IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received March 15, 2019, accepted April 4, 2019, date of publication April 11, 2019, date of current version April 25, 2019.

Digital Object Identifier 10.1109/ACCESS.2019.2910758

Secure Transmission Schemes for Two-Way Relay Networks

MIAO LUO[1], XIAOPING LI[2], JIANQUAN WANG[3], QINYE YIN[1], WANBIN TANG[3], AND SHAOQIAN LI[3], (Fellow, IEEE)

[1]School of Electronic and Information Engineering, Xi'an Jiaotong University, Xi'an 710049, China
[2]School of Mathematical Science, University of Electronic Science and Technology of China, Chengdu 611731, China
[3]National Key Laboratory of Science and Technology on Communications, University of Electronic Science and Technology of China, Chengdu 611731, China

Corresponding author: Xiaoping Li (lixiaoping.math@uestc.edu.cn)

This work was supported in part by the NSFC under Grant 61701086 and Grant 61271169, and in part by the Fundamental Research Funds for the Central Universities under Grant ZYGX2016KYQD143.

ABSTRACT We investigate the physical-layer security problems of two-way relay networks in this paper. The whole network consists of two legitimate users and one eavesdropper, where the legal users need the help of some intermediate nodes to exchange information. We propose joint jamming and relaying mechanism, where a jamming node is selected from all intermediate nodes, to create interference upon eavesdropper, while other nodes are used to relay data for two users. All intermediate nodes are subjected to per-node power constraints. Based on null-space beamforming, we propose two different transmission schemes when the number of relay nodes is large enough. One scheme is designed to maximize the secrecy sum rate (MSSR) of the network, and the other is designed to maximize the minimum secrecy rate (MMSR) between two users. In the MMSR scheme, a series of semi-definite programming problems with a rank-1 constraint needs to be solved. We prove that this rank-1 constraint does not affect the solutions of original problems. In addition, we propose two modified secure transmission schemes when the number of relay nodes is less abundant. In short, no matter how many intermediate nodes in the communication networks, one can find suitable transmission schemes to ensure communication security.

INDEX TERMS Jamming, null-space beamforming, physical-layer security, relay, two-way networks, wireless communication.

I. INTRODUCTION

Transmission security plays an important role in wireless networks, due to its openness and broadcasting characteristics of wireless channels. In recent years, secure communication has become more and more important with the wide application of mobile devices. The purpose of secure communication is to enable legitimate users successfully receiving their desired data, while the eavesdroppers are not able to interpret them. Physical-layer security is a complement to traditional data encryption technology in the field of secure communication [1]. Traditional encryption technology adopted in upper layers relies on the computing power of users. It may become vulnerable because computing machines are becoming more and more powerful in modern times.

Physical-layer security is based on the concept of secrecy capacity, which was first introduced by Shannon in 1949 [2].

The associate editor coordinating the review of this manuscript and approving it for publication was Cristina Rottondi.

The basic idea of physical-layer security is to exploit the physical characteristics of channels to transmit messages securely. Physical-layer security has been studied extensively for several decades [3]–[8]. Most of researches in physical-layer security concentrate on two aspects: secure beamforming and jamming (aritificial noises). The latter is used mainly to deteriorate the channel quality of eavesdroppers, while the former can usually both improve the communication quality of legitimate users and reduce information leakage to eavesdroppers. In this paper, we focus on the physical-layer security in two-way relay networks. In [9]–[11], the authors proposed secure beamforming designs for two-way relay networks. However, in [9], one complete information transmission between legitimate users requires three time slots, while in our paper two phases are needed. In Phase 1, the two source nodes transmits data to relays; in Phase 2, the relays retransmit a weighted version of the data they heard in Phase 1 to their corresponding destination nodes. We use the amplify-and-forward (AF)

protocol here, while in some papers, decode-and-forward (DF) protocol was considered [12], [13].

All of the investigations in [10], [11] based on the assumption that all the relay nodes in whole communication system under a total power constraint. The total transmitting power of all relay nodes in the network is below a threshold value and can be allocated freely among all relay nodes. Motivated by these works, we consider per-node power constraints of intermediate nodes in this paper. In other words, every intermediate node has its own power constraint. When the number of intermediate nodes is abundant for null-space beamforming, we propose two different cooperative relaying and jamming schemes under per-node power constraints. The first one is to maximize the secrecy sum rate (MSSR) of the whole communication system. The second one is to maximize the minimum secrecy rate (MMSR) between the two legal users. Besides, the two modified transmission schemes to enhance the security performance for less number of intermediate nodes are presented. In [11], a multi-antenna beamforming scheme was adopted to maximize the secrecy rate of the relay networks. However, in some communication networks, multiple antennas are unavailable due to the size and complexity constraints of the transmitter. In this paper, all the nodes are equipped with a single antenna. Moreover, single-antenna nodes and multi-node cooperation are used to construct one virtual multi-antenna distributed system, thereby enhancing the security performance of a relay network.

It is worth mentioning that, in the vast majority of existing relay-and-jamming security communication works, few of them consider the problem of insufficient number of communication nodes. This potential situation is generally ignored when the number of antennas available is insufficient. While in our paper, no matter how many intermediate nodes in the communication networks, one can find suitable transmission schemes to ensure communication security of the networks.

The rest of the paper is organized as follows. In Section II, we introduce the system model of the two-way relay networks to be studied. In Section III, based on null-space beamforming, we propose two different secure transmission schemes MSSR and MMSR when the number of relay nodes is large enough. In Section IV, we propose two modified schemes for a less abundant relays. Numerical results are presented in Section V, and Section VI concludes our work.

II. SYSTEM MODEL

We consider the secure communication problem of a two-way wireless wire-tap network. The communication system consists of two legitimate users, $\mathbb{T}_1$ and $\mathbb{T}_2$, and one eavesdropper $\mathbb{E}$, as shown in Fig. 1. In the model, $\mathbb{T}_1$ and $\mathbb{T}_2$ want to communicate with each other. However, there is no direct link between them due to far distance or other reasons [14], [15], they can only communicate by the aid of N intermediate nodes. $\mathbb{T}_1$, $\mathbb{T}_2$, $\mathbb{E}$, and N intermediate nodes in the whole wireless network are all equipped with a single antenna, which operate in a half-duplex mode.

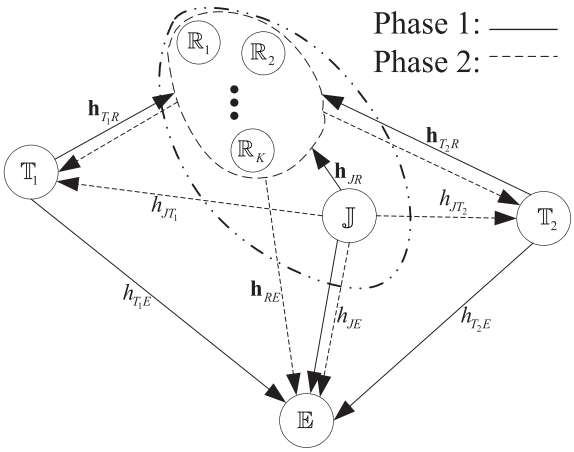

FIGURE 1. System model of a two-way network.

One complete communication process between $\mathbb{T}_1$, $\mathbb{T}_2$ requires two consecutive phases. In Phase 1, legitimate users $\mathbb{T}_1$ and $\mathbb{T}_2$ transmit their signals s_1, s_2 simultaneously, N intermediate nodes and $\mathbb{E}$ can both receive the data, we normalize $E\{|s_i|^2\} = 1$ for $i = 1, 2$, where $E(\cdot)$ is the mathematical expectation of a random variable. At the same time, the jamming node $\mathbb{J}$ sends interference signal z_1 to confuse the eavesdropper $\mathbb{E}$. The data transmission process of Phase 1 is shown in Fig. 1 with solid line. We select a node $\mathbb{J}$ from all N intermediate nodes to create intentional interference upon $\mathbb{E}$, while other $K = N - 1$ intermediate nodes operate in relay mode to help $\mathbb{T}_1$, $\mathbb{T}_2$ delivering data to corresponding destination nodes using an amplify-and-forward (AF) protocol. In what follows, $\boldsymbol{h}_{i,j}(h_{i,j})$ represents the channel gain between nodes i and j, where $i = \mathbb{T}_1, \mathbb{T}_2, \mathbb{R}, \mathbb{J}$ and $j = \mathbb{R}, \mathbb{T}_1, \mathbb{T}_2, \mathbb{E}$. The former lowercase bold-faced $\boldsymbol{h}$ denotes a column vector and the latter represents a number. All channel coefficients $\boldsymbol{h}_{i,j}(h_{i,j})$ are assumed to undergo flat fading and are quasistatic, which follow 0-mean, circularly symmetric complex Gaussian random variables with variance equals one [13].

Time division duplex (TDD) mode is adopted in this system so that the channels are reciprocal [16], [17], i.e., $\boldsymbol{h}_{RT_1} = \boldsymbol{h}_{T_1R}^T$, $\boldsymbol{h}_{RT_2} = \boldsymbol{h}_{T_2R}^T$. Superscript in $\boldsymbol{h}^T$ denotes the transposition of $\boldsymbol{h}$. In this paper, we assume global channel state information (CSI) is available by channel estimation technology [18]–[21]. This assumption corresponds to the scenario when the 'eavesdropper' is actually a legitimate user in the communication network but not be allowed to get specific information sometimes, i.e., it is not the target user. The received signals of K relay nodes and $\mathbb{E}$ in Phase 1 are

$$\boldsymbol{y}_R = \sqrt{P_T}\boldsymbol{h}_{T_1R}s_1 + \sqrt{P_T}\boldsymbol{h}_{T_2R}s_2 + \sqrt{P_J^{(1)}}\boldsymbol{h}_{JR}z_1 + \boldsymbol{n}_R, \quad (1)$$

and

$$y_E^{(1)} = \sqrt{P_T}h_{T_1E}s_1 + \sqrt{P_T}h_{T_2E}s_2 + \sqrt{P_J^{(1)}}h_{JE}z_1 + n_E^{(1)}, \quad (2)$$

where P_T denotes the transmitting power of source nodes $\mathbb{T}_1$ and $\mathbb{T}_2$; $P_J^{(1)}$ is the transmitting power of jamming node $\mathbb{J}$ in

$$
\begin{aligned}
y_{T_1} &= \sqrt{P_T}\boldsymbol{h}_{RT_1}\mathrm{diag}\{\boldsymbol{w}\}\boldsymbol{h}_{T_1R}s_1 + \sqrt{P_T}\boldsymbol{h}_{RT_1}\mathrm{diag}\{\boldsymbol{w}\}\boldsymbol{h}_{T_2R}s_2 + \sqrt{P_J^{(1)}}\boldsymbol{h}_{RT_1}\mathrm{diag}\{\boldsymbol{w}\}\boldsymbol{h}_{JR}z_1 + \sqrt{P_J^{(2)}}h_{JT_1}z_2 + \bar{n}_{T_1} \\
&= \sqrt{P_T}\boldsymbol{h}_{RT_1}\mathrm{diag}\{\boldsymbol{h}_{T_1R}\}\boldsymbol{w}s_1 + \sqrt{P_T}\boldsymbol{h}_{RT_1}\mathrm{diag}\{\boldsymbol{h}_{T_2R}\}\boldsymbol{w}s_2 + \sqrt{P_J^{(1)}}\boldsymbol{h}_{RT_1}\mathrm{diag}\{\boldsymbol{h}_{JR}\}\boldsymbol{w}z_1 + \sqrt{P_J^{(2)}}h_{JT_1}z_2 + \bar{n}_{T_1} \\
&= \boldsymbol{a}_1^{\dagger}\boldsymbol{w}s_1 + \boldsymbol{b}_1^{\dagger}\boldsymbol{w}s_2 + \boldsymbol{c}_1^{\dagger}\boldsymbol{w}z_1 + \sqrt{P_J^{(2)}}h_{JT_1}z_2 + \bar{n}_{T_1}, \qquad (3) \\
y_{T_2} &= \sqrt{P_T}\boldsymbol{h}_{RT_2}\mathrm{diag}\{\boldsymbol{w}\}\boldsymbol{h}_{T_1R}s_1 + \sqrt{P_T}\boldsymbol{h}_{RT_2}\mathrm{diag}\{\boldsymbol{w}\}\boldsymbol{h}_{T_2R}s_2 + \sqrt{P_J^{(1)}}\boldsymbol{h}_{RT_2}\mathrm{diag}\{\boldsymbol{w}\}\boldsymbol{h}_{JR}z_1 + \sqrt{P_J^{(2)}}h_{JT_2}z_2 + \bar{n}_{T_2} \\
&= \sqrt{P_T}\boldsymbol{h}_{RT_2}\mathrm{diag}\{\boldsymbol{h}_{T_1R}\}\boldsymbol{w}s_1 + \sqrt{P_T}\boldsymbol{h}_{RT_2}\mathrm{diag}\{\boldsymbol{h}_{T_2R}\}\boldsymbol{w}s_2 + \sqrt{P_J^{(1)}}\boldsymbol{h}_{RT_2}\mathrm{diag}\{\boldsymbol{h}_{JR}\}\boldsymbol{w}z_1 + \sqrt{P_J^{(2)}}h_{JT_2}z_2 + \bar{n}_{T_2} \\
&= \boldsymbol{a}_2^{\dagger}\boldsymbol{w}s_1 + \boldsymbol{b}_2^{\dagger}\boldsymbol{w}s_2 + \boldsymbol{c}_2^{\dagger}\boldsymbol{w}z_1 + \sqrt{P_J^{(2)}}h_{JT_2}z_2 + \bar{n}_{T_2}, \qquad (4) \\
y_E^{(2)} &= \sqrt{P_T}\boldsymbol{h}_{RE}\mathrm{diag}\{\boldsymbol{w}\}\boldsymbol{h}_{T_1R}s_1 + \sqrt{P_T}\boldsymbol{h}_{RE}\mathrm{diag}\{\boldsymbol{w}\}\boldsymbol{h}_{T_2R}s_2 + \sqrt{P_J^{(1)}}\boldsymbol{h}_{RE}\mathrm{diag}\{\boldsymbol{w}\}\boldsymbol{h}_{JR}z_1 + \sqrt{P_J^{(2)}}h_{JE}z_2 + \bar{n}_E^{(2)} \\
&= \sqrt{P_T}\boldsymbol{h}_{RE}\mathrm{diag}\{\boldsymbol{h}_{T_1R}\}\boldsymbol{w}s_1 + \sqrt{P_T}\boldsymbol{h}_{RE}\mathrm{diag}\{\boldsymbol{h}_{T_2R}\}\boldsymbol{w}s_2 + \sqrt{P_J^{(1)}}\boldsymbol{h}_{RE}\mathrm{diag}\{\boldsymbol{h}_{JR}\}\boldsymbol{w}z_1 + \sqrt{P_J^{(2)}}h_{JE}z_2 + \bar{n}_E^{(2)} \\
&= \boldsymbol{a}_E^{\dagger}\boldsymbol{w}s_1 + \boldsymbol{b}_E^{\dagger}\boldsymbol{w}s_2 + \boldsymbol{c}_E^{\dagger}\boldsymbol{w}z_1 + \sqrt{P_J^{(2)}}h_{JE}z_2 + \bar{n}_E^{(2)}. \qquad (5)
\end{aligned}
$$

this phase; $\boldsymbol{n}_R$ is the additive white Gaussian noise (AWGN) at K relay nodes, all the elements in $\boldsymbol{n}_R$ are assumed to be mutually independent complex Gaussian random variables with 0-mean and variance equals 1; $n_E^{(1)}$ is AWGN at $\mathbb{E}$ in Phase 1.

In Phase 2, K relay nodes amplify their received signal with weighting coefficients $\mathrm{diag}\{\boldsymbol{w}\}$, where $\boldsymbol{w} = [w_1, w_2, \ldots, w_K]^T$ and $\mathrm{diag}\{\cdot\}$ denotes a diagonal matrix with diagonal elements $\{\cdot\}$. Then, their re-transmitting signal is $\boldsymbol{x}_R = \mathrm{diag}\{\boldsymbol{w}\}\boldsymbol{y}_R$. The jamming node $\mathbb{J}$ sends interference signal z_2 at the same time to deteriorate the channel condition of $\mathbb{E}$, denoted by the dotted line in Fig. 1. The received signals at $\mathbb{T}_1$, $\mathbb{T}_2$ and $\mathbb{E}$ are expressed in (3)-(5), as shown at the top of this page with $\boldsymbol{a}_1 \triangleq \sqrt{P_T}\mathrm{diag}\{\boldsymbol{h}_{T_1R}^{\dagger}\}\boldsymbol{h}_{RT_1}^{\dagger}$, $\boldsymbol{b}_1 \triangleq \sqrt{P_T}\mathrm{diag}\{\boldsymbol{h}_{T_2R}^{\dagger}\}\boldsymbol{h}_{RT_1}^{\dagger}$, $\boldsymbol{c}_1 \triangleq \sqrt{P_J^{(1)}}\mathrm{diag}\{\boldsymbol{h}_{JR}^{\dagger}\}\boldsymbol{h}_{RT_1}^{\dagger}$, $\boldsymbol{a}_2 \triangleq \sqrt{P_T}\mathrm{diag}\{\boldsymbol{h}_{T_1R}^{\dagger}\}\boldsymbol{h}_{RT_2}^{\dagger}$, $\boldsymbol{b}_2 \triangleq \sqrt{P_T}\mathrm{diag}\{\boldsymbol{h}_{T_2R}^{\dagger}\}\boldsymbol{h}_{RT_2}^{\dagger}$, $\boldsymbol{c}_2 \triangleq \sqrt{P_J^{(1)}}\mathrm{diag}\{\boldsymbol{h}_{JR}^{\dagger}\}\boldsymbol{h}_{RT_2}^{\dagger}$, $\boldsymbol{a}_E \triangleq \sqrt{P_T}\mathrm{diag}\{\boldsymbol{h}_{T_1R}^{\dagger}\}\boldsymbol{h}_{RE}^{\dagger}$, $\boldsymbol{b}_E \triangleq \sqrt{P_T}\mathrm{diag}\{\boldsymbol{h}_{T_2R}^{\dagger}\}\boldsymbol{h}_{RE}^{\dagger}$, $\boldsymbol{c}_E \triangleq \sqrt{P_J^{(1)}}\mathrm{diag}\{\boldsymbol{h}_{JR}^{\dagger}\}\boldsymbol{h}_{RE}^{\dagger}$, $\bar{n}_{T_1} = \boldsymbol{h}_{RT_1}\mathrm{diag}\{\boldsymbol{w}\}\boldsymbol{n}_R + n_{T_1}$, $\bar{n}_{T_2} = \boldsymbol{h}_{RT_2}\mathrm{diag}\{\boldsymbol{w}\}\boldsymbol{n}_R + n_{T_2}$, $\bar{n}_E^{(2)} = \boldsymbol{h}_{RE}\mathrm{diag}\{\boldsymbol{w}\}\boldsymbol{n}_R + n_E^{(2)}$. Superscript in $\boldsymbol{h}^{\dagger}$ denotes the conjugate transposition of $\boldsymbol{h}$. n_{T_1}, n_{T_2}, $n_E^{(2)}$ are AWGN at $\mathbb{T}_1$, $\mathbb{T}_2$, and $\mathbb{E}$ in Phase 2, respectively. They are assumed following 0-mean random variables with variance 1. Hence, the total power consumed by all K relay nodes is

$$
\begin{aligned}
P_r &= \|\boldsymbol{x}_R\|^2 \\
&= \boldsymbol{w}^{\dagger}\left(P_T\boldsymbol{R}_{T_1T_1} + P_T\boldsymbol{R}_{T_2T_2} + P_J^{(1)}\boldsymbol{R}_{JJ} + \sigma^2\boldsymbol{I}\right)\boldsymbol{w} \\
&= \boldsymbol{w}^{\dagger}\boldsymbol{T}\boldsymbol{w}, \qquad (6)
\end{aligned}
$$

where $\boldsymbol{R}_{T_1T_1} \triangleq \mathrm{diag}\{\boldsymbol{h}_{T_1R}\}\mathrm{diag}\{\boldsymbol{h}_{T_1R}^*\}$, $\boldsymbol{R}_{T_2T_2} \triangleq \mathrm{diag}\{\boldsymbol{h}_{T_2R}\}\mathrm{diag}\{\boldsymbol{h}_{T_2R}^*\}$, $\boldsymbol{R}_{JJ} \triangleq \mathrm{diag}\{\boldsymbol{h}_{JR}\}\mathrm{diag}\{\boldsymbol{h}_{JR}^*\}$, $\boldsymbol{h}^*$ indicates conjugation of $\boldsymbol{h}$,

$$
\boldsymbol{T} \triangleq P_T\boldsymbol{R}_{T_1T_1} + P_T\boldsymbol{R}_{T_2T_2} + P_J^{(1)}\boldsymbol{R}_{JJ} + \sigma^2\boldsymbol{I} \qquad (7)
$$

and $\boldsymbol{I}$ denoting the identity matrix. The n-th relay node's transmitting power can be written as $\left[\boldsymbol{w}\boldsymbol{w}^{\dagger}\right]_{n,n}[\boldsymbol{T}]_{n,n}$ with constrained power $P_R(n)$, where $[\boldsymbol{A}]_{n,n}$ denotes the (n, n)-th element of matrix $\boldsymbol{A}$, and $n = 1, 2, \ldots, K$.

Note that $\mathbb{T}_1$ and $\mathbb{T}_2$ know their own transmitting signals and CSI, and $\boldsymbol{w}$ can be calculated by their available CSI. Hence, $\mathbb{T}_1$ and $\mathbb{T}_2$ can subtract the resulting self-interference components $\boldsymbol{a}_1^{\dagger}\boldsymbol{w}s_1$ and $\boldsymbol{b}_2^{\dagger}\boldsymbol{w}s_2$ from (3) and (4) as in [18], [22]. After removing the self-interference components, the final obtained information of $\mathbb{T}_1$, $\mathbb{T}_2$ are

$$
\tilde{y}_{T_1} = \boldsymbol{b}_1^{\dagger}\boldsymbol{w}s_2 + \boldsymbol{c}_1^{\dagger}\boldsymbol{w}z_1 + \sqrt{P_J^{(2)}}h_{JT_1}z_2 + \bar{n}_{T_1}, \qquad (8)
$$

$$
\tilde{y}_{T_2} = \boldsymbol{a}_2^{\dagger}\boldsymbol{w}s_1 + \boldsymbol{c}_2^{\dagger}\boldsymbol{w}z_1 + \sqrt{P_J^{(2)}}h_{JT_2}z_2 + \bar{n}_{T_2}. \qquad (9)
$$

Next, we propose two secure communication schemes based on the system models in Fig. 1.

III. SECURE BEAMFORMING SCHEMES WHEN $K \geq 3$

In this paper, we adopt the achievable secrecy rate as the measure to consider the security transmission problems of two-way relay networks, which is common in the measurement of security performances in networks [23], [24]. It is worth mentioning that, secure transmission performance measures can be total error rate of the two communication links, the smaller end-to-end SNR of the two communication links or the outage probability of the network, for example, in [25]–[27].

Let $I(X; Y)$ be the mutual information between X and Y, where X is the source input, Y is the channel output at target user or the eavesdropper. Then, the instantaneous secrecy rate for the source node $\mathbb{T}_i$ can be expressed as [28]

$$
\begin{aligned}
R_{T_i} &= \left[I\left(\tilde{y}_{T_i}; s_j\right) - I\left(y_E^j; s_j\right)\right]^+ \\
&= \left[\frac{1}{2}\log_2\left(1 + \Gamma_i\right) - \frac{1}{2}\log_2\left(1 + \Gamma_E^j\right)\right]^+, \qquad (10)
\end{aligned}
$$

where $i, j = 1, 2, i \neq j$, $[a]^+ = \max(0, a)$; Γ_i denotes the signal to interference-plus-noise ratio (SINR) of the "virtual" channel $\mathbb{T}_j$ to $\mathbb{T}_i$; Γ_E^j denotes the SINR of the channel $\mathbb{T}_j$ to $\mathbb{E}$. The overall secrecy performance of the system is characterized by achievable secrecy sum rate, which is the sum of the two sources' secrecy rate:

$$R_{sum} = R_{T_1} + R_{T_2}. \tag{11}$$

Assuming P_T, $P_J^{(1)}$ and $P_J^{(2)}$ are fixed. Then, R_{sum} is a function of weighting coefficients $\boldsymbol{w}$. Hence, the objective is to determine $\boldsymbol{w}$ maximizing $R_{sum}(\boldsymbol{w})$ of this wireless communication network, subjecting to per-node power constraints $P_R = [P_R(1), P_R(2), \ldots, P_R(K)]$, i.e.,

$$\begin{aligned} &\max_{\boldsymbol{w}} R_{sum}(\boldsymbol{w}) \\ &s.t. \left[\boldsymbol{w}\boldsymbol{w}^\dagger\right]_{n,n} [\boldsymbol{T}]_{n,n} \leq P_R(n), \quad n = 1, 2, \ldots, K \end{aligned} \tag{12}$$

To obtain $R_{sum}(\boldsymbol{w})$, we need to get R_{T_1} and R_{T_2} according to (11). Hence, $I\left(\tilde{y}_{T_i}; s_j\right)$ and $I\left(y_E^j; s_j\right)$ in (10) should be calculated, which are given below.

According to $\tilde{y}_{T_i}$ in (8)-(9), $I\left(\tilde{y}_{T_i}; s_j\right)$ are

$$\begin{aligned} I\left(\tilde{y}_{T_1}; s_2\right) &= \frac{1}{2}\log_2\left(1+\Gamma_1\right) \\ &= \frac{1}{2}\log_2\left(1 + \frac{\boldsymbol{w}^\dagger \boldsymbol{R}_{b_1}\boldsymbol{w}}{\boldsymbol{w}^\dagger \boldsymbol{R}_{c_1}\boldsymbol{w} + P_J^{(2)}\left|h_{JT_1}\right|^2 + \boldsymbol{w}^\dagger \boldsymbol{R}_{T_1T_1}\boldsymbol{w} + 1}\right) \\ &= \frac{1}{2}\log_2\left(1 + \frac{\gamma_{T_2,T_1}}{\gamma_{J_1,T_1} + \gamma_{J_2,T_1} + \gamma_{R,T_1} + 1}\right) \end{aligned} \tag{13}$$

and

$$\begin{aligned} I\left(\tilde{y}_{T_2}; s_1\right) &= \frac{1}{2}\log_2\left(1+\Gamma_2\right) \\ &= \frac{1}{2}\log_2\left(1 + \frac{\boldsymbol{w}^\dagger \boldsymbol{R}_{a_2}\boldsymbol{w}}{\boldsymbol{w}^\dagger \boldsymbol{R}_{c_2}\boldsymbol{w} + P_J^{(2)}\left|h_{JT_2}\right|^2 + \boldsymbol{w}^\dagger \boldsymbol{R}_{T_2T_2}\boldsymbol{w} + 1}\right) \\ &= \frac{1}{2}\log_2\left(1 + \frac{\gamma_{T_1,T_2}}{\gamma_{J_1,T_2} + \gamma_{J_2,T_2} + \gamma_{R,T_2} + 1}\right), \end{aligned} \tag{14}$$

where $\boldsymbol{R}_{b_1} \triangleq \boldsymbol{b}_1\boldsymbol{b}_1^\dagger$, $\boldsymbol{R}_{c_1} \triangleq \boldsymbol{c}_1\boldsymbol{c}_1^\dagger$, $\boldsymbol{R}_{a_2} \triangleq \boldsymbol{a}_2\boldsymbol{a}_2^\dagger$, and $\boldsymbol{R}_{c_2} \triangleq \boldsymbol{c}_2\boldsymbol{c}_2^\dagger$. Note that $\gamma_{i,j}$ indicates the total power consumed by transmitting signals of channel $\boldsymbol{h}_{i,j}$. Then, $\gamma_{J_1,j}$, $\gamma_{J_2,j}$ means the total power consumed by jamming node $\mathbb{J}$ in Phase 1 and Phase 2, respectively. It is not difficult to obtain that

$$\begin{aligned} &\gamma_{T_2,T_1} = \boldsymbol{w}^\dagger \boldsymbol{R}_{b_1}\boldsymbol{w}, \gamma_{J_1,T_1} = \boldsymbol{w}^\dagger \boldsymbol{R}_{c_1}\boldsymbol{w}, \gamma_{J_2,T_1} = P_J^{(2)}\left|h_{JT_1}\right|^2, \\ &\gamma_{R,T_1} = \boldsymbol{w}^\dagger \boldsymbol{R}_{T_1T_1}\boldsymbol{w}, \gamma_{T_1,T_2} = \boldsymbol{w}^\dagger \boldsymbol{R}_{a_2}\boldsymbol{w}, \gamma_{J_1,T_2} = \boldsymbol{w}^\dagger \boldsymbol{R}_{c_2}\boldsymbol{w}, \\ &\gamma_{J_2,T_2} = P_J^{(2)}\left|h_{JT_2}\right|^2, \gamma_{R,T_2} = \boldsymbol{w}^\dagger \boldsymbol{R}_{T_2T_2}\boldsymbol{w}. \end{aligned}$$

Hence, Γ_i in (10) can be described as

$$\Gamma_i = \frac{\gamma_{T_j,T_i}}{\gamma_{J_1,T_i} + \gamma_{J_2,T_i} + \gamma_{R,T_i} + 1}. \tag{15}$$

Remark 1: Since $\boldsymbol{b}_1 \triangleq \sqrt{P_T}\mathrm{diag}\{\boldsymbol{h}_{T_2R}^\dagger\}\boldsymbol{h}_{RT_1}^\dagger$, $\boldsymbol{a}_2 \triangleq \sqrt{P_T}\mathrm{diag}\{\boldsymbol{h}_{T_1R}^\dagger\}\boldsymbol{h}_{RT_2}^\dagger$, and channels are reciprocal under the TDD mode, we have

$$\gamma_{T_2,T_1} = \boldsymbol{w}^\dagger \boldsymbol{R}_{b_1}\boldsymbol{w} = \boldsymbol{w}^\dagger \boldsymbol{R}_{a_2}\boldsymbol{w} = \gamma_{T_1,T_2}.$$

This implies that the total power consumed by transmitting data from $\mathbb{T}_2$ to $\mathbb{T}_1$ is the same as that from $\mathbb{T}_1$ to $\mathbb{T}_2$.

Next, we give the value of $I\left(y_E^j; s_j\right)$ in (10). In that follows, we consider a simple case in which eavesdropper $\mathbb{E}$ applies maximal ratio combining (MRC) to its received signals in Phase 1 and Phase 2 [29].

According to MRC, $\mathbb{E}$ combines the received signals by multiplying $y_E^{(1)}$ in (2) and $y_E^{(2)}$ in (5) with weighting factors k_1^j and k_2^j, respectively. The combined eavesdropping signal is

$$y_E^j = k_1^j y_E^{(1)} + k_2^j y_E^{(2)}, \tag{16}$$

where $k_1^2 = \frac{\sqrt{P_T}h_{T_2E}^\dagger}{\sigma_{e_1,s_1}^2}$, $k_2^2 = \frac{\boldsymbol{w}^\dagger \boldsymbol{b}_E}{\sigma_{e_2,s_1}^2}$, $k_1^1 = \frac{\sqrt{P_T}h_{T_1E}^\dagger}{\sigma_{e_1,s_2}^2}$, $k_2^1 = \frac{\boldsymbol{w}^\dagger \boldsymbol{a}_E}{\sigma_{e_2,s_2}^2}$. σ_{e_1,s_l}^2, $\sigma_{e_2,s_l}^2 (l = 1, 2)$ represent the total interference and noise terms caused by s_l in $y_E^{(1)}$ and $y_E^{(2)}$, respectively. Note that

$$\begin{aligned} \sigma_{e_1,s_1}^2 &= P_T|h_{T_1E}|^2 + P_J^{(1)}|h_{JE}|^2 + 1 \triangleq \gamma_{T_1,E} + \gamma_{J_1,E} + 1, \\ \sigma_{e_2,s_1}^2 &= \boldsymbol{w}^\dagger \boldsymbol{R}_{a_E}\boldsymbol{w} + \boldsymbol{w}^\dagger \boldsymbol{R}_{c_E}\boldsymbol{w} + P_J^{(2)}|h_{JE}|^2 + \boldsymbol{w}^\dagger \boldsymbol{R}_{RE}\boldsymbol{w} + 1 \\ &\triangleq \gamma_{T_1,R,E} + \gamma_{J,R,E} + \gamma_{J_2,E} + \gamma_{R,E} + 1 \\ \sigma_{e_1,s_2}^2 &= P_T|h_{T_2E}|^2 + P_J^{(1)}|h_{JE}|^2 + 1 \triangleq \gamma_{T_2,E} + \gamma_{J_1,E} + 1, \\ \sigma_{e_2,s_2}^2 &= \boldsymbol{w}^\dagger \boldsymbol{R}_{b_E}\boldsymbol{w} + \boldsymbol{w}^\dagger \boldsymbol{R}_{c_E}\boldsymbol{w} + P_J^{(2)}|h_{JE}|^2 + \boldsymbol{w}^\dagger \boldsymbol{R}_{RE}\boldsymbol{w} + 1 \\ &\triangleq \gamma_{T_2,R,E} + \gamma_{J,R,E} + \gamma_{J_2,E} + \gamma_{R,E} + 1, \end{aligned}$$

$\boldsymbol{R}_{a_E} \triangleq \boldsymbol{a}_E\boldsymbol{a}_E^\dagger$, $\boldsymbol{R}_{c_E} = \boldsymbol{c}_E\boldsymbol{c}_E^\dagger$, $\boldsymbol{R}_{RE} \triangleq \mathrm{diag}\{\boldsymbol{h}_{RE}\}\mathrm{diag}\{\boldsymbol{h}_{RE}^*\}$, and $\boldsymbol{R}_{b_E} = \boldsymbol{b}_E\boldsymbol{b}_E^\dagger$,

$$\begin{aligned} &\gamma_{T_1,E} = P_T|h_{T_1E}|^2, \gamma_{J_1,E} = P_J^{(1)}|h_{JE}|^2, \gamma_{T_1,R,E} = \boldsymbol{w}^\dagger \boldsymbol{R}_{a_E}\boldsymbol{w}, \\ &\gamma_{J,R,E} = \boldsymbol{w}^\dagger \boldsymbol{R}_{c_E}\boldsymbol{w}, \gamma_{J_2,E} = P_J^{(2)}|h_{JE}|^2, \gamma_{R,E} = \boldsymbol{w}^\dagger \boldsymbol{R}_{RE}\boldsymbol{w}, \\ &\gamma_{T_2,E} = P_T|h_{T_2E}|^2, \gamma_{T_2,R,E} = \boldsymbol{w}^\dagger \boldsymbol{R}_{b_E}\boldsymbol{w}. \end{aligned}$$

Hence, Γ_E^j in (10) can be described as

$$\begin{aligned} \Gamma_E^j &= \frac{\gamma_{T_j,E}}{\gamma_{T_i,E} + \gamma_{J_1,E} + 1} \\ &\quad + \frac{\gamma_{T_j,R,E}}{\gamma_{T_i,R,E} + \gamma_{J,R,E} + \gamma_{J_2,E} + \gamma_{R,E} + 1} \\ &= \upsilon_j + \frac{\gamma_{T_j,R,E}}{\gamma_{T_i,R,E} + \gamma_{J,R,E} + \gamma_{J_2,E} + \gamma_{R,E} + 1}. \end{aligned} \tag{17}$$

where $i, j = 1, 2, i \neq j$. Since CSI of $\mathbb{E}$ is available, we can design $\boldsymbol{w}$ in the null space of $\boldsymbol{a}_E^\dagger$ and $\boldsymbol{b}_E^\dagger$ to completely eliminate information leakage to eavesdropper according to (5). Let $\boldsymbol{a}_E^\dagger\boldsymbol{w} = \boldsymbol{b}_E^\dagger\boldsymbol{w} = 0$, $\boldsymbol{w} = \boldsymbol{Q}_\perp\boldsymbol{v}$, where $\boldsymbol{Q} \triangleq \left[\boldsymbol{a}_E^\dagger; \boldsymbol{b}_E^\dagger\right]$, and $\boldsymbol{Q}_\perp$ is the projection matrix onto the null space of $\boldsymbol{Q}$. Clearly, the columns of $\boldsymbol{Q}_\perp$ constitute an orthogonal basis for the null space of $\boldsymbol{Q}$, and $\boldsymbol{v}$ is any $K-2$ column vector. Note that this design leads to zero information leakage to $\mathbb{E}$ in Phase 2. Hence, it is not necessary to send z_2 in this phase. To this aim, we can set $P_J^{(2)} = 0$. Consequently, Γ_1 and Γ_2 in (15) can be simplified as

$$\Gamma_i = \frac{\gamma_{T_j,T_i}}{\gamma_{J_1,T_i} + \gamma_{R,T_i} + 1}, \tag{18}$$

and Γ_E^j in (17) can be simplified as $\Gamma_E^j = \upsilon_j$. Thus, $I\left(y_E^j; s_j\right)$ in (10) is a constant.

Remark 2: Observing (3) and (4), to eliminate the interference to $\mathbb{T}_1$ and $\mathbb{T}_2$ by z_1, we can further design $\boldsymbol{w}$ in the null space of $\boldsymbol{c}_1^\dagger$ and $\boldsymbol{c}_2^\dagger$, i.e.,

$$\boldsymbol{c}_1^\dagger \boldsymbol{w} = \boldsymbol{c}_2^\dagger \boldsymbol{w} = 0.$$

With all the above designs of $\boldsymbol{w}$, we have

$$\boldsymbol{w} = \boldsymbol{H}_\perp \boldsymbol{v}_1,$$

where $\boldsymbol{H} \triangleq \left[\boldsymbol{a}_E^\dagger; \boldsymbol{b}_E^\dagger; \boldsymbol{c}_1^\dagger; \boldsymbol{c}_2^\dagger\right]$, $\boldsymbol{v}_1$ is any $K-4$ column vector. This design needs more intermediate nodes for K must satisfying $K > 4$. More number requirement means more complexity of the whole communication system. Simulation results show that this design leads to no improvement of secure performance, we shall prove this phenomenon in later content.

A Simple Selection Criteria of Optimal $\mathbb{J}$: With the previous consideration and discussion, we have

$$\Gamma_E^j = \upsilon_j = \frac{P_T |h_{T_j E}|^2}{P_T |h_{T_i E}|^2 + P_J^{(1)} |h_{JE}|^2 + 1}. \tag{19}$$

To minimize the information leakage to eavesdropper $\mathbb{E}$, we should select a jamming node $\mathbb{J}$ by maximizing $|h_{JE}|$. The specific implementation process is as follows: we compare N channel coefficients from every intermediate node to $\mathbb{E}$ to find the biggest one. The node corresponding to the maximum coefficient is the optimal $\mathbb{J}$. Once $\mathbb{J}$ is determined, all other channel coefficients are determined accordingly.

According to (11) and (10), the achievable secrecy sum rate of two-way wireless relay network in Fig. 1 is

$$R_{sum}(\boldsymbol{w}) = \frac{1}{2}\log_2\left(\frac{1+\Gamma_1}{1+\upsilon_2}\right) + \frac{1}{2}\log_2\left(\frac{1+\Gamma_2}{1+\upsilon_1}\right). \tag{20}$$

Although the eavesdropper's mutual information is a constant υ_i, this secrecy sum rate is still a product of two correlated generalized Rayleigh quotient problems and thus difficult to be solved. Recall that the design $\boldsymbol{w} = \boldsymbol{Q}_\perp \boldsymbol{v}$ needs $K-2$ for K is a positive integer. Next, we will propose two different solvable schemes to guarantee the secure communication of the two-way relay network when $K - 2 \geq 1$.

A. MAXIMIZE SUM SECRECY RATE (MSSR)

The objective function of (20) is non-convex, we resort to an alternative method which is called "rate-split" [30] to solve this problem. The optimization problem can be formulated as

$$\begin{aligned}
&\max_{\boldsymbol{w}} R_{sum} \\
&s.t.\ R_{T_1} = \frac{1}{2}\log_2\left(\frac{1+\Gamma_1}{1+\upsilon_2}\right) \geq \eta R_{sum} && \text{(21a)} \\
&\quad R_{T_2} = \frac{1}{2}\log_2\left(\frac{1+\Gamma_2}{1+\upsilon_1}\right) \geq (1-\eta) R_{sum} && \text{(21b)} \\
&\quad \boldsymbol{w} = \boldsymbol{Q}_\perp \boldsymbol{v} && \text{(21c)} \\
&\quad \left[\boldsymbol{w}\boldsymbol{w}^\dagger\right]_{n,n} [\boldsymbol{T}]_{n,n} \leq P_R(n), \quad n = 1, \ldots, K, && \text{(21d)}
\end{aligned}$$

where η is the rate-split parameter, $0 \leq \eta \leq 1$. For any given η, the constraints (21a) (21b) impose a rate-split between two legitimate users $\mathbb{T}_1$ and $\mathbb{T}_2$; (21c) eliminates information leakage to $\mathbb{E}$ in Phase 2; (21d) represents the power constraints on each relay node.

The whole process consists of two parts. For the first part, η is changed from 0 to 1. By solving (21) under each fixed value of $\eta(k)$, we can get a series of $R_{sum}(\eta(k))$ with $\eta = [0, \delta, 2\delta, \ldots, 1]$, where δ is an extremely small positive real number. For the second part, we do one-dimensional comparison in all $R_{sum}(\eta(k))$ to find out the maximum $R_{sum}(\eta^o)$ under the optimal rate-split scheme η^o.

Next, we obtain $R_{sum}(\eta(k))$. Set R_{sum} to a fixed value r under $\eta(k)$, substituting Γ_1 and Γ_2 into (21), we get

$$\begin{aligned}
&\max_{\boldsymbol{w}} r \\
&s.t.\ \Gamma_1 = \frac{\boldsymbol{w}^\dagger \boldsymbol{R}_{b_1} \boldsymbol{w}}{\boldsymbol{w}^\dagger \boldsymbol{R}_{c_1} \boldsymbol{w} + \boldsymbol{w}^\dagger \boldsymbol{R}_{T_1 T_1} \boldsymbol{w} + 1} \geq \alpha_1 && \text{(22a)} \\
&\quad \Gamma_2 = \frac{\boldsymbol{w}^\dagger \boldsymbol{R}_{b_1} \boldsymbol{w}}{\boldsymbol{w}^\dagger \boldsymbol{R}_{c_2} \boldsymbol{w} + \boldsymbol{w}^\dagger \boldsymbol{R}_{T_2 T_2} \boldsymbol{w} + 1} \geq \alpha_2 && \text{(22b)} \\
&\quad \boldsymbol{w} = \boldsymbol{Q}_\perp \boldsymbol{v} && \text{(22c)} \\
&\quad \left[\boldsymbol{w}\boldsymbol{w}^\dagger\right]_{n,n} [\boldsymbol{T}]_{n,n} \leq P_R(n), \quad n = 1, \ldots, K, && \text{(22d)}
\end{aligned}$$

where $\alpha_1 = 2^{2\eta r}(1+\upsilon_2) - 1$, $\alpha_2 = 2^{2(1-\eta)r}(1+\upsilon_1) - 1$. The reason for replacing $\boldsymbol{w}^\dagger \boldsymbol{R}_{a_2} \boldsymbol{w}$ with $\boldsymbol{w}^\dagger \boldsymbol{R}_{b_1} \boldsymbol{w}$ in (22b) has been explained in *Remark 1*.

Then we substitute the third constraint (22c) into other three constraints (22a), (22b), and (22d). After some tedious derivation, we have

$$\begin{aligned}
&\max_{\boldsymbol{v}} r \\
&s.t.\ \left|\boldsymbol{v}^\dagger \boldsymbol{Q}_\perp^\dagger \boldsymbol{b}_1\right| \geq \sqrt{\alpha_1} \left\| \left[\boldsymbol{v}^\dagger \boldsymbol{Q}_\perp^\dagger \sqrt{\boldsymbol{R}_{T_1 T_1}}, \boldsymbol{v}^\dagger \boldsymbol{Q}_\perp^\dagger \boldsymbol{c}_1, 1\right] \right\| \\
&\quad \left|\boldsymbol{v}^\dagger \boldsymbol{Q}_\perp^\dagger \boldsymbol{b}_1\right| \geq \sqrt{\alpha_2} \left\| \left[\boldsymbol{v}^\dagger \boldsymbol{Q}_\perp^\dagger \sqrt{\boldsymbol{R}_{T_2 T_2}}, \boldsymbol{v}^\dagger \boldsymbol{Q}_\perp^\dagger \boldsymbol{c}_2, 1\right] \right\| \\
&\quad \left|\boldsymbol{Q}_\perp^{(n)} \boldsymbol{v}\right| \leq \sqrt{P_R(n) / [\boldsymbol{T}]_{n,n}}, && \text{(23)}
\end{aligned}$$

where $|\cdot|$ is the absolute value of a complex scalar, $\|\cdot\|$ means the Frobenius norm of a vector/matrix. Clearly, this is a standard second order convex cone programming (SOCP) problem.

To obtain $R_{sum}(\eta(k))$, we turn to the following algorithm based on a bisection method for r, where r is a fixed value of R_{sum} within a iteration. Assume that $r_{low} < r < r_{up}$, where r_{low} and r_{up} are the lower and upper limits of r, respectively. We solve the 'feasible-or-not' problem (24) for the given value of r in this interval. If this problem is feasible, which indicating that r hasn't reached the maximum rate under $\eta(k)$, then we can increase the value of r, replace r_{low} with r to obtain a new lower bound and replace r with $(r + r_{up})/2$; if it is infeasible, which indicating r has exceeded the maximum rate of the two-way communication network, then the value of r should be decreased, we replace r_{up} with r to obtain

Algorithm 1 Iterative Algorithm for MSSR Scheme

Input: $\boldsymbol{h}_{i,j}, P_T, P_R, \varepsilon, \eta(\varepsilon$ is a minimal positive real number).
Output: $R_{sum}(\eta(k))$, ultimately get $R_{sum}(\eta^o)$
Initialize $\eta(0) = 0, k = 1$;
while $\eta(k) < 1$ **do**
initialize $r_{low} = 0, r_{up} = r_{max}$;
repeat
For the given value of $r = \frac{1}{2}(r_{low} + r_{up})$, solving 'feasible-or-not' problem (24) by CVX (a package for specifying and solving convex programs) [31], [32];
If (24) is feasible, we set $r_{low} = r$, otherwise, set $r_{up} = r$;
until $r_{up} - r_{low} \leq \varepsilon$
Calculate $R_{sum}(\eta(k))$ with the obtained $\boldsymbol{v}$;
$k = k + 1, \eta(k) = \eta(k-1) + \delta$ (δ is step size for η);
end while
Compare all the $R_{sum}(\eta(k))$, find maximum $R_{sum}(\eta^o)$.

a new upper bound and replace r with $(r_{low} + r)/2$. Next, we solve problem (24) with the new value of r, this process is repeated over and over again until the value of r is no longer increasing. Through this iteration, we can converge to the maximum value of r under the rate split scheme $\eta(k)$. The whole iteration method is shown in Algorithm 1.

$$\begin{aligned} &\textbf{Find } \boldsymbol{v} \\ &s.t. \text{the same as (23)} \end{aligned} \tag{24}$$

For the proposed MSSR scheme, we have the following result.

Theorem 1: Let $\boldsymbol{W}_1$ and $\boldsymbol{W}_2$ be the sets of $\boldsymbol{w}$ satisfying all the constraints in (21a)-(21d) and $\boldsymbol{w} = \boldsymbol{Q}_\perp \boldsymbol{v}$ in $\boldsymbol{W}_1$, $\boldsymbol{w} = \boldsymbol{H}_\perp \boldsymbol{v}_1$ in $\boldsymbol{W}_2$, respectively, where $\boldsymbol{Q} = \left[\boldsymbol{a}_E^\dagger; \boldsymbol{b}_E^\dagger\right]$ and $\boldsymbol{H} = \left[\boldsymbol{a}_E^\dagger; \boldsymbol{b}_E^\dagger; \boldsymbol{c}_1^\dagger; \boldsymbol{c}_2^\dagger\right]$. Let $R_{sum,1}^*$ and $R_{sum,2}^*$ denote the optimal summation rate under $\boldsymbol{W}_1$ and $\boldsymbol{W}_2$. Then, we have

$$R_{sum,1}^* \geq R_{sum,2}^*.$$

Proof: As we design $\boldsymbol{w}$ in the null space of $\boldsymbol{a}_E^\dagger$ and $\boldsymbol{b}_E^\dagger$ to completely eliminate information leakage to eavesdropper $\mathbb{E}$, the eavesdropper can only obtain information from Phase 1. Hence, either the constraint $\boldsymbol{w} = \boldsymbol{H}_\perp \boldsymbol{v}_1$ is added or not, Γ_i is the same as (18), the expression of R_{sum}^* is always (20). As $\boldsymbol{w} = \boldsymbol{H}_\perp \boldsymbol{v}_1$ is an additional constraint, we have

$$W_2 \subseteq W_1.$$

For $R_{sum,2}^*$, it has the same expression of the objective function but has less alternative $\boldsymbol{w}$. Hence, $R_{sum,1}^* \geq R_{sum,2}^*$. This completes the proof of the theorem. ■

Theorem 1 shows that the design of $\boldsymbol{w}$ leading to no improvement of secure performance of system. The experimental results also validate this conclusion. Note that the computation load of the MSSR scheme is heavy. For each different channel, to get the final R_{sum}, we need to solve problem (24) many many times. Assume that the time consumed for program solving 'feasible-or-not' problem (24) to run once is t_{base}, the total time required to get R_{sum} is $\text{scale}_r \cdot \text{scale}_\eta \cdot t_{base}$, where $\text{scale}_\eta \approx 1/\delta$, $\text{scale}_r \propto \log_2(r_{max})$. Next, we propose a reduced-complexity secure scheme to improve the system's security performance.

B. MAXIMIZE MINIMUM SECRECY RATE (MMSR)

From (11), we can see that the two-way relay communication system can be decoupled into 2 one-way channels. Hence, it is possible to find $\boldsymbol{w}$ that maximizes the lower secrecy rate between R_{T_1} and R_{T_2}. To this end, we consider the following objective function

$$\begin{aligned} &\max_{\boldsymbol{w}} \min(R_{T_1}, R_{T_2}) \\ &s.t. \ \boldsymbol{w} = \boldsymbol{Q}_\perp \boldsymbol{v} \\ &\quad \left[\boldsymbol{w}\boldsymbol{w}^\dagger\right]_{n,n} [\boldsymbol{T}]_{n,n} \leq P_R(n), \quad n = 1, 2, \ldots, K \end{aligned} \tag{25}$$

where R_{T_i} is in the form of (10) with Γ_i in (18) and Γ_E^j in (19). Furtherly, considering the monotonicity of logarithmic function, (25) can be simplified as

$$\begin{aligned} &\max_{\boldsymbol{w}} \min\left(\frac{1+\Gamma_1}{1+\upsilon_2}, \frac{1+\Gamma_2}{1+\upsilon_1}\right) \\ &s.t. \ \boldsymbol{w} = \boldsymbol{Q}_\perp \boldsymbol{v} \\ &\quad \left[\boldsymbol{w}\boldsymbol{w}^\dagger\right]_{n,n} [\boldsymbol{T}]_{n,n} \leq P_R(n), \quad n = 1, 2, \ldots, K \end{aligned} \tag{26}$$

However, (26) is a non-convex problem, we can not solve it efficiently. If we let

$$t = \min\left(\frac{1+\Gamma_1}{1+\upsilon_2}, \frac{1+\Gamma_2}{1+\upsilon_1}\right),$$

then (26) can be converted into a convex problem as

$$\begin{aligned} &\max_{\boldsymbol{w}} t \\ &s.t. \ \Gamma_1 \geq t(1+\upsilon_2) - 1 \triangleq \alpha_a \\ &\quad \Gamma_2 \geq t(1+\upsilon_1) - 1 \triangleq \alpha_b \\ &\quad \boldsymbol{w} = \boldsymbol{Q}_\perp \boldsymbol{v} \\ &\quad \left[\boldsymbol{w}\boldsymbol{w}^\dagger\right]_{n,n} [\boldsymbol{T}]_{n,n} \leq P_R(n), \quad n = 1, \ldots, K \end{aligned} \tag{27}$$

Therefore, the problem can be solved by the convex optimization theory. Recall that

$$\begin{aligned} \Gamma_1 &= \frac{\boldsymbol{w}^\dagger \boldsymbol{R}_{b_1} \boldsymbol{w}}{\boldsymbol{w}^\dagger \boldsymbol{R}_{T_1 T_1} \boldsymbol{w} + \boldsymbol{w}^\dagger \boldsymbol{R}_{c_1} \boldsymbol{w} + 1}, \\ \upsilon_2 &= \frac{P_T |h_{T_2 E}|^2}{P_T |h_{T_1 E}|^2 + P_J^{(1)} |h_{JE}|^2 + 1}, \\ \Gamma_2 &= \frac{\boldsymbol{w}^\dagger \boldsymbol{R}_{b_1} \boldsymbol{w}}{\boldsymbol{w}^\dagger \boldsymbol{R}_{T_2 T_2} \boldsymbol{w} + \boldsymbol{w}^\dagger \boldsymbol{R}_{c_2} \boldsymbol{w} + 1}, \\ \upsilon_1 &= \frac{P_T |h_{T_1 E}|^2}{P_T |h_{T_2 E}|^2 + P_J^{(1)} |h_{JE}|^2 + 1}. \end{aligned}$$

Algorithm 2 Iterative Algorithm for MMSR Scheme

Input: $\boldsymbol{h}_{i,j}, P_T, P_R, \varepsilon_t$ (ε_t is a minimal positive real number).
Output: $\boldsymbol{V}$, ultimately get R_{sum}
Initialize $t_{low}=0$, $t_{up}=t_{max}$;
repeat
For the given value of $t=\frac{1}{2}(t_{low}+t_{up})$, solving problem (29) with t by CVX toolbox;
If it is feasible, set $t_{low}=t$, otherwise, set $t_{up}=t$;
until $t_{up}-t_{low}\le\varepsilon_t$
Calculate R_{sum} by using formulas (18), (19), (10), (11) with the obtained $\boldsymbol{V}$.

Hence, (27) can be finally transformed into a semi-definite programming (SDP) problem as

$$\begin{aligned}&\max_{\boldsymbol{V}}\ t\\ &s.t.\ \mathrm{trace}\left(\bar{\boldsymbol{R}}_{b_1}\boldsymbol{V}\right)\ge\alpha_a\left\{\mathrm{trace}\left[\left(\bar{\boldsymbol{R}}_{T_1T_1}+\bar{\boldsymbol{R}}_{c_1}\right)\boldsymbol{V}\right]+1\right\}\\ &\quad\mathrm{trace}\left(\bar{\boldsymbol{R}}_{b_1}\boldsymbol{V}\right)\ge\alpha_b\left\{\mathrm{trace}\left[\left(\bar{\boldsymbol{R}}_{T_2T_2}+\bar{\boldsymbol{R}}_{c_2}\right)\boldsymbol{V}\right]+1\right\}\\ &\quad\left[\boldsymbol{Q}_\perp\boldsymbol{V}\boldsymbol{Q}_\perp^\dagger\right]_{n,n}[\boldsymbol{T}]_{n,n}\le P_R(n),\quad n=1,2,\ldots,K\\ &\quad\boldsymbol{V}\succcurlyeq 0,\mathrm{rank}(\boldsymbol{V})=1\end{aligned}\tag{28}$$

where trace($\boldsymbol{A}$) is the trace of matrix $\boldsymbol{A}$, $\boldsymbol{V}=\boldsymbol{v}\boldsymbol{v}^\dagger$, $\bar{\boldsymbol{R}}_{b_1}=\boldsymbol{Q}_\perp^\dagger\boldsymbol{R}_{b_1}\boldsymbol{Q}_\perp$, $\bar{\boldsymbol{R}}_{T_1T_1}=\boldsymbol{Q}_\perp^\dagger\boldsymbol{R}_{T_1T_1}\boldsymbol{Q}_\perp$, $\bar{\boldsymbol{R}}_{c_1}=\boldsymbol{Q}_\perp^\dagger\boldsymbol{R}_{c_1}\boldsymbol{Q}_\perp$, $\bar{\boldsymbol{R}}_{T_2T_2}=\boldsymbol{Q}_\perp^\dagger\boldsymbol{R}_{T_2T_2}\boldsymbol{Q}_\perp$, $\bar{\boldsymbol{R}}_{c_2}=\boldsymbol{Q}_\perp^\dagger\boldsymbol{R}_{c_2}\boldsymbol{Q}_\perp$. Note that rank($\boldsymbol{V}$) = 1 and $\boldsymbol{V}$ constrained to be a symmetric positive semidefinite matrix expressed as $V\succcurlyeq 0$. Hence, (28) is still a non-convex problem because of its non-convex constraint rank($\boldsymbol{V}$) = 1. As will prove later, the dropping-operation does not affect the results. Based on this, the rank-1 constraint can be dropped for convenience of obtaining the relaxed version of problem (28). Then, the so-obtained semi-definite relaxed (SDR) problem can be efficiently solved by using the bisection method. To find the maximal t iteratively, the 'feasible-or-not' problem (29) is introduced, as shown in *Algorithm 2*.

$$\begin{aligned}&\textbf{Find } \boldsymbol{V}\\ &s.t.\ \mathrm{trace}\left(\bar{\boldsymbol{R}}_{b_1}\boldsymbol{V}\right)\ge\alpha_a\left\{\mathrm{trace}\left[\left(\bar{\boldsymbol{R}}_{T_1T_1}+\bar{\boldsymbol{R}}_{c_1}\right)\boldsymbol{V}\right]+1\right\}\\ &\quad\mathrm{trace}\left(\bar{\boldsymbol{R}}_{b_1}\boldsymbol{V}\right)\ge\alpha_a\left\{\mathrm{trace}\left[\left(\bar{\boldsymbol{R}}_{T_2T_2}+\bar{\boldsymbol{R}}_{c_2}\right)\boldsymbol{V}\right]+1\right\}\\ &\quad\left[\boldsymbol{Q}_\perp\boldsymbol{V}\boldsymbol{Q}_\perp^\dagger\right]_{n,n}[\boldsymbol{T}]_{n,n}\le P_R(n),\quad n=1,\cdots,K\\ &\quad\boldsymbol{V}\succcurlyeq 0.\end{aligned}\tag{29}$$

If $\boldsymbol{V}$ obtained from Algorithm 2 is of rank one, there is nothing more to do, we rewrite it directly as $\boldsymbol{V}=\boldsymbol{v}\boldsymbol{v}^\dagger$, $\boldsymbol{v}$ will be a feasible-and-optimal solution of problem (28).

Theorem 2: The solution of (29) must be rank-one.

Proof: For (29), let us first write out its Lagrangian function (30), as shown at the bottom of this page, where λ,μ, $\boldsymbol{\zeta}=[\zeta_1,\zeta_2,\ldots,\zeta_K]$ is the Lagrangian dual variables for its first three constraints, respectively. And $\boldsymbol{Z}$ is the Lagrangian dual variable for the constraint $\boldsymbol{V}\succcurlyeq 0$. Let $\frac{\partial L}{\partial\boldsymbol{V}}=0$, then the corresponding KKT conditions are

$$\boldsymbol{Z}=\lambda\alpha_a\bar{\boldsymbol{R}}_{T_1T_1}+\mu\alpha_b\bar{\boldsymbol{R}}_{T_2T_2}+diag(\boldsymbol{\zeta})-(\lambda+\mu)\bar{\boldsymbol{R}}_{b_1}\tag{31}$$

$$\boldsymbol{Z}\boldsymbol{V}=0\tag{32}$$

$$\boldsymbol{V}\succcurlyeq 0,\boldsymbol{Z}\succcurlyeq 0,\lambda\ge 0,\mu\ge 0,\zeta_i\ge 0,i=1,\quad 2,\ldots,K.\tag{33}$$

The key to showing the rank-one structure of $\boldsymbol{V}$ lies in (31). Let

$$\boldsymbol{B}=\lambda\alpha_a\bar{\boldsymbol{R}}_{T_1T_1}+\mu\alpha_b\bar{\boldsymbol{R}}_{T_2T_2}+\mathrm{diag}(\boldsymbol{\zeta}).$$

Note that $\bar{\boldsymbol{R}}_{T_1T_1}$, $\bar{\boldsymbol{R}}_{T_2T_2}$, diag($\boldsymbol{\zeta}$) are all positive semidefinite matrix, then $\boldsymbol{B}$ is positive definite, and thus has full rank. By denoting $\boldsymbol{B}^{1/2}$ as a positive definite square root of $\boldsymbol{B}$, we have

$$\begin{aligned}\mathrm{rank}(\boldsymbol{Z})&=\mathrm{rank}\left(\boldsymbol{B}^{-1/2}\boldsymbol{Z}\boldsymbol{B}^{-1/2}\right)\\&=\mathrm{rank}\left(\boldsymbol{I}-(\lambda+\mu)\left(\boldsymbol{B}^{-1/2}\bar{\boldsymbol{H}}_\perp^\dagger\boldsymbol{b}_1\right)\left(\boldsymbol{B}^{-1/2}\bar{\boldsymbol{H}}_\perp^\dagger\boldsymbol{b}_1\right)^\dagger\right)\\&\ge K-3.\end{aligned}\tag{34}$$

Note that $\boldsymbol{Z}$ is a $(K-2)\times(K-2)$ matrix. Hence,

$$\mathrm{rank}(\boldsymbol{Z})\le K-2,$$

which means

$$\mathrm{rank}(\boldsymbol{Z})=K-3\text{ or }K-2.$$

For rank($\boldsymbol{Z}$) = $K-2$, (32) can only be satisfied by $\boldsymbol{V}=\boldsymbol{0}$, it is not a applicable solution of $\boldsymbol{V}$.

For rank($\boldsymbol{Z}$) = $K-3$, (32) is achieved only when $\boldsymbol{V}$ lies in the nullspace of $\boldsymbol{Z}$, the dimension of which is one. This means that any optimal $\boldsymbol{V}$ must be of rank one. ■

Assume that the time consumed for program solving 'feasible-or-not' problem (29) to run once is t_{1base}, the total time required is $\mathrm{scale}_t\cdot t_{1base}$, where $\mathrm{scale}_t\propto\log_2(t_{max})$, which means MMSR scheme taking just about a small percentage of the time of MSSR scheme. As can be seen from the previous content, time consumed by MSSR scheme is nearly $\mathrm{scale}_\eta\cdot t_{MMSR}$, where t_{MMSR} denotes the time consumed by using the MMSR scheme.

IV. MODIFIED SECURE TRANSMISSION SCHEMES WHEN $K<3$

As discussed above, to completely eliminate information leakage to $\mathbb{E}$ in Phase 2, we design $\boldsymbol{a}_E^\dagger\boldsymbol{w}=\boldsymbol{b}_E^\dagger\boldsymbol{w}=0$, which requires $K-2\ge 1$. If we further design $\boldsymbol{c}_1^\dagger\boldsymbol{w}=\boldsymbol{c}_2^\dagger\boldsymbol{w}=0$ to eliminate the interference to $\mathbb{T}_1$, $\mathbb{T}_2$ by jamming signal z_1,

$$\begin{aligned}L(\boldsymbol{V},\boldsymbol{Z})=t&-\lambda\left\{\mathrm{trace}\left[\left(\alpha_a\bar{\boldsymbol{R}}_{T_1T_1}-\bar{\boldsymbol{R}}_{b_1}\right)\boldsymbol{V}\right]+\alpha_a\right\}-\mu\left\{\mathrm{trace}\left[\left(\alpha_b\bar{\boldsymbol{R}}_{T_2T_2}-\bar{\boldsymbol{R}}_{b_1}\right)\boldsymbol{V}\right]+\alpha_b\right\}\\&-\sum_{i=1}^{K}\zeta_i\left[\left(\bar{\boldsymbol{H}}_\perp\boldsymbol{V}\bar{\boldsymbol{H}}_\perp^\dagger\right)_{i,i}-P_R(i)/[\boldsymbol{T}]_{i,i}\right]+\mathrm{trace}\left(\boldsymbol{V}\boldsymbol{Z}\right)\end{aligned}\tag{30}$$

$$
\begin{aligned}
&\textbf{Find } \boldsymbol{w} \\
&s.t.\ \left|\boldsymbol{w}^{\dagger}\boldsymbol{b}_1\right| \geq \sqrt{\alpha_c}\left\|\left[\boldsymbol{w}^{\dagger}\sqrt{\boldsymbol{R}_{T_1T_1}}, \boldsymbol{w}^{\dagger}\boldsymbol{c}_1, \sqrt{P_J^{(2)}|h_{JT_1}|^2+1}\right]\right\| \\
&\quad \left|\boldsymbol{w}^{\dagger}\boldsymbol{b}_1\right| \geq \sqrt{\beta_c}\left\|\left[\boldsymbol{w}^{\dagger}\sqrt{\boldsymbol{R}_{T_2T_2}}, \boldsymbol{w}^{\dagger}\boldsymbol{c}_2, \sqrt{P_J^{(2)}|h_{JT_2}|^2+1}\right]\right\| \\
&\quad \left|\boldsymbol{w}^{\dagger}\boldsymbol{a}_E\right| \leq \sqrt{\varsigma_1-\upsilon_1}\left\|\left[\boldsymbol{w}^{\dagger}\boldsymbol{b}_E, \boldsymbol{w}^{\dagger}\boldsymbol{c}_E, \sqrt{\boldsymbol{R}_{RE}}, \sqrt{P_J^{(2)}|h_{JE}|^2+1}\right]\right\| \\
&\quad \left|\boldsymbol{w}^{\dagger}\boldsymbol{b}_E\right| \leq \sqrt{\varsigma_2-\upsilon_2}\left\|\left[\boldsymbol{w}^{\dagger}\boldsymbol{a}_E, \boldsymbol{w}^{\dagger}\boldsymbol{c}_E, \sqrt{\boldsymbol{R}_{RE}}, \sqrt{P_J^{(2)}|h_{JE}|^2+1}\right]\right\| \\
&\quad \boldsymbol{w}(n) \leq \sqrt{P_R(n)/[\boldsymbol{T}]_{n,n}}
\end{aligned} \tag{36}
$$

$$
\begin{aligned}
&\textbf{Find } \boldsymbol{W} \\
&s.t.\ \operatorname{trace}\left\{\left[\boldsymbol{R}_{b_1}-t_c\left(\boldsymbol{R}_{T_1T_1}+\boldsymbol{R}_{c_1}\right)\right]\boldsymbol{W}\right\} \geq t_c\left(P_J^{(2)}\left|h_{JT_1}\right|^2+1\right) \\
&\quad \operatorname{trace}\left\{\left[\boldsymbol{R}_{b_1}-t\left(\boldsymbol{R}_{T_2T_2}+\boldsymbol{R}_{c_2}\right)\right]\boldsymbol{W}\right\} \geq t_c\left(P_J^{(2)}\left|h_{JT_2}\right|^2+1\right) \\
&\quad \operatorname{trace}\left\{\left[\left(\varsigma_1-\upsilon_1\right)\left(\boldsymbol{R}_{bE}+\boldsymbol{R}_{cE}+\boldsymbol{R}_{RE}\right)-\boldsymbol{R}_{aE}\right]\boldsymbol{W}\right\} \geq -\left(\varsigma_1-\upsilon_1\right)\left(P_J^{(2)}\left|h_{JE}\right|^2+1\right) \\
&\quad \operatorname{trace}\left\{\left[\left(\varsigma_2-\upsilon_2\right)\left(\boldsymbol{R}_{aE}+\boldsymbol{R}_{cE}+\boldsymbol{R}_{RE}\right)-\boldsymbol{R}_{bE}\right]\boldsymbol{W}\right\} \geq -\left(\varsigma_2-\upsilon_2\right)\left(P_J^{(2)}\left|h_{JE}\right|^2+1\right) \\
&\quad [\boldsymbol{W}]_{n,n} \leq P_R(n)/[\boldsymbol{T}]_{n,n}, \quad (n=1,2,\ldots,K) \\
&\quad \boldsymbol{W} \succcurlyeq 0, \operatorname{rank}(\boldsymbol{W})=1
\end{aligned} \tag{38}
$$

this even requires $K-4 \geq 1$. However, in some scene, the number of intermediate nodes N can not be big enough to support these designs. When the shortage of intermediate nodes happens, null-space beamforming can not be implemented. We propose two modified security communication schemes to improve applicability and practicability of the MSSR/MMSR designs.

Noted that $P_J^{(2)} \neq 0$, which is because that we cannot use null-space beamforming technology to eliminate information leakage to $\mathbb{E}$. In order to deteriorate the channel quality of $\mathbb{E}$, it is necessary to transmit interference signals z_2 in Phase 2.

A new parameter has been introduced this time, ς_j indicates the maximal tolerable SINR of channel $\mathbb{T}_j$ to $\mathbb{E}$, i.e., $\Gamma_E^j \leq \varsigma_j$. The modified scheme of MSSR scheme can be described as

$$
\begin{aligned}
&\max_{\boldsymbol{w}} R_{sum} \\
&s.t.\ \frac{1}{2}\log_2\left(1+\Gamma_1\right) \geq \eta R_{sum} \\
&\quad \frac{1}{2}\log_2\left(1+\Gamma_2\right) \geq (1-\eta)R_{sum} \\
&\quad \Gamma_E^j \leq \varsigma_j, \quad (j=1,2) \\
&\quad \left[\boldsymbol{w}\boldsymbol{w}^{\dagger}\right]_{n,n}[\boldsymbol{T}]_{n,n} \leq P_R(n), \quad n=1,2,\ldots,K
\end{aligned} \tag{35}
$$

The subsequent deduction process is similar to that in subsection A of Section III. After a tedious derivation, we get the 'feasible-or-not' SOCP problem shown in (36), as shown at the top of this page, where $\alpha_c = 2^{2\eta r}-1$ and $\beta_c = 2^{2(1-\eta)r}-1$. Then, the iteration method in Algorithm 1 can be used to get the secrecy rate of this transmission scheme, except that 'feasible-or-not' SOCP problem (24) changing into (36).

The modified scheme of MMSR scheme can be described as

$$
\begin{aligned}
&\max_{\boldsymbol{w}} \min\left(\Gamma_1,\Gamma_2\right) \\
&s.t.\ \Gamma_E^j \leq \varsigma_j, \quad (j=1,2) \\
&\quad \left[\boldsymbol{w}\boldsymbol{w}^{\dagger}\right]_{n,n}[\boldsymbol{T}]_{n,n} \leq P_R(n), \quad n=1,2,\ldots,K
\end{aligned} \tag{37}
$$

Let $t_c = \min\left(\Gamma_1,\Gamma_2\right)$, then problem (37) can be transformed into a semi-definite programming (SDP) problem (38), as shown at the top of this page, by using (15) and (17), where $\boldsymbol{W} = \boldsymbol{w}\boldsymbol{w}^{\dagger}$. The process of solving (38) is similar to Algorithm 2 in the previous chapter, except the'feasible-or-not' SDP problem (29) replaced by (38).

Discussion of ς_j: As (17) shows, Γ_E^j must be greater than υ_j. To this aim, we set $\varsigma_j = \upsilon_j + \Delta\upsilon_j$ for some positive value $\Delta\upsilon_j$. Considering the difference of the channel $\mathbb{T}_1$ to $\mathbb{E}$ and $\mathbb{T}_2$ to $\mathbb{E}$, we set $\Delta\upsilon_j = \kappa\upsilon_j$, where κ is a real number. As will be seen in simulations, the performance of this setting is better than fixed value $\Delta\upsilon_j$.

V. SIMULATION RESULTS

In this section, we give some simulations for the proposed MSSR, MMSR, and two modified transmission schemes. All of the channel coefficients in simulations are randomly generated, which are complex 0-mean Gaussian random vectors with covariance equals one as in [18], [22].

To compare the performances of different designs for $\boldsymbol{Q}$, we set $\boldsymbol{Q}_1 = \left[\boldsymbol{a}_E^{\dagger}; \boldsymbol{b}_E^{\dagger}\right]$ and $\boldsymbol{Q}_2 = \left[\boldsymbol{a}_E^{\dagger}; \boldsymbol{b}_E^{\dagger}; \boldsymbol{c}_1^{\dagger}; \boldsymbol{c}_2^{\dagger}\right]$. The constrained power of relay nodes is $P_R = [6\text{dBW}, \ldots, 6\text{dBW}]$. The range of P_T is 4dBW–9dBW. Parameters ε in

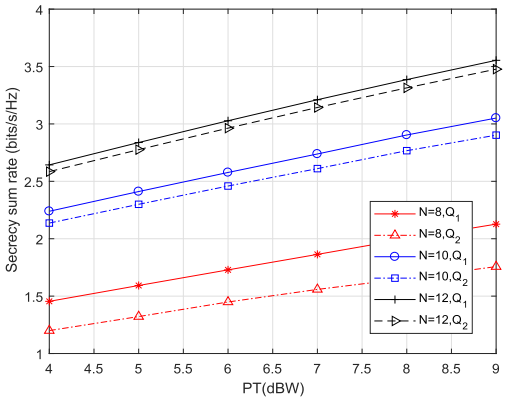

FIGURE 2. R_{sum} of MSSR scheme for different $\boldsymbol{Q}$.

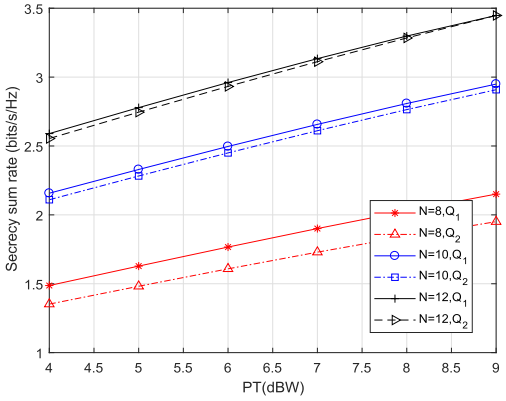

FIGURE 3. R_{sum} of MMSR scheme for different $\boldsymbol{Q}$.

Algorithm 1 and ε_t in Algorithm 2 are both set to be 0.01, the step size δ of η in Algorithm 1 is 0.01, too. Fig. 2 and Fig. 3 give the simulation results of MSSR scheme and MMSR scheme for different $\boldsymbol{Q}$, respectively. The number of Monte Carlo experiments is 1000 for each P_T. From the figures, one can not difficult to find that the sum secrecy rate R_{sum} is better when $\boldsymbol{Q} = \boldsymbol{Q}_1$, though it needs a smaller N. With the increase of N, the difference between these two secure transmission schemes gets smaller and smaller, eventually tends to zero. With both a better performance and smaller N-need, we can choose low complexity design of $\boldsymbol{Q}_1$ in actual use. The reason why $\boldsymbol{Q}_1$ has a better performance than $\boldsymbol{Q}_2$ can be explained by Theorem 1. Besides, one can not difficult to find that higher P_T and bigger N lead to a higher R_{sum}.

Next, we verify the performances of MSSR scheme and MMSR scheme when $K \geq 3$. In the simulations, we design $\boldsymbol{w}$ only with $\boldsymbol{Q}_1$ as different $\boldsymbol{Q}$ lead to the same conclusion. One can see from Fig. 4 that there is a very small difference between R_{sum} for the two schemes. Compared with the MSSR scheme, MMSR scheme has a much lower computational complexity. Simulation result shows that running time of MMSR scheme is nearly 1% of MSSR scheme, which is in consistent with the analysis in Section III, time consumed by MSSR scheme is nearly $\text{scale}_\eta \cdot t_{MMSR}$.

In Fig. 5, we compare the R_{sum} of optimally selected $\mathbb{J}$ in N intermediate nodes and randomly selected $\mathbb{J}$ with $\boldsymbol{Q} = \boldsymbol{Q}_1$.

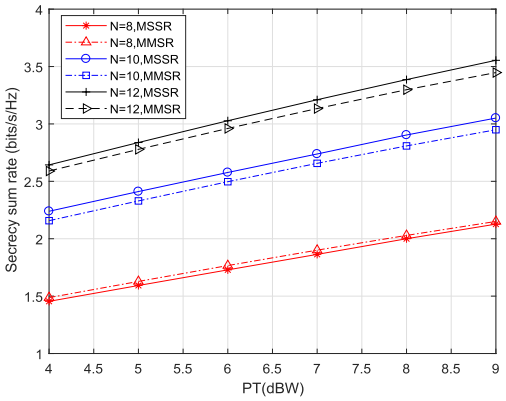

FIGURE 4. R_{sum} of MSSR and MMSR for $\boldsymbol{Q}_1$.

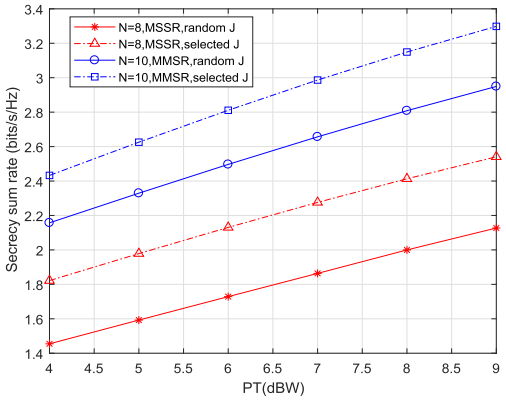

FIGURE 5. R_{sum} with selected $\mathbb{J}$ and random $\mathbb{J}$.

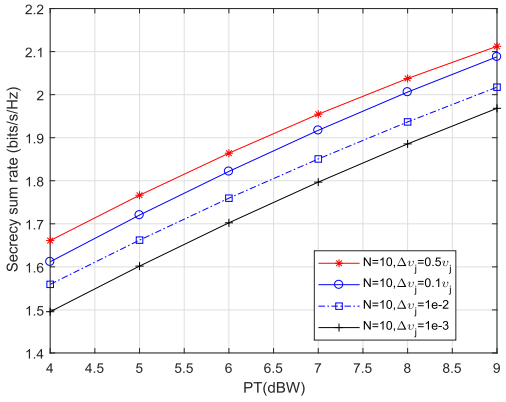

FIGURE 6. R_{sum} of modified MMSR with different $\Delta\upsilon_j$.

Simulation results show that optimally selected jamming node $\mathbb{J}$ can improve R_{sum} significantly than the case of random selection the jamming nodes, no matter which scheme you adopt. This is because the optimal $\mathbb{J}$ has a maximal $|h_{JE}|$ in all of the N intermediate nodes, which can minimize the information leakage to eavesdropper $\frac{1}{2}\log_2\left(1+\Gamma_E^j\right)$.

In Fig. 6, we verify the performances of the modified MMSR scheme with various values of $\Delta\upsilon_j$. One can see from the figure that the fixed minimal real number $\Delta\upsilon_j$ has a lower performance of R_{sum} than unfixed $\Delta\upsilon_j$. This is because

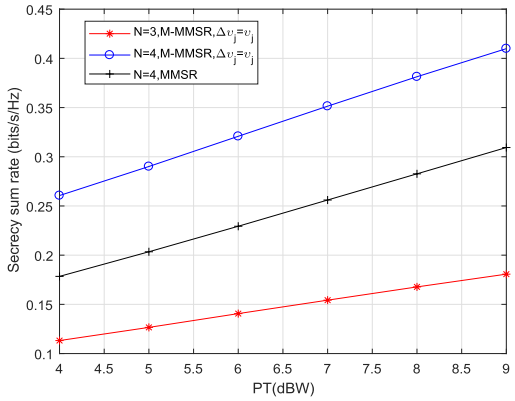

FIGURE 7. R_{sum} of modified MMSR when K close to 3.

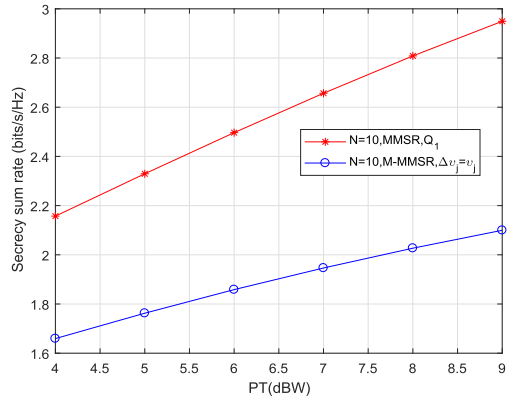

FIGURE 8. R_{sum} of modified MMSR when $K \gg 3$.

the previous settings do not take the actual difference of the channel $\mathbb{T}_1$ to $\mathbb{E}$ and $\mathbb{T}_2$ to $\mathbb{E}$ into account. When $\Delta\upsilon_j$ is fixed, the same Δ-SINR restrictions are imposed on both different eavesdropping channels.

In Fig. 7 and Fig. 8, we verify the performances of the modified secure transmission schemes when K is close to 3 and $K \gg 3$, respectively. From the figures, one can find that the modified scheme has a better performance of R_{sum} than the MMSR scheme when $N = 4$. Hence, when the number of intermediate node is not large enough for applying null-space beamforming, one can turn to the modified schemes to get an acceptable result. However, when $K \gg 3$, as shown in Fig. 8, it is better to adopt the MMSR scheme for its excellent performance than the modified scheme.

VI. CONCLUSIONS AND FUTURE WORK

In this paper, we proposed two schemes to enhance the physical-layer communication security of a two-way wireless relay network with one eavesdropper, where the legal users do not have a direct link but can just resort to intermediate nodes in the system for help. To solve this secure problem, a joint relaying-and-jamming strategy has been adopted, in which one selected intermediate node transmit jamming signal to jam the eavesdropper, while the others intermediate nodes adopt distributed beamforming to improve the channel quality to legitimate users. All the intermediate nodes are under per-node power constraints. When the number of relay nodes is large enough to support null-space beamforming, we proposed MSSR scheme and MMSR scheme based on null-space beamforming. Besides, we proposed two modified secure transmission schemes when the number of intermediate nodes is less abundant for the previously mentioned null-space beamfoming. As the future work, we will consider the impact of channel estimation errors. Besides, the security schemes with multi-jamming nodes in multi-eve situations will be considered.

REFERENCES

[1] J. H. Cheon and J. Kim, "A hybrid scheme of public-key encryption and somewhat homomorphic encryption," *IEEE Trans. Inf. Forensics Security*, vol. 10, no. 5, pp. 1052–1063, May 2015.

[2] C. E. Shannon, "Communication theory of secrecy systems," *Bell Labs Tech. J.*, vol. 28, no. 4, pp. 656–715, Oct. 1949.

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

[4] P. Wang, G. Yu, and Z. Zhang, "On the secrecy capacity of fading wireless channel with multiple eavesdroppers," in *Proc. IEEE Int. Symp. Inf. Theory*, Jun. 2007, pp. 1301–1305.

[5] M. I. Zahurul and T. Ratnarajah, "Secrecy capacity and secure outage performance for Rayleigh fading SIMO channel," in *Proc. IEEE Int. Conf. Acoust., Speech Signal Process. (ICASSP)*, May 2011, pp. 1900–1903.

[6] J. Yang and X.-H. Cao, "Distributed relay selection for two-way relaying networks based on power conservation," in *Proc. Int. Conf. Wireless Commun. Sensor Netw.*, Dec. 2014, pp. 262–265.

[7] S. Ghasemi-Goojani, S. Karimi-Bidhendi, and H. Behroozi, "On the capacity region of asymmetric Gaussian two-way line channel," *IEEE Trans. Commun.*, vol. 64, no. 9, pp. 3669–3682, Sep. 2016.

[8] L. R. Ximenes, "Unified joint symbol and channel estimation with interference subtraction for one-way and two-way MIMO relaying systems," in *Proc. IEEE 10th Latin-Amer. Conf. Commun. (LATINCOM)*, Nov. 2018, pp. 1–6.

[9] Z. Ma, Y. Lu, L. Shen, Y. Liu, and N. Wang, "Cooperative Jamming and relay beamforming design for physical layer secure two-way relaying," in *Proc. Int. Conf. Cyber-Enabled Distrib. Comput. Knowl. Discovery (CyberC)*, Oct. 2018, pp. 333–339.

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

[11] Y. Hao, T. Lv, and H. Gao, "AN-aided robust secure beamforming design in MIMO two-way relay systems with PNC," in *Proc. IEEE Wireless Commun. Netw. Conf. (WCNC)*, Apr. 2018, pp. 1–6.

[12] J. Wang, J. Chen, H. Duan, H. Ba, and J. Wu, "Jammer selection for secure two-way DF relay communications with imperfect CSI," in *Proc. 16th Int. Conf. Adv. Commun. Technol. (ICACT)*, Feb. 2014, pp. 300–303.

[13] T.-X. Zheng, H.-M. Wang, and H. Deng, "Improving anti-eavesdropping ability without eavesdropper's CSI: A practical secure transmission design perspective," *IEEE Wireless Commun. Lett.*, vol. 7, no. 6, pp. 946–949, Dec. 2018.

[14] C. Zhang, J. Ge, Z. Xia, and H. Wang, "A novel half-jamming protocol for secure two-way relay systems using a full-duplex jamming relay," in *Proc. 3rd IEEE Int. Conf. Comput. Commun. (ICCC)*, Dec. 2017, pp. 786–790.

[15] Y. T. Sagar, J. Yang, H. M. Kwon, and W. Nam, "Achievable rate of a two-way relay channel with structured code under Rayleigh fading," in *Proc. Int. Conf. Comput., Netw. Commun. (ICNC)*, Feb. 2014, pp. 644–648.

[16] J. Ran and L. Li, "An adaptive method utilizing channel reciprocity in TDD-LTE system," in *Proc. IET Int. Conf. Commun. Technol. Appl. (ICCTA)*, Oct. 2011, pp. 896–900.

[17] Z. Shi, Q. Wang, J. Jin, D. Jiang, and G. Liu, "Achievability of the channel reciprocity and its benefit in TDD system," in *Proc. 5th Int. ICST Conf. Commun. Netw. China*, Aug. 2010, pp. 1–4.

[18] Y. Yang, C. Sun, H. Zhao, H. Long, and W. Wang, "Algorithms for secrecy guarantee with null space beamforming in two-way relay networks," *IEEE Trans. Signal Process.*, vol. 62, no. 8, pp. 2111–2126, Apr. 2014.

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

[20] Z. Chen, Y. Dong, P. Fan, and K. Ben Letaief, "Optimal throughput for two-way relaying: Energy harvesting and energy co-operation," *IEEE J. Sel. Areas Commun.*, vol. 34, no. 5, pp. 1448–1462, May 2016.
[21] Q. Li, Q. Zhang, and J. Qin, "Secure relay beamforming for SWIPT in amplify-and-forward two-way relay networks," *IEEE Trans. Veh. Technol.*, vol. 65, no. 11, pp. 9006–9019, Nov. 2016.
[22] S. Shahbazpanahi and M. Dong, "A semi-closed-form solution to optimal distributed beamforming for two-way relay networks," *IEEE Trans. Signal Process.*, vol. 60, no. 3, pp. 1511–1516, Mar. 2012.
[23] S. Suganya, P. Shanmugapriya, and T. R. Priyadharshini, "Improving security in two-way relay networks by optimal relay and jammer selection," in *Proc. IEEE Int. Conf. Emerg. Trends Comput., Commun. Nanotechnol. (ICECCN)*, Mar. 2013, pp. 276–281.
[24] A. Papadogiannis, A. G. Burr, and M. Tao, "On the maximum achievable sum-rate of interfering two-way relay channels," *IEEE Commun. Lett.*, vol. 16, no. 1, pp. 72–75, Jan. 2012.
[25] K. Hu, Q. Gao, Z. Wang, and W. Huang, "Outage performance of two-way decode-and-forward relaying over block fading channels," in *Proc. IEEE 9th Int. Conf. Commun. Softw. Netw. (ICCSN)*, May 2017, pp. 51–55.
[26] X. Liu, "Outage probability of secrecy capacity over correlated log-normal fading channels," *IEEE Commun. Lett.*, vol. 17, no. 2, pp. 289–292, Feb. 2013.
[27] B. Zhong and Z. Zhang, "Secure full-duplex two-way relaying networks with optimal relay selection," *IEEE Commun. Lett.*, vol. 21, no. 5, pp. 1123–1126, May 2017.
[28] 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.
[29] 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.
[30] 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, Jun. 2009.
[31] CVX Research. (Dec. 2018). *CVX: MATLAB Software for Disciplined Convex Programming, Version 2.1*. [Online]. Available: http://cvxr.com/cvx
[32] M. Grant and S. Boyd, "Graph implementations for nonsmooth convex programs, in *Recent Advances in Learning and Control* (Lecture Notes in Control and Information Sciences), V. Blondel, S. Boyd, and H. Kimura, Eds. Springer, 2008, pp. 95–110. [Online]. Available: http://stanford.edu/~boyd/grap_dcp.html and http://cvxr.com/cvx/citing/

MIAO LUO received the B.S. degree from the School of Electronic and Information Engineering, Xi'an Jiaotong University, Xi'an, China, in 2009, where she is currently pursuing the Ph.D. degree. Her research interests include the areas of cooperative communications and physical layer security.

XIAOPING LI received the B.S. degree in mathematics from Sichuan Normal University, in 2006, and the Ph.D. degree in information and communication engineering from Xi'an Jiaotong University, in 2016.

From 2006 to 2010, he was an Assistant Professor with the College of Information Engineering, Tarim University, Alar, China. From 2013 to 2015, he was a Visiting Scholar with the Department of Electrical and Computer Engineering, University of Delaware, Newark. He is currently a Lecturer with the University of Electronic Science and Technology of China. His main research interests include signal processing theory, physical layer security, computer cryptography, and coding theory.

JIANQUAN WANG received the B.S. degree in communication engineering from the University of Electronic Science and Technology of China (UESTC), Chengdu, China, in 2013, where he is currently pursuing the Ph.D. degree in communication system. His research interests include physical-layer security, low probability of interception communication, and game theory.

QINYE YIN received the B.S., M.S., and Ph.D. degrees in communication and electronic systems from Xi'an Jiaotong University, Xi'an, China, in 1982, 1985, and 1989, respectively. Since 1989, he has been a Faculty Member with Xi'an Jiaotong University, where he is currently a Professor with the Information and Communications Engineering Department and the Chair of the Academy Committee, School of Electronic and Information Engineering.

WANBIN TANG received the B.Eng., M.Eng., and Ph.D. degrees in electrical engineering from the University of Electronic Science and Technology of China (UESTC), in 1993, 1998, and 2013, respectively. From 2006 to 2007, he was a Visiting Scholar with U.C. Berkeley. He is currently a Professor with the National Key Laboratory of Science and Technology on Communications, UESTC. His current research interests include cognitive radio and signal processing in wireless communication.

SHAOQIAN LI (M'02–SM'12–F'16) received the B.E. degree in communication technology from Xidian University, Xi'an, China, in 1981, and the M.E. degree in information and communication systems from the University of Electronic Science and Technology of China (UESTC), Chengdu, China, in 1984.

In 1984, he joined UESTC as an Academic Member, where he has been a Professor of information and communication systems, since 1997, and a Ph.D. Supervisor, since 2000. He is currently the Director of the National Key Laboratory of Science and Technology on Communications, UESTC. He holds more than 60 granted and filed patents. His general interests include the areas of wireless and mobile communications, anti-jamming technologies, and signal processing for communications subjects. He has published more than 100 journal papers, 100 conference papers, and two edited books in the above-mentioned areas. His current research topics focus on multiple-antenna signal processing technologies for mobile communications, cognitive radios, and coding and modulation for the next-generation mobile broadband communications systems. He has been a member of the Communication Expert Group of the National 863 Plan, since 1998, and the FuTURE Project, since 2005. He is currently a member of the Board of Communications and Information Systems, Academic Degrees Committee, State Council of China, and Expert Group of Key Special-Project on Next-Generation Broadband Wireless Mobile Communications of China (approved by the State Council, since 2007). He has served for various IEEE conferences as a Technical Program Committee (TPC) Member. He is also an Editorial Board Member of the *Chinese Science Bulletin* and the *Chinese Journal of Radio Science*. He was a TPC Co-Chair of the 2005, 2006, and 2008 IEEE International Conference on Communications, Circuits, and Systems.