# Cooperative Jamming and Beamforming in Amplify-and-Forward Relay Systems for Physical-Layer Security

Henan Lei, Li Guo, Jianwei Zhang
Key Lab of Universal Wireless Communications, Ministry of Education
Beijing University of Posts and Telecommunications
Beijing 100876, China, Email: {leihenan, guoli, zhangjianwei}@bupt.edu.cn.

***Abstract*—In this paper, we propose a hybrid cooperative beamforming and jamming scheme to enhance the physical-layer security in the two-way relay network with an eavesdropper and a primary receiver. Cooperative beamforming and jamming are designed to maximize the secrecy rate with a total transmit power constraint of the relays and interference power constraint at the primary receiver. The beamformer weights can be obtained by solving a semidefinite programming (SDP). And a method based on the first order Taylor polynomial which has lower complexity but comparable performance is introduced. Simulations show the joint scheme greatly improves the security.**

## I. Introduction

Physical layer security technique has attracted significant attentions recently, which exploits the physical characteristic of wireless channel to guarantee the message being transmitted securely. In [1], Wyner developed the concept of wire-tap channel and established the possibility of creating secure links without relying on the privacy cryptograph. And Wyner proposed the notion of secrecy capacity, defined as the maximum rate received at the legitimate receiver, while keeping the eavesdropper completely ignorant of the transmitted messages. Wyner's approach was extended to Gaussian wiretap channels and broadcast channels in later works [2].

Cooperative transmission has attracted much attention to enhance the capacity of a wireless channel. The current efforts to improve the secrecy rate in the context of cooperative communications can be roughly classified into three categories, cooperative beamforming, cooperative jamming, and hybrid relaying and jamming. Cooperative beamforming [3] helps to improve the channel quality to the legitimate destination, while cooperative jamming (also called artificial noise) degrades the channel condition of the eavesdroppers [4]. Hybrid relaying and jamming schemes to secure the networks were proposed in [5], where some nodes adopt distributed beamforming to relay the message and others jam the eavesdroppers. They will improve the security of the data transmission.

Artificial jamming signals in cooperative jamming can be divided into four categories [6]: 1) Gaussian noise, which is the same as the additive noise at the receiver [7]; 2) noise pre-known at the legitimate receivers, which impacts only on the performance of eavesdroppers [8]; 3) random codewords of a public codebook known by all nodes in the system including the eavesdroppers. The jamming signals can be decoded at the receiver and canceled from the received signal [9]; and 4) useful signals for other legitimate terminals in the system [10].

In this paper, the secrecy capacity of the two-phase two-way relaying system with an eavesdropper and a primary receiver is investigated. A new cooperative beamforming and jamming scheme is presented to improve the system security. Source node transmits both user and predefined jamming signals to the relay node in phase I. In phase II relay nodes forward the information which contains jamming signal using distributed beamforming. Under such a scheme, both phases are secured. We apply two beamforming approaches to investigate the problem of secrecy rate maximization in the cognitive relay network. Firstly, the maximum secrecy rate is obtained by well-studied interior-point based methods. Then, an iterative algorithm of lower complexity is proposed to solve the secrecy rate maximization problem.

Throughout this paper, the key mathematical notations are used as follows: vectors and matrices are denoted by uppercase and lowercase bold letters, respectively. Scalars are denoted by lowercase letters. $rank(\mathbf{X})$, $tr(\mathbf{X})$ denote the rank and the trace of matric $\mathbf{X}$, respectively. We represent the exception of $x$ as $E[x]$ and $\succeq$ denotes the generalized inequality. Transpose, conjugate, Hermitian transpose and the maximum eigenvalue of matrix $\mathbf{A}$ are denoted as $\{\bullet\}^T$, $\{\bullet\}^*$ and $\{\bullet\}^H$ and $\lambda_{\max}(\mathbf{A})$ respectively.

## II. System Model

We consider an AF relay network in which a source S wants to send information to the destination D under the existence of an eavesdropper E and a primary receiver PR. There are N intermediate relay nodes $R_n$, n=1, 2, . . . , N, between S and D. Each node in the whole network is only equipped with a single antenna, and is subject to the half-duplex constraint. We assume there is no direct connection between S and D. In this paper we propose a joint cooperative beamforming and jamming scheme. In phase I, source node transmits user and

This work was supported by National Natural Science Foundation of China (Grant No.61271178), National Key Scientific and Technological Project of China (No. 2012ZX03004005002, No. 2012ZX03003007 and No. 2013ZX03003004).

QSHINE 2015, August 19-20, Taipei, Taiwan
Copyright © 2015 ICST
DOI 10.4108/eai.19-8-2015.2261538

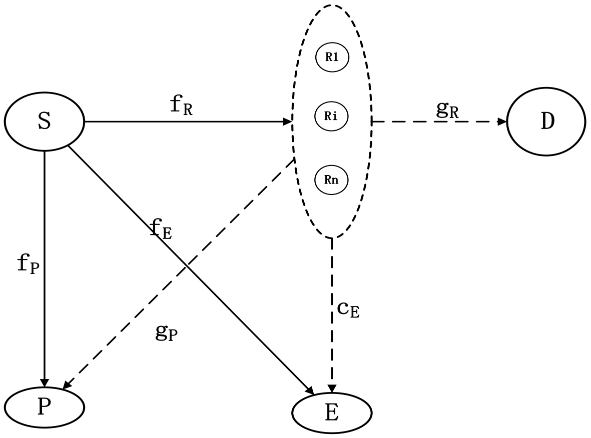

Fig. 1. Joint cooperative beamforming and jamming scheme, where the solid lines and the dash lines are the transmissions in phase I and II, respectively.

pre-defined jamming signals simultaneously. In phase II, relays forward the receiving siganls using distributed beamforming. E is passive with the intension of interpreting the source information from R and S without trying to modify it. E does not transmit any signals but receives the signals transmitted by all the nodes and tries to wiretap the information for the legitimate receiver. PR receives the signal from S and R as interference. The quasi-stationary flat-fading channel coefficients between all these nodes, $\mathbf{f}_R$, $f_P$, $f_E$, $\mathbf{g}_R$, $\mathbf{g}_P$ and $\mathbf{c}_E$ are also shown in Fig. 1. Signal transmission under AF protocol requires two phases. During phase I, S broadcasts its data. The signals received at Rn, PR and E are, respectively,

$$\mathbf{y}_R = \sqrt{P_s}\mathbf{f}_R s + \sqrt{P_j}\mathbf{f}_R z + \mathbf{n}_R \tag{1}$$

$$y_P^{(1)} = \sqrt{P_s} f_P s + \sqrt{P_j} f_P z + n_P^{(1)} \tag{2}$$

$$y_E^{(1)} = \sqrt{P_s} f_E s + \sqrt{P_j} f_E z + n_E^{(1)} \tag{3}$$

where $\mathbf{y}_R \triangleq [y_{R,1}, y_{R,2}, \ldots, y_{R,N}]^T$, $P_s$ and $P_j$ are the transmit powers of the signal and the jammer, respectively, z is the jamming signal, $\mathbf{n}_R$, $n_P^{(1)}$ and $n_E^{(1)}$ are the additive noises. We normalize $E\left\{|s|^2\right\} = E\left\{|z|^2\right\} = 1$.

In phase II, the relay nodes will forward the received signal to D using distributed beamforming, which grants E another opportunity to get the information. The signal transmitted by the relay nodes is

$$\mathbf{x_R} = \mathbf{W} * \mathbf{y}_R \tag{4}$$

where $\mathbf{W}$ is the beamformer matrix in the form of $\mathbf{W} = diag([w_1^*, w_2^*, \ldots, w_N^*])$, and diag is a diagonal matrix. Due to the total power constraint of relay nodes, we should have $E\{|x_R|^2\} \le P_R$. The received signals at D, E and PR are

$$y_D = \sqrt{P_s}\mathbf{g}_R^T\mathbf{W}\mathbf{f}_R s + \sqrt{P_j}\mathbf{g}_R^T\mathbf{W}\mathbf{f}_R z + \mathbf{g}_R^T\mathbf{W}\mathbf{n}_R + n_D \tag{5}$$

$$y_E^{(2)} = \sqrt{P_s}\mathbf{c}_E^T\mathbf{W}\mathbf{f}_R s + \sqrt{P_j}\mathbf{c}_E^T\mathbf{W}\mathbf{f}_R z + \mathbf{c}_E^T\mathbf{W}\mathbf{n}_R + n_E^{(2)} \tag{6}$$

$$y_P^{(2)} = \sqrt{P_s}\mathbf{g}_P^T\mathbf{W}\mathbf{f}_R s + \sqrt{P_j}\mathbf{g}_P^T\mathbf{W}\mathbf{f}_R z + \mathbf{g}_P^T\mathbf{W}\mathbf{n}_R + n_P^{(2)} \tag{7}$$

For the receiver D, the pre-defined jamming signal, $\mathbf{f}_R$ and $\mathbf{g}_R$ are available, the remaining part can be manipulated as

$$y_D = \sqrt{P_s}\mathbf{w}^H \alpha_{fg} s + \mathbf{g}_R^T\mathbf{W}\mathbf{n}_R + n_D \tag{8}$$

where $\alpha_{fg} \triangleq [f_{R,1}g_{R,1}, f_{R,2}g_{R,2}, \ldots, f_{R,\mathrm{N}}g_{R,N}]^T$, and $\mathbf{w} \triangleq [w_1, w_2, \ldots, w_\mathrm{N}]^T$. For the eavesdropper, each transmission phase grants it an opportunity to get the information. Combining (3) and (6) yields the receiving model of E in the whole procedure as

$$\mathbf{y}_E = \begin{bmatrix} \sqrt{P_s} f_E \\ \sqrt{P_s}\mathbf{w}^H\alpha_{cf} \end{bmatrix} s + \begin{bmatrix} \sqrt{P_j} f_E \\ \sqrt{P_j}\mathbf{w}^H\alpha_{cf} \end{bmatrix} z + \mathbf{n}_E \tag{9}$$

where $\mathbf{n}_E = \begin{bmatrix} n_E^{(1)} \\ c_E^T\mathbf{W}\mathbf{n}_R + n_E^{(2)} \end{bmatrix}$ with $\alpha_{cf} = [f_{R,1}c_{E,1}, f_{R,2}c_{E,2}, \ldots f_{R,N}c_{E,N}]^T$. For the PR, combining (2) and (7) the whole receiving signal is

$$\mathbf{y}_P = \begin{bmatrix} \sqrt{P_s} f_P \\ \sqrt{P_s}\mathbf{w}^H\alpha_{fp} \end{bmatrix} s + \begin{bmatrix} \sqrt{P_j} f_P \\ \sqrt{P_j}\mathbf{w}^H\alpha_{fp} \end{bmatrix} z + \mathbf{n_P} \tag{10}$$

where $\mathbf{n}_P = \begin{bmatrix} n_P^{(1)} \\ g_P^T\mathbf{W}\mathbf{n}_R + n_P^{(2)} \end{bmatrix}$ with $\alpha_{fp} = [f_{R,1}g_{P,1}, f_{R,2}g_{P,2}, \ldots f_{R,N}g_{P,N}]^T$.

We assume that all the noise terms $n_D$, $n_P^{(1)}$, $n_E^{(1)}$, $n_P^{(2)}$, $n_E^{(2)}$ and $\mathbf{n}_R$ are zero-mean and time-spatially white independent complex Gaussian random variables with variance $\delta^2$, and the jamming signal z is a complex Gaussian random variable.

Since the signal which relays receive contains jamming signal, we don't need to use another relay to transmit jamming signal. So when the source node transmits source and pre-defined jamming signal simultaneously, both phases are secured.

## III. Secrecy Scheme With Eavesdropper'CSI

Let us define

$$\mathbf{R}_{fg} = \alpha_{fg}{\alpha_{fg}}^H \tag{11}$$

$$\mathbf{R}_{cf} = \alpha_{cf}{\alpha_{cf}}^H \tag{12}$$

$$\mathbf{R}_{fp} = \alpha_{fp}{\alpha_{fp}}^H \tag{13}$$

$$\mathbf{R}_{gg} \triangleq diag(|g_{R,1}|^2, ..., |\mathrm{g}_{R,N}|^2) \tag{14}$$

$$\mathbf{R}_{cc} \triangleq diag(|c_{E,1}|^2, ..., |\mathrm{c}_{E,N}|^2) \tag{15}$$

$$\mathbf{R}_{pp} \triangleq diag(|g_{P,1}|^2, ..., |\mathrm{g}_{p,N}|^2) \tag{16}$$

To consider the the physical layer security, we adopt the achievable maximum secrecy rate as the measurement

$$C_s = \max\left[(I(y_D; s) - I(y_E; s))\right]^+ \tag{17}$$

where $[a]^+$ = max(0;$a$), and $I(\cdot,\cdot)$ is the mutual information. In the proposed scheme, we hope to achieve the maximum secrecy rate by searching the optimal w. (We assume that Ps and Pj are fixed). Then, the received SNR at the destination and eavesdropper can be reformulated, respectively, as

$$\Gamma_d = \frac{P_s tr(\alpha_{fg}{\alpha_{fg}}^H \mathbf{w}\mathbf{w}^H)}{\delta^2(1 + tr(\mathbf{R}_{gg}\mathbf{w}\mathbf{w}^H))} \tag{18}$$

$$\Gamma_e = \frac{P_s({f_E f_E}^H + \mathbf{w}^H \alpha_{fc}{\alpha_{fc}}^H \mathbf{w})}{P_j({f_E f_E}^H + \mathbf{w}^H \alpha_{fc}{\alpha_{fc}}^H \mathbf{w}) + \delta^2(2 + \mathbf{w}^H \mathbf{R}_{cc}\mathbf{w})} \tag{19}$$

where tr( ) represents the trace of a matrix. It is obvious that we only have to maximize the term inside the logarithm function in (17). With these notations, we can write the objective function of the optimization problem as

$$\begin{aligned}
&\frac{1+\Gamma_d}{1+\Gamma_e} \\
&= \frac{1 + \frac{P_s tr(\alpha_{fg}{\alpha_{fg}}^H \mathbf{w}\mathbf{w}^H)}{\delta^2(1+tr(\mathbf{R}_{gg}\mathbf{w}\mathbf{w}^H))}}{1 + \frac{P_s({f_E f_E}^H + \mathbf{w}^H\mathbf{R}_{fg}\mathbf{w})}{P_j({f_E f_E}^H + \mathbf{w}^H\mathbf{R}_{fg}\mathbf{w}) + \delta^2(2+\mathbf{w}^H\mathbf{R}_{cc}\mathbf{w})}} \\
&= \frac{\delta^2(1 + tr(\mathbf{R}_{gg}\mathbf{w}\mathbf{w}^H)) + P_s tr(\alpha_{fg}{\alpha_{fg}}^H \mathbf{w}\mathbf{w}^H)}{\delta^2(1 + tr(\mathbf{R}_{gg}\mathbf{w}\mathbf{w}^H))} \\
&\times \frac{P_j({f_E f_E}^H + \mathbf{w}^H\mathbf{R}_{fg}\mathbf{w}) + \delta^2(2 + \mathbf{w}^H\mathbf{R}_{cc}\mathbf{w})}{(P_j + P_s)({f_E f_E}^H + \mathbf{w}^H\mathbf{R}_{fg}\mathbf{w}) + \delta^2(2 + \mathbf{w}^H\mathbf{R}_{cc}\mathbf{w})}
\end{aligned} \tag{20}$$

If we denote $t_1 = \frac{\delta^2(1+tr(\mathbf{R}_{gg}\mathbf{w}\mathbf{w}^H))+P_s tr(\alpha_{fg}{\alpha_{fg}}^H\mathbf{w}\mathbf{w}^H)}{\delta^2(1+tr(\mathbf{R}_{gg}\mathbf{w}\mathbf{w}^H))}$, $t_2 = \frac{P_j({f_E f_E}^H+\mathbf{w}^H\mathbf{R}_{fc}\mathbf{w})+\delta^2(2+\mathbf{w}^H\mathbf{R}_{cc}\mathbf{w})}{(P_j+P_s)\times({f_E f_E}^H+\mathbf{w}^H\mathbf{R}_{fc}\mathbf{w})+\delta^2\times(2+\mathbf{w}^H\mathbf{R}_{cc}\mathbf{w})}$, and define $\mathbf{X} \triangleq \mathbf{w}\mathbf{w}^\mathbf{H}$ using the similar semidefinite programming method as described in [11], we can express the optimization problem as

$$\begin{aligned}
&\max_{\mathbf{X},t_1,t_2} \quad t_1 t_2 \\
&s.t. \quad P_s tr(\mathbf{R}_{fg}\mathbf{X}) \geq \delta^2(1 + tr(\mathbf{R}_{gg}\mathbf{X}))(t_1 - 1) \\
&P_j({f_E f_E}^H + tr(\mathbf{R}_{cf}\mathbf{X})) - t_2(P_j + P_s)({f_E f_E}^H + tr(\mathbf{R}_{cf}\mathbf{X})) \\
&\geq \delta^2(2 + tr(\mathbf{R}_{cc}\mathbf{X}))(t_2 - 1) \\
&and \quad tr(\mathbf{R}\mathbf{X}) \leq P_R, P_I \leq I_{th}, and \quad \mathbf{X} \geq 0
\end{aligned} \tag{21}$$

where $\mathbf{X} \geq 0$ means that $\mathbf{X}$ is a symmetric positive semidefinite matrix, $\mathbf{R} = (Ps + Pj)\mathbf{f_R}\mathbf{f_R^H} + \sigma^2\mathbf{I}$, $P_I = (Ps + Pj)\mathbf{f}_R{\mathbf{f}_R}^H + (Ps+Pj)\mathbf{w}\mathbf{R}_{fp}\mathbf{w}^H + \sigma^2\mathbf{w}\mathbf{R}_{gg}\mathbf{w}^H$. Since X by definition is a rank one matrix, finding the optimal weights is in general a nonconvex optimization problem. Thus, we above ignore the rank constraint, and hence employ semidefinite relaxation (SDR) [12]. If the matrix $\mathbf{X}_{opt}$ obtained by solving the above optimization problem happens to be rank one, then its principal component will be the optimal solution to the original problem. Otherwise, randomization method in [13] is employed to obtain $\mathbf{w}_{opt}$.

When there is total power constraint, we can easily compute the maximum values of $t_1$ and $t_2$ separately since now we have Rayleigh quotient problems.

$$\begin{aligned}
&t_{1,u} \\
&= \max_{tr(\mathbf{RX})\leq P_R} \frac{\delta^2\mathbf{w}\mathbf{R}_{gg}\mathbf{w}^H + \delta^2 + P_s\mathbf{w}\mathbf{R}_{fg}\mathbf{w}^H}{\delta^2 + \delta^2\mathbf{w}\mathbf{R}_{gg}\mathbf{w}^H} \\
&= \max_{tr(\mathbf{RX})\leq P_R} \frac{\mathbf{w}(\delta^2\mathbf{R}_{gg} + \frac{\delta^2\mathbf{R}}{P_R} + P_s\mathbf{R}_{fg})\mathbf{w}^H}{\mathbf{w}(\delta^2\mathbf{R}_{gg} + \frac{\delta^2\mathbf{R}}{P_R})\mathbf{w}^H} \\
&= \lambda_{\max}(\delta^2\mathbf{R}_{gg} + \frac{\delta^2\mathbf{R}}{P_R} + P_s\mathbf{R}_{fg}, \delta^2\mathbf{R}_{gg} + \frac{\delta^2\mathbf{R}}{P_R})
\end{aligned} \tag{22}$$

where $\lambda_{\max}(\mathbf{A}, \mathbf{B})$ is the largest generalized eigenvalue of the matrix pair $(\mathbf{A}, \mathbf{B})^2$.

Similarly, maximum values of $t_2$ under total power constraint is

$$\begin{aligned}
&t_{2,u} \\
&= \max_{tr(\mathbf{RX})\leq P_R} \frac{P_j({f_E f_E}^H + \mathbf{w}^H\mathbf{R}_{fc}\mathbf{w}) + \delta^2(2 + \mathbf{w}^H\mathbf{R}_{cc}\mathbf{w})}{(P_j + P_s)({f_E f_E}^H + \mathbf{w}^H\mathbf{R}_{fc}\mathbf{w}) + \delta^2(2 + \mathbf{w}^H\mathbf{R}_{cc}\mathbf{w})} \\
&= \max_{tr(\mathbf{RX})\leq P_R} \frac{\mathbf{w}^H(P_j\mathbf{R}_{fc} + \delta^2\mathbf{R}_{cc} + \frac{(P_j {f_E f_E}^H + 2\delta^2)}{P_R}\mathbf{R})\mathbf{w}}{\mathbf{w}^H((P_j + P_s)\mathbf{R}_{fc} + \delta^2\mathbf{R}_{cc} + \frac{((P_j+P_s){f_E f_E}^H + 2\delta^2)}{P_R}\mathbf{R})\mathbf{w}} \\
&= \lambda_{\max}(P_j\mathbf{R}_{fc} + \delta^2\mathbf{R}_{cc} + \frac{(P_j {f_E f_E}^H + 2\delta^2)}{P_R}\mathbf{R}, \\
&(P_j + P_s)\mathbf{R}_{fc} + \delta^2\mathbf{R}_{cc} + \frac{((P_j + P_s){f_E f_E}^H + 2\delta^2)}{P_R}\mathbf{R})
\end{aligned} \tag{23}$$

Note that for total power constraints, the maximum values of $t_1$ and $t_2$ are obtained separately above, and these values are in general attained by different $\mathbf{X} = \mathbf{w}\mathbf{w}^H$. For those X values that correspond to $t_{1,u}$, we can compute the corresponding $t_2$ and denote it as $t_{2,l}$. Then, log($t_{1,u}, t_{2,l}$) will serve as our amplify-and-forward achievable rates for total power constraints, respectively. With the achievable rates, we propose the following algorithm to iteratively search over $t_1$ and $t_2$ to get the optimal $t_{1,o}$ and $t_{2,o}$ that maximize the product $t_1 t_2$ by checking the following feasibility problem[14].

$$\begin{aligned}
&find \qquad \mathbf{X} \geq 0 \\
&s.t \quad P_s tr(\mathbf{R}_{fg}\mathbf{X}) \geq \delta^2(1 + tr(\mathbf{R}_{gg}\mathbf{X}))(t_1 - 1) \\
&P_j({f_E f_E}^H + tr(\mathbf{R}_{cf}\mathbf{X})) - t_2(P_j + P_s)({f_E f_E}^H + tr(\mathbf{R}_{cf}\mathbf{X})) \\
&\geq \delta^2(2 + tr(\mathbf{R}_{cc}\mathbf{X}))(t_2 - 1) \\
&and \quad tr(\mathbf{R}\mathbf{X}) \leq P_R, P_I \leq I_{th}
\end{aligned} \tag{24}$$

Actually, we can use its proposed Algorithm to get the Optimal value.

## IV. THE LOWER COMPLEXITY METHOD

In the last section, the maximum secrecy rate is obtained by characterizing the rate region via the rate-profile method. However, it requires an exhaustive search which is of great complexity. In this section, an approach of lower complexity is introduced to maximize the secrecy rate. The optimization problem can be mathematically formulated as

$$\begin{array}{ll} \max\limits_{\mathbf{w}} & R_d - R_e \\ s.t. & P_I \leq I_{th} \\ & tr(\mathbf{RX}) \leq P_R \end{array} \tag{25}$$

Based on SDR and the same definition $\mathbf{X} = \mathbf{w}\mathbf{w}^H$, (25) can be transformed into the following problem:

$$\begin{array}{ll} \max\limits_{\mathbf{X}} & \log(\frac{\delta^2 + tr(\mathbf{AX})}{\delta^2(1 + tr(\mathbf{R}_{gg}\mathbf{X}))}) - \log(\frac{\mathbf{D} + tr(\mathbf{EX})}{\mathbf{B} + tr(\mathbf{CX})}) \\ & P_I \leq I_{th} \\ s.t. & tr(\mathbf{RX}) \leq P_R \\ & \mathbf{X} \geq 0 \end{array} \tag{26}$$

where $\mathbf{A} = P_s\mathbf{R}_{fg} + \sigma^2\mathbf{R}_{gg}$, $B = P_j f_E f_E^H + 2\delta^2$, $\mathbf{C} = \delta^2\mathbf{R}_{cc} + P_j\mathbf{R}_{cf}$, $D = (P_s + P_j) f_E f_E^H + 2\delta^2$, $\mathbf{E} = \delta^2\mathbf{R}_{cc} + P_j\mathbf{R}_{cf} + P_s\mathbf{R}_{cf}$. Note that the scalar $\frac{1}{2}$ is dropped and the natural logarithm is used instead for simplicity. Using the property log(x/y)=log (x)-log (y) and introducing variables $\theta_1$, $\theta_2$, $\phi_1$, $\phi_2$, we can convert (26) into (27).

$$\begin{array}{l} \max\limits_{\mathbf{X},\theta_m,\phi_m} \log(\theta_1) + \log(\theta_2) - \log(\phi_1) - \log(\phi_2) \\ s.t. \quad \delta^2 + tr(\mathbf{AX}) = \theta_1 \\ \quad B + tr(\mathbf{CX}) = \theta_2 \\ \quad \delta^2(1 + tr(\mathbf{R}_{gg}\mathbf{X})) = \phi_1 \\ \quad D + tr(\mathbf{EX}) = \phi_2 \\ \quad P_I \leq I_{th} \\ \quad tr(\mathbf{RX}) \leq P_R \\ \quad \mathbf{X} \geq 0 \end{array} \tag{27}$$

**Table 1** Iterative Algorithm for problem(27)

```
Initialization $\phi_{1,0}$,$\phi_{2,0}$,$\varsigma > 0$,n = 0
Repeat
    Solve problem(27)with the given $\phi_{1,0}$,$\phi_{2,0}$ and find the optimal value $f_n^*$ and $\phi_1^n$,$\phi_2^n$
    Update $\phi_{1,0}$,$\phi_{2,0}$:$\phi_{1,0} = \phi_1^n$,$\phi_{2,0} = \phi_2^n$
Until $|f_n^* - f_{n-1}^*| \leq \varsigma$
```

Unfortunately, the above problem is non-convex because of the objective function, which is actually the difference of convex function. Inspired by the linear approximation approach in [15] and reference therein, we introduce two new variables $\pi_1$, $\pi_2$ and use the first order Taylor polynomial in (28) to convert (27) into a solvable problem as shown in (29).

$$\log(\phi_m) \approx \log(\phi_{m,0}) + \frac{1}{\phi_{m,0}}(\phi_m - \phi_{m,0}), m = 1, 2 \tag{28}$$

$$\begin{array}{l} \max\limits_{\mathbf{X},\theta_m,\phi_m,\pi_m} \log(\theta_1) + \log(\theta_2) - \pi_1 - \pi_2 \\ s.t. \quad \delta^2 + tr(\mathbf{AX}) = \theta_1 \\ \quad B + tr(\mathbf{CX}) = \theta_2 \\ \quad \delta^2(1 + tr(\mathbf{R}_{gg}\mathbf{X})) = \phi_1 \\ \quad D + tr(\mathbf{EX}) = \phi_2 \\ \quad P_I \leq I_{th} \\ \quad tr(\mathbf{RX}) \leq P_R \\ \quad \mathbf{X} \geq 0 \\ \quad \log(\phi_{m,0}) + \frac{1}{\phi_{m,0}}(\phi_m - \phi_{m,0}) \leq \pi_m \end{array} \tag{29}$$

Problem (29) is a semidefinite programming problem and can easily be solved using standard convex optimization algorithm. However, (29) is not equal to (27) as the right side of (28) is just a first order approximation of the left side. And only if $\phi_{m,0}$ equals to the optimal $\phi_{m,opt}$ is the right side of (28) equals to the left side. Thus, in order to solve (27) accurately, inspired by the POTDC method in [16], we introduce a iterative algorithm as described in table 1. A convergence proof of the algorithm can be built based on [16] and simulation results verify the efficiency of the algorithm in the next section[17].

## V. Simulation Results

In the simulation cases, all the channel coefficients are randomly generated in each simulation run, as complex zero-mean Gaussian random vectors with unit covariance. The noise power $\sigma^2$ is normalized to be at 0dB. We use CVX toolbox to solve the SDP problem.

Figure 2 displays the maximum secrecy rate versus the maximum total transmit power of relays with Ps = 5dB, Ith = -5dB, Pj = 0dB or Pj = 5dB, N = 3 or N = 6. As it is depicted in the figure, the performance increases as the number of relays increases and the secrecy rate obtained with method in III and that in IV are coincident. And the secrecy has been significantly improved with the hybrid cooperative beamforming and jamming scheme.

In order to further study the influence of N, we present the secrecy rate versus N with Ith = -5dB , PR = 5dB or PR = 10dB, Ps = 5dB, Pj = 0dB or Pj = 5dB. As shown in Fig. 3, the secrecy rate increases as the number of relays becomes large and the growing rate slows down.

Figure 4 displays the maximum secrecy rate versus the maximum total transmit power of relays with Ps = 5dB, Pj = 0dB or Pj = 5dB, N = 3 or N = 6. And Ith changes from -24dB to -4dB with step of 2dB. As it is depicted in the figure, the performance becomes better as Ith increases. In addition, as shown in both figure 2 and figure 4, the more relays has a better performance than the more Pj power.

## VI. Conclusion

In this paper, we investigate the sercrecy rate maximization problem in the cognitive two-way relay network with an interference power constraint at the PRX and a total transmit power constraint of the relays. we have proposed a joint

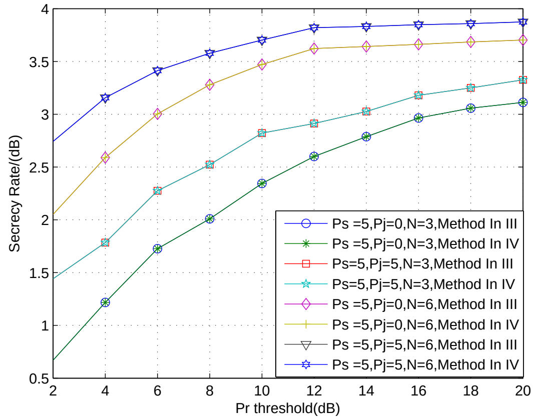

Fig. 2. Maximum secrecy rate vs the total power of relays.

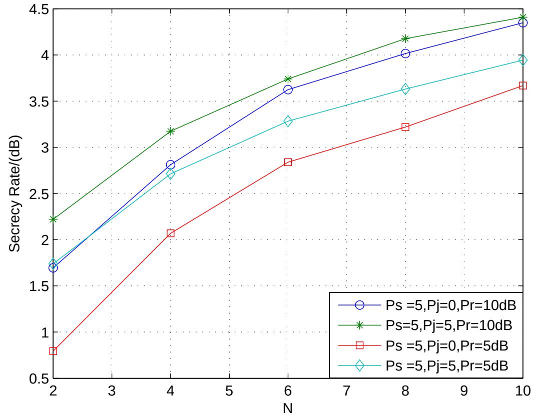

Fig. 3. Maximum secrecy rate vs the number of relays

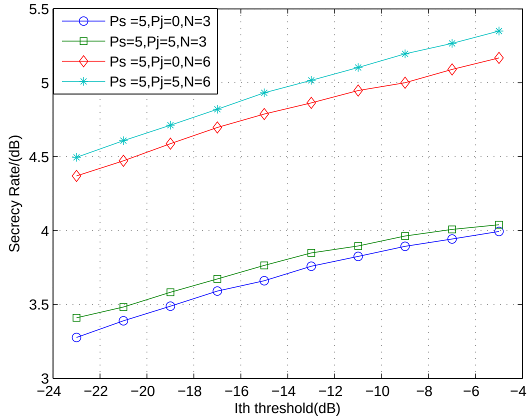

Fig. 4. Maximum secrecy rate vs interference power at PRX

cooperative beamforming and jamming scheme to enhance the security. Two methods are devised to obtain the optimal solutions. The first method is the rate region method and the second one is a lower complexity algorithm based on SDR and the first order Taylor polynomial. Simulation results verify that the secrecy rate obtained by these two methods are coincident and the joint scheme greatly improves the security.

## References

[1] A. D. Wyner, The wire-tap channel, Bell Syst. Tech. J., vol. 54, no. 8, pp. 1355-1387, Oct. 1975.

[2] S. K. Leung-Yan-Cheong and M. E. Hellman, The Gaussian wire-tap channel, IEEE Trans. Inf. Theory, vol. 24, no. 4, pp. 451-456, Jul. 1978.

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

[4] I. Krikidis, J. Thompson, S. Mclaughlin, Relay selection for secure cooperative networks with jamming, IEEE Trans. Wireless Commun., vol.8, no.10, pp. 5003-5011, Oct. 2009

[5] H.-M. Wang, M. Luo and Q. Yin, Hybrid cooperative relaying and jamming for secure two-way relay networks, in Proc. IEEE GLOBECOM, Dec. 2012, pp. 4846-4850.

[6] Hang Long, Wei Xiang, Jing Wang, et al., Cooperative jamming and power allocation in three-phase two-way relaying wiretap systems, in Proc. IEEE Wireless Communications and Networking Conference (WCNC) 2013, Shanghai, China, pp. 4216-4220, Apr. 2013.

[7] I. Krikidis, J. Thompson and S. Mclaughlin, Relay selection for secure cooperative networks with jamming, IEEE Trans. Wireless Comms., vol. 8, no. 10, pp. 5003-5011, Oct. 2009.

[8] Lun Dong, H. Yousefizadeh, and H. Jafarkhani, Cooperative jamming and power allocation for wireless relay networks in presence of eavesdropper, in Proc. IEEE ICC, Kyoto, Japan, June 2011, pp. 1-5.

[9] E. Tekin and A. Yener, Achievable rates for the general Gaussian multiple access wire-tap channel with collective secrecy, in Proc. Allerton Conference on Communication, Control, and Computing (ACCCC), Monticello, IL, Sep. 2006, pp. 1-5.

[10] O. Simeone and P. Popovski, Secure communications via cooperating base stations, IEEE Communications Letters, vol. 12, no. 3, pp. 188-190, Mar. 2008.

[11] J. Zhang and M. C. Gursoy, ”Collaborative relay beamforming for secrecy,” to appear in the Proc. of the IEEE International Conference on Communication (ICC), Cape Town, South Africa, May 2010. Available: http://arxiv.orglabs/0910.4132

[12] V. Nassab, S. Shahbazpanahi, A. Grami, and Z.-Q. Luo,” Distributed beamforming for relay networks based on second order statistics of the channel state information,” IEEE Trans. on Signal Proc., Vol. 56, No 9, pp. 4306-4316, Sept. 2008.

[13] Z.-Q. Luo, Wing-kin Ma, Anthony So, Y. Ye, and S. Zhang, Semidefinite Relaxation of Quadratic Optimization Problems, IEEE Signal Processing Magazine, vol. 27, no. 3, May 2010, pp. 20-34.

[14] Junwei Zhang and Mustafa Cenk Gursoy Department of Electrical Engineering University of Nebraska-Lincoln, ”Relay Beamforming Strategies for Physical-Layer Security” submitted to Information Sciences and Systems (CISS), the 44th Annual Conference,March 2010

[15] J. Zhang, F. Roemer, M. Haardt, A. Khabbazibasmenj, and S. A. Vorobyov, Sum rate maximization for multi-pair two-way relaying with single-antenna amplify and forward relays, in Proc. IEEE Int. Conj on Acoustics, Speech, and Signal Processing (ICASSP), Kyoto, Japan, Mar. 2012.

[16] A. Khabbazibasmenj, F. Roemer, S. A. Vorobyov, and M. Haardt, Sum-Rate Maximization in Two-Way AF MIMO Relaying: Polynomial Time Solutions to a Class of DC Programming Problems, submitted to IEEE Trans. Signal Processing,July 2012.

[17] Jianwei Zhang, Li Guo, Tianyu Kang, Peng Zhang,”Cooperative Beamforming in Cognitive Radio Network with Two-Way Relay” submitted to Vehicular Technology Conference (VTC Spring), 2014 IEEE 79th,May 2014.