EURASIP Journal on Wireless Communications and Networking

RESEARCH Open Access

Joint distributed beamforming and jamming schemes in decode-and-forward relay networks for physical layer secrecy

Chengmin Gu and Chao Zhang*

Abstract

In this paper, we propose joint cooperative beamforming and jamming schemes in decode-and-forward (DF) relay networks for physical layer secrecy. In DF relay networks, only the relays decoding the message from the source correctly have to join in the forwarding phase and the relays with decoding error are not utilized sufficiently. Taking this property into consideration, we let the relays decoding successfully transmit information signals and the relays decoding in error transmit jamming signal to improve the secrecy capacity of system. For this purpose, we design a bi-level optimization algorithm to search the optimal beamforming vector and jamming vector for the relays via the semi-definite relaxation (SDR). In addition, for balancing the cost of system and secrecy performance, we also study some suboptimal schemes to improve information secrecy. Finally, the simulation results show that the optimal scheme outperforms all other simulated schemes and the suboptimal schemes achieve good tradeoff between secrecy performance and computational complexity.

Keywords: Physical layer secrecy, Distributed beamforming, Jamming, Relay networks

1 Introduction

For openness and broadcast properties in wireless communications, information carried by radio waves is vulnerable to be intercepted by the unintended users. Traditional secrecy mechanisms, which depend on data encryption in application layer, mainly utilize unaffordable computation complexity to prevent the eavesdroppers to obtain the encrypted messages. However, with the rapid development of computing apparatuses, the traditional encryption technology confronts the unprecedented challenge. Thus, to achieve information security in wireless transmission, physical layer secrecy, which takes advantage of intrinsic characteristics of the wireless channels to achieve transmission security without applying encryption technology, has drawn much attention and been applied into many scenarios [1–4].

On the other hand, relay-aided cooperative communication technology has been applied in wireless scenarios, since it can extend the coverage and improve the reliability of signal transmission [5]. Additionally, relay-aided cooperative networks have been proved to be able to enhance the transmission security [6, 7]. In the multiple-relay networks without the direct link from the source to the destination, Cooperative beamforming (CB), single-relay and single-jammer (SRSJ) scheme, single-relay and multiple-jammer (SRMJ) scheme, multiple-relay and single jammer (MRSJ) scheme, and multiple-relay and multiple-jammer (MRMJ) scheme are five main transmission schemes for physical layer secrecy. In the CB-based relay systems, relays just perform distributed beamforming directly to the legal destination in order to enlarge the capacity of legal channel as much as possible [8–11]. In the SRSJ scheme, for relaxing the requirement of signal synchronization, how to select the best pair of forwarding relay and jammer was addressed in [12]. In the SRMJ scheme, the best relay is picked out to forward the information and the left relays transmit jamming signals to confuse the eavesdropper [13]. Alternatively, the MRSJ scheme selects the best jammer from all relays and let left relays perform cooperative beamforming to the legal user [14]. As the relay with amplify-and-forward (AF) scheme can always transmit signals to the destination [15], the MRMJ

*Correspondence: chaozhang@mail.xjtu.edu.cn
School of Electronics and Information Engineering, Xi'an Jiaotong University, Xi'an 710049, China

scheme, in which some relays are used to transmit information to the legal destination and left ones produce jamming signals to improve the secrecy capacity of the information transmission, is usually investigated in AF relay networks [16–18]. In DF relay networks, a MRMJ scheme was proposed in [19], where the relays without decoding error are divided into two groups, one for information beamforming and the other one for cooperative jamming. However, it does not make the most of the relays that cannot decode the message from the source successfully to enhance the secrecy of information transmission. In [20], a simultaneous beamforming and jamming scheme was proposed in DF relay networks. However, the relays deocoding in error are not sufficiently exploited. A MRMJ scheme with fixed jamming and beamforming set was proposed in [21]. Similarly, a multi-relay secrecy transmission scheme with a dedicated multi-antenna jammer was proposed in [22]. Both [21] and [22] have deployed dedicated jamming nodes which have no ability of forwarding information to the legal destination. If there exists the direct link from the source to the destination, cooperative jamming (CJ) and transmission switching between CB and CJ were also proposed to improve the system secrecy [23, 24]. Moreover, joint CB and CJ schemes in co-located multi-antenna scenarios were also investigated in [25] and [26]. In [27], we have investigated the optimal joint CB and CJ scheme for the DF relay networks with direct links from the source to destination and eavesdropper. However, the assumptions on relay set partition and the inference cancelation are difficult to be implemented. In this paper, we consider a more practical scenario for the joint beamforming and jamming scheme in the DF relay networks and provide optimal scheme and suboptimal schemes with lower complexity to investigate the proposed idea of joint beamforming and jamming well. In [28], Guo et al. also addressed the power allocation in a joint beanforming and jamming scheme in DF relay networks to achieve the maximum secrecy rate.

In this paper, we intend to employ joint cooperative beamforming and jamming to improve the secrecy capacity in DF relay networks without direct link between the source and the destination. In DF relay networks, only the relays decoding the message from the source correctly have to forward information to the legitimate destination during the relaying phase. To efficiently utilize all relays, the relays decoding successfully consist of the beamforming set, where relays perform distributed beamforming to transmit information signals. At the same time, the relays decoding in error belong to the jamming set, where the relays transmit jamming to disturb the eavesdropper. Herein, our goal is to design the beamforming vector and jamming vector in order to maximize the achievable secrecy capacity under the constraint of total relay power. For this purpose, we design a based bi-level optimization algorithm to search the optimal beamforming vector and jamming vector for the relays via the semi-definite relaxation. In addition, for balancing the cost of system and secrecy performance, we also study some suboptimal schemes to improve information secrecy. Finally, by our numerical results, the optimal scheme outperforms all existing schemes and the proposed suboptimal schemes. In addition, some suboptimal schemes with low computational complexity also have better secrecy performance than existing schemes.

Compared to existing work, the contributions of this paper are as follows:

- In most existing work, the relays decoding in error are not usually utilized during the cooperative transmission phase. In this paper, taking the distinguishing feature of DF relay into consideration, we employ the relays decoding in error to transmit jamming signals to improve the secrecy of cooperative transmission.
- How to design the beamforming vector and jamming vector in order to maximize the achievable secrecy capacity under the constraint of total relay power is provided. To reduce the computation complexity, we also propose four suboptimal designs.
- Through simulations, we compare the proposed designs with existing CB, SRMJ, MRSJ and SRSJ schemes and prove that the optimal design and some suboptimal designs outperform the existing schemes. The suitable scenarios of these proposed designs are also addressed.

We adopt the following notations. Bold uppercase letters denote matrices and bold lowercase letters denote column vectors. Transpose and conjugate transpose are represented by $(\cdot)^T$ and $(\cdot)^H$ respectively; $\mathbf{I}_K$ is the identity matrix of $K \times K$; $\mathbb{C}^n$ denotes the space of $n \times 1$ column vector with complex entries; $\mathrm{Tr}(\cdot)$ is the trace of the matrix; $\mathrm{Rank}(\cdot)$ denotes the rank of a matrix; $\|\cdot\|^2$ is the two-norm of a vector; $\mathbf{A} \succeq \mathbf{0}$ and $A \succ \mathbf{0}$ mean that $\mathbf{A}$ is positive semi-definite and definite matrix, respectively; $\mathbf{x} \perp \mathbf{y}$ denotes vector $\mathbf{x}$ and vector $\mathbf{y}$ are orthogonal; $\mathbf{x} \parallel \mathbf{y}$ denotes vector $\mathbf{x}$ and vector $\mathbf{y}$ are parallel; $\mathbb{E}\{\cdot\}$ denotes expectation.

2 System model and transmission scheme

2.1 System model

As depicted in Fig. 1, we study a wireless relay network which consists of a source node (S), N $(N \geq 1)$ relay nodes, a desired destination node (D) and a single eavesdropper (E). We assume that these relays are trusted during the information transmission. Each node is equipped with one omni-directional antenna and operates in the half duplex mode. We assume that the channel coefficient h_{ij} from the node i to the node j, $1 \leq i,j \leq N$, follows complex Gaussian distribution with zero mean and variance

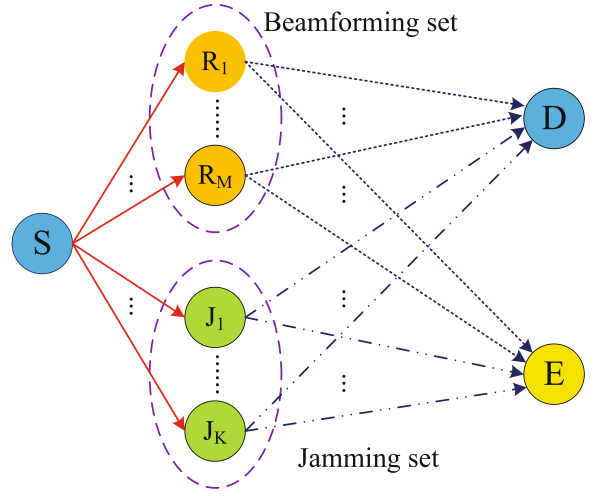

Fig. 1 System model

$K_0 d_{ij}^{-\beta}\sigma_{ij}^2$, i.e., $h_{ij} \sim \mathcal{CN}\left(0, K_0 d_{ij}^{-\beta}\sigma_{ij}^2\right)$, where K_0 is the gain constant determined by transmitting and receiving antennas, d_{ij} denotes the distance between node i and node j, β is path loss factor, and σ_0^2 stands for the small scale fading. Considering the disperse relays, we assume that all channels experience independent and identically distributed (i.i.d.) small-scale fading, i.e., $\sigma_{ij}^2 = \sigma_0^2$. Furthermore, the channels are assumed to be reciprocal, i.e., $h_{ij} = h_{ji}$. Owing to the path loss and shadow fading, there does not exist a direct link from source to destination or eavesdropper. We consider a slow-fading channel scenario, where the channel coefficients keep constant in one transmission block T and vary from block to block. The noise at the receiver follows complex Gaussian distribution with zero mean and variance N_0. Additionally, although we consider the nodes with one antenna in the system model, it is easy to extend the analysis and results into a multi-antenna scenario.

2.2 Transmission scheme

The whole cooperative transmission is separated into two phases: source broadcasting and relay transmitting.

2.2.1 Source broadcasting

The source broadcasts its intended signal x in the whole network; the relays receive the information-bearing signal and tries to decode the message, owing to there does not exist a direct link from source to destination or eavesdropper. Thus, the information transmitting in the source broadcasting phase is secure. Then, the received signal at the ith relay can be written as

$$y_{si} = \sqrt{P_s} h_{si} x + n_{si} \tag{1}$$

where P_s is the transmit power of the source, h_{si} is the channel coefficient from source to the ith relay, and n_{si} is the receiver noise. Also, x is the normalized information symbol, i.e., $\mathbb{E}\{|x|^2\} = 1$. If the ith relay can decode the received message correctly, it will join the information transferring in the relay transmitting phase. Otherwise, the ith relay is assigned to jam the eavesdropper. We assume all transmitted information blocks are protected by an ideal error control coding. In other words, if the received signal-to-noise ratio (SNR) of the ith relay, i.e., $\gamma_{si} = P_s|h_{si}|^2/N_0$, is larger than the threshold γ_{th}, where $\gamma_{th} = 2^{2R_0} - 1$ and R_0 is the target information transmission rate, the receiver can decode the information packet correctly. Thus, if $\gamma_{si} \geq \gamma_{th}$, then the ith relay belongs to $\mathcal{D}$. Otherwise, it is in the set $\mathcal{J}$. As a result, each relay knows whether it can decode the message from the source successfully and which set it belongs to. Without loss of generality, we set $\mathcal{D} = \{R_1, R_2, \cdots, R_M\}$ and $\mathcal{J} = \{J_1, J_2, \cdots, J_K\}$, where $1 \leq R_i, J_i \leq N$ are the indexes of these relays (see Fig. 1) and there is $M + K = N$. Additionally, we assume that all receiver noises have the same noise power N_0.

We define the weight coefficient vector of set $\mathcal{D}$ for beamforming as $\mathbf{w}_R = \left[w_{R_1}^*, w_{R_2}^*, \cdots, w_{R_M}^*\right]^T$ and weight coefficient vector of set $\mathcal{J}$ for jamming as $\mathbf{w}_J = \left[w_{J_1}^*, w_{J_2}^*, \cdots, w_{J_K}^*\right]^T$. Moreover, $\mathbf{h}_{rd} = \left[h_{R_1D}, h_{R_2D}, \cdots, h_{R_MD}\right]^T$ represents the channel vector from the beamforming set to the destination and $\mathbf{h}_{je} = \left[h_{J_1E}, h_{J_2E}, \cdots, h_{J_KE}\right]^T$ denotes the channel vector from the jamming set to the eavesdropper. Before relay transmitting, the destination can transmit a training signal to let each relay estimate the channel coefficient from the destination to itself. Note that the eavesdropper is often a wireless user unauthorized to access the message for the destination [29]. Hence, the eavesdropper is able to cooperatively transmit training signal to all relays. Then, each relay can obtain its channel coefficient h_{id}, $i = 1, 2, ..., N$. Moreover, we set up a central control node (CCN), which can be a relay node or a dedicated node. After that, each relay reports its related channel information to the CCN. Therefore, the CCN can compute the beamforming vector $\mathbf{w}_R$ for the relays in set $\mathcal{D}$ and jamming vector $\mathbf{w}_J$ for the relays in set $\mathcal{J}$. In the following analysis, we assume that all receivers can estimate their received channel coefficients perfectly to exploit the ideal performance and check up the theoretical feasibility of our proposals. The effect of estimation error will be discussed in future work. Whereas, the source node has no knowledge of its transmitting channel state information due to practical constraint.

2.2.2 Relay transmitting

The relays in set $\mathcal{D}$ transmit the information symbol x to the destination, while the relays in set $\mathcal{J}$ radiate jamming symbol z to achieve secure transmission. The received signal at the destination is given by

$$y_{rd} = \mathbf{w}_R^H \mathbf{h}_{rd} x + \mathbf{w}_J^H \mathbf{h}_{jd} z + n_{rd} \tag{2}$$

and the received signal at the eavesdropper can be expressed as

$$y_{re} = \mathbf{w}_R^H \mathbf{h}_{re} x + \mathbf{w}_J^H \mathbf{h}_{je} z + n_{re} \tag{3}$$

where z is independent of x, and $\mathbb{E}\{|z|^2\} = 1$, n_{rd} and n_{re} are receiver noise power at the destination and the eavesdropper, respectively. Considering the total relay power constraint, we have $\|\mathbf{w}_R\|^2 + \|\mathbf{w}_J\|^2 \leq P_t$. Therefore, the information transmission capacity $C_d(M)$ at the destination is

$$C_d(M) = \frac{1}{2}\log_2\left(1 + \frac{\mathbf{w}^H \widetilde{\mathbf{H}}_{rd}\mathbf{w}}{\mathbf{w}^H \widetilde{\mathbf{H}}_{jd}\mathbf{w} + N_0}\right) \tag{4}$$

and the capacity $C_e(M)$ at the eavesdropper can be expressed as

$$C_e(M) = \frac{1}{2}\log_2\left(1 + \frac{\mathbf{w}^H \widetilde{\mathbf{H}}_{re}\mathbf{w}}{\mathbf{w}^H \widetilde{\mathbf{H}}_{je}\mathbf{w} + N_0}\right) \tag{5}$$

where M denotes the cardinal of beamforming set, $\mathbf{w} = \left[\mathbf{w}_R^T \; \mathbf{w}_J^T\right]^T$, $\widetilde{\mathbf{H}}_{rd} = \widetilde{\mathbf{h}}_{rd}\widetilde{\mathbf{h}}_{rd}^H$, $\widetilde{\mathbf{H}}_{re} = \widetilde{\mathbf{h}}_{re}\widetilde{\mathbf{h}}_{re}^H$, $\widetilde{\mathbf{H}}_{jd} = \widetilde{\mathbf{h}}_{jd}\widetilde{\mathbf{h}}_{jd}^H$, $\widetilde{\mathbf{H}}_{je} = \widetilde{\mathbf{h}}_{je}\widetilde{\mathbf{h}}_{je}^H$. Herein, $\widetilde{\mathbf{h}}_{rd} = \left[\mathbf{h}_{rd}^T, \mathbf{0}_{1\times K}\right]^T$, $\widetilde{\mathbf{h}}_{re} = \left[\mathbf{h}_{re}^T, \mathbf{0}_{1\times K}\right]^T$, $\widetilde{\mathbf{h}}_{jd} =[\mathbf{0}_{1\times M}, \mathbf{h}_{jd}^T]^T$, $\widetilde{\mathbf{h}}_{je} = \left[\mathbf{0}_{1\times M}, \mathbf{h}_{je}^T\right]^T$. Then, the secrecy capacity of the whole transmission conditioned on the set $\mathcal{D}$ and $\mathcal{J}$ is given by

$$C_s(M) = \max\{0,\; C_d(M) - C_e(M)\} \tag{6}$$

Note that $C_s(M) = 0$ means the eavesdropper can obtain no less correct information than the destination, which is called completely unsafe transmission and should be avoided. Our aim herein is to maximize the secrecy capacity $C_s(M)$ as much as possible with the power constraint of relays.

3 Optimal design for maximizing secrecy capacity

In this section, we intend to design $\mathbf{w}_R$ and $\mathbf{w}_J$ to maximize the secrecy capacity under the total relay power constraint. On the basis of the previous section, the problem of secrecy capacity maximization under the power constraint can be expressed as

$$\begin{aligned} &\max_{\mathbf{w}} \; \{C_d(M) - C_e(M)\} \\ &\text{s.t. } \|\mathbf{w}\|^2 \leq P_t \end{aligned} \tag{7}$$

Since secrecy capacity is the difference of two concave functions, it is a non-convex optimization in general. To deal with this issue, we will conduct a series of transformations to turn it into a convex problem, which can be solved by some available solvers.

Firstly, by introducing an auxiliary variable $0 < \tau \leq 1$, the problem of (7) can be equivalently rewritten as

$$\max_{\mathbf{w},\tau} \quad \log_2\left(1 + \frac{\mathbf{w}^H \widetilde{\mathbf{H}}_{rd}\mathbf{w}}{\mathbf{w}^H \widetilde{\mathbf{H}}_{jd}\mathbf{w} + N_0}\right) - \log_2\left(\frac{1}{\tau}\right) \tag{8}$$

$$\text{s.t.} \quad \log_2\left(1 + \frac{\mathbf{w}^H \widetilde{\mathbf{H}}_{re}\mathbf{w}}{\mathbf{w}^H \widetilde{\mathbf{H}}_{je}\mathbf{w} + N_0}\right) \leq \log_2\left(\frac{1}{\tau}\right) \tag{9}$$

$$\|\mathbf{w}\|^2 \leq P_t \tag{10}$$

Then, on account of monotony property of logarithm function, the optimization problem can be further simplified as

$$\begin{aligned} \min_{\mathbf{W},\tau} \quad & \frac{\mathrm{Tr}\left(\widetilde{\mathbf{H}}_{jd}\mathbf{W}\right) + N_0}{\left[\mathrm{Tr}\left(\widetilde{\mathbf{H}}_{jd} + \widetilde{\mathbf{H}}_{rd}\right)\mathbf{W} + N_0\right]\tau} \\ \text{s.t.} \quad & \frac{\mathrm{Tr}\left(\widetilde{\mathbf{H}}_{je}\mathbf{W}\right) + N_0}{\left[\mathrm{Tr}\left(\widetilde{\mathbf{H}}_{je} + \widetilde{\mathbf{H}}_{re}\right)\mathbf{W} + N_0\right]\tau} \geq 1 \\ & \mathrm{Tr}(\mathbf{W}) \leq P_t,\; \mathbf{W} \succeq \mathbf{0} \\ & \mathrm{Rank}(\mathbf{W}) = 1 \end{aligned} \tag{11}$$

where $\mathbf{W} = \mathbf{w}\mathbf{w}^H$ is a rank-one square matrix. To solve the problem of (11), we employ the idea of SDR in [30] to drop the rank-one non-convex constraint. After the relaxation transformation, the problem of (11) is still a non-convex optimization problem owing to the presence of auxiliary variable τ. However, the problem of (11) can be treated as the quasi-convex problem for each fixed τ [31]. Therefore, it can be treated as a bi-level optimization problem: the outer-level optimization is about auxiliary variable τ and the inner-level optimization is a quasi-convex problem.

3.1 Inner-level optimization

Since (11) is a quasi-convex problem given a τ, we can employ the classical bisection method [31] to seek the optimum $\mathbf{W}^\star$. Nevertheless, it may incur huge computational complexity. Thanks to the Charnes-Cooper transformation [32], we can convert the linear fractional optimization problem into the linear optimization problem, which can be solved efficiently by convex optimization tools. Define

$$\mathbf{Z} = \frac{\mathbf{W}}{\left[\mathrm{Tr}\left(\widetilde{\mathbf{H}}_{jd} + \widetilde{\mathbf{H}}_{rd}\right)\mathbf{W} + N_0\right]\tau} \quad \text{and}$$

$$\psi = \frac{1}{\left[\mathrm{Tr}\left(\widetilde{\mathbf{H}}_{jd} + \widetilde{\mathbf{H}}_{rd}\right)\mathbf{W} + N_0\right]\tau},$$

then the problem (11) without a rank-one constraint can be equivalently described as

$$\begin{aligned} \min_{\mathbf{Z},\psi} \quad & \mathrm{Tr}\left(\widetilde{\mathbf{H}}_{jd}\mathbf{Z}\right) + \psi N_0 \\ \text{s.t.} \quad & \tau\left(\mathrm{Tr}\left(\widetilde{\mathbf{H}}_{jd} + \widetilde{\mathbf{H}}_{rd}\right)\mathbf{Z} + \psi N_0\right) = 1 \\ & \tau\left(\mathrm{Tr}\left(\widetilde{\mathbf{H}}_{je} + \widetilde{\mathbf{H}}_{re}\right)\mathbf{Z} + \psi N_0\right) \le \mathrm{Tr}\left(\widetilde{\mathbf{H}}_{je}\mathbf{Z}\right) + \psi N_0 \\ & \mathrm{Tr}(\mathbf{Z}) \le \psi P_t \\ & \psi > 0,\ \mathbf{Z} \succeq \mathbf{0} \end{aligned} \tag{12}$$

Note that there is $\mathbf{Z} = \psi\mathbf{W}$. Using the well-known CVX toolbox [31], we can solve problem (12) easily.

3.2 Outer-level optimization

To find the optimal solution $\tau^\star$, we have to play an exhaustive searching with the general range $0 < \tau \le 1$. In order to further reduce the computational complexity, we must shrink the scope of τ. On one hand, observing (9), we have

$$\tau \le \frac{1}{1 + \frac{\mathbf{w}^H\widetilde{\mathbf{H}}_{re}\mathbf{w}}{\mathbf{w}^H\widetilde{\mathbf{H}}_{je}\mathbf{w} + N_0}} \tag{13}$$

It means τ should be less than $\max\left\{\left(1 + \frac{\mathbf{w}^H\widetilde{\mathbf{H}}_{re}\mathbf{w}}{\mathbf{w}^H\widetilde{\mathbf{H}}_{je}\mathbf{w} + N_0}\right)^{-1}\right\}$. Therefore, we have to solve the problem

$$\min_{\mathbf{w}\in\mathbb{C}^N} \frac{\mathbf{w}^H\mathbf{A}\mathbf{w}}{\mathbf{w}^H\mathbf{B}\mathbf{w}} \tag{14}$$

where $\mathbf{A} = \widetilde{\mathbf{H}}_{re} \succeq 0$ and $\mathbf{B} = \widetilde{\mathbf{H}}_{je} + \frac{N_0}{P_t}\mathbf{I}_K \succ 0$. As the objective function of (14) is the generalized Rayleigh quotient problem [33], the minimum of (14) is equal to $\lambda_{\min}(\mathbf{B}^{-1}\mathbf{A})$ which stands for the minimum eigenvalue of $\mathbf{B}^{-1}\mathbf{A}$. Due to $\mathbf{B}^{-1}\mathbf{A}$ a is semi-definite matrix, the eigenvalues of $\mathbf{B}^{-1}\mathbf{A}$ are not less than zero [33]. Then, we have

$$\tau \le \frac{1}{1 + \lambda_{\min}\left(\mathbf{B}^{-1}\mathbf{A}\right)} = \tau_{\max} \tag{15}$$

On the other hand, considering that the secrecy capacity must be non-negative, by (8) we can obtain

$$\tau \ge \frac{1}{1 + \frac{\mathbf{w}^H\widetilde{\mathbf{H}}_{rd}\mathbf{w}}{\mathbf{w}^H\widetilde{\mathbf{H}}_{jd}\mathbf{w} + N_0}} \ge \frac{1}{1 + \lambda_{\max}\left(\mathbf{D}^{-1}\mathbf{C}\right)} = \tau_{\min} \tag{16}$$

where $\mathbf{C} = \widetilde{\mathbf{H}}_{rd}$, $\mathbf{D} = \widetilde{\mathbf{H}}_{jd} + \frac{N_0}{P_t}\mathbf{I}_K$, and $\lambda_{\max}(\mathbf{D}^{-1}\mathbf{C})$ represents the maximum eigenvalue of the matrix $\mathbf{D}^{-1}\mathbf{C}$. Note that $\tau_{\max}$ and $\tau_{\min}$ are independent on $\mathbf{w}$. Therefore, the outer optimization is formulated as

$$\begin{aligned} \min_{\tau} \quad & \phi(\tau) \\ \text{s.t.} \quad & \tau_{\min} \le \tau \le \tau_{\max} \end{aligned} \tag{17}$$

where $\phi(\tau) = \mathrm{Tr}(\widetilde{\mathbf{H}}_{jd}\mathbf{Z}^\star(\tau)) + \psi^\star(\tau)N_0$ and $\mathbf{Z}^\star(\tau)$ and $\psi^\star(\tau)$ are solutions of the inner-level optimization problem (12) given a τ. After one-dimension searching during $[\,\tau_{\min}, \tau_{\max}]$, the optimal $\tau^\star$ that makes $\phi(\tau)$ minimum can be found.

As a result, we finally obtain the solution of problem (11), i.e., $\tau^\star$ and $\mathbf{W}^\star = \mathbf{Z}^\star/\psi^\star$. If $\mathrm{Rank}(\mathbf{W}^\star) = 1$, we can obtain $\mathbf{w}^\star$ via singular value decomposition (SVD) [34] from $\mathbf{W}^\star$. If the rank of $\mathbf{W}^\star$ is larger than one, we can extract an approximate solution from $\mathbf{W}^\star$ via using the Gaussian Randomization Procedure (GRP) in [30]. To make it more clearly, we draw the procedure of solving the optimization problem in Algorithm 1.

Algorithm 1 Solving Problem (11)

```
Obtain $\widetilde{\mathbf{H}}_{jd}$, $\widetilde{\mathbf{H}}_{rd}$, $\widetilde{\mathbf{H}}_{re}$, $\tau_{\min}$, $\tau_{\max}$.
$L = (\tau_{\max} - \tau_{\min})/\Delta_\tau$ and $\phi_{\min} = +\infty$
For $i = 0 : 1 : L$
Begin
$\tau_i = \tau_{\min} + i * \Delta_\tau$
Using CVX tool box to solve (12), obtain $\phi(\tau_i) = \mathrm{Tr}(\widetilde{\mathbf{H}}_{jd}\mathbf{Z}^\star(\tau_i)) + \psi^\star(\tau_i)N_0$
If $\phi(\tau_i) < \phi_{\min}$, then $\phi_{\min} = \phi(\tau_i)$, $\tau^\star = \tau_i$ and $\mathbf{W}^\star = \mathbf{Z}(\tau_i)^\star/\psi^\star(\tau_i)$ .
Endif
End for loop
If $\mathrm{Rank}(\mathbf{W}^\star) = 1$, $\mathbf{w}^\star$ is obtained via using SVD.
If $\mathrm{Rank}(\mathbf{W}^\star) > 1$, an approximate solution can be got via using GRP.
```

4 Suboptimal designs with low complexity

It can be seen that the proposed optimal design always incurs huge computational complexity in general. To reduce the computational complexity, we can rewrite the equivalent problem of (7) as

$$\begin{aligned} \max_{P_r,P_j} & \left\{\max_{\mathbf{w}_R,\mathbf{w}_J}\{C_d(M) - C_e(M)\}\right\} \\ \text{s.t.}\ & 0 \le \|\mathbf{w}_R\|^2 \le P_r \\ & 0 \le \|\mathbf{w}_J\|^2 \le P_j \\ & P_r + P_j = P_t \end{aligned} \tag{18}$$

It means that we can firstly determine the optimal directions of $\mathbf{w}_R$ and $\mathbf{w}_J$ and then seek the optimal power allocation between $\mathbf{w}_R$ and $\mathbf{w}_J$. Furthermore, given a fixed $\mathbf{w}_R$, we just need to search the optimal $\mathbf{w}_J$ in a space with lower dimension than $\mathbf{w}$ and vice versa. From this point, we propose the following suboptimal designs in which $\mathbf{w}_R$ or $\mathbf{w}_J$ is directly determined by related channel information and the other weight vector is optimized to maximize the secrecy capacity.

4.1 Information beam determined schemes

4.1.1 $\mathbf{w}_R \perp \mathbf{h}_{re}$ *scheme*

Considering the information, beamforming vector completely lies on the null space of relay-eavesdropper channel, that is to say, there does not exist any information leakage to the unintended user in the relay transmitting phase, i.e., $C_e(M) = 0$. Therefore, there is no need to jam the eavesdropper. The optimization problem of (18) in this case is equivalently formulated as

$$\begin{aligned} \max_{\mathbf{w}_R} \quad & \|\mathbf{w}_R^H \mathbf{h}_{rd}\|^2 \\ \text{s.t.} \quad & \mathbf{w}_R^H \mathbf{h}_{re} = 0 \\ & \|\mathbf{w}_R\|^2 \le P_t \end{aligned} \tag{19}$$

Using the Lagrange multiplier optimization technique directly in [31], we can obtain the solution as

$$\mathbf{w}_R^\star = \frac{\sqrt{P_t}\,(\mathbf{I}_M - \mathbf{P})\,\mathbf{h}_{rd}}{\|(\mathbf{I}_M - \mathbf{P})\,\mathbf{h}_{rd}\|}, \tag{20}$$

where $\mathbf{P} = \mathbf{h}_{re}(\mathbf{h}_{re}^H \mathbf{h}_{re})^{-1}\mathbf{h}_{re}^H$ is the orthogonal projection matrix onto the subspace spanned by $\mathbf{h}_{rd}$. Note that the problem of (19) implies that it can be solved for $M \geqslant 2$. Herein, if the number of relays in the beamforming set is one, i.e.,$M = 1$, the solution of (19) is

$$\mathbf{w}_R^\star = \frac{\sqrt{P_t} h_{rd}}{|h_{rd}|} \tag{21}$$

4.1.2 $\mathbf{w}_R \parallel \mathbf{h}_{rd}$ *scheme*

As the maximum ratio transmission (MRT) in multiantenna systems is an efficient strategy to achieve larger capacity [18], we let the relays decoding successfully perform MRT strategy, where the information beamforming vector directly points to the desired destination. Thus, the information beamforming vector can be expressed as [35]

$$\mathbf{w}_R^\star = \frac{\sqrt{P_t - P_j}\,\mathbf{h}_{rd}}{\|\mathbf{h}_{rd}\|} \tag{22}$$

Substitute (22) into (18), the optimization problem of (18) can be equivalently expressed as

$$\begin{aligned} \max_{\mathbf{w}_J, P_j} \ & \log_2\left(1 + \frac{\left(P_t - P_j\right)\cdot\|\mathbf{h}_{rd}\|^2}{\mathbf{w}_J^H \mathbf{H}_{jd}\mathbf{w}_J + N_0}\right) \\ & - \log_2\left(1 + \frac{(P_t - P_j)\cdot\|\mathbf{h}_{rd}^* \mathbf{h}_{re}\|^2}{\|\mathbf{h}_{rd}\|^2\left(\mathbf{w}_J^H \mathbf{H}_{je}\mathbf{w}_J + N_0\right)}\right) \\ \text{s.t.}\ & 0 \le \|\mathbf{w}_J\|^2 \le P_j \\ & 0 \le P_j \le P_t \end{aligned} \tag{23}$$

Similarly, given a $P_j \in [0, P_t]$, we introduce an auxiliary variable ν to equivalently convert the above problem as

$$\begin{aligned} \max_{\mathbf{w}_J, P_j} \ & \log_2\left(1 + \frac{\left(P_t - P_j\right)\cdot\|\mathbf{h}_{rd}\|^2}{\mathbf{w}_J^H \mathbf{H}_{jd}\mathbf{w}_J + N_0}\right) - \log_2\left(\frac{1}{\nu}\right) \\ \text{s.t.}\ & \log_2\left(1 + \frac{\left(P_t - P_j\right)\cdot\|\mathbf{h}_{rd}^* \mathbf{h}_{re}\|^2}{\|\mathbf{h}_{rd}\|^2\left(\mathbf{w}_J^H \mathbf{H}_{je}\mathbf{w}_J + N_0\right)}\right) \le \log_2\left(\frac{1}{\nu}\right) \\ & 0 \le \|\mathbf{w}_J\|^2 \le P_j \end{aligned} \tag{24}$$

Due to the monotony property of logarithm function, it is equivalent to solve the problem

$$\begin{aligned} \min_{\mathbf{W}_J, \nu} \ & \frac{\mathrm{Tr}\left(\mathbf{H}_{jd}\mathbf{W}_J\right) + N_0}{\left[\mathrm{Tr}\left(\mathbf{H}_{jd}\mathbf{W}_J\right) + N_0 + \left(P_t - P_j\right)\|\mathbf{h}_{rd}\|^2\right]\nu} \\ \text{s.t.}\ & \frac{\|\mathbf{h}_{rd}\|^2 \mathrm{Tr}\left(\mathbf{H}_{je}\mathbf{W}_J\right) + \|\mathbf{h}_{rd}\|^2 N_0}{\left[\|\mathbf{h}_{rd}\|^2\left(\mathrm{Tr}\left(\mathbf{H}_{je}\mathbf{W}_J\right) + N_0\right) + \left(P_t - P_j\right)\|\mathbf{h}_{rd}^* \mathbf{h}_{re}\|^2\right]\nu} \ge 1 \\ & \mathrm{Tr}\left(\mathbf{W}_J\right) \le P_j,\ \mathbf{W}_J \succeq \mathbf{0} \\ & \mathrm{Rank}\left(\mathbf{W}_J\right) = 1 \end{aligned} \tag{25}$$

where $\mathbf{W}_J = \mathbf{w}_J\mathbf{w}_J^H$ is a rank-one matrix. Observe (25) and (11), we can also apply Algorithm 1 to solve the problem (25). Then, we can obtain the optimal jamming vector $\mathbf{w}_J^\star$ for a given P_j.

In order to achieve the optimal power allocation between P_r and P_j, we appeal to the one-dimension searching on P_j over the interval $[0, P_t]$. So that, we can finally obtain the optimal $P_j^\star$, $P_r^\star$, $\mathbf{w}_R^\star$ and $\mathbf{w}_J^\star$.

4.2 Jamming beam determined schemes

4.2.1 $\mathbf{w}_J \perp \mathbf{h}_{jd}$ *scheme*

We firstly consider a null-steering beamforming method to guarantee the jamming beamforming vector that completely lies on the null space of $\mathbf{h}_{jd}$ [35]. Therefore, $\mathbf{w}_J$ does not affect $C_d(M)$. For a given P_j, to suppress $C_e(M)$ as much as possible, we have the optimization problem on $\mathbf{w}_J$,

$$\begin{aligned} \max_{\mathbf{w}_J} \quad & \|\mathbf{w}_J^H \mathbf{h}_{je}\|^2 \\ \text{s.t.} \quad & \mathbf{w}_J^H \mathbf{h}_{jd} = 0 \\ & 0 \le \|\mathbf{w}_J\|^2 \le P_j \end{aligned} \tag{26}$$

When relays in the jammming set is larger than one, applying Lagrange multiplier optimization [8, 31], we can obtain the solution of (26)

$$\mathbf{w}_J^\star = \begin{cases} \sqrt{P_j}\frac{(\mathbf{I}_K - \mathbf{Q})\mathbf{h}_{je}}{\|(\mathbf{I}_K - \mathbf{Q})\mathbf{h}_{je}\|} & \text{if } K \ge 2, \\ \sqrt{P_j}\frac{\mathbf{h}_{je}}{\|\mathbf{h}_{je}\|} & \text{if } K = 1. \end{cases} \tag{27}$$

where $\mathbf{Q} = \mathbf{h}_{jd}(\mathbf{h}_{jd}^H \mathbf{h}_{jd})^{-1}\mathbf{h}_{jd}^H$ is the orthogonal projection matrix onto the subspace spanned by $\mathbf{h}_{je}$. Given a

P_j, substitute $\mathbf{w}_J^\star$ into (18), the optimization problem is equivalent to the problem

$$\begin{aligned} \max_{\mathbf{w}_R} \quad & \frac{\mathbf{w}_R^H \widetilde{\mathbf{E}} \mathbf{w}_R}{\mathbf{w}_R^H \widetilde{\mathbf{F}} \mathbf{w}_R} \\ \text{s.t.} \quad & \|\mathbf{w}_R\|^2 \leq P_t - P_j \end{aligned} \tag{28}$$

where $\widetilde{\mathbf{E}} = \frac{1}{\sqrt{P_t - P_j}} \mathbf{I}_M + \frac{1}{N_0} \mathbf{H}_{rd}$ and $\widetilde{\mathbf{F}} = \frac{1}{\sqrt{P_t - P_j}} \mathbf{I}_M + \frac{\mathbf{H}_{re}}{\sqrt{P_t - P_j} |\mathbf{w}_J^{\star H} \mathbf{h}_{je}|^2 + N_0}$. Like (14), the solution of (28) is

$$\mathbf{w}_R^\star = \sqrt{P_t - P_j} \cdot \zeta_{max} \left(\widetilde{\mathbf{F}}^{-1} \widetilde{\mathbf{E}} \right) \tag{29}$$

in which $\zeta_{max}(\widetilde{\mathbf{F}}^{-1}\widetilde{\mathbf{E}})$ represents the eigenvector corresponding to the maximum eigenvalue of the matrix $\widetilde{\mathbf{F}}^{-1}\widetilde{\mathbf{E}}$. Similarly, we also need to search the optimal $P_j^\star$ during the interval $[0, P_t]$ to maximize $C_s(M)$.

4.2.2 $\mathbf{w}_J \parallel \mathbf{h}_{je}$ *scheme*

In this case, we let the jamming beamforming aim at the eavesdropper directly to shrink the capacity of the eavesdropper as much as possible. Then, the jamming beamforming vector can be expressed as

$$\mathbf{w}_J^\star = \sqrt{P_j} \frac{\mathbf{h}_{je}}{\|\mathbf{h}_{je}\|} \tag{30}$$

Substitute (30) into (18), the maximization problem of secrecy capacity can be further reformulated as

$$\begin{aligned} \max_{\mathbf{w}_R} \quad & \frac{\mathbf{w}_R^H \widetilde{\mathbf{G}} \mathbf{w}_R}{\mathbf{w}_R^H \widetilde{\mathbf{H}} \mathbf{w}_R} \\ \text{s.t.} \quad & \|\mathbf{w}_R\|^2 \leq P_t - P_j \end{aligned} \tag{31}$$

where $\widetilde{\mathbf{G}} = \frac{1}{\sqrt{P_t - P_j}} \mathbf{I}_M + \frac{1}{N_0} \mathbf{H}_{rd}$ and $\widetilde{\mathbf{H}} = \frac{1}{\sqrt{P_t - P_j}} \mathbf{I}_M + \frac{\mathbf{H}_{re}}{\sqrt{P_t - P_j} |\mathbf{w}_J^{\star H} \mathbf{h}_{je}|^2 + N_0}$. Thus, the optimal information beamforming vector of (31) is

$$\mathbf{w}_R^\star = \sqrt{P_t - P_j} \cdot \phi_{max}(\widetilde{\mathbf{H}}^{-1} \widetilde{\mathbf{G}}) \tag{32}$$

where $\phi_{max}(\widetilde{\mathbf{H}}^{-1}\widetilde{\mathbf{G}})$ denotes the eigenvector corresponding to the maximum eigenvalue of matrix $\widetilde{\mathbf{H}}^{-1}\widetilde{\mathbf{G}}$.

Thus, for a $P_j \in [0, P_t]$ we can obtain $\mathbf{w}_J^\star(P_j)$ and $\mathbf{w}_R^\star(P_j)$. After checking enough power configurations, we ultimately obtain the global optimal solution $(\mathbf{w}_R^\star, \mathbf{w}_J^\star, P_j^\star)$ that makes $C_s(M)$ become maximum.

4.3 Computational complexity analysis

In this subsection, we intend to compare the computational complexities of these proposed schemes. Since these designed schemes have different beamforming and jamming patterns in the relaying phase, we just need to analyze the computational complexity of computing the beamforming and jamming vectors given the beamforming set $|\mathcal{D}| = M$ and jamming set $|\mathcal{J}| = K$. Note that there is $N = M + K$.

4.3.1 Computational complexity of the optimal scheme

By Algorithm 1, we first need to determine τ_{min} and τ_{max}, which means we need to solve the Rayleigh quotient problem to get $\lambda_{min}(\mathbf{B}^{-1}\mathbf{A})$ in (15) and $\lambda_{max}(\mathbf{D}^{-1}\mathbf{C})$ in (16). Due to [33], the computational complexity of Rayleigh quotient problem is $\mathcal{O}(22N^2)$. So, the computational complexity of determining τ_{min} and τ_{max} is $\mathcal{O}(44N^2)$. During the searching scope $[\tau_{min}, \tau_{max}]$, there are τ_i, $i = 1, 2, \ldots, L$ so that the problem (12) will be operated L times. According to [25] and [36], the computational complexity of an inner level optimization (12) is $\mathcal{O}\left((N+1)^{0.5}(2(N+1)^3 + 4(N+1)^2 + 8)\right) \log(1/\epsilon)$ in which ϵ is the accuracy of solving the SDP. Please note that in Algorithm 1, running L times of problem (12) is activated after τ_{min} and τ_{max} are determined. It means computing τ_{min} and τ_{max} is only run once and the above two steps are performed sequentially. In addition, as the GRP is activated in a very slight probability and most of results from SDP meet the rank-one constraint, we only consider the computational complexity of SVD herein. Due to [36], the computational complexity of SVD is $\mathcal{O}(N^3)$. Therefore, the total computational complexity of the proposed optimal scheme is $\mathcal{O}\left(44N^2\right) + \mathcal{O}(N^3) + \mathcal{O}\left(L((N+1)^{0.5}(2(N+1)^3 + 4(N+1)^2 + 8))\right) \log(1/\epsilon)$.

4.3.2 Computational complexity of $\mathbf{w}_R \perp \mathbf{h}_{re}$ *scheme*

In $\mathbf{w}_R \perp \mathbf{h}_{re}$ scheme, we just need to calculate (20). Therefore, the computational complexity is $\mathcal{O}(M^2)$ [33].

4.3.3 Computational complexity of $\mathbf{w}_R \parallel \mathbf{h}_{rd}$ *scheme*

To obtain $\mathbf{w}_R^\star$, we have to calculate (22) with computational complexity $\mathcal{O}(M^2)$. After that, in order to get $\mathbf{w}_J^\star$, the proposed Algorithm 1 is also applied to solve (25). Moreover, it is assumed that we have L_p times of the above two steps in the one-dimension searching over $[0, P_t]$. As a result, the computational complexity of $\mathbf{w}_R \parallel \mathbf{h}_{rd}$ scheme can be expressed as

$$\begin{aligned} &\mathcal{O}\left(L_p M^2\right) + \mathcal{O}\left(44 L_p K^2\right) + \mathcal{O}(L_p K^3) \\ &\quad + \mathcal{O}\left(L_p L\left((K+1)^{0.5}(2(K+1)^3 \right.\right. \\ &\quad \left.\left. + 4(K+1)^2 + 8\right) \log(1/\epsilon))\right). \end{aligned}$$

4.3.4 Computational complexity of $\mathbf{w}_J \perp \mathbf{h}_{jd}$ *Scheme*

In $\mathbf{w}_J \perp \mathbf{h}_{jd}$ scheme, we just need to calculate (27) and (29). Thus, in the light of [33], the computational complexity of $\mathbf{w}_J \perp \mathbf{h}_{jd}$ scheme is $\mathcal{O}\left(L_p K^2\right) + \mathcal{O}\left(22 L_p M^2\right)$.

4.3.5 Computational complexity of $\mathbf{w}_J \parallel \mathbf{h}_{je}$ *scheme*

Similar to $\mathbf{w}_J \perp \mathbf{h}_{jd}$ scheme, the computational complexity is also $\mathcal{O}\left(L_p K^2\right) + \mathcal{O}\left(22 L_p M^2\right)$.

4.3.6 Comparison

In summary, we listed the computational complexity of all proposed schemes in Table 1. Note that the one-dimension searching times L and L_p always keep constant

Table 1 Computational complexity of all schemes

Scheme	Complexity
Optimal	$\mathcal{O}\left(44N^2\right)+\mathcal{O}(N^3)+\mathcal{O}\left(L\left((N+1)^{0.5}\left(2(N+1)^3 +4(N+1)^2+8\right)\right)\right)\log(1/\epsilon)$
$\mathbf{w}_R\perp\mathbf{h}_{re}$	$\mathcal{O}(M^2)$
$\mathbf{w}_R\parallel\mathbf{h}_{rd}$	$\mathcal{O}\left(L_pM^2\right)+\mathcal{O}\left(44L_pK^2\right)+\mathcal{O}(L_pK^3)$ $+\mathcal{O}\left(L_pL((K+1)^{0.5}(2(K+1)^3+4(K+1)^2+8)\log(1/\epsilon))\right)$
$\mathbf{w}_J\perp\mathbf{h}_{jd}$	$\mathcal{O}\left(L_pK^2\right)+\mathcal{O}\left(22L_pM^2\right)$
$\mathbf{w}_J\parallel\mathbf{h}_{je}$	$\mathcal{O}\left(L_pK^2\right)+\mathcal{O}\left(22L_pM^2\right)$

if N increases, we just focus on the amounts of computational complexity as N, K and M increase. As N is no less than M and K, we have two conclusions:

- The optimal scheme has the most computational complexity among all proposed schemes.
- $\mathbf{w}_R\perp\mathbf{h}_{re}$ scheme incurs least computational complexity among all proposed schemes.

5 Numerical results

In this section, numerical results are presented to evaluate the secrecy performance of our proposed optimal and suboptimal designs. As shown in Fig. 2, without loss of generality, we consider the scenario that the source, the eavesdropper, the destination are located in a straight line, and relays are randomly distributed around the middle point between the source and destination. The location of these nodes are shown in Fig. 2. We suppose that all relays are so close that they have the same location in our simulations. The other parameters are set as $K_0 = 1$, $\beta = 3$, and $\sigma_0^2 = 1$ [19]. The SNR threshold that relay decodes the received message correctly is 3 dB. Moreover, we set the additive Gaussian noise power $N_0 = 1$mW. As the benchmarks of our designs, we also simulate the performances of CB, SRSJ, SRMJ, and MRSJ schemes with optimal beamforming to achieve the maximum secrecy capacity. Note that the optimal beamforming vectors and power for CB, SRSJ, SRMJ, and MRSJ schemes are obtained by exhaustive searching. For SRSJ, SRMJ, and MRSJ schemes, to perform the jamming relay selection in DF relay networks, we give the priority to select the jamming relay among the relays failing to decode the message and have to pick out the best jamming relay if all relays decode the message from the source correctly.

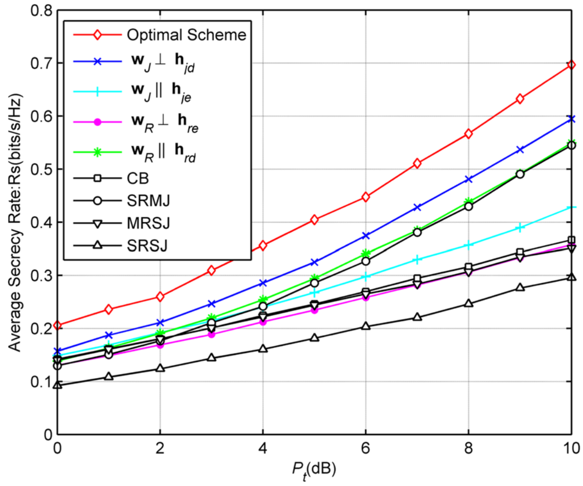

Fig. 3 The average secrecy capacity versus total transmit power of relays, $P_s = 0$ dB, $N = 5$

Figure 3 shows the secrecy performance of various secrecy transmission schemes versus P_t. Explicitly, the proposed optimal scheme outperforms all other schemes. Except the optimal scheme, the suboptimal scheme $\mathbf{w}_J\perp\mathbf{h}_{jd}$ has the maximum secrecy capacity than left transmission schemes. As a result, if the system cannot afford the huge computational complexity of the proposed optimal scheme, the $\mathbf{w}_J\perp\mathbf{h}_{jd}$ scheme in this paper is recommended to achieve the good tradeoff between the secrecy capacity and computational complexity. Besides, in this scenario, $\mathbf{w}_R\parallel\mathbf{h}_{rd}$ scheme achieves similar performances as the SRMJ scheme. $\mathbf{w}_J\parallel\mathbf{h}_{je}$ scheme can obtain larger secrecy capacity than CB, MRSJ, and SRSJ schemes.

In Fig. 4, we show the average secrecy performance of these transmission schemes versus the number of relays N. Obviously, the average secrecy capacity increases as N increases. The optimal scheme always achieves the maximum secrecy capacity among all transmission schemes. Similarly, the $\mathbf{w}_J\perp\mathbf{h}_{jd}$ scheme with lower complexity has the second best performance. When $N = 3$, we can see that the performance gaps become drastically slight. The reason is that there is no enough degree of freedom

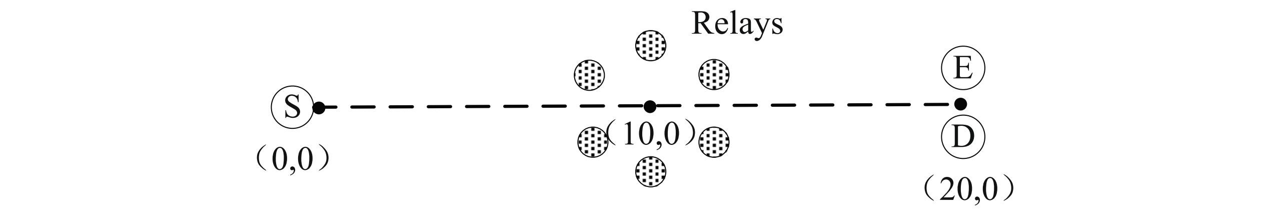

Fig. 2 Scenario used for numerical experiments

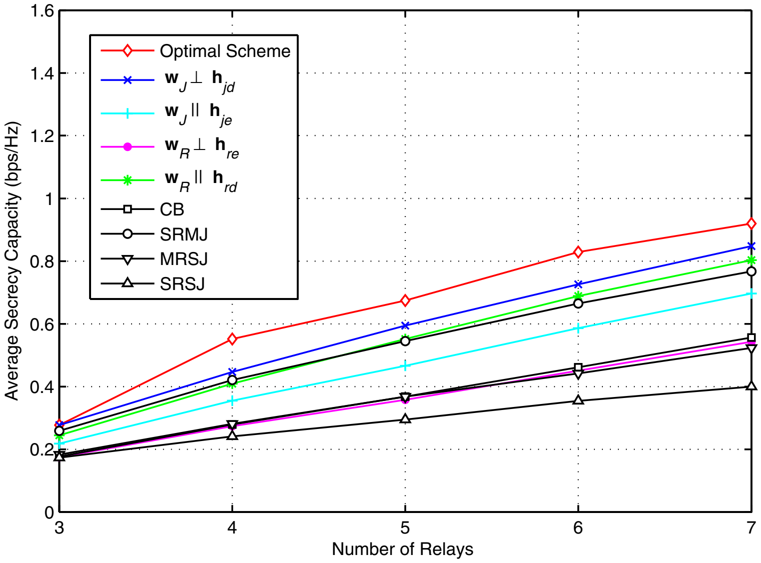

Fig. 4 The average secrecy capacity as a function of the number of relays N for DF relay network, $P_t = 10$ dB, $P_s = 0$ dB

to make these transmission schemes produce different results. Meanwhile, as N increases, the performance gap between arbitrary two schemes increases. That is to say the proposed schemes are more suitable for large-scale DF relay networks.

To investigate the effects of the relay positions on the secrecy performances of these transmission schemes, we draw the average secrecy capacity versus d_{sr} in Fig. 5. The proposed optimal scheme always perform the best secrecy performance among all these transmission schemes. Interestingly, there two extreme cases worth observing. When these relays approach the source closely, the optimal scheme, $\mathbf{w}_J \perp \mathbf{h}_{jd}$ scheme, $\mathbf{w}_J \parallel \mathbf{h}_{je}$ scheme, $\mathbf{w}_R \perp \mathbf{h}_{re}$ scheme and CB scheme have nearly the same performance. This is because the probability of the relay decoding the message from the source correctly tends to be 1, so that above mentioned schemes can almost employ all relays to perform information beamforming. When the relays approach the destination, all transmission schemes tend to incur zero secrecy capacity, which means the relay network can not provide physical layer secrecy. The reason is that the probability of the relay decoding the

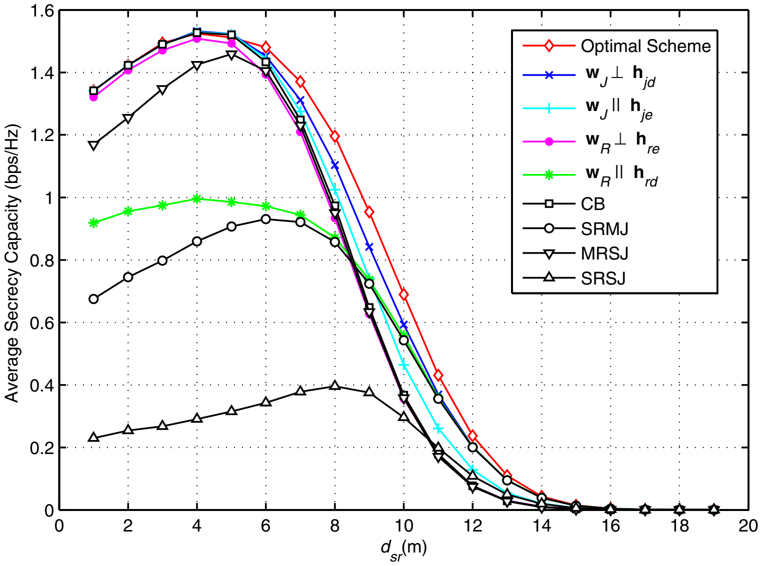

Fig. 5 The average secrecy capacity versus the distance from source to relays (d_{sr}), $P_t = 10$ dB, $N = 5$

message from the source successfully tends to be zero. Meanwhile, we can see that there exists an optimal d_{sr} for each schemes in Fig. 5. For example, with the simulation parameters, $d_{sr} \approx 4$ m is the optimal distance to achieve the best secrecy rate for the optimal scheme, $\mathbf{w}_J \perp \mathbf{h}_{jd}$ scheme, $\mathbf{w}_J \parallel \mathbf{h}_{je}$ scheme, $\mathbf{w}_R \perp \mathbf{h}_{re}$ scheme, and CB scheme. $d_{sr} \approx 5$ m is the optimal distance for the MRSJ scheme. Similarly, other schemes also have the optimal d_{sr} in Fig. 5. Even though we can place these relays arbitrarily, the optimal scheme also performs the maximum secrecy rate among all schemes. In summary, if the relays approach the source, we can choose one of $\mathbf{w}_J \perp \mathbf{h}_{jd}$ scheme, $\mathbf{w}_J \parallel \mathbf{h}_{je}$ scheme, $\mathbf{w}_R \perp \mathbf{h}_{re}$ scheme, and CB scheme to configure the secrecy transmission. Otherwise, the optimal scheme is recommended to achieve the maximum secrecy capacity and the $\mathbf{w}_J \perp \mathbf{h}_{jd}$ scheme is suggested in the aspect of tradeoff between secrecy performance and computational complexity.

6 Conclusions

In this paper, we proposed an optimal scheme and four suboptimal schemes with low computational complexity in the DF relay networks to enhance the transmission security. Unlike the prior works, the proposed transmission schemes utilize the property of DF relays to let the relays decoding incorrectly transmit jamming signals to confound the eavesdropper and the relays decoding correctly transmit information beamforming to the destination. By our numerical results, the optimal scheme outperforms all existing schemes and the proposed suboptimal schemes. In addition, some suboptimal schemes with low computational complexity also have better secrecy performance than existing schemes. Moreover, we found that our proposed schemes are more suitable for the large-scale relay networks and the scenarios where relays are near the middle position between the source and destination.

Funding

The work was supported in part by the National Natural Science Foundation of China under Grant No. 61431011, NSFC, China, and the Fundamental Research Funds for the Central Universities, XJTU, China.

Authors' contributions

CG and CZ proposed the ideas in this paper. CG performed the analysis and simulations and wrote the paper. CZ reviewed and edited the manuscript. All authors read and approved the manuscript.

Competing interests

The authors declare that they have no competing interests.

Publisher's Note

Received: 9 June 2017 Accepted: 24 November 2017
Published online: 06 December 2017

References

1. M Bloch, J Barros, *Physical-Layer Security: From Information Theory to Security Engineering*. (Cambridge University Press, Cambridge, 2011)
2. A Mukherjee, S Fakoorian, J Huang, AL Swindlehurst, Principles of physical layer security in multiuser wireless networks: a survey. IEEE Commun. Surveys Tuts. **16**(3), 1550–1573 (2014)
3. N Yang, HA Suraweera, IB Collings, C Yuen, Physical layer security of TAS/MRC with antenna correlation. IEEE Trans. Inf. Forensic Secur. **8**(1), 254–259 (2013)
4. J Zhang, C Yuen, CK Wen, S Jin, KK Wong, H Zhu, Large system secrecy rate analysis for SWIPT MIMO wiretap channels. IEEE Trans. Inf. Forensic Secur. **11**(1), 74–85 (2015)
5. X Chen, C Zhong, C Yuen, HH Chen, Multi-antenna relay aided wireless physical layer security. IEEE Commun. Mag. **53**(12), 40–46 (2015)
6. R Bassily, E Ekrem, X He, E Tekin, J Xie, MR Bloch, S Ulukus, A Yener, Cooperative security at the physical layer: a summary of recent advances. IEEE Signal Process. Mag. **30**(5), 16–28 (2013)
7. A Kuhestani, A Mohammadi, M Noori, Optimal power allocation to improve secrecy performance of non-regenerative cooperative systems using an untrusted relay. IET Commun. **10**(8), 962–968 (2016)
8. L Dong, Z Han, AP Petropulu, HV Poor, Improving wireless physical layer security via cooperating relays. IEEE Trans. Signal Process. **58**(3), 1875–1888 (2010)
9. C Jeong, I Kim, DI 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**(1), 310–325 (2012)
10. Y Yang, Q Li, W Ma, J Ge, PC Ching, Cooperative secure beamforming for AF relay networks with multiple eavesdroppers. IEEE Signal Process. Lett. **20**(1), 35–38 (2013)
11. X Gong, H Long, H Yin, F Dong, B Ren, Robust amplify-and-forward relay beamforming for security with mean square error constraint. IET Commun. **9**(8), 1081–1087 (2015)
12. L Wang, Y Cai, Y Zou, W Yang, L Hanzo, Joint relay and jammer selection improves the physical layer security in the face of CSI feedback delays. IEEE Trans. Veh. Technol. **65**(8), 6259–6274 (2016)
13. C Wang, H Wang, X Xia, Hybrid opportunistic relaying and jamming with power allocation for secure cooperative networks. IEEE Trans. Wireless Commun. **14**(2), 589–605 (2015)
14. H Wang, M Luo, X Xia, Q Yin, Joint cooperative beamforming and jamming to secure AF relay systems with individual power constraint and no eavesdropper's CSI. IEEE Signal Process. Lett. **20**(1), 39–42 (2013)
15. X Chen, L Lei, H Zhang, C Yuen, Large-scale MIMO relaying techniques for physical layer security: AF or DF? IEEE Trans. Wirel. Commun. **14**(9), 5135–5146 (2015)
16. M Lin, J Ge, Y Yang, An effective secure transmission scheme for af relay networks with two-hop information leakage. IEEE Commun. Lett. **17**(8), 1676–1679 (2013)
17. S Vishwakarma, A Chockalingam, in *Proc.IEEE Int. Conf. Commun. (ICC)*. Amplify-and-forward relay beamforming for secrecy with cooperative jamming and imperfect CSI (IEEE, Budapest, 2013), pp. 1640–1645
18. H Hui, A Swindlehurst, G Li, J Liang, Secure relay and jammer selection for physical layer security. IEEE Signal Process. Lett. **22**(8), 1147–1151 (2015)
19. L Wang, C Cao, M Song, Y Cheng, in *Proc.IEEE Int. Conf. Commun. (ICC)*. Joint cooperative relaying and jamming for maximum secrecy capacity in wireless networks (IEEE, Sydney, 2014), pp. 4448–4453
20. X Guan, Y Cai, Y Wang, W Yang, in *Proc of IEEE PIMRC, Toronto, Canada*. Increasing secrecy capacity via joint design of cooperative beamforming and jamming (IEEE, Toronto, 2011), pp. 1279–1283
21. N Kolokotronis, A Manos, in *Proc.IEEE Signal Process. Conf. (EUSIPCO)*. Improving physical layer security in DF relay networks via two-stage cooperative jamming, (2016), pp. 1173–1177
22. ER Alotaibi, KA Hamdi, Optimal cooperative relaying and jamming for secure communication. IEEE Wireless Commun. Lett. **6**, 689–692 (2015)
23. J Li, AP Petropulu, S Weber, On cooperative relaying schemes for wireless physical layer security. IEEE Trans. Signal Process. **59**(10), 4985–4997 (2011)
24. Z Lin, Y Cai, W Yang, L Wang, Robust secure switching transmission in multi-antenna relaying systems: cooperative jamming or decode-and-forward beamforming. IET Commun. **10**(13), 1673–1681 (2016)
25. B Li, Z Fei, Robust beamforming and cooperative jamming for secure transmission in DF relay systems. EURASIP J. Wireless Commun (2016). Networking. doi:10.1186/s13638–016-0560-1

26. J Myung, H Heo, J Park, Joint beamforming and jamming for physical layer security. ETRI. **37**(6), 898–905 (2015)
27. C Gu, C Zhang, in *Proc.of IEEE International Conference on Communication Systems (ICCS)*. Adaptive distributed beamforming and jamming in DF relay networks for physical layer secrecy (IEEE, Shenzhen, 2016), pp. 1–5
28. H Guo, Z Yang, L Zhang, J Zhu, Y Zou, in *Proc.of IEEE ICC*. Optimal power allocation for joint cooperative beamforming and jamming assisted wireless networks (IEEE, Paris, 2017)
29. M Bloch, J Barros, MRD Rodrigues, SW McLaughlin, Wireless information-theoretic security. IEEE Trans. Inf. Theory. **54**(6), 2515–2534 (2008)
30. Z Luo, W Ma, A So, Y Ye, S Zhang, Semidefinite relaxation of quadratic optimization problems. IEEE Signal Process. Mag. **27**(3), 20–34 (2010)
31. S Boyd, L Vandenberghe, *Convex Optimization*. (Cambridge University Press, Cambridge, 2004)
32. A Charnes, W Cooper, Programming with linear fractional functionals. Naval Res. Logist Quarter. **9**, 181–186 (1962)
33. GH Golub, CF Van Loan, *Matrix Computations*, 3rd edn. (The John Hopkins Univ. Press, Baltimore, 1996)
34. RA Horn, CR Johnson, *Matrix Analysis*. (Cambridge University Press, Cambridge, 1985)
35. A Goldsmith, *Wireless Communications*. (Cambridge University Press, Cambridge, 2004)
36. M Lobo, L Vandenberghe, S Boyd, H Lebret, Applications of second-order cone programming. Linear Algebra Appl. **284**, 193–228 (1998)