).} \end{aligned}, \tag{22}$$

which is a convex SDP, and therefore can be efficiently solved to obtain the global optimum by the available solvers, e.g. CVX [13].

It also should be noted that, since the rank-one constraint is dropped in (22), the optimal solution W* is not necessarily rank-one. Based on the rank reduction results for general SDPs, namely, Lemma 3.1 in [12], we can derive that rank(W*)=1 or rank(W*)=2. Therefore, if rank(W*)=1, the optimal beamforming vector w* can be retrieved from W* exactly. If rank(W*)=2, Gaussian randomization method [11] can be applied to obtain an approximated w*. Interestingly, the optimal solution W* in our simulations are all rank-one, which means that w* can be retrieved from W* exactly.

3.2. Optimal Design for RBwA

In RBwA, $P_{\mathrm{R}} = E\{\mathbf{x}_{\mathrm{R}}^{(\mathrm{RBwA})}(\mathbf{x}_{\mathrm{R}}^{(\mathrm{RBwA})})^H\} = P_{\mathrm{A}}\mathbf{w}^H\mathbf{D}_{\mathrm{A}}\mathbf{w} + P_{\mathrm{B}}\mathbf{w}^H\mathbf{D}_{\mathrm{B}}\mathbf{w} + \sigma^2\mathbf{w}^H\mathbf{w} + \mathrm{tr}(\mathbf{\Sigma})$. Compared with the P_{R} of RBoA, the P_{R} of RBwA has one more term, i.e., the last term $\mathrm{tr}(\mathbf{\Sigma})$, which actually is the power of artificial noise. Similarly to the analysis for RBoA, by substituting (15), (16), (17) and (18) into problem (19), we have that

$$\begin{aligned}
\min_{\mathbf{w},\boldsymbol{\Sigma}} \quad & P_{\mathrm{A}}\mathbf{w}^H\mathbf{D}_{\mathrm{A}}\mathbf{w} + P_{\mathrm{B}}\mathbf{w}^H\mathbf{D}_{\mathrm{B}}\mathbf{w} + \sigma^2\mathbf{w}^H\mathbf{w} + \mathrm{tr}(\boldsymbol{\Sigma}) \\
\text{s.t.} \quad & \frac{P_{\mathrm{B}}\mathbf{w}^H\mathbf{G}_{\mathrm{AB}}\mathbf{w}}{\sigma^2\mathbf{w}^H\mathbf{D}_{\mathrm{A}}\mathbf{w} + \mathrm{tr}(\mathbf{H}_{\mathrm{A}}\boldsymbol{\Sigma}) + \sigma^2} \geq \gamma_{\mathrm{A}} \\
& \frac{P_{\mathrm{A}}\mathbf{w}^H\mathbf{G}_{\mathrm{AB}}\mathbf{w}}{\sigma^2\mathbf{w}^H\mathbf{D}_{\mathrm{B}}\mathbf{w} + \mathrm{tr}(\mathbf{H}_{\mathrm{B}}\boldsymbol{\Sigma}) + \sigma^2} \geq \gamma_{\mathrm{B}} \\
& \frac{P_{\mathrm{A}}\mathbf{w}^H\mathbf{G}_{\mathrm{AB}}\mathbf{w}}{\sigma^2\mathbf{w}^H\mathbf{D}_{\mathrm{B}}\mathbf{w} + \mathrm{tr}(\mathbf{H}_{\mathrm{B}}\boldsymbol{\Sigma}) + \sigma^2} \geq \gamma_{\mathrm{B}} \\
& \frac{P_{\mathrm{A}}\mathbf{w}^H\mathbf{G}_{\mathrm{AE}}\mathbf{w}}{P_{\mathrm{B}}\mathbf{w}^H\mathbf{G}_{\mathrm{BE}}\mathbf{w} + \sigma^2\mathbf{w}^H\mathbf{D}_{\mathrm{E}}\mathbf{w} + \mathrm{tr}(\mathbf{F}_{\mathrm{E}}\boldsymbol{\Sigma}) + \sigma^2} \leq \gamma_{\mathrm{E_A}} - \eta_{\mathrm{E_A}} \\
& \frac{P_{\mathrm{B}}\mathbf{w}^H\mathbf{G}_{\mathrm{BE}}\mathbf{w}}{P_{\mathrm{A}}\mathbf{w}^H\mathbf{G}_{\mathrm{AE}}\mathbf{w} + \sigma^2\mathbf{w}^H\mathbf{D}_{\mathrm{E}}\mathbf{w} + \mathrm{tr}(\mathbf{F}_{\mathrm{E}}\boldsymbol{\Sigma}) + \sigma^2} \leq \gamma_{\mathrm{E_B}} - \eta_{\mathrm{E_B}}
\end{aligned} \quad . \tag{24}$$

Here, we also focus the case when $\eta_{\mathrm{E_A}} \leq \gamma_{\mathrm{E_A}}$ and $\eta_{\mathrm{E_B}} \leq \gamma_{\mathrm{E_B}}$. It can be observed that when $\boldsymbol{\Sigma} = 0$, problem (24) can be degenerated into problem (20), which implies that the feasible set of problem (20) is a subset of the feasible set of problem (24) and $P_{\mathrm{R}}^{*(\mathrm{RBwA})} \leq P_{\mathrm{R}}^{*(\mathrm{RBoA})}$.

Since problem (24) is also nonconvex, by using the SDP relaxation theory, problem (24) also can be relaxed to be convex. Let $\mathbf{W} = \mathbf{w}\mathbf{w}^H$, problem (24) can be relaxed as

$$\min_{\mathbf{W},\boldsymbol{\Sigma}} \quad P_{\mathrm{A}}\mathrm{tr}(\mathbf{D}_{\mathrm{A}}\mathbf{W}) + P_{\mathrm{B}}\mathrm{tr}(\mathbf{D}_{\mathrm{B}}\mathbf{W}) + \sigma^2\mathrm{tr}(\mathbf{W}) + \mathrm{tr}(\boldsymbol{\Sigma}) \tag{25a}$$

$$\text{s.t.} \quad \sigma^2\gamma_{\mathrm{A}}\mathrm{tr}(\mathbf{D}_{\mathrm{A}}\mathbf{W}) - P_{\mathrm{B}}\mathrm{tr}(\mathbf{G}_{\mathrm{AB}}\mathbf{W}) + \gamma_{\mathrm{A}}\mathrm{tr}(\mathbf{H}_{\mathrm{A}}\boldsymbol{\Sigma}) + \sigma^2\gamma_{\mathrm{A}} \leq 0 \tag{25b}$$

$$\sigma^2\gamma_{\mathrm{B}}\mathrm{tr}(\mathbf{D}_{\mathrm{B}}\mathbf{W}) - P_{\mathrm{A}}\mathrm{tr}(\mathbf{G}_{\mathrm{AB}}\mathbf{W}) + \gamma_{\mathrm{B}}\mathrm{tr}(\mathbf{H}_{\mathrm{B}}\boldsymbol{\Sigma}) + \sigma^2\gamma_{\mathrm{B}} \leq 0 \tag{25c}$$

$$P_{\mathrm{A}}\mathrm{tr}(\mathbf{G}_{\mathrm{AE}}\mathbf{W}) - \sigma^2(\gamma_{\mathrm{E_A}} - \eta_{\mathrm{E_A}})\mathrm{tr}(\mathbf{D}_{\mathrm{E}}\mathbf{W}) - (\sigma^2 + P_{\mathrm{B}}\mathrm{tr}(\mathbf{G}_{\mathrm{BE}}\mathbf{W}) + \mathrm{tr}(\mathbf{F}_{\mathrm{E}}\boldsymbol{\Sigma}))(\gamma_{\mathrm{E_A}} - \eta_{\mathrm{E_A}}) \leq 0 \tag{25d}$$

$$P_{\mathrm{B}}\mathrm{tr}(\mathbf{G}_{\mathrm{BE}}\mathbf{W}) - \sigma^2(\gamma_{\mathrm{E_B}} - \eta_{\mathrm{E_B}})\mathrm{tr}(\mathbf{D}_{\mathrm{E}}\mathbf{W}) - (\sigma^2 + P_{\mathrm{A}}\mathrm{tr}(\mathbf{G}_{\mathrm{AE}}\mathbf{W}) + \mathrm{tr}(\mathbf{F}_{\mathrm{E}}\boldsymbol{\Sigma}))(\gamma_{\mathrm{E_B}} - \eta_{\mathrm{E_B}}) \leq 0 \tag{25e}$$

$$\mathbf{W} \pm 0 \tag{25f}$$

$$\mathrm{rank}(\mathbf{W}) = 1 \tag{25g}$$

Following the SDP relaxation theory, the hard constraint $\mathrm{rank}(\mathbf{W}) = 1$ also can be neglected and the then the new relaxed problem is given by

$$\begin{aligned}
\min_{\mathbf{W},\boldsymbol{\Sigma}} \quad & P_{\mathrm{A}}\mathrm{tr}(\mathbf{D}_{\mathrm{A}}\mathbf{W}) + P_{\mathrm{B}}\mathrm{tr}(\mathbf{D}_{\mathrm{B}}\mathbf{W}) + \sigma^2\mathrm{tr}(\mathbf{W}) + \mathrm{tr}(\boldsymbol{\Sigma}) \\
\text{s.t.} \quad & \text{(25b),(25c),(25d),(25e),(25f)}
\end{aligned} \quad , \tag{26}$$

which is a convex SDP, and the global optimal solution can be obtainedby the available solvers. Futhermore, the beamforming vector w* can be retrieved from W* exactly, since W* is always rank-one in our simulation, although it cannot be proved theoretically.

It should be noted that the two schemes proposed in our manuscript can be extended to the case of existing multi-eavesdropper scenario directly. When there are multiple eavesdroppers in the system, the number of the secure constraint will be two times of the eavesdropper's number for the optimization problem and the SDP relaxation method can also be applied to solve the optimization problem.

4. Simulation Results

In this section, we provide some simulation results to validate the effectiveness and the performance of our proposed schemes. As mentioned previously, when the received SINR at E in the MA phase are higher than the predefined threshold, i.e., $\eta_{\mathrm{E_A}} > \gamma_{\mathrm{E_A}}$ or $\eta_{\mathrm{E_B}} > \gamma_{\mathrm{E_B}}$ the

secrecy of the communication cannot be achieved. We therefore just consider the cases that $\eta_{E_A} \le \gamma_{E_A}$ and $\eta_{E_B} \le \gamma_{E_B}$. The relaxed convex optimization problems (22) and (26) are solved by CVX tools [13].

Firstly, we select an example to show the effectiveness of the proposed schemes. The number of relay nodes K is set to 4. The uniform linear array (ULA) channel model is adopted to keep the space between successive array elements being half of the carrier wavelength, where the channel vectors $\mathbf{h}_R$, $\mathbf{f}_R$ and $\mathbf{g}_R$ poss a Vandermonde structure. $V(\varphi)=[1,e^{j\theta},...,e^{j(K-1)\theta}]^T/\sqrt{K}$, $\theta=-\pi\sin(\varphi\pi/180)$ and $\varphi\in[-90^\circ,90^\circ)$. The direction of A, B and E are set to be 10°, 85° and 25°, respectively. Therefore $\mathbf{h}_R=V(10^\circ)$, $\mathbf{f}_R=V(85^\circ)$ and $\mathbf{g}_R=V(25^\circ)$. Other parameters are set as follows. $|h_E|=|f_E|=0.7$, $P_A=P_B=11\text{dBW}$, $\gamma_{E_A}=\gamma_{E_B}=2\text{dBW}$, and $\gamma_A=\gamma_B=15\text{dBW}$.

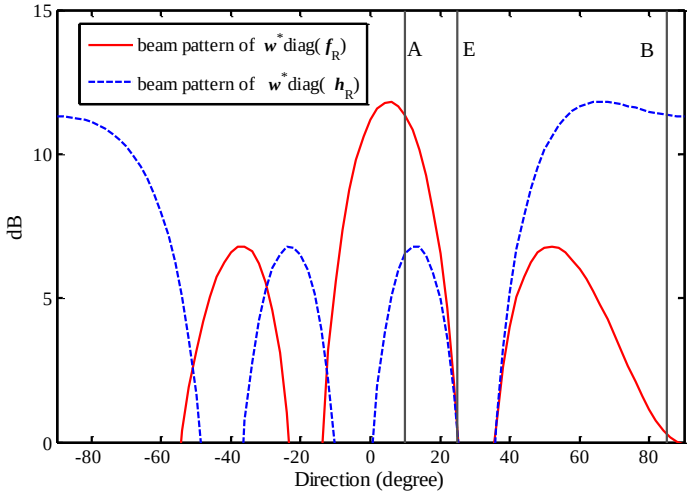


Fig. 2. Optimal beam patterns of RBoA with $\mathbf{h}_R=V(10^\circ)$, $\mathbf{f}_R=V(85^\circ)$, $\mathbf{g}_R=V(25^\circ)$

Through solving the problem in (22) and (26), the total transmit power consumed by the relay nodes in RBoA and RBwA are 20.6dBW and 17dBW, respectively. This apparently demonstrates that RBwA consumes much less power than RBoA.

Moreover, the beam patterns of $\mathbf{w}^*\text{diag}(\mathbf{h}_R)$ and $\mathbf{w}^*\text{diag}(\mathbf{f}_R)$ for problem (22) are shown in **Fig. 2** and the beam patterns of $\mathbf{w}^*\text{diag}(\mathbf{h}_R)$, $\mathbf{w}^*\text{diag}(\mathbf{f}_R)$ and $\mathbf{\Sigma}^*$ for problem (26) are shown in **Fig. 3**. Actually, the beam patterns of $\mathbf{w}^*\text{diag}(\mathbf{h}_R)$ and $\mathbf{w}^*\text{diag}(\mathbf{f}_R)$ represent the total power consumed by the relay nodes associated with the transmissions from A to B and from B to A, respectively. From **Fig. 2** and **Fig. 3**, it can be seen that in the two proposed schemes, the obtained main power (information) of beam patterns $\mathbf{w}^*\text{diag}(\mathbf{h}_R)$ and $\mathbf{w}^*\text{diag}(\mathbf{f}_R)$ focus towards B and A very well, respectively. Meanwhile, both $\mathbf{w}^*\text{diag}(\mathbf{h}_R)$ and $\mathbf{w}^*\text{diag}(\mathbf{f}_R)$ degrade sharply along the direction of E. It also implies that using our proposed schemes, the main power (information) can be focused towards to B and A with less leakage power towards E. Moreover, from **Fig. 3**, one can see that $\mathbf{\Sigma}^*$ focus its main beam power (interference) towards E, and the artificial noise power towards A and B are relatively very low. Since $\mathbf{\Sigma}^*$ actually represents the power consumption of the designed artificial noise at the relay nodes, it demonstrates that the designed artificial noise can greatly bring down the received SINR at E while only causing extremely small impact on the received SINR of the two sources. Therefore, secure two-way relay transmission can be achieved.

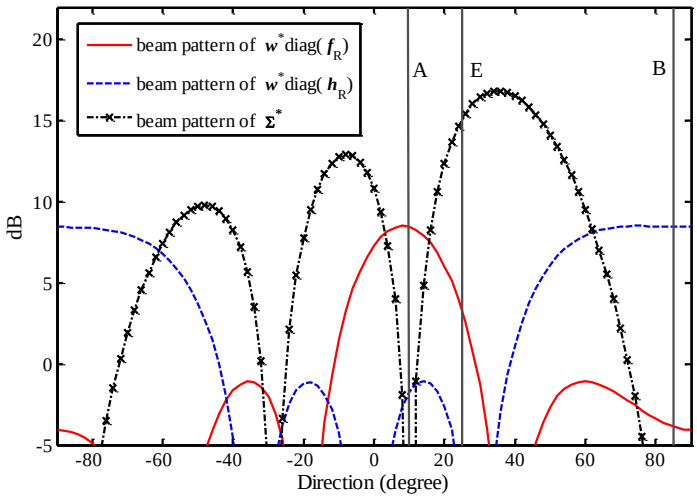


Fig. 3. Optimal beam patterns of RBwA with $\mathbf{h}_R = V(10^\circ)$, $\mathbf{f}_R = V(85^\circ)$, $\mathbf{g}_R = V(25^\circ)$

Secondly, we compare the infeasibility rate, i.e., the percentage of infeasibility (%) of problems (22) and (26) out of 1000 simulation trials, and power consumption of the two proposed schemes. In these simulations, the channel vectors are generated as complex zeros-mean Gaussian random vectors. The channel covariance for $\mathbf{h}_R$ is set to 7dBW, and the other channel covariances are all set to 5dBW. The transmit powers of P_A and P_B are set to 12dBW, the predefined security thresholds are set to $\gamma_{E_A} = \gamma_{E_B} = 2\text{dBW}$, and the QoS thresholds are set to $\gamma_A = \gamma_B = \gamma$. Fig. 4 shows the infeasibility rate versus γ when K are selected to be 6, 8 and 10, respectively. It can be observed that the infeasibility rate of RBwA is always lower than RBoA and infeasibility rates of both schemes decrease with the increase of the value of K.

Furthermore, **Fig. 5** plots the total consumed power P_R by the relay nodes versus γ when both of two proposed schemes are feasible. It can be seen that the power consumption of RBwA is always less than that of RBoA. Additionally, the power consumption gap between the two schemes becomes gradually larger with the increase of γ. It also shows that the total power consumed by the relay nodes decreases with the growth of the number of relay nodes. It therefore can be stated that more relay nodes could lead to low power consumption and low infeasibility rate, and by introducing optimally designed artificial noise, secure bemforming performance can be improved.

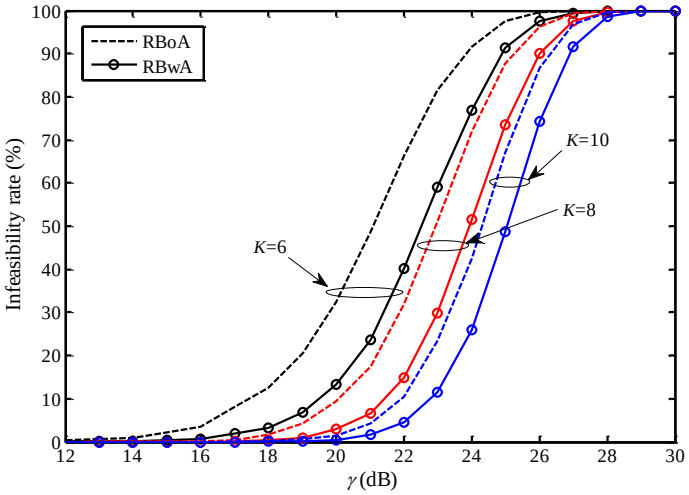


Fig. 4. Comparison of the infeasibility rates of RBoA and RBwA, when K =6, 8 and 10, respectively

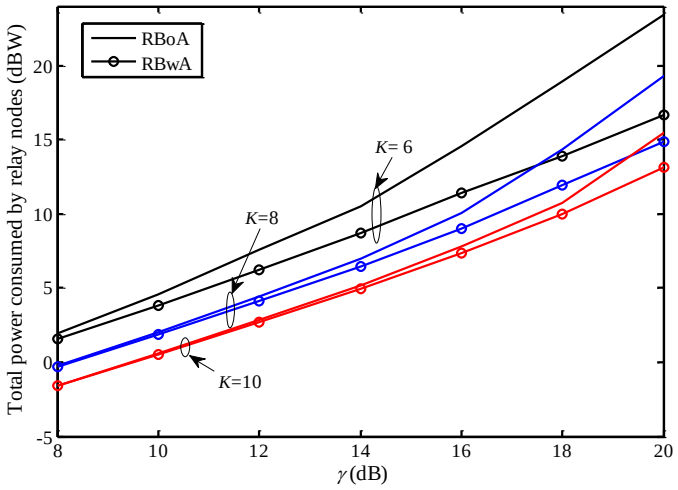


Fig. 5. Comparison of the total power consumed by the relay nodes in RBoA and RBwA, when K =6, 8 and 10, respectively

Thirdly, we also compare the performance of our two proposed schemes with the null space based beamforming scheme. In Section I, we introduced a beamforming scheme proposed in [7], which designed the beamforming vector in the null space of eavesdropper's channel to maximize the secrecy sum rate of the two-way relay system. By the null space based relay beamforming design, the secrecy of the two-way transmission can also be enhanced. In the following simulations, we will compare the power consumption and infeasibility rate performance of such null space based method with our schemes. Moreover, the relay beamforming scheme without security constraint is also considered as a benchmark in our comparisons. Specifically, in the simulations, the channel vectors are generated as complex zeros-mean Gaussian random vectors. The channel covariance $\mathbf{h}_R$ is set to 7dBW, and the other channel covariances are all set to 5dBW. The transmit powers of P_A and P_B are set to 12dBW. We also set the QoS threshold to $\gamma_A = \gamma_B = 22$dB and security threshold to

$\gamma_{E_A} = \gamma_{E_B} = \gamma_E$. Fig. 6 shows the infeasibility rate of the two proposed schemes versus γ_E, where the null space based scheme and the relay beamforming scheme without security constraint are also simulated. It shows that the relay beamforming scheme without security constraint always has the lowest infeasibility rate among the four schemes. The reason is that no security constraint gives rise to more feasible solutions. It also shows that the infeasibility rate of RBwA is very close to that of the scheme with no security constraint, where, however, in more than 99% cases RBwA meets the security requirements, which implies a very good performance of RBwA. It also shows that, with the increase of γ_E, the infeasibility rate of RBoA decreases from 74% to 40%, while the infeasibility rate of null space based scheme is unchanged with the varying γ_E. The reason is that, in the null space based scheme, $\gamma_{E_A} = \gamma_{E_B} = -\infty$dB, which is independent with γ_E.

Besides, the curves of the consumed power versus γ_E for the four schemes in feasible cases are plotted in **Fig. 7**. It can be seen that, compared with the three secure relay beamforming schemes, the total power consumption of relay beamforming scheme without security constraint is always lowest, which implies that the secure relay beamforming schemes enhance the secrecy of the two-way relay networks at the expense of more power consumption at relay nodes. From **Fig. 7**, it also can be observed that, RBwA scheme always achieves the lowest power consumption among the three secure relay beamforming schemes and the power consumed by the two proposed schemes decreases with the growth of γ_E. Additionally, one can also see that the power consumption of the null space based scheme seems constant. The reason is that the null space based scheme's performance is independent with γ_E, which was explained previously.

From the simulations presented above, it consequently can be stated that, the two proposed schemes outperform other secure beamforming design methods in terms of low power consumption and low infeasibility rate. Moreover, RBwA always has better performance than RBoA.

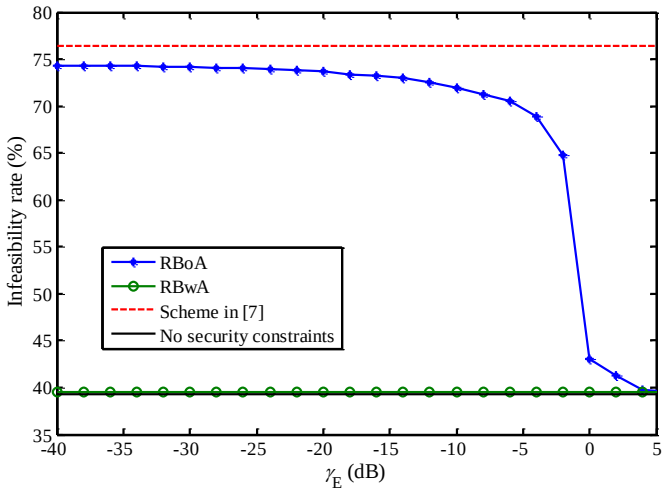


Fig. 6. Comparison of the infeasibility rates of the proposed schemes and the scheme in [7]

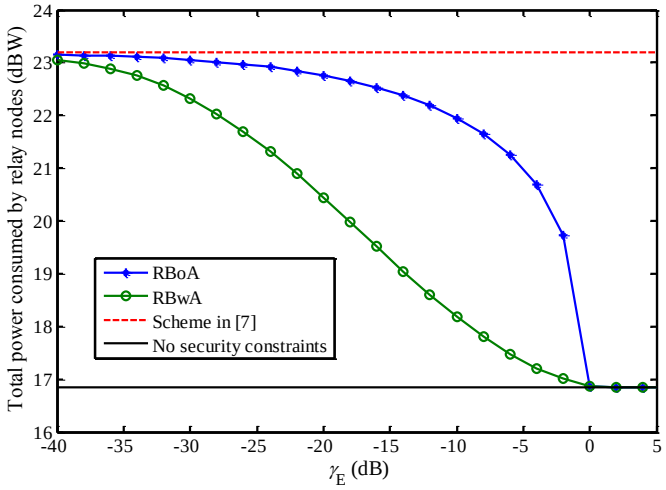


Fig. 7. Comparison of the total power consumed by the relay nodes of the proposed schemes and the scheme in [7]

5. Conclusions

This paper studied the relay beamforming design for multi-relay two-way relay networks in the presence of an eavesdropper. We presented two beamfoming methods, i.e., RBoA and RBwA. The received SINR at the receiver was used as the security and QoS measurement. We formulated optimization problems for the two methods to optimally design beamforming vectors and artificial noise vector to minimize the total energy consumption. SDP relaxation theory was used for solving the problems. Simulation results demonstrated the effectiveness of our proposed schemes and showed that RBwA outperforms RBoA in terms of high power efficiency and low infeasibility rate, which indicated that by jointly design the artificial noise and beamforming vector, the performance secure bemforming for two-way relay systems can be greatly improved.

References

[1] A. D. Wyner, "The wire-tap channel," *Bell System Technical Journal*, vol. 54, no. 8, pp. 1355-1387, 1975. Article (CrossRef Link)

[2] A. Khisti, and G. Wornell, "Secure transmission with multiple antennas I: the MISOME wiretap channel," *IEEE Transactions on Information Theory*, vol. 56, no. 7, pp. 2088-2104, 2010. Article (CrossRef Link)

[3] F. Oggier, and B. Hassibi, "The secrecy capacity of the MIMO wiretap channel," *IEEE Transactions on Information Theory*, vol. 57, no. 8, pp. 4961-4972, 2011. Article (CrossRef Link)

[4] L. Dong, Z. Han, A. P. Petropulu, and H. V. Poor, "Amplify-and-forward based cooperation for secure wireless communications," in *Proc. of IEEE Int. Conf. on Acoustics, Speech, and Signal Processing*, pp. 2613 - 2616, April 19-24, 2009. Article (CrossRef Link)

[5] J. Zhang, and M. C. Gursoy, "Collaborative relay beamforming for secure broadcasting," in *Proc. of IEEE Wireless Communications and Networking Conf.*, pp. 1-6, April, 18-21, 2010. Article (CrossRef Link)

[6] L. Dong, Z. Han, A. P. Petropulu, and H. V. Poor,, "Improving wireless physical layer security via cooperating relays," *IEEE Transactions on Signal Processing*, vol. 58, no. 3, pp. 1875-1888, 2010. Article (CrossRef Link)

[7] H. Wang, Q. Yin, and X. Xia, "Improving the physical-layer security of wireless two-way relaying via analog network coding," in *Proc. of IEEE Global Telecommunications Conf.*, pp. 1-6, December 5-9, 2011. Article (CrossRef Link)

[8] W.-C. Liao, T.-H Chang, W.-K. Ma, and C.-Y. Chi, "Joint transmit beamforming and artificial noise design for QoS discrimination in wireless downlink," in *Proc. of IEEE Int. Conf. on Acoustics, Speech, and Signal Processing*,, pp. 2562-2565, March 14-19, 2010. Article (CrossRef Link)

[9] W.-C. Liao, T.-H Chang, W.-K. Ma, and C.-Y. Chi, "QoS-based transmit beamforming in the presence of eavesdroppers: an optimized artificial-noise-aided approach," *IEEE Transactions on Signal Processing*, vol. 59, no. 3, pp. 1202-1216, 2011. Article (CrossRef Link)

[10] M. Bloch, J. O. Barros, M. R. D. Rodrigues, and S. W. McLaughlin, "Wireless information-theoretic security," *IEEE Transactions on Information Theory*, vol.54, no. 6, pp. 2515–2534, June 2008. Article (CrossRef Link)

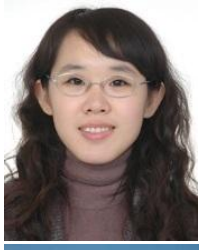
[11] Z.-Q. Luo, W.-K. Ma, A. So, Y. Ye, and S. Zhang, "Semidefinite relaxation of quadratic optimization problems," *IEEE Signal Processing Magazine*, vol. 27, no. 3, pp. 20-34, 2010. Article (CrossRef Link)

[12] Y. Huang, and D. P. Palomar, "Rank-constrained separable semidefinite programming with applications to optimal beamforming," *IEEE Transactions on Signal Processing*, vol. 58, no. 2, pp. 664-678, 2010. Article (CrossRef Link)

[13] M. Grant, and S. Boyd, CVX: MATLAB software for disciplined, Convex Programming, June 2009. Article (CrossRef Link)

Dandan Li received her BS degree in computer science from Beijing Jiaotong University (BJTU), Beijing, China, in June 2007. She is currently pursuing for the Ph.D degree in Information and Communication Engineering. Her research interests include wireless relay networks, wireless network coding, et al.

Ke Xiong received his BS degree and PhD degree in computer science from BJTU, Beijing, China, in June 2004 and Jan. 2010, respectively. He worked as a postdoc research fellow Department of E.E., Tsinghua University, Beijing, China, from April 2010 to Mar. 2013. Now, he is an asistant professor with School of Computer and Information Technology, BJTU. His research interests include wireless relay networks, wireless network coding. multimedia communication and processing, next-generation Internet, and digital signal processing.



Guanyao Du received her BS degree in computer science from BJTU, Beijing, China, in June 2008. She is currently pursuing for the Ph.D degree in Information and Communication Engineering. Her research interests include wireless relay networks, wireless network coding, et al.

Zhengding Qiu received the BS and MS degrees from BJTU, Beijing, in 1967 and 1981, respectively. Since 1981, he has worked at Institute of Information Science, BJTU, where he became a full professor in 1991. He was a research scholar of Pittsburgh University, USA, and a visiting research fellow of Kent University, UK, from 1989 to 1991 and from 1999 to 2000, respectively. He is currently a fellow of the Chinese Institute of Communications and a senior member of Chinese Institute of Electronics and Railway. His research interests include digital signal processing, multimedia communication & processing and parallel processing.