# Increasing Secrecy Capacity via Joint Design of Cooperative Beamforming and Jamming

**Xinrong Guan[1], Yueming Cai[1, 2], Weiwei Yang[1], Yunpeng Cheng[1] and Junquan Hu[1]**
1 Department of Wireless Communications, PLA University of Science and Technology,
No.2 Biaoying, Yudao Street, 210007, Nanjing – China
[2]National Mobile Communications Research Laboratory, Southeast University,
Sipailou Road, 210096, Nanjing– China
[E-mail: {ywygxr, yww_1010, ypcheng}@yahoo.com, caiym@vip.sina.com]
*Corresponding author: Xinrong Guan

*Received September 24, 2011; revised December 14, 2011; revised February 13, 2012; accepted March 19, 2012; published April 25, 2012*

## Abstract

In this paper, we propose a hybrid cooperative scheme to improve the secrecy rate for a cooperative network in presence of multiple relays. Each relay node transmits the mixed signal consisting of weighted source signal and intentional noise. The problem of power allocation, the joint design of beamforming and jamming weights are investigated, and an iterative scheme is proposed. It is demonstrated by the numerical results that the proposed hybrid scheme further improves secrecy rate, as compared to traditional cooperative schemes.

***Keywords***: physical layer security, cooperative communication, cooperative beamforming, artificial jamming, joint design

A part of this paper appeared in IEEE PIMRC 2011, September 11-14, Toronto, Canada. In this version, we further investigate how to implement the joint design scheme in both DF and AF protocols and present more numerical results. This work was supported by the National Natural Science Foundation of China under Grant 60972051 and 61001107, the Important National Science & Technology Specific Project under Grant 2010ZX03006-002-04.

**http://dx.doi.org/10.3837/tiis.2012.04.005**

## 1. Introduction

Due to the broadcast nature of the wireless medium, all users within the coverage area of a transmission can overhear the source message. As an important issue in wireless networks, security is typically addressed at higher network layers. However, there have been considerable researches attempt at addressing security at the physical (PHY) layer, following the pioneering work of [1], in which Wyner showed that secure communication is possible without relying on secret keys if the eavesdropper's channel is a degraded version of the main channel. The feasibility of traditional PHY layer security approaches based on single antenna systems is hampered by channel conditions: if the source-destination channel is worse than the eavesdropper's channel, the secrecy rate is typically zero [2]. To overcome this limitation, some related works are proposed by taking advantages of multiple antenna systems, such as multiple-input multiple-output (MIMO), single-input multiple-output (SIMO) and multiple-input single-output (MISO) systems [3][4][5][6][7][8][9]. Unfortunately, due to size limitations and cost, it is impractical to equip multiple antennas at communication nodes for many applications. Therefore, user cooperation is considered as an effective approach to improve PHY layer security. Cooperative schemes proposed by recent works can usually be categorized into two fashions, cooperative beamforming and cooperative jamming.

**Cooperative beamforming:** This is a two-stage scheme. In the first one, the source broadcasts message, thus the relays, the destination, and the eavesdropper receive it. In the second one, the relays multiplex the source message with the designed beam weights and forward it, which is under constraints of PHY layer security. In [10], a relay beamforming system based on decode-and-forward (DF) is designed for secrecy capacity maximization or transmitting power minimization. In [11], suboptimal closed-form solutions that optimize bounds on secrecy capacity are proposed for amplify-and-forward (AF). However, these studies are conducted only under total relay power constraints. DF and AF beamforming under both total and individual power constraints are studied in [12] and [13] respectively. It is shown that the design under total power constraints leads to a generalized eigenvalue problem and a closed-form solution is available. Under individual power constraints, the relay beamforming is usually formulated as an optimization problem and solved by using approach such as semidefinite programming or second-order cone programming [12]. Anyway, all above mentioned researches don't take the presence of multiple eavesdroppers into account, which makes it more difficult to obtain the optimal relay weights. Assuming that the number of relays is greater than the number of eavesdroppers, some criterions for suboptimal weight design is considered in [14], for example, by nulling the forwarded signal at the eavesdroppers.

**Cooperative jamming:** This scheme usually exploits intended noise to degrade the eavesdropper's channel so that secret communication can be guaranteed. It is first pointed out in [15] that introducing artificial noise in transmission along with source signal can enlarge secrecy rate region as the artificial noise causes additional interference to the eavesdropper. In [16], the authors derive the optimal power control and artificial noise parameter for cooperative secret communication in a symmetric interference channel. In [17], the PHY layer security for two-way relay channel with friendly jammers is studied. In such a two-way relay channel, source-destination information exchange deeply relies on the relay node, which may be not reliable and overhear the message. Therefore, friendly jammers are used to interfere with the malicious relay. In [18], the authors consider a communication

aided by a relay equipped with multiple antennas, which transmits a jamming signal to the eavesdropper while the source broadcast the message signal. Weights assignment of antenna elements and power allocation of source and relay are investigated. Besides, cooperative jamming in the presence of multiple eavesdroppers is also studied in [14].

Now that both beamforming and friendly jamming can improve the secrecy capacity, the joint design of them may be a more effective approach. Inspired by this, we propose a novel hybrid cooperative scheme, in which the relay transmits not only source signal but also intended noise, i.e. they are mixed into a hybrid signal and transmitted together. Via beamforming weights design, the receive SNR at the destination is increased. Meanwhile, the receive SNR at the eavesdropper is decreased by the jamming signal. As a result, the rate at the destination is increased while the rate at the eavesdropper is decreased, i.e. the achievable secrecy capacity is further enlarged. Moreover, the proposed scheme is a generalized one, and the traditional cooperative beamforming can be regarded as a special case of our proposed hybrid scheme.

In this paper, we investigate the hybrid scheme design issue for DF and AF model respectively, aiming at maximizing the achievable secrecy rate under total relay power constraint. In our analysis, the weights design is formulated as a generalized eigenvector problem. And the optimal power allocation is modeled as an extreme value problem for a single variable function. However, since these two problems are correlated with each other, it is difficult to obtain the closed-form solution. We present an iterative algorithm to solve this problem, of which the advantage is verified by the numerical results.

The rest of the work is organized as follows. Section 2 presents the system model and some backgrounds of our work. Section 3 and section 4 deals with the joint design problem for DF and AF, respectively. Section 5 depicts the numerical results, and the last section concludes the paper.

## 2. System Model and Problem Formulation

We consider a wireless communication model consisting of one source node, $N$ relay nodes, one destination node, and one eavesdropper, as depicted in **Fig. 1**.

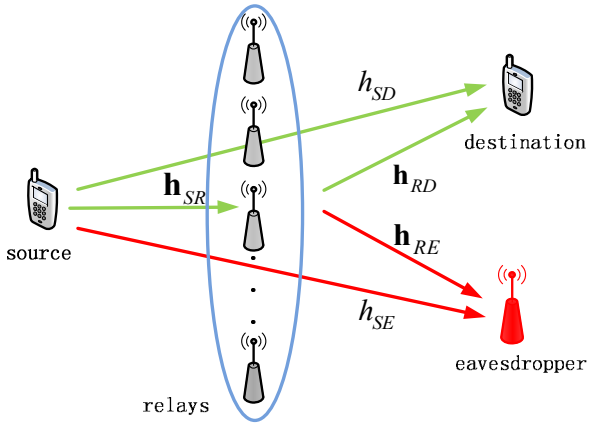



**Fig. 1.** Communication model.

All channels are assumed to undergo flat fading, remain constant over one frame and change independently from one frame to another. The channel gain contains the path loss and the Rayleigh fading coefficient, i.e. $h_{ab} = d_{ab}^{-c/2} e^{j\theta}$, where $d_{ab}$ is the distance between the nodes $a$ and $b$, $c$ is the path loss exponent and $\theta$ is a random phase. The noise at any node is assumed to be white complex Gaussian with zero mean and variance $\sigma^2$, i.e. $CN(0,\sigma^2)$. We denote the complex channel gain between the source and the destination by $h_{SD}$, the channel between the source and the eavesdropper by $h_{SE}$, the channel vector ($N \times 1$) between the source and the $N$ relays by $\mathbf{h}_{SR}$, the channel vector ($N \times 1$) between the N relays and the destination by $\mathbf{h}_{RD}$, and the channel vector ($N \times 1$) between the N relays and the eavesdropper by $\mathbf{h}_{RE}$. We assume the global channel statement information (CSI) is available and even the eavesdropper's channels are known, which is a common assumption in the PHY security literature. This assumption is feasible and reasonable for some applications. For example, in cellular systems some MUs may have certain demands to the physical layer security. Therefore, other MUs should be taken as potential eavesdroppers when base station serves such users. Thanks to the channel estimation, the BS can access all the channel states, including that of the potential eavesdropper's link. Besides, as described in [19], information on the eavesdropper's channels can be estimated when it is active in the network and its transmissions can be monitored. We denote by $\boldsymbol{\alpha}$ the normalized beamforming weights vector ($N \times 1$), by $\boldsymbol{\beta}$ the normalized jamming weights vector ($N \times 1$), by $\|\cdot\|$ the 2-norm of a vector, and by $\mathbf{I_N}$ the identity matrix of size $N \times N$. Conjugate, transpose, and conjugate transpose are represented by $(\cdot)^*$, $(\cdot)^T$, and $(\cdot)^H$. And $diag(\mathbf{a})$ denotes a diagonal matrix with the elements of the vector $\mathbf{a}$.

As we know, the PHY layer secrecy rate can be defined as follows

$$\begin{aligned} R_s &= \max\{\log(1+\frac{P_D}{N_D}) - \log(1+\frac{P_E}{N_E}),\ 0\} \\ &= \max\{\log(\underbrace{\frac{N_E}{N_D}}_{w_1}\underbrace{\frac{N_D+P_D}{N_E+P_E}}_{w_2}),\ 0\} \end{aligned} \tag{1}$$

in which $P_D$ and $P_E$ is the power of the received signal at the destination and the eavesdropper, respectively, $N_D$ is the power of complex noise at the destination, and $N_E$ is the power of complex noise at the eavesdropper. Obviously, there are two different means to improve $R_s$, i.e. by increasing $w_1$ and increasing $w_2$. Actually, beamforming scheme benefits from an increase in $w_2$ while cooperative jamming benefits from an increase in $w_1$. Inspired by this, we propose a joint design of beamforming and jamming, in which $w_1$ and $w_2$ can be increased simultaneously. In this model, the relays no longer transmit only source signal or only artificial noise, but transmit a hybrid signal consisting of them.

Therefore, our work is different from the aforementioned researches in two aspects: 1) The proposed scheme is a generalized one and can easily be reduced to traditional beamforming scheme, like that presented in [14]. 2) The corresponding iterative solution for the hybrid scheme design is presented, which can further improve the secrecy rate, as compared to traditional cooperative schemes.

During the following discussion, the hybrid scheme design problems with and without direct links in DF and AF models are investigated in detail. Meanwhile, the traditional beamforming and jamming are also presented to make a comparison between these different

cooperative schemes. For notational convenience, we assume all relays decode correctly in DF case[1].

## 3. Decode-and-Forward

### 3.1 Existing Direct Links

#### 3.1.1 Hybrid Scheme

In the first time slot, the source broadcasts a symbol $x$ to the destination and the relays with transmitting power of $P_0$. During the second slot, all relays decode the source symbol and retransmit it, with mixing an intended interference signal $n_J$. We denote by $P_S$ the total power allocated for beamforming, and by $P_J$ the total power allocate for jamming. Of course, we have $P_S + P_J = P_R$ as a total transmitting power constraint for all of the relays. Therefore, the received signals at the destination in these two slots are

$$\begin{aligned} y_d^{(1)} &= h_{SD}\sqrt{P_0}x + n_D \\ y_d^{(2)} &= \mathbf{h}_{RD}^{\ T}(\boldsymbol{\alpha}\sqrt{P_S}x + \boldsymbol{\beta}\sqrt{P_J}n_J) + n_D \end{aligned} \tag{2}$$

We consider the relays use the same codewords as the source. With the maximal ratio combining (MRC) at the destination node, the rate can be written as

$$\begin{aligned} R_{dDF} &= \frac{1}{2}\log(1 + P_0\gamma_{SD} + \frac{P_S\,|\,\mathbf{h}_{RD}^{\ T}\boldsymbol{\alpha}\,|^2}{P_J\,|\,\mathbf{h}_{RD}^{\ T}\boldsymbol{\beta}\,|^2 + \sigma^2}) \\ &= \frac{1}{2}\log\frac{\boldsymbol{\beta}^H\mathbf{B}\boldsymbol{\beta} + \boldsymbol{\alpha}^H\mathbf{H}_{RD}\boldsymbol{\alpha}}{\boldsymbol{\beta}^H\mathbf{A}\boldsymbol{\beta}} \end{aligned} \tag{3}$$

in which $\gamma_{SD} = |\,h_{SD}\,|^2/\sigma^2$, $\mathbf{A} = P_J\mathbf{h}_{RD}^{\ *}\mathbf{h}_{RD}^{\ T} + \sigma^2\mathbf{I}_N$, $\mathbf{B} = (1 + P_0\gamma_{SD})\mathbf{A}$, and $\mathbf{H}_{RD} = (P_R - P_J)\mathbf{h}_{RD}^{\ *}\mathbf{h}_{RD}^{\ T}$.

At the eavesdropper, the received signals in these two slots are respectively obtained as

$$\begin{aligned} y_e^{(1)} &= h_{SE}\sqrt{P_0}x + n_E \\ y_e^{(2)} &= \mathbf{h}_{RE}^{\ T}(\boldsymbol{\alpha}\sqrt{P_S}x + \boldsymbol{\beta}\sqrt{P_J}n_J) + n_E \end{aligned} \tag{4}$$

Consequently, the corresponding rate is

$$\begin{aligned} R_{eDF} &= \frac{1}{2}\log(1 + P_0\gamma_{SE} + \frac{P_S\,|\,\mathbf{h}_{RE}^{\ T}\boldsymbol{\alpha}\,|^2}{P_J\,|\,\mathbf{h}_{RE}^{\ T}\boldsymbol{\beta}\,|^2 + \sigma^2}) \\ &= \frac{1}{2}\log\frac{\boldsymbol{\beta}^H\mathbf{B}'\boldsymbol{\beta} + \boldsymbol{\alpha}^H\mathbf{H}_{RE}\boldsymbol{\alpha}}{\boldsymbol{\beta}^H\mathbf{A}'\boldsymbol{\beta}} \end{aligned} \tag{5}$$

in which $\gamma_{SE} = |\,h_{SE}\,|^2/\sigma^2$, $\mathbf{A}' = P_J\mathbf{h}_{RE}^{\ *}\mathbf{h}_{RE}^{\ T} + \sigma^2\mathbf{I}_N$, $\mathbf{B}' = (1 + P_0\gamma_{SE})\mathbf{A}'$, and $\mathbf{H}_{RE} = (P_R - P_J)\mathbf{h}_{RE}^{\ *}\mathbf{h}_{RE}^{\ T}$. From (3) and (5), the achievable secrecy rate can be written as

$$\begin{aligned} R_{sDF}(P_J, \boldsymbol{\alpha}, \boldsymbol{\beta}) &= \frac{1}{2}\log[\frac{P_J\,|\,\mathbf{h}_{RE}^{\ T}\boldsymbol{\beta}\,|^2 + \sigma^2}{P_J\,|\,\mathbf{h}_{RD}^{\ T}\boldsymbol{\beta}\,|^2 + \sigma^2}\frac{(1+P_0\gamma_{SD})(P_J\,|\,\mathbf{h}_{RD}^{\ T}\boldsymbol{\beta}\,|^2 + \sigma^2) + P_S\,|\,\mathbf{h}_{RD}^{\ T}\boldsymbol{\alpha}\,|^2}{(1+P_0\gamma_{SE})(P_J\,|\,\mathbf{h}_{RE}^{\ T}\boldsymbol{\beta}\,|^2 + \sigma^2) + P_S\,|\,\mathbf{h}_{RE}^{\ T}\boldsymbol{\alpha}\,|^2}] \\ &= \frac{1}{2}\log(\frac{\boldsymbol{\beta}^H\mathbf{A}'\boldsymbol{\beta}}{\boldsymbol{\beta}^H\mathbf{A}\boldsymbol{\beta}}\frac{\boldsymbol{\beta}^H\mathbf{B}\boldsymbol{\beta} + \boldsymbol{\alpha}^H\mathbf{H}_{RD}\boldsymbol{\alpha}}{\boldsymbol{\beta}^H\mathbf{B}'\boldsymbol{\beta} + \boldsymbol{\alpha}^H\mathbf{H}_{RE}\boldsymbol{\alpha}}) \end{aligned} \tag{6}$$

[1] This assumption is feasible in some applications, e.g. when the distance between the relay stations and the source is short. And even if not all relays decode the information message correctly, we can perform the same scheme in the same way, by using the correctly decoding relays only. And other researchers make this assumption as well in the references [9] [11][12][13].

As a result, the problem of maximizing the achievable secrecy rate can be formulated as

$$\arg\max_{P_J,\boldsymbol{\alpha},\boldsymbol{\beta}} \underbrace{\frac{\boldsymbol{\beta}^H\mathbf{A}'\boldsymbol{\beta}}{\boldsymbol{\beta}^H\mathbf{A}\boldsymbol{\beta}}}_{W_1}\underbrace{\frac{\boldsymbol{\alpha}^H\mathbf{C}\boldsymbol{\alpha}}{\boldsymbol{\alpha}^H\mathbf{C}'\boldsymbol{\alpha}}}_{W_2} \quad s.t. \quad \begin{cases} P_S \in (0, P_R] \\ P_J \in [0, P_R) \\ P_S + P_J = P_R \end{cases} \tag{7}$$

in which $\mathbf{C} = \boldsymbol{\beta}^H\mathbf{B}\boldsymbol{\beta}\mathbf{I}_N + \mathbf{H}_{RD}$, $\mathbf{C}' = \boldsymbol{\beta}^H\mathbf{B}'\boldsymbol{\beta}\mathbf{I}_N + \mathbf{H}_{RE}$. Notice the constraint $P_J \in [0, P_R)$, i.e. full power using for jamming would not be adopted. The maximum value of $W_1$ corresponds to the maximal eigenvalue of matrix $\mathbf{A}^{-1}\mathbf{A}'$, and the corresponding unit-norm eigenvector is the optimal $\boldsymbol{\beta}$. Similarly, the maximum value of $W_2$ corresponds to the maximal eigenvalue of matrix $(\mathbf{C}')^{-1}\mathbf{C}$, and the corresponding unit-norm eigenvector is the optimal $\boldsymbol{\alpha}$. Unfortunately, this weights design problem is still a difficult one because these two generalized eigenvector problems are correlated. Furthermore, excepting optimizing the beamforming and jamming weights to maximize the secrecy rate, the optimal power allocation problem needs being solved as well. Therefore, we derive a suboptimal weights design scheme later.

On one hand, for a given $P_J$, the optimal jamming weights vector $\boldsymbol{\beta}$ can be obtained as

$$\boldsymbol{\beta}_{opt} = \max eig_{unit}(\mathbf{A}^{-1}\mathbf{A}') \tag{8}$$

in which $\max eig_{unit}(\cdot)$ means the unit-norm eigenvector of a matrix that corresponds to its maximum eigenvalue. Substitute $\boldsymbol{\beta}_{opt}$ into $\mathbf{C}$ and $\mathbf{C}'$, then the optimal beamforming weights vector $\boldsymbol{\alpha}$ can be derived as following

$$\boldsymbol{\alpha}_{opt} = \max eig_{unit}[(\mathbf{C}')^{-1}\mathbf{C}] \tag{9}$$

As $P_J$, $\boldsymbol{\alpha}$ and $\boldsymbol{\beta}$ are all obtained, the achievable secrecy rate can be calculated as

$$R_{sDF}(P_J, \boldsymbol{\alpha}, \boldsymbol{\beta}) = \frac{1}{2}\log\left(\frac{\boldsymbol{\beta}_{opt}{}^H\mathbf{A}'\boldsymbol{\beta}_{opt}}{\boldsymbol{\beta}_{opt}{}^H\mathbf{A}\boldsymbol{\beta}_{opt}}\frac{\boldsymbol{\alpha}_{opt}{}^H\mathbf{C}\boldsymbol{\alpha}_{opt}}{\boldsymbol{\alpha}_{opt}{}^H\mathbf{C}'\boldsymbol{\alpha}_{opt}}\right) \tag{10}$$

On the other hand, if $\boldsymbol{\alpha}$ and $\boldsymbol{\beta}$ are given, the achievable secrecy rate in (6) can be rewritten as a function of the single variable $P_J$, i.e.

$$\begin{aligned} R_{sDF}(P_J) &= \frac{1}{2}\log\left(\frac{a_1P_J^2 + b_1P_J + c_1}{a_2P_J^2 + b_2P_J + c_2}\right) \\ &= \frac{1}{2}\log\left[\frac{a_1}{a_2} + \frac{(b_1 - a_1b_2/a_2)P_J + (c_1 - a_1c_2/a_2)}{a_2P_J^2 + b_2P_J + c_2}\right] \end{aligned} \tag{11}$$

where

$$\begin{cases} a_1 = [(1+P_0\gamma_{SD})|\mathbf{h}_{RD}{}^T\boldsymbol{\beta}|^2 - |\mathbf{h}_{RD}{}^T\boldsymbol{\alpha}|^2]|\mathbf{h}_{RE}{}^T\boldsymbol{\beta}|^2 \\ b_1 = [(1+P_0\gamma_{SD})|\mathbf{h}_{RD}{}^T\boldsymbol{\beta}|^2 - |\mathbf{h}_{RD}{}^T\boldsymbol{\alpha}|^2]\sigma^2 + |\mathbf{h}_{RE}{}^T\boldsymbol{\beta}|^2[P_R|\mathbf{h}_{RD}{}^T\boldsymbol{\alpha}|^2 + (1+P_0\gamma_{SD})\sigma^2] \\ c_1 = [P_R|\mathbf{h}_{RD}{}^T\boldsymbol{\alpha}|^2 + (1+P_0\gamma_{SD})\sigma^2]\sigma^2 \end{cases}$$
$$\begin{cases} a_2 = [(1+P_0\gamma_{SE})|\mathbf{h}_{RE}{}^T\boldsymbol{\beta}|^2 - |\mathbf{h}_{RE}{}^T\boldsymbol{\alpha}|^2]|\mathbf{h}_{RD}{}^T\boldsymbol{\beta}|^2 \\ b_2 = [(1+P_0\gamma_{SE})|\mathbf{h}_{RE}{}^T\boldsymbol{\beta}|^2 - |\mathbf{h}_{RE}{}^T\boldsymbol{\alpha}|^2]\sigma^2 + |\mathbf{h}_{RD}{}^T\boldsymbol{\beta}|^2[P_R|\mathbf{h}_{RE}{}^T\boldsymbol{\alpha}|^2 + (1+P_0\gamma_{SE})\sigma^2] \\ c_2 = [P_R|\mathbf{h}_{RE}{}^T\boldsymbol{\alpha}|^2 + (1+P_0\gamma_{SE})\sigma^2]\sigma^2 \end{cases} \tag{12}$$

Taking the derivative and setting it to zero, the optimal value of $P_J$ is the solution within $[0, P_R]$ of the following quadratic equation

$$(a_2b_1 - a_1b_2)P_J^{\,2} + 2(a_2c_1 - a_1c_2)P_J + (b_2c_1 - b_1c_2) = 0 \tag{13}$$

If no solution exists within $[0, P_R)$, it holds that $P_J = 0$, which corresponds to traditional beamforming.

It is generally difficult to obtain a closed-form solution for the optimal $P_J$, $\boldsymbol{\alpha}$ and $\boldsymbol{\beta}$. In the following part, we use an iterative algorithm to reach the solution of $P_J$, $\boldsymbol{\alpha}$ and $\boldsymbol{\beta}$. The proposed iterative algorithm is summarized as follows.

**Table 1.** Iterative algorithm for DF protocol

| | |
|---|---|
| **a)** | **Initialization:** $i = 0$, $P_J^{(0)} = 0$, and $P_S^{(0)} = P_R - P_J^{(0)}$. |
| **b)** | **Iterative Update Process** |
| i. | $\mathbf{A} \leftarrow P_J^{(i)}$, $\mathbf{A}' \leftarrow P_J^{(i)}$, solve (8) and (9) for $\boldsymbol{\beta}^{(i)}$ and $\boldsymbol{\alpha}^{(i)}$. |
| ii. | Solve (6) for $R_{sDF}^{(i)}$ by using $P_S^{(i)}$, $P_J^{(i)}$, $\boldsymbol{\beta}^{(i)}$ and $\boldsymbol{\alpha}^{(i)}$. |
| iii. | (12) $\leftarrow \boldsymbol{\alpha}^{(i)}, \boldsymbol{\beta}^{(i)}$, solve (13) for $P_J^{(i+1)}$ |
| iv. | Repeat step i and ii, until $R_{sDF}^{(i)}$ cannot be improved. |

From analysis above presented, it is easy to observe that the optimal value of $P_J$ is not a constant, but a function of channel gains, i.e. $\gamma_{SD}$, $\gamma_{RD}$, $\gamma_{SE}$ and $\gamma_{RE}$. This implies that $P_J = 0$, which is a constant, is not the optimal solution, and the secrecy rate in our proposed hybrid scheme is larger than that in pure beamforming scheme.

### 3.1.2 Beamforming Scheme

In this part, we present the special case of the proposed hybrid scheme, in which we set the jamming weights to zero. Substituting $P_J = 0$ into (2), then the **received** signals at the destination would be

$$\begin{aligned} y_d^{(1)} &= h_{SD}\sqrt{P_0}\,x + n_D \\ y_d^{(2)} &= \mathbf{h}_{RD}^{\,T}\boldsymbol{\alpha}\sqrt{P_R}\,x + n_D \end{aligned} \tag{14}$$

Accordingly, the rate at the destination is

$$R_{dDF} = \frac{1}{2}\log\left(1 + P_0\gamma_{SD} + \frac{P_R\,|\,\mathbf{h}_{RD}^{\,T}\boldsymbol{\alpha}\,|^2}{\sigma^2}\right) \tag{15}$$

where $\gamma_{SD} = |\,h_{SD}\,|^2/\sigma^2$. Respectively, the received signals at the eavesdropper is

$$\begin{aligned} y_e^{(1)} &= h_{SE}\sqrt{P_0}\,x + n_E \\ y_e^{(2)} &= \mathbf{h}_{RE}^{\,T}\boldsymbol{\alpha}\sqrt{P_R}\,x + n_E \end{aligned} \tag{16}$$

Consequently, the rate at the eavesdropper is

$$R_{eDF} = \frac{1}{2}\log\left(1 + P_0\gamma_{SE} + \frac{P_R\,|\,\mathbf{h}_{RE}^{\,T}\boldsymbol{\alpha}\,|^2}{\sigma^2}\right) \tag{17}$$

where $\gamma_{SE} = |\,h_{SE}\,|^2/\sigma^2$. As a result, the achievable secrecy rate is

$$R_{SDF} = \frac{1}{2}\log[\frac{(1+P_0\gamma_{SD})\sigma^2 + P_R|\mathbf{h}_{RD}{}^T\boldsymbol{\alpha}|^2}{(1+P_0\gamma_{SE})\sigma^2 + P_R|\mathbf{h}_{RE}{}^T\boldsymbol{\alpha}|^2}] = \frac{1}{2}\log\frac{\boldsymbol{\alpha}^H\mathbf{H}_{RD}'\boldsymbol{\alpha}}{\boldsymbol{\alpha}^H\mathbf{H}_{RE}'\boldsymbol{\alpha}} \tag{18}$$

where $\mathbf{H}_{RE}' = (1+P_0\gamma_{SE})\sigma^2\mathbf{I}_N + P_R\mathbf{h}_{RE}^*\mathbf{h}_{RE}{}^T$, $\mathbf{H}_{RD}' = (1+P_0\gamma_{SD})\sigma^2\mathbf{I}_N + P_R\mathbf{h}_{RD}^*\mathbf{h}_{RD}{}^T$. The problem of maximizing secrecy rate can be formulated as

$$\arg\max_{\boldsymbol{\alpha}} \frac{\boldsymbol{\alpha}^H\mathbf{H}_{RD}'\boldsymbol{\alpha}}{\boldsymbol{\alpha}^H\mathbf{H}_{RE}'\boldsymbol{\alpha}} \tag{19}$$

The maximal value of (19) corresponds to the maximal eigenvalue of the matrix $\mathbf{H}_{RE}'^{(-1)}\mathbf{H}_{RD}'$. This result is as the same as that of the DF beamforming scheme presented in [14].

As aforementioned, beamforming scheme with $P_J = 0$, not the optimal value of $P_J$, is a special case of the hybrid scheme. In another word, it only increases the $w_2$ part in (1). Therefore, it must holds that the secrecy rate achieved in traditional beamforming could not be higher than that achieved in the proposed hybrid scheme.

### 3.1.3 Jamming Scheme

Now we discuss the traditional jamming scheme. While the source transmits, the relays send a weighted jamming signal to confound the eavesdropper.

The received signal at the destination is

$$y_d = h_{SD}\sqrt{P_0}x + \mathbf{h}_{RD}{}^T\boldsymbol{\beta}\sqrt{P_R}n_J + n_D \tag{20}$$

and the received signal at the eavesdropper equals to

$$y_e = h_{SE}\sqrt{P_0}x + \mathbf{h}_{RE}\boldsymbol{\beta}\sqrt{P_R}n_J + n_E \tag{21}$$

From (20) and (21), the rate at the destination and the eavesdropper is

$$R_{dDF} = \log(1+\frac{P_0|h_{SD}|^2}{P_R|\mathbf{h}_{RD}{}^T\boldsymbol{\beta}|^2+\sigma^2}) \qquad R_{eDF} = \log(1+\frac{P_0|h_{SE}|^2}{P_R|\mathbf{h}_{RE}{}^T\boldsymbol{\beta}|^2+\sigma^2}) \tag{22}$$

As a result, the achievable secrecy rate is given by

$$R_{sDF} = \log(\frac{P_R|\mathbf{h}_{RE}{}^T\boldsymbol{\beta}|^2+\sigma^2}{P_R|\mathbf{h}_{RD}{}^T\boldsymbol{\beta}|^2+\sigma^2}\frac{P_0|h_{SD}|^2+P_R|\mathbf{h}_{RD}{}^T\boldsymbol{\beta}|^2+\sigma^2}{P_0|h_{SE}|^2+P_R|\mathbf{h}_{RE}{}^T\boldsymbol{\beta}|^2+\sigma^2}) \tag{23}$$

which is a product of two correlated generalized eigenvector problems and is quite difficult to obtain the optimal solution. The authors in [14] proposed a suboptimal scheme, in which the jamming signal at the destination is nulled out, i.e. $\mathbf{h}_{RD}{}^T\boldsymbol{\beta} = 0$. Then the secrecy rate maximization problem was formulated as

$$\begin{aligned} &\arg\max_{\boldsymbol{\beta}} |\mathbf{h}_{RE}{}^{T}\boldsymbol{\beta}|^2 \\ &s.t. \; |\mathbf{h}_{RD}{}^{T}\boldsymbol{\beta}| = 0 \end{aligned} \tag{24}$$

Finally the achievable secrecy rate is calculated as

$$R_{sDF} = \log(\underbrace{\frac{P_R|\mathbf{h}_{RE}{}^{T}\boldsymbol{\beta}|^2+\sigma^2}{\sigma^2}}_{w_1}\underbrace{\frac{P_0|h_{SD}|^2+\sigma^2}{P_0|h_{SE}|^2+P_R|\mathbf{h}_{RE}{}^{T}\boldsymbol{\beta}|^2+\sigma^2}}_{w_2}) \tag{25}$$

Obviously, jamming increase $w_1$ part, but $w_2$ part is even decrease as compared to direct transmission. Intuitively, this is not an optimal scheme to improve secrecy rate. And when $\mathbf{h}_{RE} \to 0$, e.g. eavesdropper is far from the destination, the secrecy rate obtained by jamming equals to that in direct transmission, which means power is wasted. However, notice the secrecy rate at (6), for $w_1$ part, we obtained the maximal value that it can reach, which is of course larger than that obtained by (25). Meanwhile, for $w_2$ part we also derive the maximal value that it can reach. Therefore the secrecy performance in our proposed scheme outperforms that in jamming. And the above mentioned conclusions will be verified in our latter presented numerical results.

## 3.2 No Direct Links

### 3.2.1 Hybrid Scheme

If there is no direct link between the source and the destination, as well as between the source and the eavesdropper, the cooperative scheme design would be an interesting topic. Since the destination can not receive the source signal directly, the traditional jamming scheme does not work. The relays must use part of the power to forward the source signal; of course it reduces to traditional beamforming while the total is used for forwarding. We aim to derive the optimal power allocation and corresponding weight vector design. The received signal at the destination and the eavesdropper is written as

$$\begin{aligned} y_d &= \mathbf{h}_{RD}{}^{T}(\boldsymbol{\alpha}\sqrt{P_S}x + \boldsymbol{\beta}\sqrt{P_J}n_J) + n_D \\ y_e &= \mathbf{h}_{RE}{}^{T}(\boldsymbol{\alpha}\sqrt{P_S}x + \boldsymbol{\beta}\sqrt{P_J}n_J) + n_E \end{aligned} \tag{26}$$

Accordingly, the rate can be obtained respectively as

$$\begin{aligned} R_{dDF} &= \frac{1}{2}\log(1+\frac{P_S|\mathbf{h}_{RD}{}^{T}\boldsymbol{\alpha}|^2}{P_J|\mathbf{h}_{RD}{}^{T}\boldsymbol{\beta}|^2+\sigma^2}) = \frac{1}{2}\log\frac{\boldsymbol{\beta}^H\mathbf{A}\boldsymbol{\beta}+\boldsymbol{\alpha}^H\mathbf{H}_{RD}\boldsymbol{\alpha}}{\boldsymbol{\beta}^H\mathbf{A}\boldsymbol{\beta}} \\ R_{eDF} &= \frac{1}{2}\log(1+\frac{P_S|\mathbf{h}_{RE}{}^{T}\boldsymbol{\alpha}|^2}{P_J|\mathbf{h}_{RE}{}^{T}\boldsymbol{\beta}|^2+\sigma^2}) = \frac{1}{2}\log\frac{\boldsymbol{\beta}^H\mathbf{A}'\boldsymbol{\beta}+\boldsymbol{\alpha}^H\mathbf{H}_{RE}\boldsymbol{\alpha}}{\boldsymbol{\beta}^H\mathbf{A}'\boldsymbol{\beta}} \end{aligned} \tag{27}$$

in which $\mathbf{A} = P_J\mathbf{h}_{RD}{}^{*}\mathbf{h}_{RD}{}^{T} + \sigma^2\mathbf{I}_N$, $\mathbf{H}_{RD} = (P_R - P_J)\mathbf{h}_{RD}{}^{*}\mathbf{h}_{RD}{}^{T}$, $\mathbf{A}' = P_J\mathbf{h}_{RE}{}^{*}\mathbf{h}_{RE}{}^{T} + \sigma^2\mathbf{I}_N$, and $\mathbf{H}_{RE} = (P_R - P_J)\mathbf{h}_{RE}{}^{*}\mathbf{h}_{RE}{}^{T}$. The secrecy rate to be maximized is

$$R_{sDF}(P_J, \boldsymbol{\alpha}, \boldsymbol{\beta}) = \frac{1}{2}\log(\frac{\boldsymbol{\beta}^H\mathbf{A}'\boldsymbol{\beta}}{\boldsymbol{\beta}^H\mathbf{A}\boldsymbol{\beta}}\frac{\boldsymbol{\beta}^H\mathbf{A}\boldsymbol{\beta}+\boldsymbol{\alpha}^H\mathbf{H}_{RD}\boldsymbol{\alpha}}{\boldsymbol{\beta}^H\mathbf{A}'\boldsymbol{\beta}+\boldsymbol{\alpha}^H\mathbf{H}_{RE}\boldsymbol{\alpha}}) \tag{28}$$

Consequently, the optimization problem of maximum achievable secrecy rate can be formulated as

$$\arg\max_{P_J,\boldsymbol{\alpha},\boldsymbol{\beta}} \underbrace{\frac{\boldsymbol{\beta}^H \mathbf{A}'\boldsymbol{\beta}}{\boldsymbol{\beta}^H \mathbf{A}\boldsymbol{\beta}}}_{W_1} \underbrace{\frac{\boldsymbol{\alpha}^H \mathbf{C}\boldsymbol{\alpha}}{\boldsymbol{\alpha}^H \mathbf{C}'\boldsymbol{\alpha}}}_{W_2}$$
$$s.t. \quad \begin{cases} P_S \in (0, P_R] \\ P_J \in [0, P_R) \\ P_S + P_J = P_R \end{cases} \tag{29}$$

in which $\mathbf{C} = \boldsymbol{\beta}^H \mathbf{A}\boldsymbol{\beta} + \mathbf{H}_{RD}$, $\mathbf{C}' = \boldsymbol{\beta}^H \mathbf{A}'\boldsymbol{\beta} + \mathbf{H}_{RE}$. The algorithm in **Table 1** can be applied to solve the optimization problem in (29) as well.

#### 3.2.2 Beamforming Scheme

If we set the jamming weights vector to zero in the generalized hybrid cooperative scheme, we have the special case i.e. traditional beamforming. In this condition, the achievable secrecy rate is written as

$$\begin{aligned} R_{sDF} &= \frac{1}{2}\log\frac{\sigma^2 + P_R |\mathbf{h}_{RD}{}^T \boldsymbol{\alpha}|^2}{\sigma^2 + P_R |\mathbf{h}_{RE}{}^T \boldsymbol{\alpha}|^2} \\ &= \frac{1}{2}\log\frac{\boldsymbol{\alpha}^H \mathbf{H}_{RD}'\boldsymbol{\alpha}}{\boldsymbol{\alpha}^H \mathbf{H}_{RE}'\boldsymbol{\alpha}} \end{aligned} \tag{30}$$

where $\mathbf{H}_{RE}' = \sigma^2 \mathbf{I}_N + P_R \mathbf{h}_{RE}^* \mathbf{h}_{RE}^T$, and $\mathbf{H}_{RD}' = \sigma^2 \mathbf{I}_N + P_R \mathbf{h}_{RD}^* \mathbf{h}_{RD}^T$. And the corresponding maximal value of the secrecy rate in (30) is the maximal eigenvalue of the matrix $\mathbf{H}_{RE}'^{(-1)} \mathbf{H}_{RD}'$. As the same, the traditional beamforming scheme can be viewed as a special case of the generalized hybrid scheme. In another word, beamforming only increase the $w_2$ part in (1). As a result, the secrecy performance in beamforming can not outperform that in the hybrid cooperation.

Because no direct links exist, the traditional jamming scheme does not work in this condition.

## 4. Amplify-and-Forward

### 4.1 Existing Direct Links

#### 4.1.1 Hybrid Scheme

In AF model, all the relays receive different versions of the source signal but do not decode them. Since that, the received signals at the destination is

$$\begin{aligned} y_d^{(1)} &= h_{SD}\sqrt{P_0}x + n_D \\ y_d^{(2)} &= \mathbf{h}_{RD}{}^T \{\sqrt{P_S} diag(\mathbf{l})[diag(\mathbf{h}_{SR})x + diag(\mathbf{n}_R)]\boldsymbol{\alpha} + \boldsymbol{\beta}\sqrt{P_J} n_J\} + n_D \end{aligned} \tag{31}$$

in which $\mathbf{l} = [l_1, l_2, .., l_N]$ is a vector that consists of each relay's scaling factor, i.e. $l_i = 1/\sqrt{|h_{SRi}|^2 P_0 + \sigma^2}$, $n_J$ is the intended noise, $\mathbf{n}_R = [n_{R1}, n_{R2}, ...n_{RN}]$ is a vector consisting of complex noise at each relay, and $n_D$ is noise at the destination. For simplification, we denote that $\mathbf{h}_{SRD}{}^T = \mathbf{h}_{RD}{}^T diag(\mathbf{l}) diag(\mathbf{h}_{SR})$, $\mathbf{n}_{RD}{}^T = \mathbf{h}_{RD}{}^T diag(\mathbf{n}_R)$. As a result, the rate at the destination is

$$\begin{aligned} R_{dAF} &= \frac{1}{2}\log(1+P_0\gamma_{SD}+\frac{P_S\,|\,\mathbf{h}_{SRD}{}^T\boldsymbol{\alpha}\,|^2}{P_S\,|\,\mathbf{n}_{RD}{}^T\boldsymbol{\alpha}\,|^2+P_J\,|\,\mathbf{h}_{RD}{}^T\boldsymbol{\beta}\,|^2+\sigma^2}) \\ &= \frac{1}{2}\log\frac{\boldsymbol{\alpha}^H\mathbf{H}_1'\boldsymbol{\alpha}+\boldsymbol{\beta}^H\mathbf{H}_2'\boldsymbol{\beta}}{\boldsymbol{\alpha}^H\mathbf{H}_1\boldsymbol{\alpha}+\boldsymbol{\beta}^H\mathbf{H}_2\boldsymbol{\beta}} \end{aligned} \tag{32}$$

where $\mathbf{H}_1 = P_S\mathbf{n}_{RD}{}^*\mathbf{n}_{RD}{}^T+\sigma^2\mathbf{I}_N$, $\mathbf{H}_1' = (1+P_0\gamma_{SD})\mathbf{H}_1+P_S\mathbf{h}_{SRD}{}^*\mathbf{h}_{SRD}{}^T$, $\mathbf{H}_2 = P_J\mathbf{h}_{RD}{}^*\mathbf{h}_{RD}{}^T$, and $\mathbf{H}_2' = (1+P_0\gamma_{SD})\mathbf{H}_2$. At the eavesdropper, the received signals in these two slots are respectively written as

$$\begin{aligned} y_e^{(1)} &= h_{SE}\sqrt{P_0}x+n_D \\ y_e^{(2)} &= \mathbf{h}_{RE}{}^T\{\sqrt{P_S}\,diag(\mathbf{l})[diag(\mathbf{h}_{SR})x+diag(\mathbf{n}_R)]\boldsymbol{\alpha}+\boldsymbol{\beta}\sqrt{P_J}n_J\}+n_E \end{aligned} \tag{33}$$

Accordingly, the rate at the eavesdropper is

$$\begin{aligned} R_{eAF} &= \frac{1}{2}\log(1+P_0\gamma_{SE}+\frac{P_S\,|\,\mathbf{h}_{SRE}{}^T\boldsymbol{\alpha}\,|^2}{P_S\,|\,\mathbf{n}_{RE}{}^T\boldsymbol{\alpha}\,|^2+P_J\,|\,\mathbf{h}_{RE}{}^T\boldsymbol{\beta}\,|^2+\sigma^2}) \\ &= \frac{1}{2}\log\frac{\boldsymbol{\alpha}^H\mathbf{H}_3'\boldsymbol{\alpha}+\boldsymbol{\beta}^H\mathbf{H}_4'\boldsymbol{\beta}}{\boldsymbol{\alpha}^H\mathbf{H}_3\boldsymbol{\alpha}+\boldsymbol{\beta}^H\mathbf{H}_4\boldsymbol{\beta}} \end{aligned} \tag{34}$$

where $\mathbf{h}_{SRE}{}^T = \mathbf{h}_{RE}{}^T diag(\mathbf{l})diag(\mathbf{h}_{SR})$, $\mathbf{n}_{RE}{}^T = \mathbf{h}_{RE}{}^T diag(\mathbf{n}_R)$, $\mathbf{H}_3 = P_S\mathbf{n}_{RE}{}^*\mathbf{n}_{RE}{}^T+\sigma^2\mathbf{I}_N$, $\mathbf{H}_3' = (1+P_0\gamma_{SE})\mathbf{H}_3+P_S\mathbf{h}_{SRE}{}^*\mathbf{h}_{SRE}{}^T$, $\mathbf{H}_4 = P_J\mathbf{h}_{RE}{}^*\mathbf{h}_{RE}{}^T$, and $\mathbf{H}_4' = (1+P_0\gamma_{SE})\mathbf{H}_4$. Finally the achievable secrecy rate is obtained as

$$R_{sAF} = \frac{1}{2}\log(\frac{\boldsymbol{\alpha}^H\mathbf{H}_1'\boldsymbol{\alpha}+\boldsymbol{\beta}^H\mathbf{H}_2'\boldsymbol{\beta}}{\boldsymbol{\alpha}^H\mathbf{H}_1\boldsymbol{\alpha}+\boldsymbol{\beta}^H\mathbf{H}_2\boldsymbol{\beta}}\frac{\boldsymbol{\alpha}^H\mathbf{H}_3\boldsymbol{\alpha}+\boldsymbol{\beta}^H\mathbf{H}_4\boldsymbol{\beta}}{\boldsymbol{\alpha}^H\mathbf{H}_3'\boldsymbol{\alpha}+\boldsymbol{\beta}^H\mathbf{H}_4'\boldsymbol{\beta}}) \tag{35}$$

It is too difficult to obtain the optimal solution for the problem of maximizing $R_{sAF}$ in (35). Since that, a suboptimal solution is presented as follows.

Firstly, we derive the optimal jamming weights vector. We null out the intended noise at the destination, while maximizing it at the eavesdropper. Under the nulling constraint, the corresponding jamming weights $\boldsymbol{\beta}_0$ can be derived according to the following criterion

$$\begin{aligned} &\arg\max_{\boldsymbol{\beta}}\,|\,\mathbf{h}_{RE}{}^T\boldsymbol{\beta}\,|^2 \\ &s.t. \quad \begin{cases}\mathbf{h}_{RD}{}^T\boldsymbol{\beta}=0\\ \boldsymbol{\beta}^H\boldsymbol{\beta}=1\end{cases} \end{aligned} \tag{36}$$

The problem in (36) is referred to as the null-steering beamformer in the literature of array signal processing. It can be introduced to solve the null-steering jammer problem as well. The optimal solution for the problem in (36) is given by

$$\boldsymbol{\beta}_0 = \varepsilon\,\|\,\mathbf{h}_{RD}\,\|^2\,\mathbf{h}_{RE}{}^* - \varepsilon\mathbf{h}_{RD}{}^T\mathbf{h}_{RE}{}^*\mathbf{h}_{RD}{}^* \tag{37}$$

where the scalar $\varepsilon$ is given by

$$\varepsilon = \sqrt{\frac{1}{\|\,\mathbf{h}_{RD}\,\|^4\|\,\mathbf{h}_{RE}\,\|^2-\|\,\mathbf{h}_{RD}\,\|^2|\,\mathbf{h}_{RD}{}^*\mathbf{h}_{RE}{}^T\,|^2}} \tag{38}$$

Secondly, we derive beamforming weights vector $\boldsymbol{\alpha}$. As $\boldsymbol{\beta}_0$ is given, the secrecy rate $R_{sAF}$ in (35) can be rewritten as

$$R_{sAF}=\frac{1}{2}\log(\underbrace{\frac{\boldsymbol{\alpha}^H\mathbf{H}_1'\boldsymbol{\alpha}}{\boldsymbol{\alpha}^H\mathbf{H}_1\boldsymbol{\alpha}}}_{w_1}\underbrace{\frac{\boldsymbol{\alpha}^H\mathbf{H}_5\boldsymbol{\alpha}}{\boldsymbol{\alpha}^H\mathbf{H}_5'\boldsymbol{\alpha}}}_{w_2}) \tag{39}$$

in which $\mathbf{H}_5=\mathbf{H}_3+\boldsymbol{\beta}_0^H\mathbf{H}_4\boldsymbol{\beta}_0\mathbf{I}_N$ , $\mathbf{H}_5'=\mathbf{H}_3'+\boldsymbol{\beta}_0^H\mathbf{H}_4'\boldsymbol{\beta}_0\mathbf{I}_N$. Notice that the maximum and minimum value of $w_1$ corresponds to the maximal eigenvalue $\lambda_{\max 1}$ and the minimal eigenvalue $\lambda_{\min 1}$ of matrix $\mathbf{H}_1^{-1}\mathbf{H}_1'$. In the same way, the maximum and minimum value of $w_2$ corresponds to the maximal eigenvalue $\lambda_{\max 2}$ and the minimal eigenvalue $\lambda_{\min 2}$ of matrix $(\mathbf{H}_5')^{-1}\mathbf{H}_5$. Thus we derive the beamforming vector $\boldsymbol{\alpha}$ according to the following criterion

$$\boldsymbol{\alpha}_0=\begin{cases}\max eig_{unit}(\mathbf{H}_1^{-1}\mathbf{H}_1') & \text{if } \lambda_{\max 1}\lambda_{\min 2}>\lambda_{\max 2}\lambda_{\min 1}\\ \max eig_{unit}[(\mathbf{H}_5')^{-1}\mathbf{H}_5] & \text{if } \lambda_{\max 1}\lambda_{\min 2}<\lambda_{\max 2}\lambda_{\min 1}\end{cases} \tag{40}$$

The reason is if we choose $\max eig_{unit}(\mathbf{H}_1^{-1}\mathbf{H}_1')$ when $\lambda_{\max 1}\lambda_{\min 2}>\lambda_{\max 2}\lambda_{\min 1}$, it holds that $w_1=\lambda_{max1}$, and the lower bounds of $w_2$ is $\lambda_{\min 2}$, so the lower bounds of secrecy rate is $\lambda_{\max 1}\lambda_{\min 2}$; otherwise, if we choose $\max eig_{unit}[(\mathbf{H}_5')^{-1}\mathbf{H}_5]$, the lower bounds of the secrecy rate is $\lambda_{\max 2}\lambda_{\min 1}$. As $\lambda_{\max 1}\lambda_{\min 2}>\lambda_{\max 2}\lambda_{\min 1}$, therefore it is better to choose the former one as the beamforming weights vector.

Lastly, since that $\boldsymbol{\beta}_0$ and $\boldsymbol{\alpha}_0$ are fixed, the secrecy rate in (35) can be rewritten as a function of the only variable $P_S$, i.e.

$$\begin{aligned}R_{sAF}(P_S)&=\frac{1}{2}\log(\frac{e_1P_S^2+f_1P_S+g_1}{e_2P_S^2+f_2P_S+g_2})\\&=\frac{1}{2}\log[\frac{e_1}{e_2}+\frac{(f_1-e_1f_2/e_2)P_S+(g_1-e_1g_2/e_2)}{e_2P_S^2+f_2P_S+g_2}]\end{aligned} \tag{41}$$

in which

$$\begin{cases}e_1=[(1+P_0\gamma_{SD})|\mathbf{n}_{RD}^T\boldsymbol{\alpha}|^2+|\mathbf{h}_{RSD}^T\boldsymbol{\alpha}|^2](|\mathbf{n}_{RE}^T\boldsymbol{\alpha}|^2-|\mathbf{h}_{RE}^T\boldsymbol{\beta}|^2)\\ f_1=(|\mathbf{n}_{RE}^T\boldsymbol{\alpha}|^2-|\mathbf{h}_{RE}^T\boldsymbol{\beta}|^2)(1+P_0\gamma_{SD})\sigma^2+(P_R|\mathbf{h}_{RE}^T\boldsymbol{\beta}|^2+\sigma^2)[(1+P_0\gamma_{SD})|\mathbf{n}_{RD}^T\boldsymbol{\alpha}|^2+|\mathbf{h}_{RSD}^T\boldsymbol{\alpha}|^2]\\ g_1=(1+P_0\gamma_{SD})\sigma^2+(P_R|\mathbf{h}_{RE}^T\boldsymbol{\beta}|^2+\sigma^2)\end{cases}$$
$$\begin{cases}e_2=|\mathbf{n}_{RD}^T\boldsymbol{\alpha}|^2[(1+P_0\gamma_{SE})(|\mathbf{n}_{RE}^T\boldsymbol{\alpha}|^2-|\mathbf{h}_{RE}^T\boldsymbol{\beta}|^2)+|\mathbf{h}_{RSE}^T\boldsymbol{\alpha}|^2]\\ f_2=|\mathbf{n}_{RD}^T\boldsymbol{\alpha}|^2(1+P_0\gamma_{SE})(P_R|\mathbf{h}_{RE}^T\boldsymbol{\beta}|^2+\sigma^2)+[(1+P_0\gamma_{SE})(|\mathbf{n}_{RE}^T\boldsymbol{\alpha}|^2-|\mathbf{h}_{RE}^T\boldsymbol{\beta}|^2)+|\mathbf{h}_{RSE}^T\boldsymbol{\alpha}|^2]\sigma^2\\ g_2=\sigma^2(1+P_0\gamma_{SE})(P_R|\mathbf{h}_{RE}^T\boldsymbol{\beta}|^2+\sigma^2)\end{cases} \tag{42}$$

Taking the derivative, setting it to zero, and solving the following quadratic problem yields the optimal power allocation $P_S^{root}$

$$(e_2f_1-e_1f_2)P_S^2+2(e_2g_1-e_1g_2)P_S+(f_2g_1-f_1g_2)=0 \tag{43}$$

If there is no solution within $[0,P_R]$, it holds that $P_S=0$ or $P_S=P_R$. As a result, an iterative algorithm can be illustrated as follows.

**Table 2.** Iterative algorithm for AF protocol

**c) Initialization:** $i=0$, $P_J^{(0)}=0$, and $P_S^{(0)}=P_R-P_J^{(0)}$.

**d) Iterative Update Process**

v. Solve (37) and (40) for $\boldsymbol{\beta}^{(i)}$ and $\boldsymbol{\alpha}^{(i)}$.

vi. Solve (35) for $R_{sAF}^{(i)}$ by using $P_S^{(i)}$, $P_J^{(i)}$, $\boldsymbol{\beta}^{(i)}$ and $\boldsymbol{\alpha}^{(i)}$.

vii. (42) $\leftarrow \boldsymbol{\alpha}^{(i)}, \boldsymbol{\beta}^{(i)}$, solve (43) for $P_J^{(i+1)}$

viii. Repeat step i and ii, until $R_{sAF}^{(i)}$ cannot be improved.

As following, we present the beamforming scheme and jamming scheme as references.

#### 4.1.2 Beamforming Scheme

In traditional AF beamforming, the received signals at destination during the two time slots are written as

$$\begin{aligned} y_d^{(1)} &= h_{SD}\sqrt{P_0}x+n_D \\ y_d^{(2)} &= \mathbf{h}_{RD}^{\ T}\sqrt{P_R}\,diag(\mathbf{l})[diag(\mathbf{h}_{SR})x+diag(\mathbf{n}_R)]\boldsymbol{\alpha}+n_D \end{aligned} \tag{44}$$

The corresponding rate is derived as

$$\begin{aligned} R_{dAF} &= \frac{1}{2}\log(1+P_0\gamma_{SD}+\frac{P_R\,|\,\mathbf{h}_{SRD}^{\ T}\boldsymbol{\alpha}\,|^2}{P_R\,|\,\mathbf{n}_{RD}^{\ T}\boldsymbol{\alpha}\,|^2+\sigma^2}) \\ &= \frac{1}{2}\log\frac{\boldsymbol{\alpha}^H\mathbf{H}_1'\boldsymbol{\alpha}}{\boldsymbol{\alpha}^H\mathbf{H}_1\boldsymbol{\alpha}} \end{aligned} \tag{45}$$

in which $\mathbf{H}_1=P_R\mathbf{n}_{RD}^{*}\mathbf{n}_{RD}^{\ T}+\sigma^2\mathbf{I}_N$, $\mathbf{H}_1'=(1+P_0\gamma_{SD})\mathbf{H}_1+P_R\mathbf{h}_{SRD}^{*}\mathbf{h}_{SRD}^{\ T}$. And the received signal at the eavesdropper is

$$\begin{aligned} y_e^{(1)} &= h_{SE}\sqrt{P_0}x+n_D \\ y_e^{(2)} &= \mathbf{h}_{RE}^{\ T}\sqrt{P_R}\,diag(\mathbf{l})[diag(\mathbf{h}_{SR})x+diag(\mathbf{n}_R)]\boldsymbol{\alpha}+n_E \end{aligned} \tag{46}$$

The rate is respectively obtained as

$$\begin{aligned} R_{eAF} &= \frac{1}{2}\log(1+P_0\gamma_{SE}+\frac{P_R\,|\,\mathbf{h}_{SRE}^{\ T}\boldsymbol{\alpha}\,|^2}{P_R\,|\,\mathbf{n}_{RE}^{\ T}\boldsymbol{\alpha}\,|^2+\sigma^2}) \\ &= \frac{1}{2}\log\frac{\boldsymbol{\alpha}^H\mathbf{H}_2'\boldsymbol{\alpha}}{\boldsymbol{\alpha}^H\mathbf{H}_2\boldsymbol{\alpha}} \end{aligned} \tag{47}$$

Where $\mathbf{H}_2=P_R\mathbf{n}_{RE}^{*}\mathbf{n}_{RE}^{\ T}+\sigma^2\mathbf{I}_N$, $\mathbf{H}_2'=(1+P_0\gamma_{SE})\mathbf{H}_2+P_R\mathbf{h}_{SRE}^{*}\mathbf{h}_{SRE}^{\ T}$. From (45) and (47), the achievable secrecy rate is

$$R_{sAF}=\frac{1}{2}\log(\underbrace{\frac{\boldsymbol{\alpha}^H\mathbf{H}_1'\boldsymbol{\alpha}}{\boldsymbol{\alpha}^H\mathbf{H}_1\boldsymbol{\alpha}}}_{w_1}\underbrace{\frac{\boldsymbol{\alpha}^H\mathbf{H}_2\boldsymbol{\alpha}}{\boldsymbol{\alpha}^H\mathbf{H}_2'\boldsymbol{\alpha}}}_{w_2}) \tag{48}$$

As the same as that in the hybrid scheme, it is in general difficult to give the optimal solution to the maximal value of (48). And for the same reason, we deprive the lower bound and corresponding weights vector as

$$\boldsymbol{\alpha}_0 = \begin{cases} \max eig_{unit}(\mathbf{H}_1^{-1}\mathbf{H}_1') & \text{if } \lambda_{\max 1}\lambda_{\min 2} > \lambda_{\max 2}\lambda_{\min 1} \\ \max eig_{unit}[(\mathbf{H}_2')^{-1}\mathbf{H}_2] & \text{if } \lambda_{\max 1}\lambda_{\min 2} < \lambda_{\max 2}\lambda_{\min 1} \end{cases} \tag{49}$$

in which $\lambda_{\max 1}$ and $\lambda_{\min 1}$ corresponds to maximum and minimum eigenvalue of matrix $\mathbf{H}_1^{-1}\mathbf{H}_1'$, $\lambda_{\max 2}$ and $\lambda_{\min 2}$ corresponds to the maximum and minimum eigenvalue of matrix $(\mathbf{H}_2')^{-1}\mathbf{H}_2$.

As what we illustrate in the DF beamforming case, AF beamforming is also a special case of the proposed hybrid scheme, for which it is impossible to outperform the generalized hybrid one.

#### 4.1.3 Jamming Scheme

Because jamming scheme is independent of the forwarding model, the description of jamming is as the same as that presented in the DF model. In AF hybrid scheme, we null the jamming signal at the destination. But at the same time, the beamforming signal mixed in the hybrid signal can improve the rate at the destination. As a result the secrecy rate in our proposed scheme outperforms the secrecy rate obtained in jamming scheme.

### 4.2 No Direct Links

#### 4.2.1 Hybrid Scheme

If there is no direct link between the source and the destination, as well as between the source and the eavesdropper, the received signal at the destination and the eavesdropper is written as

$$\begin{aligned} y_d &= \mathbf{h}_{RD}^T\{\sqrt{P_S}diag(\mathbf{l})[diag(\mathbf{h}_{SR})x + diag(\mathbf{n}_R)]\boldsymbol{\alpha} + \boldsymbol{\beta}\sqrt{P_J}n_J\} + n_D \\ y_e &= \mathbf{h}_{RE}^T\{\sqrt{P_S}diag(\mathbf{l})[diag(\mathbf{h}_{SR})x + diag(\mathbf{n}_R)]\boldsymbol{\alpha} + \boldsymbol{\beta}\sqrt{P_J}n_J\} + n_E \end{aligned} \tag{50}$$

The achievable rate at the destination and the eavesdropper is respectively written as

$$\begin{aligned} R_{dAF} &= \frac{1}{2}\log(1 + \frac{P_S|\mathbf{h}_{SRD}^T\boldsymbol{\alpha}|^2}{P_S|\mathbf{n}_{RD}^T\boldsymbol{\alpha}|^2 + P_J|\mathbf{h}_{RD}^T\boldsymbol{\beta}|^2 + \sigma^2}) \\ &= \frac{1}{2}\log\frac{\boldsymbol{\alpha}^H\mathbf{H}_1''\boldsymbol{\alpha} + \boldsymbol{\beta}^H\mathbf{H}_2\boldsymbol{\beta}}{\boldsymbol{\alpha}^H\mathbf{H}_1\boldsymbol{\alpha} + \boldsymbol{\beta}^H\mathbf{H}_2\boldsymbol{\beta}} \end{aligned} \tag{51}$$

and

$$\begin{aligned} R_{eAF} &= \frac{1}{2}\log(1 + \frac{P_S|\mathbf{h}_{SRE}^T\boldsymbol{\alpha}|^2}{P_S|\mathbf{n}_{RE}^T\boldsymbol{\alpha}|^2 + P_J|\mathbf{h}_{RE}^T\boldsymbol{\beta}|^2 + \sigma^2}) \\ &= \frac{1}{2}\log\frac{\boldsymbol{\alpha}^H\mathbf{H}_3''\boldsymbol{\alpha} + \boldsymbol{\beta}^H\mathbf{H}_4\boldsymbol{\beta}}{\boldsymbol{\alpha}^H\mathbf{H}_3\boldsymbol{\alpha} + \boldsymbol{\beta}^H\mathbf{H}_4\boldsymbol{\beta}} \end{aligned} \tag{52}$$

in which $\mathbf{H}_1 = P_S\mathbf{n}_{RD}^*\mathbf{n}_{RD}^T + \sigma^2\mathbf{I}_N$, $\mathbf{H}_1'' = \mathbf{H}_1 + P_S\mathbf{h}_{SRD}^*\mathbf{h}_{SRD}^T$, $\mathbf{H}_2 = P_J\mathbf{h}_{RD}^*\mathbf{h}_{RD}^T$, $\mathbf{H}_3 = P_S\mathbf{n}_{RE}^*\mathbf{n}_{RE}^T + \sigma^2\mathbf{I}_N$, $\mathbf{H}_4 = P_J\mathbf{h}_{RE}^*\mathbf{h}_{RE}^T$, and $\mathbf{H}_3'' = \mathbf{H}_3 + P_S\mathbf{h}_{SRE}^*\mathbf{h}_{SRE}^T$.

The achievable secrecy rate can be written as

$$R_{sAF} = \frac{1}{2}\log(\frac{\boldsymbol{\alpha}^H\mathbf{H}_1''\boldsymbol{\alpha} + \boldsymbol{\beta}^H\mathbf{H}_2\boldsymbol{\beta}}{\boldsymbol{\alpha}^H\mathbf{H}_1\boldsymbol{\alpha} + \boldsymbol{\beta}^H\mathbf{H}_2\boldsymbol{\beta}}\frac{\boldsymbol{\alpha}^H\mathbf{H}_3\boldsymbol{\alpha} + \boldsymbol{\beta}^H\mathbf{H}_4\boldsymbol{\beta}}{\boldsymbol{\alpha}^H\mathbf{H}_3''\boldsymbol{\alpha} + \boldsymbol{\beta}^H\mathbf{H}_4\boldsymbol{\beta}}) \tag{53}$$

Consequently, the optimization problem of maximum achievable secrecy rate can also be solved by the iterative scheme in **Table 2**.

#### 4.2.2 Beamforming Scheme

In beamforming, the destination and the eavesdropper can only receive signal forwarded by the relays in the second time slot. The received signals at destination and eavesdropper are written as

$$\begin{aligned} y_d &= \mathbf{h}_{RD}{}^T \sqrt{P_R}\, diag(\mathbf{l})[diag(\mathbf{h}_{SR})x + diag(\mathbf{n}_R)]\boldsymbol{\alpha} + n_D \\ y_e &= \mathbf{h}_{RE}{}^T \sqrt{P_R}\, diag(\mathbf{l})[diag(\mathbf{h}_{SR})x + diag(\mathbf{n}_R)]\boldsymbol{\alpha} + n_E \end{aligned} \tag{54}$$

The rate at destination and eavesdropper is calculated as

$$\begin{aligned} R_{dAF} &= \frac{1}{2}\log(1 + \frac{P_R |\mathbf{h}_{SRD}{}^T \boldsymbol{\alpha}|^2}{P_R |\mathbf{n}_{RD}{}^T \boldsymbol{\alpha}|^2 + \sigma^2}) \\ &= \frac{1}{2}\log\frac{\boldsymbol{\alpha}^H \mathbf{H}_1' \boldsymbol{\alpha}}{\boldsymbol{\alpha}^H \mathbf{H}_1 \boldsymbol{\alpha}} \end{aligned} \tag{55}$$

and

$$\begin{aligned} R_{eAF} &= \frac{1}{2}\log(1 + \frac{P_R |\mathbf{h}_{SRE}{}^T \boldsymbol{\alpha}|^2}{P_R |\mathbf{n}_{RE}{}^T \boldsymbol{\alpha}|^2 + \sigma^2}) \\ &= \frac{1}{2}\log\frac{\boldsymbol{\alpha}^H \mathbf{H}_2' \boldsymbol{\alpha}}{\boldsymbol{\alpha}^H \mathbf{H}_2 \boldsymbol{\alpha}} \end{aligned} \tag{56}$$

in which $\mathbf{H}_1 = P_R \mathbf{n}_{RD}{}^* \mathbf{n}_{RD}{}^T + \sigma^2 \mathbf{I}_N$ $\mathbf{H}_1'' = \mathbf{H}_1 + P_R \mathbf{h}_{SRD}{}^* \mathbf{h}_{SRD}{}^T$, $\mathbf{H}_2 = P_R \mathbf{n}_{RE}{}^* \mathbf{n}_{RE}{}^T + \sigma^2 \mathbf{I}_N$, and $\mathbf{H}_2' = \mathbf{H}_2 + P_R \mathbf{h}_{SRE}{}^* \mathbf{h}_{SRE}{}^T$. Consequently, the achievable secrecy rate is

$$R_{sAF} = \frac{1}{2}\log(\frac{\boldsymbol{\alpha}^H \mathbf{H}_1' \boldsymbol{\alpha}}{\boldsymbol{\alpha}^H \mathbf{H}_1 \boldsymbol{\alpha}} \frac{\boldsymbol{\alpha}^H \mathbf{H}_2 \boldsymbol{\alpha}}{\boldsymbol{\alpha}^H \mathbf{H}_2' \boldsymbol{\alpha}}) \tag{57}$$

The solution is similar to that in (48). For the same reason of only increasing the $w_2$ part in (1), it would not perform better than the hybrid scheme.

As the same as that in DF model, jamming dose not work in the assumption of no direct links existing.

## 5. Numerical Results

In this section, the performance of the proposed hybrid scheme is investigated numerically. And direct transmission, traditional beamforming and jamming schemes are also presented as references. Refer to [14], we consider a simple two-dimensional system model as depicted in **Fig. 2**. The source is fixed at (0, 0) (unit: meter), the destination is fixed at (30, 0), 5 relays are located at (10, 0), (10, $\pm 5$) and (10, $\pm 10$), and the eavesdropper moves from (0, 0) to (100, 0). Notice that, the distance unit is related, and it can be other units. As a reasonable assumption, the source-relay distance is always smaller than that between source and destination or eavesdropper. All channels are modeled by a simple line-of-sight channel. The path loss exponent is $c = 3.5$. In DF case, we assume that all relays decode correctly. The noise power is $\sigma^2 = -60dBm$, and the total power budget of the relays is $P_R = 0dBm$. We perform 1000 independent trials of Monte Carlo experiments to derive the average results.

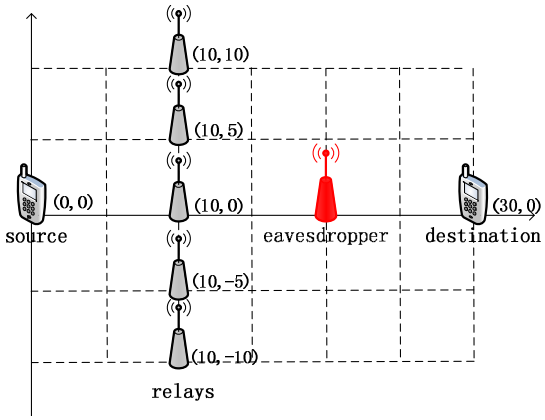



**Fig. 2.** Two-dimensional model used for numerical experiment, the eavesdropper moves from (20, 0) to (100, 0).

**Fig. 3** illustrates the received signal-to-noise ratio (SNR) at destination and eavesdropper in different cooperative schemes, which are denoted by SNRD and SNRE, respectively. We observe that the gap between SNRD and SNRE in our proposed hybrid scheme is larger than others, which implies a higher secrecy rate. SNRD in beamforming scheme is a litter higher than that in our proposed hybrid scheme. This is because in the hybrid scheme a part of the relays' power is allocated for transmitting artificial noise to decrease SNRE, while all of that is used to increase SNRD in beamforming scheme. Of course, SNRD in jamming is the lowest, because no additional power is used to increase it. But notice that SNRE decreases much more.

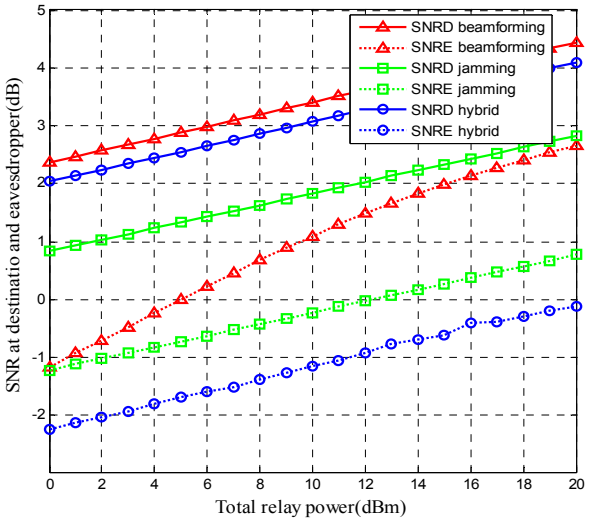



**Fig. 3.** SNR at destination and eavesdropper versus the source transmitting power, varies form 0dBm to 30dBm

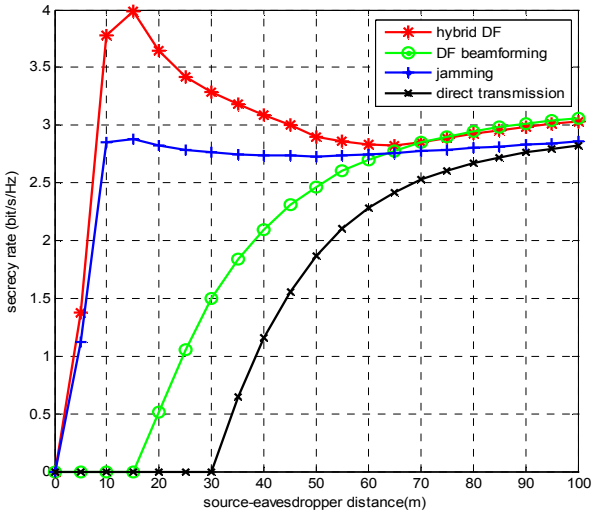



**Fig. 4.** Achievable secrecy rate versus the source-eavesdropper distance, in DF model, transmitting power of the source is $P_0 = 0dBm$ , relay is located in (10,0).

**Fig. 4** shows the achievable secrecy rate versus the source-eavesdropper distance in DF model. As expected, the secrecy rate for direct transmission is zero when the destination is farther from the source than the eavesdropper. When the source-eavesdropper distance is small, cooperative jamming performs better than beamforming. The reason is that while the eavesdropper is near the destination, friendly jamming can effectively interfere with the overhearing of the eavesdropper, while the receiving at the destination is not affected. Moreover, the proposed scheme outperforms others a lot in this area, which is because besides jamming part, the beamforming part in the hybrid signal can meanwhile enhance the rate at the destination. However, as the source-eavesdropper distance increases, traditional beamforming scheme outperforms jamming scheme, and finally it approximates the proposed hybrid scheme. That is because when the eavesdropper is very far from the source and the destination, it is not worthy spending power on transmitting jamming signals. Therefore, the gap of secrecy rate between beamforming and hybrid scheme becomes smaller and smaller. It can be observed that even when the source-eavesdropper distance is shorter than the source-relay distance, the propose hybrid scheme is the optimal one.

**Fig. 5** shows the received signal-to-noise ratio (SNR) at destination and eavesdropper for different cooperative schemes in AF model. As same as in DF, the gap between SNRD and SNRE in the hybrid scheme is the largest, while that in jamming is smallest. Without saying, a larger gap means a better secrecy performance.

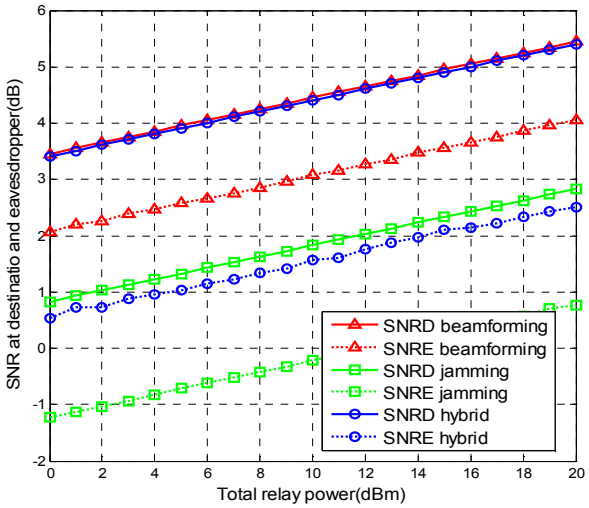



**Fig. 5.** SNR at destination and eavesdropper versus the source transmitting power, varies form 0dBm to 30dBm

**Fig. 6** shows the achievable secrecy rate versus the source-eavesdropper distance in AF model. In jamming, secrecy rate varies little as the source-distance increase. That is because the rate at the destination could not be improved by jamming. Generally, a similar conclusion as that in DF model can be drawn.

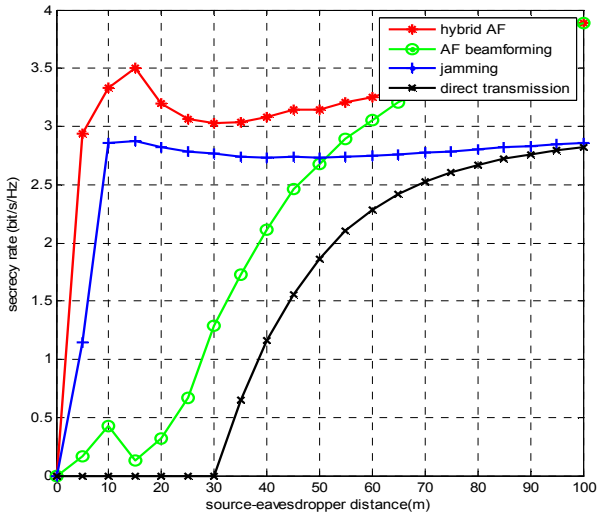



**Fig. 6.** Achievable secrecy rate versus the source-eavesdropper distance, transmitting power of the source is $P_0 = 0dBm$

As observed from Figure 7, the power allocated for jamming varies as the source-eavesdropper distance increases. The curve is consistent with the conclusion drawn from Figure 4, i.e. when jamming outperforms beamforming, more power should be allocated for jamming part of the hybrid signal. Otherwise, it is in reverse. And when the eavesdropper is very far away from the source, jamming scheme has little effect, so all power is used for beamforming part. Figure 8 shows the convergence of the proposed scheme. After nearly 30 times of iterative operation, the secrecy capacity can be achieved.

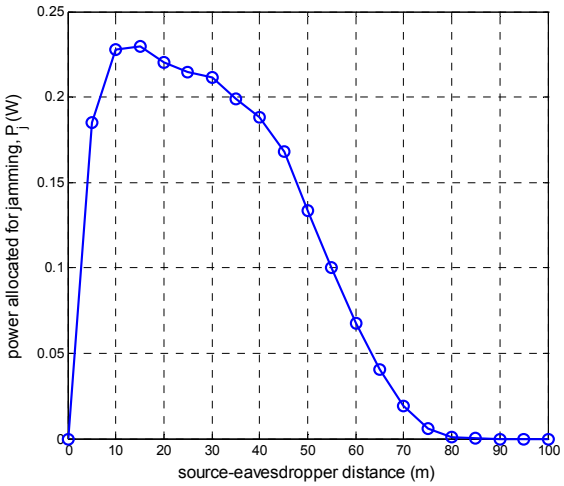



**Fig. 7.** Power allocated for jamming VS thesource-eavesdropper distance, in DF model, transmitting power of the source is $P_0 = 0dBm$

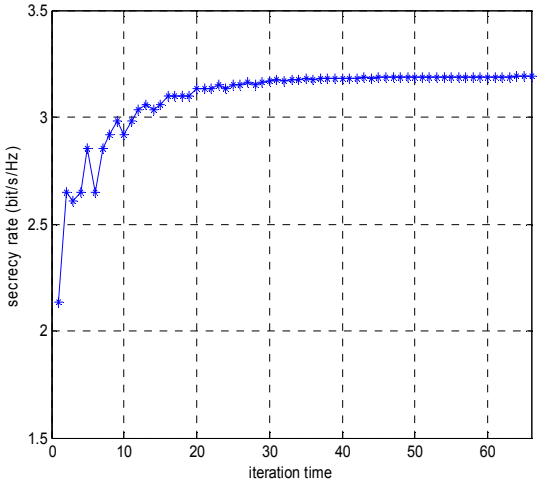



**Fig. 8.** Convergence of the proposed scheme, in DF model, transmitting power of the source is $P_0 = 0dBm$ , eavesdropper is located in (40,0)

## 6. Conclusion

In this paper, we have proposed a hybrid cooperative scheme to improve the secrecy performance of wireless communication in the presence of one eavesdropper. The problems of power allocation as well as beamforming and jamming weights optimization are solved by our presented iterative scheme. We have shown the secure performance being improved via the joint design of beamforming and jamming. The contribution of our work is that the proposed hybrid cooperative scheme is more generalized than the traditional ones, which can be easily reduced to traditional beamforming by nulling the jamming weights. It can be a useful reference in the design of cooperative schemes to increase PHY layer security. And it provides a novel view of user cooperation, which may inspire more effective works in this open issue. However, there are still plenty of researches needed in this quite open area. Further studies may include the issues such as the optimal hybrid scheme design in the presence of multiple eavesdroppers, the corresponding outage performance analysis, and the optimization problems based on partial channel knowledge, e.g. only statistical information about the eavesdropper's channel is available.

## References

[1] A. D. Wyner, "The Wire-tap Channel," *Bell Syst. Technology Journal*, vol.54, no.8, pp.1355-1387, Jan.1975.Article (CrossRef Link).

[2] S. K. Leung-Yan-Cheong and M. E. Hellman, "The gaussian wiretap channel," *IEEE Transactions Information Theory*, vol.24, pp.451–456, Jul.1978. Article (CrossRef Link).

[3] Hong Wen and Pin-Han Ho, "Physical layer technique to assist authentication based on PKI for Vehicular communication networks," *KSII Trans. on Internet and information systems*, vol.5, no.2, pp.440-456, Feb.2011. Article (CrossRef Link).

[4] F. Oggier and B. Hassibi, "The secrecy capacity of the MIMO wiretap channel," in *Proc. of IEEE International Symposium on Information Theory*, pp.524-528, Jul.2008. Article (CrossRef Link).

[5] H. Kim and J. D. Villasenor, "Secure MIMO communications in a system with equal numbers of transmit and receive antennas," *IEEE Communication Letters*, vol.12, no.5, pp.386-388, 2008. Article (CrossRef Link).

[6] A. Khisti and G. W. Wornell, "Secure transmission with multiple antennas—Part I: The MISOME Wiretap Channel," *IEEE Transactions on Information Theory*, vol.56, no.7, pp.3088–3104, 2009. Article (CrossRef Link).

[7] S. Shafiee, N. Liu, and S. Ulukus, "Towards the secrecy capacity of the Gaussian MIMO wire-tap channel: The 2-2-1 Channel," *IEEE Transactions on Information Theory*, vol.55, no.9, pp.4033–4039, 2009. Article (CrossRef Link).

[8] Oussama Souihli and Tomoaki Ohtsuki, "The two-way MIMO wire-tap channel," in *Proc. of IEEE International Conference on Communication,* pp.1-6, Jun.2009. Article (CrossRef Link).

[9] A Khisti and G. W. Wornell, "Secure transmission with multiple antennas—Part II: The MIMOME Wiretap Channel," *IEEE Transactions on Information Theory*, vol.56, no.11, pp.5515–5532, 2010. Article (CrossRef Link).

[10] L. Dong, Z. Han, A. Petropulu, and H. V. Poor, "Secure wireless communications via cooperation," in *Proc. of 46th Annual Allerton Conference Commuication, Control, and Computing*, pp.1132–1138, Sep.2008. Article (CrossRef Link).

[11] L. Dong, Z. Han, A. Petropulu, and H. V. Poor, "Amplify-and-forward based cooperation for

secure wireless communications," in *Proc. of IEEE Intl Conference Acoust. Speech Signal Processing*, pp.2613-2616, Apr.2009. Article (CrossRef Link).

[12] J. Zhang and M. C. Gursoy, "Collaborative relay beamforming for secrecy," in *Proc. of the IEEE International Conference on Communication (ICC)*, pp.1-5, May.2010. Article (CrossRef Link).

[13] J. Zhang and M. C. Gursory, "Relay beamforming strategies for physical layer security," in *Proc. of 44th Annual Conference on Information Sciences and Systems,* pp.1-6, Mar.2010. Article (CrossRef Link).

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

[15] S. Goel and R. Negi, "Guaranteeing secrecy using artificial noise," *IEEE Transactions on Wireless Communications*, vol.7, no.6, pp.2180-2189, Jun.2008. Article (CrossRef Link).

[16] J. Zhu, J. Mo, and M. Tao, "Cooperative secret communication with artificial noise in symmetric interference channel," *IEEE Communications Letters*, vol.14, no.10, Oct.2010. Article (CrossRef Link).

[17] R. Zhang, L. Song, Z. Han, B. Jiao, and M. Debbah, "Physical layer security for two way relay communications with friendly jammers," in *Proc. of IEEE GLOBECOM*, pp.1-6, Dec.6-10, 2010. Article (CrossRef Link).

[18] L. Dong, Z. Han, A. Petropulu, and H. V. Poor, "Cooperative jamming for wireless physical layer security", in *Proc. of IEEE SSP*, pp.417-420, Aug.2009. Article (CrossRef Link).

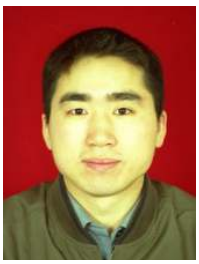
[19] M. Bloch, J. O. Barrors, M. R. D. Rodrigues, and S. W. Mclaughlin, "Wireless information-theoretical security," *IEEE Transactions on Information Theory*, vol.54, no.6, pp.2515-25, Jun.2008. Article (CrossRef Link).

**Xinrong Guan** received the B.S. degree in Communication Engineering from PLA University of Science and Technology, Nanjing, China in 2005. He is currently pursuing for the Ph.D degree in Communications and Information Systems at the Institute of Communications Engineering, PLA University of Science and Technology, Nanjing, China. His current research interest includes cooperative communications, signal processing in communications, and physical layer security.

**Yueming Cai** received the B.S. degree in Physics from Xiamen University, Xiamen, China in 1982, the M.S. degree in Micro-electronics Engineering and the Ph.D. degree in Communications and Information Systems both from Southeast University, Nanjing, China in 1988 and 1996 respectively. His current research interest includes MIMO systems, OFDM systems, signal processing in communications, cooperative communications, wireless sensor networks and physical layer security.

**Weiwei Yang** received the B.S. degree in Communications Engineering and the M.S. degree in Communications and Information Systems both from Institute of Communications Engineering, PLA University of Science and Technology, Nanjing, China in 2003 and 2006 respectively. He is currently pursuing for the Ph.D. degree at the Institute of Communications Engineering, PLA University of Science and Technology. His current research interest includes MIMO systems, OFDM systems, cooperative communications, signal processing in communications, and wireless sensor networks.

**Yunpeng Cheng** received the B.S. degree in Communications Engineering, the M.S. degree and Ph.D. degree in Communications and Information Systems from Institute of Communications Engineering, PLA University of Science and Technology, Nanjing, China in 1997, 2000, and 2003 respectively. His current research interest includes MIMO systems, cooperative signal processing in communications, and distributed beamforming.



**Junquan Hu** received the B.S. degree in fiber communications and the M.S. degree in Digital Communications from Institute of Communications Engineering, Nanjing, China in 1996 and 1999 respectively. His current research interest includes MIMO systems, cooperative communications.