doi:10.3772/j.issn.1006-6748.2020.02.010

Physical layer security transmission algorithm based on cooperative beamforming in SWIPT system[①]

Wu Guodong(武国栋), Hu Zhentao[②], Jin Yong
(School of Computer and Information Engineering, Henan University, Kaifeng 475004, P. R. China)

Abstract

Physical layer security transmission issue in simultaneous wireless information and power transfer (SWIPT) relay network with multiple eavesdropers is investigated in this paper. A novel cooperative beamforming algorithm is proposed to balance performance of cooperative jamming method and zero-forcing method. Using location prior information of eavesdropper, the proposed method imposes zero-forcing constraints on the capable eavesdropper and cooperative jamming on remaining weak eavesdropper, respectively. Compared with classical cooperative jamming or zero-forcing methods, the proposed method can compromise computational complexity and secrecy rate. Performance of the method is verified by simulation experiments.

Key words: simultaneous wireless information and power transfer (SWIPT), beamforming, cooperative jamming (CJ), zero-forcing (ZF), secrecy communication

0 Introduction

Today, with the popularization of smart terminals and the increasing growth of wireless multimedia services, the information and communication industry is rapidly developing while its huge energy demand has become an urgent problem[1]. Traditional energy harvesting (EH) technologies (such as solar energy and wind energy) had many defects, and their EH efficiency was easily affected by weather, season and geographical condition, then they could not be a stable energy source for wireless devices. At present, a technique called simultaneous wireless information and power transfer (SWIPT) has been proposed, which can provide stable and controllable energy for wireless devices while transmitting the required information for them[2,3]. In addition, the application of SWIPT technology can reduce the hardware cost of the system and extend the service life of energy-constrained devices[4-6].

However, due to the openness of its communication mode, the transmission information of SWIPT is easily intercepted and monitored by illegal devices, so that the privacy of the information is difficult to guarantee[7]. The traditional security technology relies on the cryptography system, which mainly includes technologies such as identity authentication and key generation[8]. The effectiveness of the encryption algorithm is guaranteed by the extremely high computational complexity required to crack the key. But, with increasing computing power of computer, decoding efficiency of illegal user is gradually enhancing. Traditional encryption algorithm is facing new challenge.

Recently, physical layer security (PLS) technology has provided new ideas for researchers and gradually become a research hotspot[9,10]. Hoang et al.[11] considered a cooperative wireless network scene in which a source, a destination, and multiple intermediate energy harvesting nodes coexist with multiple eavesdroppers. By selecting a pair of intermediate nodes as a relay node and a jammer, confidential and jamming signals are respectively sent to the destination and eavesdroppers. Xing and Wong[12] explored information security transmission in SWIPT multi-relay network scene, and designed a cooperative beamforming scheme based on multi-relay cooperative jamming (CJ), and then gave a global optimal solution. Although the scheme can achieve excellent secrecy rate, the computational complexity of the algorithm is high. So, Xing's algorithm is unsuitable in real-time engineering scene. Yang et al.[13] and Goel et al.[14] discussed the information se-

[①] Supported by the National Natural Science Foundation of China (No. 61771006, 61976080), the Key Research and Development Projects in Henan Province of China (No. 192102210254), the Key Research Projects of University in Henan Province of China (No. 19A413006) and the First-class Discipline Training Foundation of Henan University (No. 2018YLTD04).

[②] To whom correspondence should be addressed. E-mail: hzt@henu.edu.cn

Received on Apr. 24, 2019

curity transmission problem of relay networks in single eavesdropping and multi-eavesdropping scenarios, and designed the corresponding low-complexity suboptimal schemes based on zero-forcing (ZF) criteria. The schemes transform the original non-convex problem into a convex problem by imposing a zero-forcing constraint on the eavesdropper, which significantly reduces the complexity of the algorithm. However, as the number of eavesdropper increases, the performance achieved by algorithm will deteriorate dramatically, and it will be difficult to meet the receiver's need for secrecy rate. In addition, the algorithm is only suitable for the system in which the number of eavesdroppers is less than the number of relays.

In some practical engineering application scenarios, due to hardware limitations, algorithms are required to make reasonable compromise between computational complexity and performance. For this reason, a cooperative beamforming algorithm based on CJ and ZF is proposed in this paper. The core idea of the algorithm is to impose zero-forcing constraints on the capable eavesdroppers while suppressing the remaining weak eavesdropper using CJ method. Compared with CJ method, the proposed algorithm reduces the dimension of the target vector to be optimized, which leads to low computational complexity. Compared with ZF method, the proposed algorithm increases the spatial freedom of the target vector to be optimized and obtains high secrecy rate. The proposed algorithm has 2 advantages:

(1) Since the number of eavesdroppers who are imposed zero-forcing constraints in the algorithm is controllable, the computational complexity and performance of the algorithm implemented in this paper is also controllable, which is obviously more suitable for practical engineering applications.

(2) In addition, different from the work of Yang and Goel, the proposed algorithm does not limit the number of eavesdroppers, which is allowed to exceed the number of relays.

The rest of the paper includes 4 sections. Section 1 introduces the system model of the multi-AF (amplify and forward) relaying networks with SWIPT, and defines the secrecy rate of the relay wiretap channel. Next, through joint CJ method and ZF criteria, the secrecy rate maximization problem is formulated in Section 2, and an algorithm is designed to solve it. Then, Section 3 analyzes and evaluates the performance of the proposed method with others. Finally, conclusion is presented in Section 4.

Notations: boldface capital letters and boldface lower case letters denote matrices and vectors, respectively. Moreover, $(\cdot)^{\dagger}$, $(\cdot)^{\mathrm{T}}$ and $(\cdot)^{\mathrm{H}}$ represent the conjugate, the transpose and the conjugate transpose on matrices and vectors, respectively. $[\cdot]_{i=1}^{N}$ denotes an $N \times 1$ vector with each element indexed by i. diag$(\cdot)$ denotes the diagonal matrix of the specified vector, trace$(\cdot)$ denotes the trace of the matrix, $[\cdot]_{i,j}$ denotes the (i,j)th entry of a matrix, and $\|\cdot\|$ represents the Euclidean norm. In addition, $\mathbb{C}^{x \times y}$ represents the complex domain with dimension $x \times y$, and $\mathbf{E}[\cdot]$ denotes the expectation operator. Finally, $(x)^{+}$ is abbreviation formax$(x,0)$, $CN(\mathbf{0}, \boldsymbol{X})$ denotes the circularly symmetric complex Gaussian distribution with mean vector $\mathbf{0}$ and covariance matrix $\boldsymbol{X}$.

1 System model and problem formulation

This work considers the secrecy transmission of information in a multi-relay wireless sensor network with SWIPT as shown in Fig. 1, which includes a source node $\mathbb{S}$, a destination node $\mathbb{D}$, K eavesdropper nodes $\mathbb{E}_k$, $k = 1, \cdots, K$ and N amplify and forward (AF) relay nodes $\mathbb{R}_i$, $i = 1, \cdots, N$. And all nodes in the network are only equipped with a single antenna. In this network, the source node $\mathbb{S}$ hopes to establish stable secure communication with the destination node $\mathbb{D}$ by means of the relay nodes $\mathbb{R}$. In addition, assume that there is no direct link between $\mathbb{S}$ and $\mathbb{D}$, $\mathbb{E}$ for the simplicity of exposition.

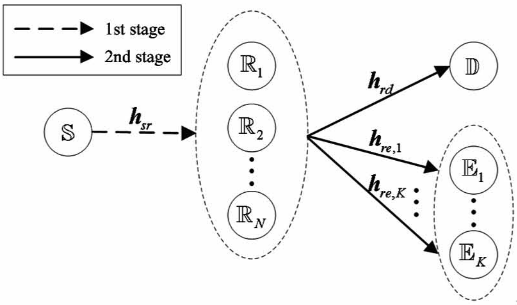

Fig. 1 System model

Assume that each AF relay node lacks external power, it need to use the power split (PS) protocol to harvest energy and receive information simultaneously. Specifically, as shown in Fig. 2, after the received signal of each relay passes through the power splitter, which split a portion of ρ_i, of the received power for EH, and the rest $1 - \rho_i$ for information receiving. After that, the havested power is subdivided into 2 parts, where γ_i of the power used for generating the artificial noise (AN) versus the rest $1 - \gamma_i$ is temporarily stored in a capacitor and used to forward information later. Meanwhile, $0 \leqslant \eta < 1$ is defined as the conversion efficiency of energy harvesting.

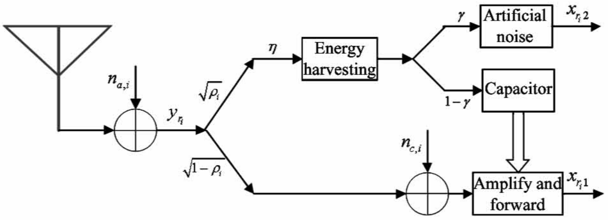

Fig. 2 The power splitting at relay

According to the AF protocol, the cooperative process is divided into 2 stages.

1.1 Transmission stage

In the first stage, the received signal of each relay can be expressed as

$$y_{r_i} = h_{sr_i}\sqrt{P_s}s + n_{a,i} \quad i \in \{1,\cdots,N\} \tag{1}$$

where, P_s is the transmit power at the source $\mathbb{S}$, $s \sim CN(0,1)$ denotes the transmit signal, h_{sr_i} represents the complex channel from the source $\mathbb{S}$ to the relay $\mathbb{R}_i$, and $n_{a,i} \sim CN(0,\sigma_{n_a}^2)$ is the additive white Gaussian noise (AWGN) at $\mathbb{R}_i$. Thus, the linearly amplified baseband equivalent signal at the relay $\mathbb{R}_i$ is given by

$$x_{r_i1} = \alpha_i(\sqrt{1-\rho_i}y_{r_i} + n_{c,i}) \quad i \in \{1,\cdots,N\} \tag{2}$$

where, α_i is the complex AF coefficient of the relay $\mathbb{R}_i$. In addition, the noise caused by the conversion of signal from the RF to the baseband is represented by $n_{c,i} \sim CN(0,\sigma_{n_c}^2)$. Moreover, the received signal of the relay $\mathbb{R}_i$ is constrained by the harvested power, i.e., $\eta(1-\gamma_i)\rho_i \mid y_{r_i} \mid^2$, and the expression of α_i can be derived as

$$\alpha_i = \sqrt{\frac{\eta(1-\gamma_i)\rho_i \mid h_{sr_i} \mid^2 P_s}{(1-\rho_i) \mid h_{sr_i} \mid^2 P_s + (1-\rho_i)\sigma_{n_a}^2 + \sigma_{n_c}^2}}e^{j\angle\alpha_i} \tag{3}$$

where $\angle\alpha_i$ is defined as the phase of the AF coefficient of the relay $\mathbb{R}_i$.

1.2 Cooperative forwarding stage

In the second stage, according to the CJ strategy, all relay nodes cooperate to generate the AN signal expressed as $\boldsymbol{x}_{r2} = [x_{r_12},\cdots, x_{r_n2}]^{\mathrm{T}}$, and define its covariance matrix as $\boldsymbol{V} = \mathbf{E}[\boldsymbol{x}_{r2}\boldsymbol{x}_{r2}^{\mathrm{H}}]$. At this time, a unique cooperative AN signal can be obtained by performing eigenvalue decomposition (EVD) on $\boldsymbol{V}$. If $\boldsymbol{V} = \widetilde{\boldsymbol{U}}\widetilde{\boldsymbol{\Sigma}}\widetilde{\boldsymbol{U}}^{\mathrm{H}}$, where $\widetilde{\boldsymbol{\Sigma}} = \mathrm{diag}([\lambda_1,\cdots,\lambda_d])$ is a diagonal matrix with $\lambda_j (j = 1,\cdots,d)$, representing all the positive eigenvalues of $\boldsymbol{V}$. Meanwhile, $\widetilde{\boldsymbol{U}} \in \mathbb{C}^{N\times d}$ is the precoding matrix satisfying $\widetilde{\boldsymbol{U}}^{\mathrm{H}}\widetilde{\boldsymbol{U}} = \boldsymbol{I}$. Then, the AN signal can be described as

$$\boldsymbol{x}_{r2} = \sum_{j=1}^{d}\sqrt{\lambda_j}u_j s'_j \tag{4}$$

where, u_j is the jth column of $\widetilde{U}$, $s'_j \sim CN(0,1)$ denotes the signal symbol of the AN. In addition, the power of the AN signal is also constrained as $\mid x_{r_i2} \mid^2 \leqslant \eta\gamma_i\rho_iP_s \mid y_{r_i} \mid^2$, which indicates that

$$\mathrm{trace}(\boldsymbol{VE}_i) \leqslant \eta\gamma_i\rho_iP_s \mid h_{sr_i} \mid^2,\ i \in \{1,\cdots,N\} \tag{5}$$

where, $\boldsymbol{E}_i = \mathrm{diag}(\boldsymbol{e}_i)$, $\boldsymbol{e}_i$ denotes a unit vector with ith element equal to 1 and the rest equal to 0.

The received signal at the destination $\mathbb{D}$ is given by

$$y_d = \boldsymbol{h}_{rd}^{\mathrm{T}}\boldsymbol{x}_{r1} + n_d \tag{6}$$

where, $\boldsymbol{h}_{rd} = [h_{r_id}]_{i=1}^{N}$ represents the complex channel from the relay $\mathbb{R}$ to the destination $\mathbb{D}$, $n_d \sim CN(0, \sigma_{n_d}^2)$ is the corresponding receiving AWGN. By combining Eqs(1), (2) and (6), y_d can be expressed as

$$y_d = \boldsymbol{h}_{rd}^{\mathrm{T}}\boldsymbol{D}_{\alpha\rho}\boldsymbol{h}_{sr}\sqrt{P_s}s + \boldsymbol{h}_{rd}^{\mathrm{T}}\boldsymbol{D}_{\alpha\rho}\boldsymbol{n}_a + \boldsymbol{h}_{rd}^{\mathrm{T}}\boldsymbol{D}_{\alpha}\boldsymbol{n}_c + n_d \tag{7}$$

where, $\boldsymbol{D}_{\alpha\rho}$ and $\boldsymbol{D}_{\alpha}$ are diagonal matrices, and their diagonals are $(\alpha_1\sqrt{1-\rho_1},\cdots,\alpha_N\sqrt{1-\rho_N})^{\mathrm{T}}$ and $(\alpha_1, \cdots,\alpha_N)^{\mathrm{T}}$, respectively. Furthermore, $\boldsymbol{h}_{sr} = [h_{sr_i}]_{i=1}^{N}$, $\boldsymbol{n}_a = [n_{a,i}]_{i=1}^{N}$ and $\boldsymbol{n}_c = [n_{c,i}]_{i=1}^{N}$.

The received signal at the eavesdropper $\mathbb{E}_k$ is given by

$$y_{e,k} = \boldsymbol{h}_{re,k}^{\mathrm{T}}\boldsymbol{D}_{\alpha\rho}\boldsymbol{h}_{sr}\sqrt{P_s}s + \boldsymbol{h}_{re,k}^{\mathrm{T}}\boldsymbol{D}_{\alpha\rho}\boldsymbol{n}_a + \boldsymbol{h}_{re,k}^{\mathrm{T}}\boldsymbol{D}_{\alpha}\boldsymbol{n}_c + \boldsymbol{h}_{re,k}^{\mathrm{T}}\sum_{j=1}^{d}\sqrt{\lambda_j}u_js'_j + n_{e,k} \tag{8}$$

where, $\boldsymbol{h}_{re,k} = [h_{r_ie,k}]_{i=1}^{N}$ represents the complex channel from the relay $\mathbb{R}$ to the eavesdropper $\mathbb{E}_k$, and $n_{e,k} \sim CN(0, \sigma_{n_{e,k}}^2)$ is the receiving AWGN at the eavesdropper $\mathbb{E}_k$.

Thus, their respective signal to interference plus noise ratios (SINRs) are defined as

$$SINR_{\mathbb{S},\mathbb{D}} = \frac{P_s \mid \boldsymbol{h}_{rd}^{\mathrm{T}}\boldsymbol{D}_{\alpha\rho}\boldsymbol{h}_{sr} \mid^2}{\mathrm{trace}(\boldsymbol{Vh}_{rd}^{\dagger}\boldsymbol{h}_{rd}^{\mathrm{T}}) + \sigma_{n_a}^2 \| \boldsymbol{h}_{rd}^{\mathrm{T}}\boldsymbol{D}_{\alpha\rho} \|^2 + \sigma_{n_c}^2 \| \boldsymbol{h}_{rd}^{\mathrm{T}}\boldsymbol{D}_{\alpha} \|^2 + \sigma_{n_d}^2} \tag{9}$$

$$SINR_{\mathbb{S},\mathbb{E},k} = \frac{P_s \mid \boldsymbol{h}_{re,k}^{\mathrm{T}}\boldsymbol{D}_{\alpha\rho}\boldsymbol{h}_{sr} \mid^2}{\mathrm{trace}(\boldsymbol{Vh}_{re,k}^{\dagger}\boldsymbol{h}_{re,k}^{\mathrm{T}}) + \sigma_{n_a}^2 \| \boldsymbol{h}_{re,k}^{\mathrm{T}}\boldsymbol{D}_{\alpha\rho} \|^2 + \sigma_{n_c}^2 \| \boldsymbol{h}_{re,k}^{\mathrm{T}}\boldsymbol{D}_{\alpha} \|^2 + \sigma_{n_{e,k}}^2} \tag{10}$$

According to the SINRs, the mutual information for the destination $\mathbb{D}$ can be calculated as $r_{\mathbb{S},\mathbb{D}} = 0.5\log(1 + SINR_{\mathbb{S},\mathbb{D}})$, and that for the eavesdropper $\mathbb{E}_k$ is $r_{\mathbb{S},\mathbb{E},k} = 0.5\log(1 + SINR_{\mathbb{S},\mathbb{E},k})$. In summary, the secrecy rate can be defined as

$$r_{\sec} = (r_{\mathbb{S},\mathbb{D}} - \max r_{\mathbb{S},\mathbb{E},k})^{+} \qquad (11)$$

2 The design of cooperative beamforming algorithm

In this section, according to CJ method and ZF criteria, a cooperative beamforming algorithm is designed. Furthermore, to simplify the description, only the static power splitting scheme is considered, and the factor of power splitting is a fixed value, i. e. , $\rho_i = \bar{\rho}$, $i \in \{1,\cdots,N\}$.

2.1 The preparation of beamforming

In order to analyze the problem conveniently, the Eq. (11) is transformed as:

$$r_{\mathbb{S},\mathbb{D}} = \frac{1}{2}\log_2\left(1 + \frac{P_s \mid \tilde{\boldsymbol{h}}_{sd}^{\mathrm{T}}\boldsymbol{\omega} \mid^2}{\mathrm{trace}(\boldsymbol{V}\boldsymbol{h}_{rd}^{\dagger}\boldsymbol{h}_{rd}^{\mathrm{T}}) + \boldsymbol{\omega}^{\mathrm{H}}\boldsymbol{D}_{sd}\boldsymbol{\omega} + \sigma_{n_d}^2}\right) \qquad (12)$$

where $\omega_i = \sqrt{1 - \gamma_i} e^{j\angle\alpha_i}$,

$$[\tilde{\boldsymbol{h}}_{sd}]_i \triangleq h_{sr_i} h_{r_i d} \sqrt{\frac{\eta\bar{\rho}(1-\bar{\rho}) \mid h_{sr_i} \mid^2 P_s}{(1-\bar{\rho})(\mid h_{sr_i} \mid^2 P_s + \sigma_{n_a}^2) + \sigma_{n_c}^2}} \qquad (13)$$

and

$$[\boldsymbol{D}_{sd}]_{i,i} \triangleq \frac{\eta\bar{\rho}P_s \mid h_{sr_i} \mid^2 \mid h_{r_i d} \mid^2((1-\bar{\rho})\sigma_{n_a}^2 + \sigma_{n_c}^2)}{(1-\bar{\rho})(\mid h_{sr_i} \mid^2 P_s + \sigma_{n_a}^2) + \sigma_{n_c}^2}, \quad i \in \{1,\cdots,N\} \qquad (14)$$

again, by defining

$$[\tilde{\boldsymbol{h}}_{se,k}]_i \triangleq h_{sr_i} h_{r_i e,k} \sqrt{\frac{\eta\bar{\rho}(1-\bar{\rho}) \mid h_{sr_i} \mid^2 P_s}{(1-\bar{\rho})(\mid h_{sr_i} \mid^2 P_s + \sigma_{n_a}^2) + \sigma_{n_c}^2}} \qquad (15)$$

and

$$[\boldsymbol{D}_{se,k}]_{i,i} \triangleq \frac{\eta\bar{\rho}P_s \mid h_{sr_i} \mid^2 \mid h_{r_i e,k} \mid^2((1-\bar{\rho})\sigma_{n_a}^2 + \sigma_{n_c}^2)}{(1-\bar{\rho})(\mid h_{sr_i} \mid^2 P_s + \sigma_{n_a}^2) + \sigma_{n_c}^2} \quad i \in \{1,\cdots,N\} \qquad (16)$$

that

$$r_{\mathbb{S},\mathbb{E},k} = \frac{1}{2}\log_2\left(1 + \frac{P_s \mid \tilde{\boldsymbol{h}}_{se,k}^{\mathrm{T}}\boldsymbol{\omega} \mid^2}{\mathrm{trace}(\boldsymbol{V}\boldsymbol{h}_{re,k}^{\dagger}\boldsymbol{h}_{re,k}^{\mathrm{T}}) + \boldsymbol{\omega}^{\mathrm{H}}\boldsymbol{D}_{se,k}\boldsymbol{\omega} + \sigma_{n_e,k}^2}\right) \qquad (17)$$

Moreover, rewrite Eq. (5) as

$$\mathrm{trace}(\boldsymbol{V}\boldsymbol{E}_i) \leqslant \eta\bar{\rho}P_s \mid h_{sr_i} \mid^2 (1 - \mid \omega_i \mid^2) \quad i \in \{1,\cdots,N\} \qquad (18)$$

2.2 The description of designed algorithm

Based on the priori information of the eavesdropper's channel, the study considers first obtaining the signal to noise ratios (SNRs) of all eavesdroppers by the traditional cooperative beamforming (CB) method. According to that, the channel-related variables will be reordered from strong to weak. Then, it constrains the confidential signal to the null space of the K_0 strong eavesdropper's channel while adopting the CJ method in the relay for the remaining $K - K_0$ weak eavesdropper. Note that the size of K_0 directly determines the computational complexity and reachable secrecy rate of the algorithm. To illustrate the realization of designed method, the framework of the proposed algorithm is given in Fig. 3.

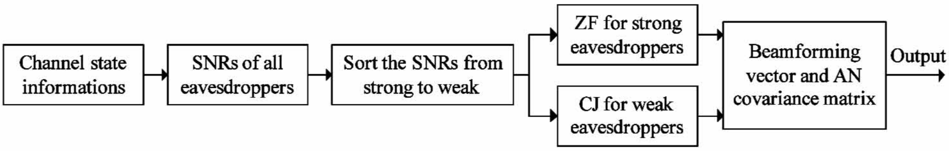
Channel state informations
SNRs of all eavesdroppers
Sort the SNRs from strong to weak
ZF for strong eavesdroppers
CJ for weak eavesdroppers
Beamforming vector and AN covariance matrix
Output

Fig. 3 The framework of the proposed algorithm

The purpose of this paper is to maximize the secrecy rate of the destination $\mathbb{D}$ by jointly optimizing the beamforming vector $\boldsymbol{\omega}$ and the AN covariance matrix $\boldsymbol{V}$. The corresponding optimization problem can be expressed as

(P1):

$$\begin{cases} \max\limits_{\omega, \boldsymbol{V} \succeq 0} (r_{\mathbb{S},\mathbb{D}} - \max r_{\mathbb{S},\mathbb{E},k})^{+} \quad k_1 \in \{K_0 + 1,\cdots,K\} \\ \text{s. t.} \\ \mathrm{trace}(\boldsymbol{V}\boldsymbol{E}_i) \leqslant \eta\bar{\rho}P_s \mid h_{sr_i} \mid^2 (1 - \mid \omega_i \mid^2) \quad i \in \{1,\cdots,N\} \\ \tilde{\boldsymbol{h}}_{se,k_0}^{\mathrm{T}}\boldsymbol{\omega} = 0 \quad k_0 \in \{1,\cdots,K_0\} \end{cases}$$

The details of the algorithm are shown in Table 1.

Remark: in Step 1, the traditional CB method is to make $K_0 = 0$ and $\boldsymbol{V} = \boldsymbol{0}$ for the problem (P1).

2.3 The solution to (P1)

Since the objective function of (P1) is a non-convex function, a two-layer optimization method is introduced[11], and a slack variable $\varphi \in (0,1]$ is added to recast (P1) into a joint problem of upper and lower layers. First, the lower-layer optimization problem can be seen as a quadratic programming (QP) problem with a given fixed φ, as follows.

(P1.1):

$$\begin{cases} \max\limits_{\omega,\boldsymbol{V}\succeq 0}\left(\dfrac{P_s \mid \tilde{\boldsymbol{h}}_{sd}^{\mathrm{T}}\boldsymbol{\omega} \mid^2}{\mathrm{trace}(\boldsymbol{V}\boldsymbol{h}_{rd}^{\dagger}\boldsymbol{h}_{rd}^{\mathrm{T}}) + \boldsymbol{\omega}^{\mathrm{H}}\boldsymbol{D}_{sd}\boldsymbol{\omega} + \sigma_{n_d}^2}\right) \\ \text{s. t.} \\ 1 + \dfrac{P_s \mid \tilde{\boldsymbol{h}}_{se,k_1}^{\mathrm{T}}\boldsymbol{\omega} \mid^2}{\mathrm{trace}(\boldsymbol{V}\boldsymbol{h}_{re,k_1}^{\dagger}\boldsymbol{h}_{re,k_1}^{\mathrm{T}}) + \boldsymbol{\omega}^{\mathrm{H}}\boldsymbol{D}_{se,k_1}\boldsymbol{\omega} + \sigma_{n_e,k_1}^2} \leqslant 1/\varphi \\ \mathrm{trace}((\boldsymbol{V} + \eta\bar{\rho}P_s \mid h_{sr_i} \mid^2 \boldsymbol{\omega}\boldsymbol{\omega}^{\mathrm{H}})\boldsymbol{E}_i) \leqslant \eta\bar{\rho}P_s \mid h_{sr_i} \mid^2 \\ \tilde{\boldsymbol{h}}_{se,k_0}^{\mathrm{T}}\boldsymbol{\omega} = 0, \\ k_1 \in \{K_0+1,\cdots,K\}, i \in \{1,\cdots,N\}, k_0 \in \{1,\cdots,K_0\} \end{cases}$$

Table 1 The compromise algorithm

```
Algorithm  CB method based on CJ and ZF
Input: $P_s$, $N$, $K$, and $K_0$.
Step 1: Initialize $\bar{\rho} = 0.5$, and get the corresponding beamforming vector $\boldsymbol{\omega}_0$ by the traditional CB method.
Step 2: Calculate the SNR of all eavesdroppers from $\boldsymbol{\omega}_0$ by Eq. (10).
Step 3: Sort the eavesdropper's channel from strong to weak by the size of the SNRs.
Step 4: Update the order of the elements within the variable associated with the eavesdroppers, i. e., Eqs (15) and (16).
Step 5: Ensure the number of ZF constraints according to $K_0$.
Step 6: Solve (P1) and obtain the beamfoming vector $\boldsymbol{\omega}$ and covariance matrix $\boldsymbol{V}$.
Output: $\{\gamma_i\}$, $\{\alpha_i\}$, and $\boldsymbol{V}$.
```

On the other hand, the upper-layer optimization problem is not only related to φ, but also to the optimal solution that can be obtained by the lower-layer optimization problem. Therefore, $f(\varphi)$ is defined as the optimal solution of (P1.1). Meanwhile, we denote $H(\varphi) = \varphi f(\varphi)$. The objective function of (P1) is expressed as

$$\frac{1}{2}(\log_2(1+f(\varphi)) - \log_2(1/\varphi)) = \frac{1}{2}\log_2(\varphi + H(\varphi)) \tag{19}$$

The above equation omits $(\ )^+$ in the original objective function. And we declare a zero secrecy rate when it is less than zero.

Therefore, the upper-layer optimization problem is described as

$$(\text{P1.2}): \max_{\varphi} \ \log_2(\varphi + H(\varphi))$$
$$\text{s. t.} \ \varphi_{\min,1} \leqslant \varphi \leqslant 1$$

Since the physical meaning of $1/\varphi - 1$ in (P1.1) is the maximum allowable SINR of the best eavesdropper's channel[12], the feasibility of a non-zero secrecy rate means

$$\varphi \geqslant \frac{1}{1 + NP_s \parallel \tilde{\boldsymbol{h}}_{sd} \parallel^2 / \sigma_{n_d}^2} = \varphi_{\min,1} \tag{20}$$

Since any φ in the feasible domain can calculate the corresponding $H(\varphi)$, and then the optimal solution of the upper-layer problem (P1.2) via a one-dimensional linear search in the interval $[\varphi_{\min,1}, 1]$ can be obtained.

Now, according to the zero-forcing criterion and the semi-definite relaxation (SDR) technique, we deal with the problem (P1.1). Specifically, let $\boldsymbol{\omega} \triangleq \boldsymbol{C}\boldsymbol{m}$, where $\boldsymbol{m} \in \mathbb{C}^{N-K_0}$ is an arbitrary vector, $\boldsymbol{C} \in \mathbb{C}^{N\times(N-K_0)}$ is a semi-unitary matrix consisting of an orthonormal basis for the null space of $\tilde{\boldsymbol{h}}_{se_0}^{\mathrm{T}} \in \mathbb{C}^{K_0\times N}$, which satisfies $\tilde{\boldsymbol{h}}_{se_0}^{\mathrm{T}}\boldsymbol{C} = \boldsymbol{0}$, where $\tilde{\boldsymbol{h}}_{se_0}$ is defined as a set of eavesdropper's channels $\tilde{\boldsymbol{h}}_{se,k_0}$, $k_0 \in \{1,\cdots,K_0\}$ which is arranged in rows. By introducing $\boldsymbol{W} = \boldsymbol{\omega}\boldsymbol{\omega}^{\mathrm{H}} = \boldsymbol{C}\boldsymbol{m}\boldsymbol{m}^{\mathrm{H}}\boldsymbol{C}^{\mathrm{H}} = \boldsymbol{C}\boldsymbol{M}\boldsymbol{C}^{\mathrm{H}}$ and ignoring the rank-one constraint of $\boldsymbol{W}$, (P1.1) is equivalent as follows:

(P1.1-SDR):

$$\begin{cases} \max\limits_{\boldsymbol{M},\boldsymbol{V}\succeq 0} \ \dfrac{\varphi P_s \mathrm{trace}(\boldsymbol{C}\boldsymbol{M}\boldsymbol{C}^{\mathrm{H}}\tilde{\boldsymbol{h}}_{\mathrm{sd}}^{\dagger}\tilde{\boldsymbol{h}}_{sd}^{\mathrm{T}})}{\mathrm{trace}(\boldsymbol{V}\boldsymbol{h}_{rd}^{\dagger}\boldsymbol{h}_{rd}^{\mathrm{T}}) + \mathrm{trace}(\boldsymbol{C}\boldsymbol{M}\boldsymbol{C}^{\mathrm{H}}\boldsymbol{D}_{sd}) + \sigma_{n_d}^2} \\ \text{s. t.} \\ \dfrac{P_s \mathrm{trace}(\boldsymbol{C}\boldsymbol{M}\boldsymbol{C}^{\mathrm{H}}\tilde{\boldsymbol{h}}_{se,k_1}^{\dagger}\tilde{\boldsymbol{h}}_{se,k_1}^{\mathrm{T}})}{\mathrm{trace}(\boldsymbol{V}\boldsymbol{h}_{re,k_1}^{\dagger}\boldsymbol{h}_{re,k_1}^{\mathrm{T}}) + \mathrm{trace}(\boldsymbol{C}\boldsymbol{M}\boldsymbol{C}^{\mathrm{H}}\boldsymbol{D}_{se,k_1}) + \sigma_{n_e,k_1}^2} \\ \leqslant 1/\varphi - 1 \\ \mathrm{trace}((\boldsymbol{V} + \eta\bar{\rho}P_s \mid h_{sr_i} \mid^2 \boldsymbol{C}\boldsymbol{M}\boldsymbol{C}^{\mathrm{H}})\boldsymbol{E}_i) \leqslant \eta\bar{\rho}P_s \mid h_{sr_i} \mid^2 \\ k_1 \in \{K_0+1,\cdots,K\}, i \in \{1,\cdots,N\} \end{cases}$$

Note that the objective function has been multiplied by φ to facilitate direct calculation compared with that of the optimization problem (P1.1).

Although (P1.1-SDR) is easier to solve than (P1.1) by SDR, considering the linear fractional form of the constraints and the objective function, it is still a quasi-convex problem[15]. Therefore, we continue to apply Charnes-Cooper transformation for equivalent convex reconstruction[16]. In particular, by substituting $\boldsymbol{M} = \hat{\boldsymbol{M}}/\xi$ and $\boldsymbol{V} = \hat{\boldsymbol{V}}/\xi$ into (P1.1-SDR), (P1.1-SDP) can be obtained:

$$\begin{cases} \max\limits_{\hat{\boldsymbol{M}},\hat{\boldsymbol{V}}\succeq 0,\xi\geqslant 0} \ P_s \mathrm{trace}(\boldsymbol{C}\hat{\boldsymbol{M}}\boldsymbol{C}^{\mathrm{H}}\tilde{\boldsymbol{h}}_{sd}^{\dagger}\tilde{\boldsymbol{h}}_{sd}^{\mathrm{T}}) \\ \text{s. t.} \\ \mathrm{trace}(\hat{\boldsymbol{V}}\boldsymbol{h}_{rd}^{\dagger}\boldsymbol{h}_{rd}^{\mathrm{T}}) + \mathrm{trace}(\boldsymbol{C}\hat{\boldsymbol{M}}\boldsymbol{C}^{\mathrm{H}}\boldsymbol{D}_{sd}) + \xi\sigma_{n_d}^2 = \varphi \\ (1/\varphi - 1)(\mathrm{trace}(\hat{\boldsymbol{V}}\boldsymbol{h}_{re,k_1}^{\dagger}\boldsymbol{h}_{re,k_1}^{\mathrm{T}}) + \mathrm{trace}(\boldsymbol{C}\hat{\boldsymbol{M}}\boldsymbol{C}^{\mathrm{H}}\boldsymbol{D}_{se,k_1}) \\ + \xi\sigma_{n_e,k_1}^2) \geqslant P_s \mathrm{trace}(\boldsymbol{C}\hat{\boldsymbol{M}}\boldsymbol{C}^{\mathrm{H}}\tilde{\boldsymbol{h}}_{se,k_1}^{\dagger}\tilde{\boldsymbol{h}}_{se,k_1}^{\mathrm{T}}) \\ \mathrm{trace}((\hat{\boldsymbol{V}} + \eta\bar{\rho}P_s \mid h_{sr_i} \mid^2 \boldsymbol{C}\hat{\boldsymbol{M}}\boldsymbol{C}^{\mathrm{H}})\boldsymbol{E}_i) \leqslant \xi\eta\bar{\rho}P_s \mid h_{sr_i} \mid^2 \\ k_1 \in \{K_0+1,\cdots,K\}, i \in \{1,\cdots,N\} \end{cases}$$

It can be found that (P1.1-SDP) is a standard convex optimization problem, which can be solved by some convex optimization toolboxes.

3 Simulation and analysis

In this section, some simulation results are shown to evaluate the performance of the proposed algorithm. Consider N relay nodes and K eavesdropper nodes randomly distributed in a circular area of radius $R = 2$ m, the source node $\mathbb{S}$ is fixed at the edge with a coordinate (-2 m, 0 m), and the corresponding destination node $\mathbb{D}$ is located at the position with a coordinate (2 m, 0 m). Furthermore, it is assumed that the channel model includes large-scale path loss and small-scale multipath fading. The unified path loss model is given by $P_L = 10^{-3} d^{-\alpha}$, where d represents the Euclidean distance between any two nodes. $\alpha = 2.5$ is the path loss exponent. In addition, $\boldsymbol{h}_{sr}$, $\boldsymbol{h}_{rd}$ and $\boldsymbol{h}_{re,k}$ are independent Rayleigh fading with zero mean and P_L variance. Other simulation parameters are set as shown in Table 2.

Table 2 Simulation parameters

Parameters	Typical values
N	10
K	7
K_0	5
P_s	30 dBm
η	50%
$\bar{\rho}$	0.5
$\sigma_{n_c}^2$	−45 dBm
$\sigma_{n_d}^2$	−120 dBm
$\sigma_{n_e,k}^2$	−120 dBm

Fig. 4 shows the secrecy rate versus the number of unconstrained eavesdroppers. It can be found that the secrecy rate of the proposed algorithm is gradually increasing with the number of unconstrained eavesdroppers. Meanwhile, from the perspective of algorithm efficiency, the dimension of the beamforming vector to be designed will also increase with the number of unrestricted eavesdroppers, which will increase the computational complexity of the algorithm. Essentially, the number of zero-forcing constraints directly affects the degree of freedom (DoF), more DoF mean higher secrecy rate and computational complexity. This implies that the proposed algorithm can achieve a tradeoff between computational complexity and secrecy rate. On the other hand, it can be observed from Fig. 4 that the curve of the proposed algorithm is gradually flat, which indicates that the method of selecting the strong eavesdroppers is effective. In addition, the CJ method and the ZF method are the upper and lower bounds of the performance for the proposed algorithm, respectively. And the proposed algorithm is always superior to the traditional CB method.

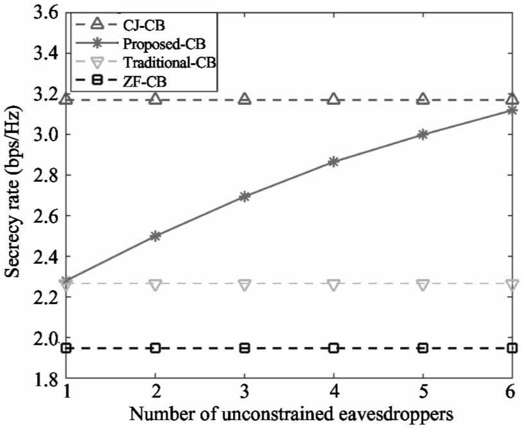

Fig. 4 The secrecy rate versus the number of unconstrained eavesdroppers

Fig. 5 shows the secrecy rate versus the number of relays. It can be seen that the proposed algorithm can always achieve a performance compromise. However, when the number of relays is large, the gap of the reachable secrecy rate of all 4 algorithms is not obvious. This shows that under the premise that the relay has more DoF, the system tends to suppress the eavesdroppers through CB instead of CJ. Therefore, if there are a large number of relays in the system, the number of constrained eavesdroppers should be increased. Obviously, avoiding these eavesdroppers with zero-forcing constraints can significantly reduce the computational complexity of the algorithm and have less impact on the secrecy rate.

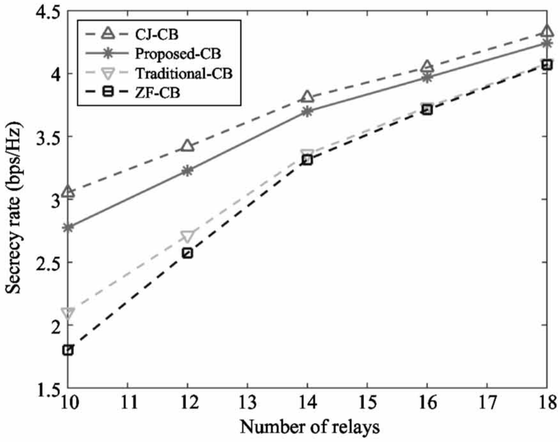

Fig. 5 The secrecy rate versus the number of relays

Fig. 6 shows the secrecy rate versus the number of relays. It can be seen that the performance gap between the proposed algorithm and the CJ method remains approximately constant over the entire range of transmit power selection, which indicates that the proposed algorithm is stable to the change of transmit power. In addition, Fig. 6 shows that in the low power phase, the secrecy rate of the algorithm is lower than that of the traditional CB method. Conversely, in the high power phase, the algorithm is superior to the traditional CB method. This is because when the transmission power of the source is low, the energy harvesting in the relay for CJ is too small, which makes the effect of the CJ not obvious, and the performance loss caused by the zero-forcing constraint cannot be compensated.

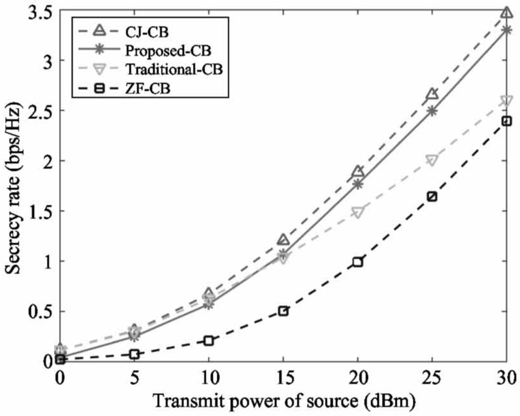

Fig. 6 The secrecy rate versus the transmit power of source

4 Conclusion

In this work, a novel cooperative beamforming algorithm is proposed to balance performance of cooperative jamming method and zero-forcing method in multi-relay network with SWIPT. Different from the pure CJ method and the pure ZF method, the proposed algorithm achieves a controllable compromise between computational complexity and confidentiality rate by controlling the number of zero-forcing constraints. Finally, the simulation results prove the rationality of the algorithm. In the next research work, an adaptive threshold selection beamforming algorithm can be designed for the number of constrained eavesdroppers by analyzing different application scenarios.

References

[1] Zhang X Y , Shi H , Zhu X , et al. Active semi-supervised learning based on self-expressive correlation with generative adversarial networks [J]. *Neurocomputing*, 2019, 345: 103-113

[2] Krikidis I, Timotheou S, Nikolaou S, et al. Simultaneous wireless information and power transfer in modern communication systems [J]. *IEEE Communications Magazine*, 2014, 52(11):104-110

[3] Bi S, Ho C K, Zhang R. Wireless powered communication: opportunities and challenges[J]. *IEEE Communications Magazine*, 2014, 53(4):117-125

[4] Lu X, Wang P, Niyato D, et al. Wireless networks with RF energy harvesting: a contemporary survey[J]. *IEEE Communications Surveys & Tutorials*, 2015, 17(2):757-789

[5] Zhang R, Ho C K. MIMO Broadcasting for simultaneous wireless information and power transfer[J]. *IEEE Transactions on Wireless Communications*, 2013, 12(5):1989-2001

[6] Zhang X Y, Shi H, Li C, et al. Learning transferable self-attentive representations for action recognition in untrimmed videos with weak supervision[C]//Proceedings of the 33rd AAAI Conference on Artificial Intelligence, California, USA, 2019: 1-8

[7] Liu L, Zhang R, Chua K C. Secrecy wireless information and power transfer with MISO beamforming [J]. *IEEE Transactions on Signal Processing*, 2014, 62(7):1850-1863

[8] Qin D Y, Zhang Y, Ma J Y, et al. OvBNN authentication based on cooperative signature for wireless sensor networks[J]. *High Technology Letters*, 2018, 24(3):63-71

[9] Ng D W K, Lo E S, Schober R. Robust beamforming for secure communication in systems with wireless information and power transfer [J]. *IEEE Transactions on Wireless Communications*, 2014, 13(8):4599-4615

[10] Lin Z, Wang L, Cai Y M, et al. Impacts of feedback delay and estimation error on secrecy performance of MISO single eavesdropper cognitive radio networks [J]. *High Technology Letters*, 2018, 24(3):33-41

[11] Hoang T M, Duong T Q, Vo N S, et al. Physical layer security in cooperative energy harvesting networks with a friendly jammer[J]. *IEEE Wireless Communications Letters*, 2017, 6(2):174-177

[12] Xing H, Wong K K, Nallanathan A, et al. Wireless powered cooperative jamming for secrecy multi-AF relaying networks[J]. *IEEE Transactions on Wireless Communications*, 2015, 15(12):7971-7984

[13] Yang Y, Li Q, Ma W K, et al. Cooperative secure beamforming for AF relay networks with multiple eavesdroppers [J]. *IEEE Signal Processing Letters*, 2013, 20(1):35-38

[14] Goel S, Negi R. Guaranteeing secrecy using artificial noise[J]. *IEEE Transactions on Wireless Communications*, 2008, 7(6):2180-2189

[15] Alabbasi A, Rezki Z, Shihada B. Energy efficient resource allocation for cognitive radios: a generalized sensing analysis[J]. *IEEE Transactions on Wireless Communications*, 2015, 14(5):2455-2469

[16] Charnes A, Cooper W W. Programming with linear fractional functionals[J]. *Naval Research Logistics*, 2010, 9(3-4): 181-186

Wu Guodong, born in 1995. He is a M. E. candidate in the School of Computer and Information Engineering, Henan University, Kaifeng, P. R. China. His main research interests include the design of algorithms for beamforming, physical layer security and non-orthogonal multiple access.