Received: 23 March 2018 | Revised: 23 May 2018 | Accepted: 11 June 2018

DOI: 10.4218/etrij.2018-0145

ORIGINAL ARTICLE

WILEY ETRI Journal

Joint optimization of beamforming and power allocation for DAJ-based untrusted relay networks

Rugui Yao[1,2] | **Yanan Lu**[1] | **Tamer Mekkawy**[1] | **Fei Xu**[1] | **Xiaoya Zuo**[1,2]

[1]School of Electronics and Information, Northwestern Polytechnical University, Xi'an, China.

[2]Research & Development Institute of Northwestern Polytechnical University in Shenzhen, Guangdong, China.

Correspondence
Rugui Yao, School of Electronics and Information, Northwestern Polytechnical University, 710072 Xi'an, China.
Email: yaorg@nwpu.edu.cn

Funding information
National Natural Science Foundation of China, Grant/Award Number: 61501376, 61701407; Science and Technology Program of Shenzhen, China, Grant/Award Number: JCYJ20170306155652174; Fundamental Research Funds for the Central Universities, Grant/Award Number: 3102018JGC006, 3102017JG02002; Aeronautical Science Foundation of China, Grant/Award Number: 2017ZC53029; Graduate Starting Seed Fund of Northwestern Polytechnical University, Grant/Award Number: ZZ2018128

Destination-assisted jamming (DAJ) is usually used to protect confidential information against untrusted relays and eavesdroppers in wireless networks. In this paper, a DAJ-based untrusted relay network with multiple antennas installed is presented. To increase the secrecy, a joint optimization of beamforming and power allocation at the source and destination is studied. A matched-filter precoder is introduced to maximize the cooperative jamming signal by directing cooperative jamming signals toward untrusted relays. Then, based on generalized singular-value decomposition (GSVD), a novel transmitted precoder for confidential signals is devised to align the signal into the subspace corresponding to the confidential transmission channel. To decouple the precoder design and optimal power allocation, an iterative algorithm is proposed to jointly optimize the above parameters. Numerical results validate the effectiveness of the proposed scheme. Compared with other schemes, the proposed scheme shows significant improvement in terms of security performance.

KEYWORDS
destination-assisted jamming, optimal power allocation, physical layer security, secrecy rate, untrusted relay network

1 | INTRODUCTION

Owing to the openness and broadcasting nature of transmission channels, wireless communications face more serious reliability and security challenges than wired communications. In wireless communication systems, traditional encryption technologies [1] are commonly utilized to ensure information security. However, the security provided by finite-length keys largely depends on the computation capability of eavesdroppers. With the development of quantum computers, this encryption method has a greater possibility of being cracked [2]. From another point of view, based on Shannon's information theory, physical layer security utilizes the time-varying nature and randomness of wireless channels to realize secure communications, which has become a hot research topic in the field of wireless communications in recent years [3]. Wyner [4] first proposed an eavesdropping channel model. Subsequently, in [5], the secrecy rate was defined as the difference between the rates of the legitimate and wiretap channels. Enhancing the legitimate channel or suppressing the wiretap channel can benefit the maximization of the achievable

secrecy rate, which could further improve the security performance of communication transmissions.

1.1 | Literature review

Owing to the constraint of transmitting nodes with respect to transmitting power and shadowing, cooperative relay technology is introduced to expand coverage, improve communication quality, and enhance the security performance of the physical layer. The relay-eavesdropper channel was studied in [6], which proved that the trusted relay can effectively improve the secrecy capacity of the system. In [7], Lai and others analyzed the impact of trusted relays' locations on the secrecy capacity, and proposed an optimized configuration of the best relay's location to achieve the maximum secrecy capacity. In [8], Fan and others quantified the impact of the correlated fading on the secure communication in multiple amplify-and-forward (AF) relaying networks. In [9], the impact of cochannel interference on the secrecy capacity was further studied for multiple AF relaying networks.

In the above literature, the relays are always assumed to be trusted. However, in some scenarios, the relays may be untrusted, resulting in severe security issues, especially in cooperative networks [10,11]. Such untrusted relays attempt to interpret the confidential information. Relay-eavesdropper channels with untrusted relays were studied in [12], which proved that untrusted relays could still help to enhance the network security, while guaranteeing the link reliability. In [13], secure communication in a single-user untrusted relay network was analyzed from a capacity perspective, and a secure transmission mechanism was then proposed based on opportunistic communication. Furthermore, when multiple relays were considered [14], the analytic formula and the lower bound of the ergodic secrecy rate were derived in [15] using the extreme value theory. In [16], a joint untrusted relay selection and power-allocation scheme were proposed to enhance the physical layer security in a cooperative network.

Moreover, when user nodes were equipped with multiple antennas, beamforming can be introduced to enhance the network security [17,18]. Beamforming vectors for a source-untrusted-relay link [19] were optimized to improve the system security performance for single-hop relay networks. In [20], efficient algorithms were proposed to jointly design the beamformers for both the source and relay in two-phase or three-phase two-way relay networks. In [21], Xiong and others proposed a joint precoding design for both the source and relay in a multiple-antenna cooperative network. However, in [21], to guarantee the simplicity of the derivation and optimization, only one symbol can be transmitted from the source without the full utilization of the degrees-of-freedom (DoFs). Then, for two-hop multi-relay networks in [22], the beamforming, power allocation, and the selection of the untrusted relay were analyzed in detail. The performance of fixed-gain beamforming in cooperative networks was studied in [23], and the closed-form expression was derived to determine the probability of discontinuity. The influence of the beamforming design on the security performance with the incomplete channel-state information (CSI) was further explored in [24].

Cooperative jamming is another technology used to combat untrusted relays or eavesdroppers. Physical layer security based on cooperative jamming was first studied in [25], which theoretically proved that third-party jamming signals can effectively improve the network secrecy capacity. Then, a destination-assisted jamming (DAJ-) based secure transmission was devised in [26] for an untrusted and energy-harvesting relay network. In [27], a new closed-form solution was derived to determine the optimal power allocation (OPA) between the base station and mobile user with friendly jamming in two-way untrusted relay networks. Owing to the high complexity for the one-way transmission optimization, we plan the optimization for two-way transmission as an extension based on the results in this paper. In [28], the power allocation and locations of confidential and jamming signals were analyzed in detail in terms of network security performance. In [29], the power allocation for multi-relay nodes was studied. The power-weighting coefficients of decode-and-forward (DF) and AF relay nodes were optimized to achieve the maximum secrecy capacity with a global power constraint. In [30], the network model was extended to a multi-antenna network, and the corresponding cooperative jamming scheme was presented. The power allocation for DAJ networks was studied in [31], where the destination acted as a friendly cooperative jammer.

1.2 | Our contribution

In this paper, a DAJ-based untrusted relay network is considered in the case where multiple antennas are installed at each node. As a special application, this technique can be used in an unmanned aerial vehicle (UAV-) [32,33] based relay network, where the relaying UAVs may only be trusted for service levels and untrusted for data levels. In 60-GHz wireless personal area networks (WPANs), all stations that are equipped with multiple antennas are noncentralized [34]. In this case, the relaying stations cannot be trusted for the transmission, where the technique proposed in this paper can also be applied. To achieve a maximum secrecy rate, beamforming and power allocation at the source and destination should be jointly optimized, which increases the computational complexity of this work. To prevent the untrusted relay from

interpreting confidential information, the destination is required to maximize its cooperative jamming signals. Given this consideration, a matched-filter precoder is introduced for cooperative jamming precoding. At the source, the transmitted precoder design should consider both source-relay and source-relay-destination links. We devised a novel transmitted precoder that is based on generalized singular-value decomposition (GSVD), which causes transmitted confidential signals to be located in the range space of the source-relay-destination channel matrix, while at the same time being orthogonal to the range space of the source-relay channel matrix. An OPA is further studied to maximize the security performance. To decouple the precoder design and OPA, an iterative algorithm is then proposed to jointly optimize the above parameters. In general, the key contributions of this work can be summarized as follows:

- We devised a two-phase DAJ-based secure transmission for multiple confidential symbols. The source transmits the confidential signal to the untrusted relay, while the destination transmits a cooperative jamming signal to the untrusted relay. In this case, the security at the untrusted relay is guaranteed and the secrecy rate for the whole network is improved.
- We formulated an optimization problem to maximize the achievable secrecy rate by jointly optimizing the precoders of the source and destination as well as the power allocation between the source and destination. A novel beamforming is proposed based on GSVD to focus the confidential signal. Moreover, the existence of the OPA factor was carefully analyzed.
- An iterative algorithm is proposed to jointly optimize the three parameters. In each iteration, the feasible solutions are discussed in detail and selected. Numerical results validate the quick convergence of the iterative algorithm.

The rest of the paper is organized as follows. Section 2 describes the system model and formulates the optimization problem. To maximize the secrecy rate, Section 3 derives the precoders as well as the OPA factor for the source and destination, which are further jointly optimized using an iterative algorithm. Numerical results and discussions are presented in Section 4. Finally, the conclusions and future works are given in Section 5.

Notations: Bold symbols in uppercase ($\mathbf{X}$) and lowercase letter ($\mathbf{x}$) denote matrices and vectors, respectively. $|\mathbf{X}|$, $\mathbf{X}^{\mathrm{H}}$, $\mathbf{X}^{\mathrm{T}}$, rank($\mathbf{X}$), Tr($\mathbf{X}$), and $\mathbf{X}^{-1}$ denote the matrix determinant, conjugate transpose, transpose, rank, trace, and inverse, respectively. $\mathbb{E}(\cdot)$ represents the expected value, while $\mathbf{I}_M$ and diag(a, b, c), respectively, represent the $M \times M$ identity matrix and diagonal matrix whose diagonal elements are a, b, and c.

2 | SYSTEM MODEL AND PROBLEM DEFINITION

This section shows the system model for the DAJ network, and how it can be used to increase the secrecy performance. Then, it presents the mathematical formula for optimizing the power allocation to achieve the highest secrecy rate.

2.1 | System model

It is assumed that a source node ($\mathcal{S}$) intends to send a confidential signal through the untrusted relay node ($\mathcal{R}$) to the destination ($\mathcal{D}$) within two time slots, as shown in Figure 1. There is no direct communication link between $\mathcal{S}$ and $\mathcal{D}$ because of long distance or shadowing. Considering the DAJ network, in the first time slot, $\mathcal{S}$ transmits confidential signals to $\mathcal{R}$, and $\mathcal{D}$ simultaneously emits cooperative jamming signals with the same frequency band to prevent $\mathcal{R}$ from decoding the confidential signals. Then, after receiving both signals in the first time slot, $\mathcal{R}$ amplifies and forwards them in the second time slot (ie, $\mathcal{R}$ works in AF mode).

In the distributed 60-GHz WPAN, all stations are symmetrical with the same configurations [34]. Also considering the future extension to two-way transmissions, $\mathcal{S}$ and $\mathcal{D}$ have the same transmission capability. In this case, we assume that the same number of antennas are installed at $\mathcal{S}$ and $\mathcal{D}$. Here, we assume that $\mathcal{S}$ and $\mathcal{D}$ both have N_{t} antennas, while $\mathcal{R}$ is equipped with N_{r} antennas. The transmitted signal vector from $\mathcal{S}$ can be expressed as $\mathbf{x}_{\mathrm{S}} = \mathbf{F}_{\mathrm{S}}\mathbf{s}_{\mathrm{S}}$, where $\mathbf{s}_{\mathrm{S}} \in \mathbb{C}^{L\times 1}$ is the modulated confidential symbol vector, and $\mathbf{F}_{\mathrm{S}} \in \mathbb{C}^{N_{\mathrm{t}}\times L}$ denotes the transmitted precoding matrix. The length of the confidential symbols, L, will be analyzed later. To fully exploit the multiplexing gain, it is recommended that $L \le N_{\mathrm{t}} \le N_{\mathrm{r}}$. However, the jamming signal is emitted from $\mathcal{D}$ in the first time slot, which is defined as $\mathbf{x}_{\mathrm{J}} = \mathbf{F}_{\mathrm{D}}\mathbf{s}_{\mathrm{J}}$, where $\mathbf{s}_{\mathrm{J}} \in \mathbb{C}^{N_{\mathrm{t}}\times 1}$ refers to the jamming symbol vector, and $\mathbf{F}_{\mathrm{D}} \in \mathbb{C}^{N_{\mathrm{r}}\times N_{\mathrm{t}}}$ denotes the jamming transmitted precoding matrix.

As in [35,36], we also assume that there is another centralized master station (MS) in charge of gathering and distributing the CSI, calculating, and delivering the OPA for

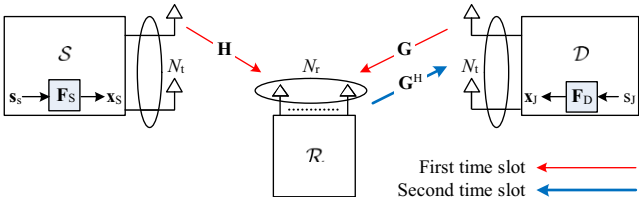


FIGURE 1 Signal transmission in two-hop DAJ-based untrusted relay network

both confidential and jamming signals at $\mathcal{S}$ and $\mathcal{D}$. However, this topic is beyond the scope of this paper. In this system, equal power is assigned to each symbol at $\mathcal{S}$ and $\mathcal{D}$, and let $\alpha \in (0, 1)$ be the power-allocation factor between confidential and jamming signals transmitted from $\mathcal{S}$ and $\mathcal{D}$, respectively, that is, $\mathbb{E}[\mathbf{s}_S\mathbf{s}_S^H] = \frac{\alpha P}{N_t}\mathbf{I}_L$, and $\mathbb{E}[\mathbf{s}_J\mathbf{s}_J^H] = \frac{(1-\alpha)P}{N_t}\mathbf{I}_{N_t}$, where P is the total power transmitted by $\mathcal{S}$ and $\mathcal{D}$. Note that α cannot take values at 0 and 1. When $\alpha = 0$, the power of transmitting confidential signals is 0, which cannot implement information communication; on the contrary, when $\alpha = 1$, the power of transmitting cooperative jamming signals is 0, which cannot interfere with the eavesdropping of untrusted relays. The transmission for the above cases is not suitable in practical applications.

Based on the above assumptions, in the first time slot, the received $N_r \times 1$ signal vector at $\mathcal{R}$ can be denoted as

$$\begin{aligned}\mathbf{y}_R &= \mathbf{H}\mathbf{x}_S + \mathbf{G}\mathbf{x}_J + \mathbf{n}_R \\ &= \mathbf{H}\mathbf{F}_S\mathbf{s}_S + \mathbf{G}\mathbf{F}_D\mathbf{s}_J + \mathbf{n}_R,\end{aligned} \tag{1}$$

where $\mathbf{H}$ and $\mathbf{G} \in \mathbb{C}^{N_r \times N_t}$ are the multiple-input multiple-output (MIMO) channel matrices from $\mathcal{S}$ to $\mathcal{R}$, and from $\mathcal{D}$ to $\mathcal{R}$, respectively, and $\mathbf{n}_R \sim \mathcal{CN}(0, {\sigma_r}^2\mathbf{I}_{N_r})$ represents the additive noise vector at $\mathcal{R}$.

Note that the relay in our system model is considered to be untrusted. In addition to the traditional relay functionality, it tends to intercept the confidential signal. The overall interference-plus-noise covariance matrix at untrusted $\mathcal{R}$ is defined as $\mathbf{Q}_R = \frac{(1-\alpha)P}{N_t}\mathbf{G}\mathbf{F}_D\mathbf{F}_D^H\mathbf{G}^H + {\sigma_r}^2\mathbf{I}_{N_r}$. Then, the instantaneous rate at $\mathcal{R}$ is calculated as

$$\begin{aligned}R_R &= \log_2\left|\mathbf{I}_{N_r} + \frac{\alpha P}{N_t}\mathbf{H}\mathbf{F}_S\mathbf{F}_S^H\mathbf{H}^H \right. \\ &\quad \left. \times\left(\frac{(1-\alpha)P}{N_t}\mathbf{G}\mathbf{F}_D\mathbf{F}_D^H\mathbf{G}^H + {\sigma_r}^2\mathbf{I}_{N_r}\right)^{-1}\right| \\ &\approx \log_2\left|\mathbf{I}_{N_r} + \frac{\alpha}{1-\alpha}\mathbf{H}\mathbf{F}_S\mathbf{F}_S^H\mathbf{H}^H(\mathbf{G}\mathbf{F}_D\mathbf{F}_D^H\mathbf{G}^H)^{-1}\right| \\ &= \log_2\left|\mathbf{I}_{N_r} + \frac{\alpha}{1-\alpha}\left(\mathbf{G}\mathbf{F}_D\mathbf{F}_D^H\mathbf{G}^H\right)^{-\frac{1}{2}}\mathbf{H}\mathbf{F}_S\mathbf{F}_S^H \right. \\ &\quad \left. \times\left(\left(\mathbf{G}\mathbf{F}_D\mathbf{F}_D^H\mathbf{G}^H\right)^{-\frac{1}{2}}\mathbf{H}\right)^H\right| \\ &= \log_2\left|\mathbf{I}_{N_r} + \frac{\alpha}{1-\alpha}\mathbf{S}_R\mathbf{F}_S\mathbf{F}_S^H\mathbf{S}_R^H\right|,\end{aligned} \tag{2}$$

where $\mathbf{S}_R = (\mathbf{G}\mathbf{F}_D\mathbf{F}_D^H\mathbf{G}^H)^{-\frac{1}{2}}\mathbf{H}$ and the second equation in (2) results from the approximation with the assumption of a high signal-to-noise ratio (SNR) for simplification. The impact of this approximation is discussed and validated in Section 4. Based on the above rate, if the untrusted relay $\mathcal{R}$ has a relatively high rate to decode the confidential signals, the system becomes insecure.

In the second time slot, the relay amplifies $\mathbf{y}_R$ with fixed gain. Note that in some practical applications, the relay is set up in advance, which has steady and sufficient power provision. Therefore, to simplify our analysis, we do not consider the power constraint at the relay. Without loss of generality, we assume that $\mathcal{R}$ retransmits the signals in all directions in an equal manner and fixed unity gain. Then, the received $N_t \times 1$ signal vector at $\mathcal{D}$ is formulated as

$$\mathbf{y}_D = \mathbf{G}^H\mathbf{H}\mathbf{x}_S + \mathbf{G}^H\mathbf{G}\mathbf{x}_J + \mathbf{G}^H\mathbf{n}_R + \mathbf{n}_D, \tag{3}$$

where $\mathbf{n}_D \sim \mathcal{CN}(0, {\sigma_d}^2\mathbf{I}_{N_t})$ is the additive noise vector at $\mathcal{D}$, and $\mathbf{G}^H$ denotes the channel matrix from $\mathcal{R}$ to $\mathcal{D}$ with the assumption of channel duality [37]. As the MS is responsible for distributing the channel information, the CSI is perfectly known at $\mathcal{D}$. Therefore, the second term in (3) is considered as back-propagating self-interference of $\mathcal{D}$, which can be subtracted perfectly. Then, the instantaneous rate at $\mathcal{D}$ can be defined as

$$\begin{aligned}R_D &= \log_2\left|\mathbf{I}_{N_r} + \frac{\alpha P}{N_t}\left({\sigma_r}^2\mathbf{G}^H\mathbf{G} + {\sigma_d}^2\mathbf{I}_{N_t}\right)^{-\frac{1}{2}}\mathbf{G}^H\mathbf{H} \right. \\ &\quad \left. \times\mathbf{F}_S\mathbf{F}_S^H\left(\left({\sigma_r}^2\mathbf{G}^H\mathbf{G} + {\sigma_d}^2\mathbf{I}_{N_t}\right)^{-\frac{1}{2}}\mathbf{G}^H\mathbf{H}\right)^H\right| \\ &= \log_2\left|\mathbf{I}_{N_t} + \frac{\alpha P}{N_t}\mathbf{S}_D\mathbf{F}_S\mathbf{F}_S^H\mathbf{S}_D^H\right|,\end{aligned} \tag{4}$$

where $\mathbf{S}_D = ({\sigma_r}^2\mathbf{G}^H\mathbf{G} + {\sigma_d}^2\mathbf{I}_{N_t})^{-\frac{1}{2}}\mathbf{G}^H\mathbf{H}$.

2.2 | Problem definition

In our scheme, we attempt to optimize the beamforming and power allocation for confidential and cooperative jamming signals to achieve secure transmission. From the perspective of physical layer security as [38], secure transmission guarantees zero or small capability for $\mathcal{R}$ to interpret the confidential signals, while verifying an achievable rate at $\mathcal{D}$ that is as large as possible. In this way, we utilize the definition of the secrecy rate in [38], which is formulated as

$$R_s = \frac{1}{2}\max\{0, R_D - R_R\}, \tag{5}$$

where R_s is non-negative, and the coefficient is $\frac{1}{2}$ because the transmission requires two time slots.

In this paper, by jointly optimizing the beamforming and power allocation, we aim to maximize the achievable secrecy rate with the total power constraint [11]. This optimization can thus be mathematically formulated as

$$\begin{aligned}\max_{\alpha,\mathbf{F}_S,\mathbf{F}_D}\ & R_s \\ \text{s.t.:}\ & \alpha \in (0,1) \\ & \mathrm{Tr}(\mathbf{F}_S\mathbf{F}_S^H) \le N_t \\ & \mathrm{Tr}(\mathbf{F}_D\mathbf{F}_D^H) \le N_t\end{aligned} \tag{6}$$

where the first constraint in (6) defines the power allocation for $\mathcal{S}$ and $\mathcal{D}$, while the transmitted precoders for confidential and cooperative jamming signals are constrained in

the second and third constraints. Actually, it is a challenging task to jointly optimize beamforming and power allocation for one-way secure transmission because the objective function is unlikely to be a convex function [39]. Generally, the power allocation is a nontrivial problem because the power allocation will affect the quality of both legitimate and eavesdropped signals. Therefore, the optimization problem is nonconvex, and there is no well-known systematic approach for solving the optimization problem instantly.

Using R_D in (4) and R_R in (2), the objective function in (6) can be rewritten as

$$R_s = \frac{1}{2}\log_2 \frac{\left|\mathbf{I}_{N_t} + \frac{\alpha P}{N_t}\mathbf{S}_D\mathbf{F}_S\mathbf{F}_S^H\mathbf{S}_D^H\right|}{\left|\mathbf{I}_{N_r} + \frac{\alpha}{1-\alpha}\mathbf{S}_R\mathbf{F}_S\mathbf{F}_S^H\mathbf{S}_R^H\right|}, \tag{7}$$

where the max operation is not considered.

3 | JOINT OPTIMIZATION OF BEAMFORMING AND POWER ALLOCATION

From (6) and (7), the optimization problem in its original form cannot be solved directly using traditional optimization methods because the objective appears as nonconvex [39], and α, $\mathbf{F}_S$, and $\mathbf{F}_D$ are cross-related. Therefore, we proposed a four-step solution that optimizes $\mathbf{F}_D$, $\mathbf{F}_S$, and α. Then, by considering the correlation between the above parameters, we finally introduce an iterative procedure to achieve the near-optimal solution.

3.1 | Optimization of $\mathbf{F}_D$

In the DAJ system, $\mathbf{F}_D$ was designed to increase the cooperative jamming signal emitted from $\mathcal{D}$ in order to prevent untrusted relay $\mathcal{R}$ from interpreting the confidential signals. As is commonly known, matched-filter precoding can maximize the received SNR; here, we thus utilized the matched-filter precoder to design $\mathbf{F}_D$ in order to concentrate the jamming signal to $\mathcal{R}$, that is, $\mathbf{F}_D = \mathbf{G}^H$. In this case, from (2), the objective function can then be converted into

$$R_s = \frac{1}{2}\log_2 \frac{\left|\mathbf{I}_{N_t} + \frac{\alpha P}{N_t}\mathbf{S}_D\mathbf{F}_S\mathbf{F}_S^H\mathbf{S}_D^H\right|}{\left|\mathbf{I}_{N_r} + \frac{\alpha}{1-\alpha}\mathbf{S}_{\overline{R}}\mathbf{F}_S\mathbf{F}_S^H\mathbf{S}_{\overline{R}}^H\right|}, \tag{8}$$

where $\mathbf{S}_{\overline{R}} = (\mathbf{G}\mathbf{G}^H\mathbf{G}\mathbf{G}^H)^{-\frac{1}{2}}\mathbf{H}$.

3.2 | Optimization of $\mathbf{F}_S$

From the expression for R_s in (8), we can observe that the transmitted precoder, $\mathbf{F}_S$, is located in both the nominator and the denominator. From the understanding of the subspace, to maximize the division in (8), $\mathbf{F}_S$ should be focused to the subspace spanned by the column of $\mathbf{S}_D$, and at the same time, be orthogonal to the subspace spanned by the column of $\mathbf{S}_{\overline{R}}$. With this subspace consideration, GSVD is a powerful tool in the design of the precoder [40–42]. Using GSVD, the covariances $\mathbf{S}_D$ and $\mathbf{S}_{\overline{R}}$ can be simultaneously diagonalized as

$$\begin{aligned}\mathbf{S}_D &= \mathbf{U}\mathbf{\Sigma}_D\mathbf{K}^H \\ \mathbf{S}_{\overline{R}} &= \mathbf{V}\mathbf{\Sigma}_R\mathbf{K}^H\end{aligned}, \tag{9}$$

where $\mathbf{U} \in \mathbb{C}^{N_t \times N_t}$ and $\mathbf{V} \in \mathbb{C}^{N_r \times N_r}$ are both unitary matrices, $\mathbf{\Sigma}_D \in \mathbb{R}^{N_t \times N_t}$ and $\mathbf{\Sigma}_R \in \mathbb{C}^{N_r \times N_t}$ are diagonal matrices, and $\mathbf{K} \in \mathbb{C}^{N_t \times N_t}$ is a common unitary matrix for $\mathbf{S}_D$ and $\mathbf{S}_{\overline{R}}$. Note that one of the most important properties for GSVD is

$$\mathbf{\Sigma}_D^T\mathbf{\Sigma}_D + \mathbf{\Sigma}_R^T\mathbf{\Sigma}_R = \mathbf{I}_{N_t}, \tag{10}$$

where the diagonal elements of $\mathbf{\Sigma}_D$, $\eta_{d,1}, \ldots, \eta_{d,N_t}$, are arranged in increasing order, that is, $0 \le \eta_{d,1} \le \cdots \le \eta_{d,N_t} \le 1$, while the elements of $\mathbf{\Sigma}_R$, $\eta_{r,1}, \ldots, \eta_{r,N_r}$, are arranged in decreasing order, that is, $1 \ge \eta_{d,1} \ge \cdots \ge \eta_{r,N_r} \ge 0$. Therefore, the objective problem in (8) can be reformulated as

$$\begin{aligned}R_s &= \frac{1}{2}\log_2 \frac{\left|\mathbf{I}_{N_t} + \frac{\alpha P}{N_t}\mathbf{U}\mathbf{\Sigma}_D\mathbf{K}^H\mathbf{F}_S\mathbf{F}_S^H\mathbf{K}\mathbf{\Sigma}_D\mathbf{U}^H\right|}{\left|\mathbf{I}_{N_r} + \frac{\alpha}{1-\alpha}\mathbf{V}\mathbf{\Sigma}_R\mathbf{K}^H\mathbf{F}_S\mathbf{F}_S^H\mathbf{K}\mathbf{\Sigma}_R\mathbf{V}^H\right|} \\ &= \frac{1}{2}\log_2 \frac{\left|\mathbf{U}\left(\mathbf{I}_{N_t} + \frac{\alpha P}{N_t}\mathbf{\Sigma}_D\mathbf{K}^H\mathbf{F}_S\mathbf{F}_S^H\mathbf{K}\mathbf{\Sigma}_D\right)\mathbf{U}^H\right|}{\left|\mathbf{V}\left(\mathbf{I}_{N_r} + \frac{\alpha}{1-\alpha}\mathbf{\Sigma}_R\mathbf{K}^H\mathbf{F}_S\mathbf{F}_S^H\mathbf{K}\mathbf{\Sigma}_R\right)\mathbf{V}^H\right|} \\ &= \frac{1}{2}\log_2 \frac{\left|\mathbf{I}_{N_t} + \frac{\alpha P}{N_t}\mathbf{\Sigma}_D\mathbf{K}^H\mathbf{F}_S\mathbf{F}_S^H\mathbf{K}\mathbf{\Sigma}_D\right|}{\left|\mathbf{I}_{N_r} + \frac{\alpha}{1-\alpha}\mathbf{\Sigma}_R\mathbf{K}^H\mathbf{F}_S\mathbf{F}_S^H\mathbf{K}\mathbf{\Sigma}_R\right|},\end{aligned} \tag{11}$$

where the last equation is based on the determinant property that similar matrices have the same determinant. By designing $\mathbf{F}_S = (\mathbf{K}^H)^{-1}$, the numerator and denominator are converted to diagonal matrices. After some simple calculations, the secrecy rate in (11) can be directly formulated as

$$\begin{aligned}R_s &= \frac{1}{2}\log_2 \prod_{i=1}^{N_t}\left(1 + \frac{\frac{\alpha P}{N_t}\eta_{d,i}^2 - \frac{\alpha}{1-\alpha}\eta_{r,i}^2}{1 + \frac{\alpha}{1-\alpha}\eta_{r,i}^2}\right) \\ &= \frac{1}{2}\sum_{i=1}^{N_t}\log_2\left(1 + \frac{\frac{\alpha P}{N_t}\eta_{d,i}^2 - \frac{\alpha}{1-\alpha}\eta_{r,i}^2}{1 + \frac{\alpha}{1-\alpha}\eta_{r,i}^2}\right).\end{aligned} \tag{12}$$

From (12), maximizing the achievable secrecy rate can be implemented by only selecting the items with positive rates. Furthermore, from (10), singular values in $\mathbf{\Sigma}_D$ and $\mathbf{\Sigma}_R$ are, respectively, arranged in descending and ascending order. These characteristics allow us to perform selection operations on $(\mathbf{K}^H)^{-1}$. Denote $(\mathbf{K}^H)^{-1} = (\mathbf{k}_1, \cdots, \mathbf{k}_M, \cdots, \mathbf{k}_{N_t})$ where $\mathbf{k}_i \in \mathbb{C}^{N_t \times 1}$ denotes the ith column of

$(\mathbf{K}^{\mathrm{H}})^{-1}$ for $i = 1, \ldots, N_{\mathrm{t}}$. With the constraint of positive rate, we have $\frac{\alpha P}{N_{\mathrm{t}}}\eta_{\mathrm{d},i}^2 > \frac{\alpha}{1-\alpha}\eta_{\mathrm{r},i}^2$, that is, $\eta_{\mathrm{d},i}^2 > \frac{N_{\mathrm{t}}}{(1-\alpha)P}\eta_{\mathrm{r},i}^2$. If $\eta_{\mathrm{d},M}^2 > \frac{N_{\mathrm{t}}}{(1-\alpha)P}\eta_{\mathrm{r},M}^2$ and $\eta_{\mathrm{d},M-1}^2 \leq \frac{N_{\mathrm{t}}}{(1-\alpha)P}\eta_{\mathrm{r},M-1}^2$, only the right $L = N_{\mathrm{t}} - M + 1$ columns of $(\mathbf{K}^{\mathrm{H}})^{-1}$ are selected as the precoder, $\mathbf{F}_{\mathrm{S}}^*$, based on the above analysis. In this case, $\mathbf{F}_{\mathrm{S}}^*$ can be formulated as

$$\mathbf{F}_{\mathrm{S}}^* = (\mathbf{k}_M, \cdots, \mathbf{k}_{N_{\mathrm{t}}}). \tag{13}$$

Using (13), we can further simplify the secrecy rate as

$$R_{\mathrm{s}} = \frac{1}{2}\sum_{i=M}^{N_{\mathrm{t}}} \log_2\left(1 + \frac{\frac{\alpha P}{N_{\mathrm{t}}}\eta_{\mathrm{d},i}^2 - \frac{\alpha}{1-\alpha}\eta_{\mathrm{r},i}^2}{1 + \frac{\alpha}{1-\alpha}\eta_{\mathrm{r},i}^2}\right). \tag{14}$$

3.3 | Optimization of α

When $0 < \alpha < 1$, R_{S} is a convex function with respect to α, whose proof can be found in the Appendix. Therefore, there must exist an optimum of α, α_{opt} to maximize the achievable secrecy rate. Considering the convex property of R_{s}, the OPA α_{opt} can be obtained by solving $\frac{\mathrm{d}R_{\mathrm{s}}}{\mathrm{d}\alpha} = 0$, where the first-order derivative of R_{S} in (14) with respect to α is shown as

$$\frac{\mathrm{d}R_{\mathrm{s}}}{\mathrm{d}\alpha} = \frac{1}{2\log 2} \times \sum_{i=M}^{N_{\mathrm{t}}}\left(\frac{\frac{P}{N_{\mathrm{t}}}\eta_{\mathrm{d},i}^2}{1 + \frac{\alpha P}{N_{\mathrm{t}}}\eta_{\mathrm{d},i}^2} - \frac{\eta_{\mathrm{r},i}^2}{(1-\alpha)^2 + \alpha(1-\alpha)\eta_{\mathrm{r},i}^2}\right). \tag{15}$$

3.4 | Iterative procedure for the joint optimization

From Section 3.2, we find that the value of α will impact the number of selected columns. On the contrary, from Section 3.3, the OPA α_{opt} is influenced by the number of selected columns. These two parameters, $\mathbf{F}_{\mathrm{S}}^*$ and α_{opt}, have across relationship. To jointly optimize $\mathbf{F}_{\mathrm{S}}$ and α, an iterative algorithm is thus devised to maximize the secrecy rate. The iterative algorithm to solve the optimization problem (6) is summarized in Algorithm 1.

Algorithm 1 Joint BF and OPA for DAJ scheme.

1. Initialize power-allocation factor, $\alpha_0 = 0.5$. Let k be the counter of iterations, which varies from 1 to N. N is the maximum number of iterations, and usually has a value of 10. Furthermore, let α_k be the calculated power allocation after the kth iteration;
2. Based on matched-filter precoders, construct the cooperative jamming precoders $\mathbf{F}_{\mathrm{D}} = \mathbf{G}^{\mathrm{H}}$.
3. Using GSVD to jointly decompose $\mathbf{S}_{\mathrm{D}}$ and $\mathbf{S}_{\overline{\mathrm{R}}}$ in (9) to find $\mathbf{K}$.

for $k = 1 : N$ **do**

$L \leftarrow \eta_{\mathrm{d},i}^2 \frac{N_{\mathrm{t}}}{(1-\alpha_{k-1})P}\eta_{\mathrm{r},i}^2$;

Construct $\mathbf{F}_{\mathrm{S}}^*$ with $\mathbf{K}$ and L as (13);

$\alpha_k \leftarrow \mathrm{Roots}\{\frac{\mathrm{d}R_{\mathrm{s}}}{\mathrm{d}\alpha} = 0\}$;

if $|\alpha_k - \alpha_{k-1}| \leq \varepsilon$ **then**

//where ε is a sufficiently small positive number that determines the accuracy of the iterative optimization result. Here, we set $\varepsilon = 0.01$;

Break;

end if

end for

3.5 | Complexity analysis

Here, we analyze the complexity of Algorithm 1. The dominated computational complexity attributes to GSVD operation and optimum searching with (15). From [42], the computational complexity of the GSVD operation is $\mathcal{O}((N_{\mathrm{t}} + N_{\mathrm{r}}) \times N_{\mathrm{t}}^2)$. In this study, we assume that the searching step for the optimum with (15) is $\Delta\alpha = 0.001$ Then, its computational complexity is $(6 \times (N_{\mathrm{t}} - M + 1) \times 1{,}000 \times N)$ in multiplication operations, where N denotes the maximum number of iterations and the number 6 represents six multiplication operations for one-step searching.

3.6 | Special cases

In this subsection, to further show the superiority of our proposed scheme, we discuss a different power-allocation scheme, namely AF relaying with equal power allocation (AF-EPA). In this case, the confidential and cooperative jamming signals are transmitted with equal power, that is, $\alpha = 0.5$. Substituting $\alpha = 0.5$ into (12), we obtain the achievable secrecy rate as

$$R_{\mathrm{s}}^{\mathrm{EPA}} = \frac{1}{2}\log_2 \prod_{i=M}^{N_{\mathrm{t}}}\left(1 + \frac{\frac{P}{2N_{\mathrm{t}}}\eta_{\mathrm{d},i}^2 - \eta_{\mathrm{r},i}^2}{1 + \eta_{\mathrm{r},i}^2}\right). \tag{16}$$

Note that in (16), the parameter M is selected with $N_{\mathrm{t}} - M + 1$, and $N_{\mathrm{t}} - M + 1$ represents the number of singular values satisfying $\frac{P}{2N_{\mathrm{t}}}\eta_{\mathrm{d},i}^2 \geq \eta_{\mathrm{r},i}^2$. Equal power allocation does not consider the difference in channels; therefore, some performance loss will exist as expected.

4 | SIMULATIONS AND RESULTS

In this section, we present some numerical results to validate our proposed algorithm. Assume that the elements of the channel matrices, $\mathbf{H}$ and $\mathbf{G}$, are all complex Gaussian random variables with zero mean and unit variances. For each

simulation, we use 10,000 independent realizations of the fading channels. The antenna configuration at the source S, the relay $\mathcal{R}$, and the destination $\mathcal{D}$ is represented as (N_t, N_r, N_t). Moreover, in all simulations, we configure $N_r > N_t$ to guarantee full multiplexing gain, and we utilize a matched-filter precoder to beamform the cooperative jamming signal in order to secure the confidential signal at the untrusted relay.

Figure 2 compares the secrecy rates of different transmitted precoders with antenna configuration (6, 8, 6). For comparison, we introduce two transmitted precoders, an equal BF to emit the confidential signals in all directions, and a random BF to beamform the transmitted signal in a random direction. From Figure 2, the proposed scheme precoder provides the highest secrecy rate at all values of SNRs, while a random BF has the lowest one because its beamforming may result in no signal arriving at the destination. Compared with equal BF, the focalization of our proposed beamforming benefits the improvement of secrecy rate. Besides, we also simulate the impact of the approximation of neglecting $\sigma_r^2\mathbf{I}_{N_r}$ in (2) in Section 2. We can find that the approximation introduces a negligible error on the performance regardless of whether the SNR is high or low.

Figures 3 and 4 compare the achievable secrecy rates for different SNR levels and different values of N_t, respectively. We observe that the secrecy rate increases with increases of SNR or N_t. This improvement can be attributed to the fact that a larger number of antennas at $\mathcal{S}$ and $\mathcal{D}$, that is, larger DoFs, help to form a narrower and more precise beam directed to $\mathcal{R}$ with higher gain. Specifically, the channel gains for $\mathbf{H}$ and $\mathbf{G}$ increase with the increase in N_t. In (1), the signals received by $\mathcal{R}$ from $\mathcal{S}$ and $\mathcal{D}$ become stronger at the same time, but the SNR at $\mathcal{R}$ does not change significantly, and thus little improvement of the rate can be realized at $\mathcal{R}$.

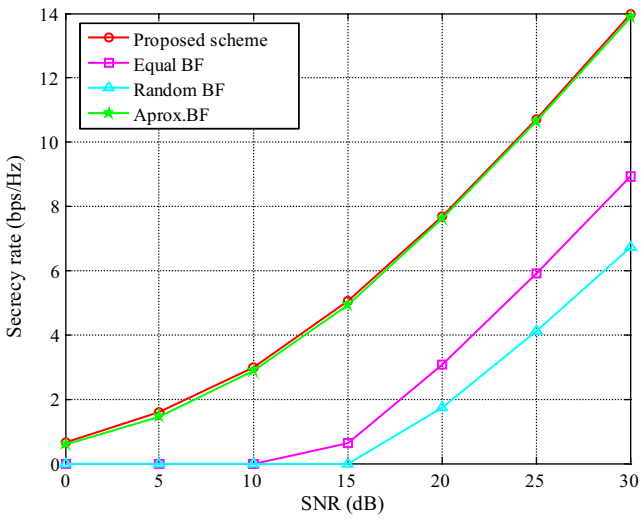


FIGURE 2 Secrecy rates for different precoders with antenna configuration (6, 8, 6)

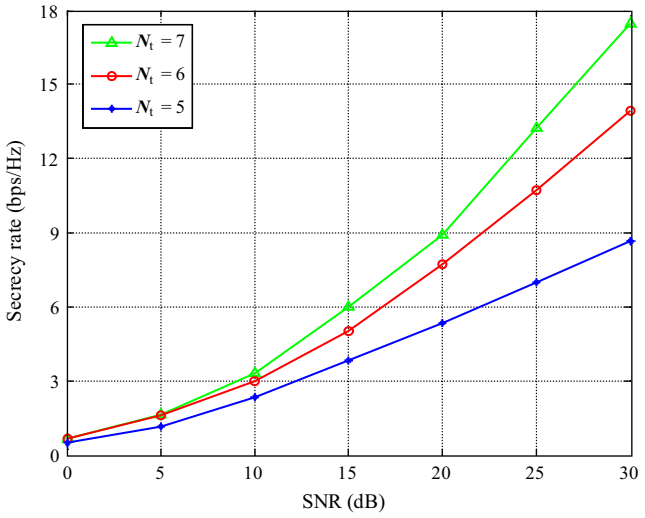


FIGURE 3 Secrecy rate of our proposed scheme for different SNR levels when $N_r = 8$

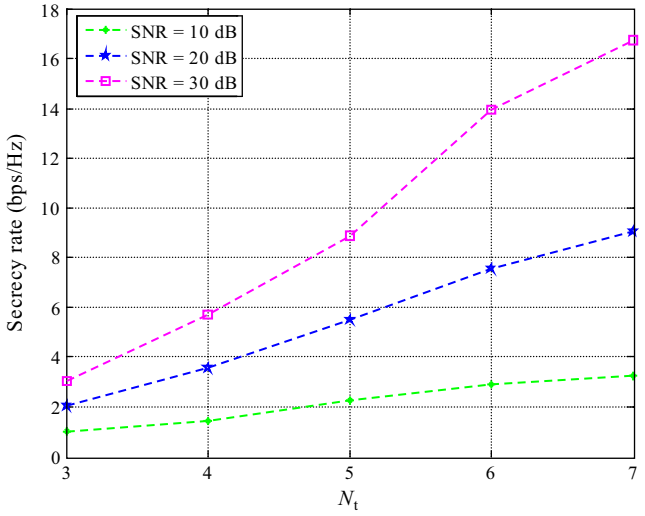


FIGURE 4 Secrecy rate of our proposed scheme for different values of N_t when $N_r = 8$

Furthermore, from (3), the jamming signal at $\mathcal{D}$ from itself is eliminated through self-interference cancellation. Therefore, the SNR at $\mathcal{D}$ will increase by fully exploiting the channel gains of both $\mathbf{H}$ and $\mathbf{G}$, which results in the increase in the rate at $\mathcal{D}$. Then, from (5), the total secrecy rate of the system will increase eventually.

Figures 5 and 6 show the achievable secrecy rates for different SNRs and different values of N_r when $N_t = 6$. In this case, the secrecy rate decreases with an increase in N_r. The eavesdropping ability of the untrusted relay is improved with an increase in N_r; then, the rate at $\mathcal{R}$ will increase. Meanwhile, in the second time slot transmission, there is no beamforming design for $\mathcal{R}$ because the relay is untrusted. Therefore, there is no significant or small increase in the secrecy rate at $\mathcal{D}$. Consequently, from (5), the secrecy rate of the system decreases.

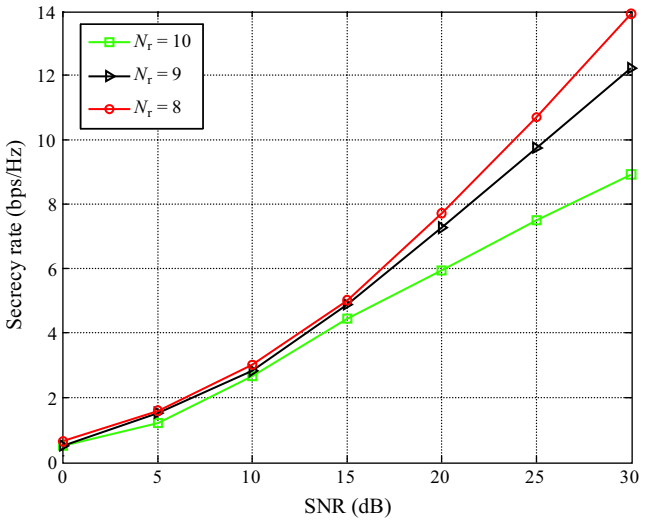


FIGURE 5 Secrecy rate of our proposed scheme for different SNR levels when $N_t = 6$

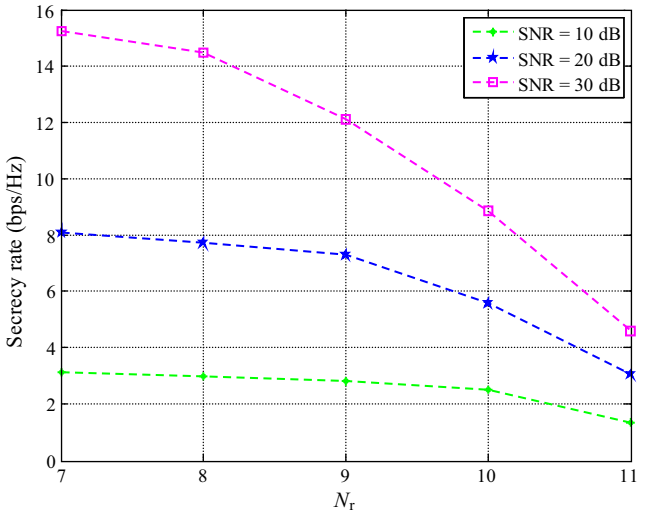


FIGURE 6 Secrecy rate of our proposed scheme for different values of N_r when $N_t = 6$

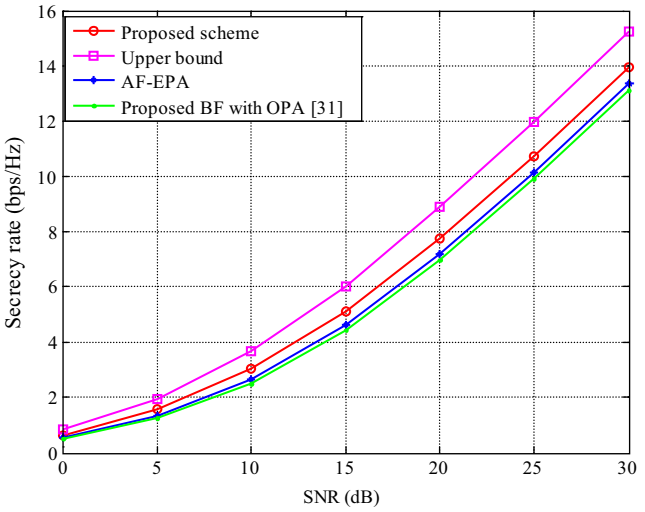


FIGURE 7 Secrecy rates for different power allocation with antenna configuration (6, 8, 6)

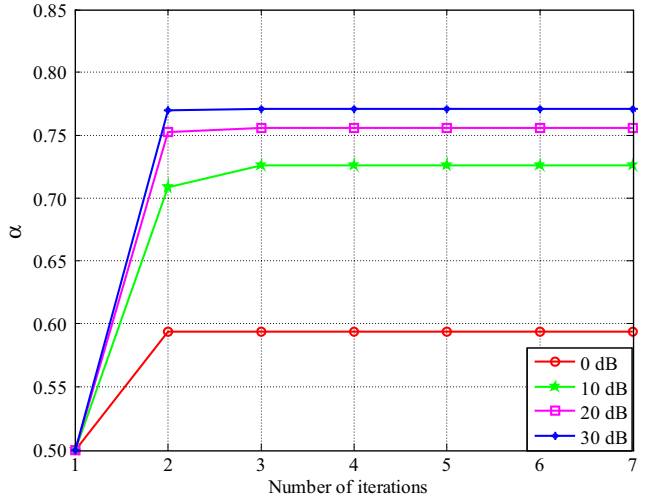


FIGURE 8 Convergence of OPA for different SNRs at $N_t = 6$ and $N_r = 8$.

In Figure 7, we compare the secrecy rates of our proposed OPA scheme, AF-EPA, and the power allocation calculated in [31] with the proposed optimized BF for the antenna configuration (6, 8, 6). In [31], Kuhestani et al. proposed an OPA for a one-way cooperative jamming network with maximum-ratio transmission (MRT) beamforming. However, the MRT beamforming was applied only at the source to maximize the received SNR with low complexity [43]. From Figure 7, it can be easily concluded that our proposed OPA and beamforming scheme has superior performance. One reason for the superiority is that the proposed beamforming was applied at both the source and the destination. Another reason is that we used GSVD to devise a novel transmitted precoder at the source to focus the beam, which could result in an improvement over MRT beamforming. Actually, our improvement is at the cost of increased complexity for the precoding design. When considering the AF-EPA scheme with equal power allocation, we determine that our proposed scheme with OPA can achieve a gain in terms of the secrecy rate.

In Figure 8, we first show the convergence of Algorithm 1 for a given channel realization at different SNRs, such as 0 dB, 10 dB, 20 dB, and 30 dB, when $N_t = 6$ and $N_r = 8$. In each simulation, the channels are randomly generated. From Figure 8, the power-allocation factor α quickly converges to the optimal values after only 3-4 iterations. Besides, the optimal values converge more quickly as the SNRs increase. At small SNRs, the impact of large noise on α requires more iterations to be smoothed. Specifically, in Figure 9, we show the convergences of Algorithm 1 for 100 randomly generated channel realizations at

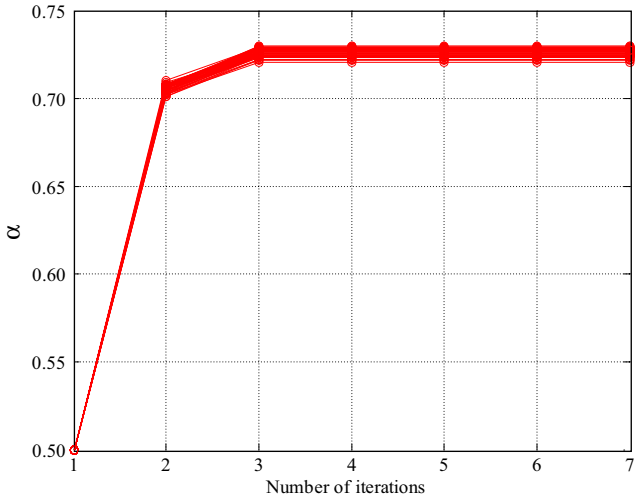


FIGURE 9 Convergence of OPA for SNR = 10 dB at $N_t = 6$ and $N_r = 8$.

SNR = 10 dB. From Figure 9, we can see that the value of α will vary on a small scale for different channel realizations and with a similar trend.

5 | CONCLUSIONS

This paper considers two-hop untrusted relay networks with multiple antennas installed, where DAJ is used to protect the confidential information from being interpreted by an untrusted relay. To achieve the twofold improvement in the rate and security, we jointly optimize the beamforming and power allocation between both the confidential signal from the source and the cooperative jamming signal from the destination. A matched-filter precoder was first designed to maximize the jamming signal. Then, the transmitted precoder is newly devised based on GSVD, which makes a confidential signal be located in the subspace of the source-relay-destination link; meanwhile, it is orthogonal to the subspace of the source-relay link. An OPA is further studied to maximize the security performance. To decouple the precoder design and OPA, an iterative algorithm is then proposed to jointly optimize the above parameters. The numerical results were presented to validate the efficiency and improvement of the proposed scheme. In future work, we will extend this work to two-way untrusted relay networks.

ACKNOWLEDGEMENTS

This work was supported in part by the National Natural Science Foundation of China (No. 61501376 and 61701407), the Science and Technology Program of Shenzhen, China (No. JCYJ20170306155652174), the Fundamental Research Funds for the Central Universities (No. 3102018JGC006 and 3102017JG02002), the Aeronautical Science Foundation of China (2017ZC53029), and the Graduate Starting Seed Fund of Northwestern Polytechnical University (No. ZZ2018128).

ORCID

Rugui Yao http://orcid.org/0000-0003-1396-3802

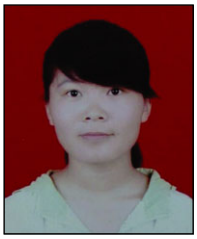
REFERENCES

1. A. Barenghi et al., *Fault injection attacks on cryptographic devices: Theory, practice, and countermeasures*, Proc. IEEE **100**, (2012), no. 11, 3056–3076.
2. A. Mukherjee et al., *Principles of physical layer security in multiuser wireless networks: A survey*, IEEE Commun. Sur. Tut. **16**, (2014), no. 3, 1550–1573.
3. N. Yang et al., *Safeguarding 5G wireless communication networks using physical layer security*, IEEE Commun. Mag. **53**, (2015), no. 4, 20–27.
4. A. D. Wyner, *The wire-tap channel*, Bell Syst. Tech. J. **54**, (1975), no. 8, 1355–1387.
5. S. Leung-Yan-Cheong and M. Hellman, *The Gaussian wire-tap channel*, IEEE Trans. Inform. Theory **24**, (1978), no. 4, 451–456.
6. J. N. Laneman, D. N. C. Tse, and G. W. Wornell, *Cooperative diversity in wireless networks: Efficient protocols and outage behavior*, IEEE Trans. Inform. Theory **50**, (2004), no. 12, 3062–3080.
7. P. Xu, Z. Ding, and X. Dai, *Achievable secrecy rates for relay-eavesdropper channel based on the application of noisy network coding*, IEEE Trans. Inform. Forens. Security **13**, (2018), no. 7 1736–1751.
8. L. Fan et al., *Secure multiuser communications in multiple amplify-and-forward relay networks*, IEEE Trans. Commun. **62**, (2014), no. 9, 3299–3310.
9. L. Fan et al., *Secure multiple amplify-and-forward relaying with cochannel interference*, IEEE J. Sel. Topics Signal Process. **10**, (2016), no. 8, 1494–1505.
10. X. He and A. Yener, Two-hop secure communication using an untrusted relay: A case for cooperative jamming, *IEEE Global Telecommun. Conf. (GLOBECOM)*, New Orleans, LO, USA, Dec, 2008, pp. 1–5.
11. R. Yao et al., *Optimised power allocation to maximise secure rate in energy harvesting relay network*, Electron. Lett. **52**, (2016), no. 22, 1879–1881.
12. Y. Oohama, Capacity theorems for relay channels with confidential messages, *IEEE Int. Symp. Inform. Theory (ISIT)*, Nice, France, 24–25, June 2007, pp. 926–930.
13. X. He and A. Yener, *Cooperation with an untrusted relay: A secrecy perspective*, IEEE Trans. Inform. Theory **56**, (2010), no. 8, 3807–3827.
14. C. Wang, H. M. Wang, and X. G. Xia, *Hybrid opportunistic relaying and jamming with power allocation for secure cooperative networks*, IEEE Trans. Wireless Commun. **14**, (2015), no. 2, 589–605.
15. L. Sun et al., *Security-aware relaying scheme for cooperative networks with untrusted relay nodes*, IEEE Commun. Lett. **19**, (2015), no. 3, 463–466.
16. A. Kuhestani, A. Mohammadi, and M. Mohammadi, *Joint relay selection and power allocation in large-scale MIMO systems with*

untrusted relays and passive eavesdroppers, IEEE Trans. Inform. Forens. Security **13**, (2018), no. 2, 341–355.
17. H. M. Wang et al., *Hybrid cooperative beamforming and jamming for physical-layer security of two-way relay networks*, IEEE Trans. Inform. Forens. Security **8**, (2013), no. 12, 2007–2020.
18. H. M. Wang, Q. Yin, and X. G. Xia, *Distributed beamforming for physical-layer security of two-way relay networks*, IEEE Trans. Signal Process. **60**, (2012), no. 7, 3532–3545.
19. C. Jeong, I. M. Kim, and D. I. Kim, *Joint secure beamforming design at the source and the relay for an amplify-and-forward MIMO untrusted relay system*, IEEE Trans. Signal Process. **60**, (2012), no. 1, 310–325.
20. J. Mo et al., *Secure beamforming for MIMO two-way communications with an untrusted relay*, IEEE Trans. Signal Process. **62**, (2014), no. 9, 2185–2199.
21. J. Xiong et al., *Destination-aided cooperative jamming for dual-hop amplify-and-forward MIMO untrusted relay systems*, IEEE Trans. Veh. Technol. **65**, (2016), no. 9, 7274–7284.
22. J. Huang and A. L. Swindlehurst, Joint transmit design and node selection for one-way and two-way untrusted relay channels, *Asilomar Conf. Signals, Syst. Comput. (ASILOMAR 2013)*, Pacific Grove, CA, USA, Nov. 2013, pp. 1555–1559.
23. D. B. da Costa and S. Aissa, Beamforming in dual-hop fixed gain relaying systems, *IEEE Int. Conf. Commun. (ICC)*, Dresden, Germany, 14–18, June 2009, pp. 1–5.
24. J. Zhang and M. C. Gursoy, Relay beamforming strategies for physical-layer security, *Annu. Conf. Inform. Sci. Syst. (CISS)*, Princeton, NJ, USA, Mar. 2010, pp. 1–6.
25. X. Tang et al., *Interference assisted secret communication*, IEEE Trans. Infom., Theory **57** (2011), no. 5, May 2011, pp. 3153–3167.
26. R. Yao et al., *Secrecy rate-optimum energy splitting for an untrusted and energy harvesting relay network*, IEEE Access **6**, (2018), 19238–19246.
27. A. Kuhestani, A. Mohammadi, and P. L. Yeoh, *Optimal power allocation and secrecy sum rate in two-way untrusted relaying networks with an external jammer*, IEEE Trans. Commun. **66**, (2018), no. 6, 2671–2684.
28. D. S. Kalogerias et al., Mobile jammers for secrecy rate maximization in cooperative networks, *IEEE Int. Conf. Acoust., Speech Signal Process. (ICASSP)*, Vancouver, Canada, May 2013, pp. 2901–2905.
29. L. Lv et al., *Improving physical layer security in untrusted relay networks: Cooperative jamming and power allocation*, IET Commun. **11**, (2017), no. 3, 393–399.
30. S. A. A. Fakoorian and A. L. Swindlehurst, *Solutions for the MIMO Gaussian wiretap channel with a cooperative jammer*, IEEE Trans. Signal Process. **59**, (2011), no. 10, 5013–5022.
31. A. Kuhestani and A. Mohammadi, *Destination-based cooperative jamming in untrusted amplify-and-forward relay networks: Resource allocation and performance study*, IET Commun. **10**, (2016), no. 1, 17–23.
32. P. B. Bok et al., Distributed flow permission inspection for mission-critical communication of untrusted autonomous vehicles, *IEEE Veh. Technol. Conf. (VTC2014-Fall)*, Vancouver, Canada, Sept. 2014, pp. 1–6.
33. D. B. Rawat, R. Grodi, and C. Bajracharya, Enhancing connectivity for communication and control in unmanned aerial vehicle networks, *IEEE Radio Wireless Symp. (RWS)*, San Diego, CA, USA, Jan. 2015, pp. 200–202.
34. H. Chu and P. Xu, Relay selection with feedback beamforming information for NLoS 60 GHz mm wave WLANs/WPANs, *IEEE Int. Conf. Commun. (ICC)*, Sydney, Australia, June 2014, pp. 5514–5519.
35. W. W. Diab, N. Yousefi, and S. Powell, System and method for mirroring power over ethernet registers in a physical layer device over a single isolation boundary, U.S. Patent 8 428 248, April 23, 2013.
36. T. Mekkawy et al., *Joint beamforming alignment with suboptimal power allocation for a two-way untrusted relay network*, IEEE Trans. Inform. Forens. Security **13**, (2018), no. 10, 2464–2474.
37. R. Zhang et al., *Optimal beamforming for two-way multi-antenna relay channel with analogue network coding*, IEEE J. Sel. Areas Commun. **27**, (2009), no. 5, 699–712.
38. T. Mekkawy et al., Optimal power allocation for achievable secrecy rate in an untrusted relay network with bounded channel estimation error, *Wireless Opt. Commun. Conf. (WOCC)*, Newark, NJ, USA, Apr. 2017, pp. 1–5.
39. X. Chen et al., *A survey on multiple-antenna techniques for physical layer security*, IEEE Commun. Sur. Tut. **19**, (2017), no. 2, 1027–1053.
40. H. M. Wang, F. Liu, and X. G. Xia, *Joint source-relay precoding and power allocation for secure amplify-and-forward MIMO relay networks*, IEEE Trans. Infom. Forens. Security **9**, (2014), no. 8, 1240–1250.
41. N. Ouyang et al., *Destination assisted jamming and beamforming for improving the security of AF relay systems*, IEEE Access **5**, (2017), 4125–4131.
42. D. Senaratne and C. Tellambura, *GSVD beamforming for two-user MIMO downlink channel*, IEEE Trans. Veh. Technol. **62**, (2013), no. 6, 2596–2606.
43. D. Tse and P. Viswanath, *Fundamentals of Wireless Communication*. Cambridge, U.K.: Cambridge Univ. Press, Sep. 2005.

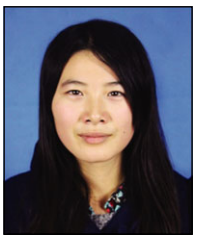
AUTHOR BIOGRAPHIES

Rugui Yao received his BS, MS, and PhD degrees in telecommunications and information systems from the School of Electronics and Information (SEI), Northwestern Polytechnical University (NPU), Xi'an, China, in 2002, 2005, and 2007, respectively. From 2007 to 2009, he worked as a postdoctoral fellow at NPU. Since 2009, he has been with the SEI, NPU, Xi'an, China, where he is now an associate professor. In 2013, he joined the ITP Lab at Georgia Tech, Atlanta, USA, as a visiting scholar. He has worked in the areas of cognitive radio networks, channel coding, OFDM transmission, and spread-spectrum systems. He is a member of the IEEE and a senior member of the Chinese Institute of Electronics.



Yanan Lu received her BS degree in telecommunications and information systems from the School of Electronics and Information (SEI), Northwestern Polytechnical University (NPU), Xi'an, China, in 2016. Since 2016, she has studied as a postgraduate in telecommunications and information systems at the SEI, NPU, Xi'an, China. Her research interests include cooperative wireless relay communications and wireless energy harvesting and relay selection.

Tamer Mekkawy received his BS and MS degrees in electrical engineering from the Military Technical College (MTC), Cairo, Egypt, in 2006 and 2014, respectively. From 2008 to 2015, he worked as a teaching assistant at the MTC. Since September 2015, he has been working toward the PhD degree at the School of Electronics and Information, Northwestern Polytechnical University, Xi'an, China. His current research area includes cooperative wireless relay communication and localization in wireless networks.



Fei Xu received her BS degree in electronic engineering from Shaanxi Normal University, Xi'an, China, in 2015, and her MS degree in telecommunications and information systems from the School of Electronics and Information, Northwestern Polytechnical University, Xi'an, China, in 2018, respectively. Her research interests include wireless communications and energy efficiency.

Xiaoya Zuo received his BS, MS, and PhD degrees in communication engineering from Northwestern Polytechnical University (NPU), Xi'an, China, in 2005, 2008, and 2011, respectively. He is currently a lecturer in the School of Electronics and Information, NPU. From September 2008 to September 2009, he was a visiting scholar in the Department of Electrical and Computer Engineering, University of Victoria, Victoria, British Columbia. His research interests include broadband wireless communications, ultra-wideband communications, millimeter-wave communication systems, and multiple-input multiple-output (MIMO) communication systems.

APPENDIX A

THE PROOF OF CONVEX CHARACTERISTICS OF R_S

In this part, we will confirm that R_s is a convex function.

From (14), we have

$$\begin{aligned} R_s &= \frac{1}{2}\log_2 \prod_{i=M,\ldots,N_t} \left(1+\frac{\frac{\alpha P}{N_t}\eta_{d,i}^2 - \frac{\alpha}{1-\alpha}\eta_{r,i}^2}{1+\frac{\alpha}{1-\alpha}\eta_{r,i}^2}\right) \\ &= \frac{1}{2}\sum_{i=M}^{N_t}\log_2\left(1+\frac{\frac{\alpha P}{N_t}\eta_{d,i}^2 - \frac{\alpha}{1-\alpha}\eta_{r,i}^2}{1+\frac{\alpha}{1-\alpha}\eta_{r,i}^2}\right) \\ &= \frac{1}{2}\sum_{i=M}^{N_t}\log_2\left(1+\frac{\frac{\alpha(1-\alpha)P}{N_t}\eta_{d,i}^2 - \alpha\eta_{r,i}^2}{1-\alpha+\alpha\eta_{r,i}^2}\right). \end{aligned} \tag{A1}$$

Considering $0 < \alpha < 1$ in (6) and $0 \le \eta_{r,i} \le 1$ in (10), we have the denominator of each summarized item in (A1), $1-\alpha-\alpha\eta_{r,1}^2 = 1-(1-\eta_{r,1}^2)\alpha > 0$. Consequently, R_s is a continuous function of α in its interval (0, 1).

The first-order derivative of R_s with respect to α can be calculated as

$$\begin{aligned} \frac{dR_s}{d\alpha} = &\frac{1}{2\log 2} \\ &\times \sum_{i=M}^{N_t}\left(\frac{\frac{P}{N_t}\eta_{d,i}^2}{1+\frac{\alpha P}{N_t}\eta_{d,i}^2} - \frac{\eta_{r,i}^2}{(1-\alpha)^2+\alpha(1-\alpha)\eta_{r,i}^2}\right). \end{aligned} \tag{A2}$$

Then, the second-order derivative of R_s with respect to α is further computed as

$$\begin{aligned} \frac{d^2R_s}{d\alpha^2} &= \frac{1}{2\log 2} \\ &\times \sum_{i=M}^{N_t}\left[-\frac{\left(\frac{\alpha P}{N_t}\right)^2}{\left(\frac{\alpha^2 P}{N_t}+1\right)^2} + \frac{\eta_{r,i}^4 - 2\eta_{r,i}^2(\alpha\eta_{r,i}^2-\alpha+1)}{(1-\alpha)^2(\alpha\eta_{r,i}^2-\alpha+1)^2}\right] \\ &= \frac{1}{2\log 2}\sum_{i=M}^{N_t}\frac{C_1^i x^2 + C_2^i x + C_3^i}{(1-\alpha)^2(\alpha\eta_{r,i}^2-\alpha+1)^2\left(\frac{\alpha^2 P}{N_t}+1\right)^2} \\ &= \frac{1}{2\log 2}\sum_{i=M}^{N_t}\frac{C^i(x)}{(1-\alpha)^2(\alpha\eta_{r,i}^2-\alpha+1)^2\left(\frac{\alpha^2 P}{N_t}+1\right)^2}, \end{aligned} \tag{A3}$$

where $C^i(x) = C_1^i x^2 + C_2^i x + C_3^i, x = \frac{P}{N_t}\eta_{d,i}^2$ and

$$\begin{aligned} C_i^i &= -\alpha^4\eta_{r,i}^4 + [2\alpha^2(\alpha-1) + 2\alpha(\alpha-1)^3]\eta_{r,i}^2 \\ &\quad - (1-\alpha)^4, \\ C_2^i &= 2\alpha\eta_{r,i}^2[(1-\eta_{r,i}^2)(2\alpha-1) - 1], \\ C_3^i &= \eta_{r,i}^2[(1-\eta_{r,i}^2)(2\alpha-1) - 1]. \end{aligned} \tag{A4}$$

From (A4), we have

$$C_2^i = 2\alpha C_3^i. \tag{A5}$$

Because $0 < \alpha < 1$, it is obvious that $C_1^i < 0$. By performing some simple calculations of C_2^i, we then have

$$\begin{aligned} C_2^i &= 2\alpha\eta_{r,i}^2[(1-\eta_{r,i}^2)(2\alpha-1) - 1] \\ &= 2\alpha\eta_{r,i}^2(k_i z - 1) \\ &= 2\alpha\eta_{r,i}^2 C_{22}(k_i, z), \end{aligned} \tag{A6}$$

where $C_{22}(k_i, z) = k_i z - 1$, $k_i = 1 - \eta_{r,i}^2$, $z = 2\alpha - 1$. Because $0 < \alpha < 1$ and $0 \le \eta_{r,i} \le 1$, we have $-1 < z < 1$ and $0 \le k_i \le 1$, respectively. We discuss the values of $C_{22}(k_i, z)$ with the following two cases of $\eta_{r,i}$.

- When $\eta_{r,i} = 1$, then $k_i = 0$. Thus, we have $C_{22}(k_i, z) = -1 < 0$.
- When $0 \le \eta_{r,i} < 1$, then $k_i \ge 0$. In this case, $C_{22}(k_i, z)$ is a monotone increasing function of z. In the interval of z, $(-1, 1)$, there exits $C_{22}(k_i, z) < C_{22}(k_i, z)|_{z=1} = k_i - 1 = -\eta_{r,i}^2 \le 0$.

From the above analysis, in general, we have $C_{22}(k_i, z) < 0$. Furthermore, from (A6), we have $C_2^i \le 0$. From (A5), we also have $C_3^i \le 0$.

For $x = \frac{P}{N_t}\eta_{d,i}^2$ and $0 \le \eta_{r,i} < 1$, we have $x \ge 0$. Considering $C_1^i < 0$, $C_2^i \le 0$, and $C_3^i \le 0$, we have $C^i(x) \le C_3^i \le 0$ based on the definition of $C^i(x)$. In (A3), the denominator of each summarized item is larger than 0, while the nominator of each summarized item, $C^i(x)$, is nonpositive. Moreover, it is impossible for all $C^i(x)$s to be equal to zero. Therefore, we can have the second-order derivative with respective of α, $\frac{d^2 R_s}{d\alpha^2} < 0$.

When considering both the continuous characteristics of R_s and its negative second-order derivative (ie, $\frac{d^2 R_s}{d\alpha^2} < 0$), we conclude that R_s is convex for $\alpha \in (0, 1)$.