JOINT NULL-SPACE BEAMFORMING AND JAMMING TO SECURE AF RELAY SYSTEMS WITH INDIVIDUAL POWER CONSTRAINT

Hui-Ming Wang, Qinye Yin, Wenjie Wang

School of Elec. and Infor. Engineering
Xi'an Jiaotong University
Xi'an,710049, Shaanxi, P. R. China
Email: xjbswhm@gmail.com

Xiang-Gen Xia

Department of Elec. and Computer Engineering
University of Delaware
Newark, DE 19716, USA
Email: xxia@ee.udel.edu

ABSTRACT

Cooperative beamforming and jamming are two efficient schemes to improve the physical-layer security of a wireless transmission in the presence of a passive eavesdropper. However, in most works they are discussed separately. In this paper, we propose a *joint* cooperative beamforming and jamming scheme to enhance the security of a cooperative relay network, where some intermediate nodes adopt distributed beamforming while the others jam the eavesdropper, simultaneously. Subjected to the more practical individual power constraint of each node, we propose a null-space beamforming based secrecy strategy. The beamformer design can be optimized by a bisection method and second-order convex cone programming (SOCP). Simulations show the joint scheme greatly improves the security.

Index Terms— Physical-layer security, cooperative beamforming, second-order convex cone programming

1. INTRODUCTION

Exploiting multiple-node cooperation to improve the physical layer security of wireless communications has attracted increasing interest very recently [1]-[11]. For a system where all terminals only equipped with single antenna, generally, there are two efficient ways to take advantages of the multiple-nodes in the system: cooperative beamforming and cooperative jamming. Cooperative beamforming helps to improve the channel quality to the legitimate destination, while cooperative jamming (also called artificial noise) degrades the channel condition of the eavesdroppers. In [1]-[3], multiple relay nodes use cooperative beamforming to help to maximize the achievable secrecy rate. In [4]-[7], relay nodes transmit jamming signals to eliminate the information leakage to the eavesdropper.

However, the data transmission in relay networks requires two phases, i.e., phase I (broadcasting phase) and phase II (relaying phase), due to the half-duplex constraint of the transceivers (let's assume that there is no direct link between source and destination), which grants the potential eavesdropper two opportunities to intercept the information. However, in almost all the above works, all relay nodes need to listen to the signal from the source during phase I, so that *no procedure is taken* to protect information secrecy [1]-[3]. Cooperative beamforming or jamming is only taken in phase II. The situation is similar for *two-way relay networks* (TWRN) [8]-[9]. All the relay nodes listen to the broadcasted signals from two terminals in phase I so that the information is revealed to the eavesdropper without any protection. Obviously, this will greatly harm the security.

To overcome this problem, in this paper, we propose a *joint* cooperative beamforming and jamming scheme for physical layer security of an amplify-and-forward (AF) based relay system, where each node is equipped with only single antenna. In the joint scheme, *during both phases*, some intermediate nodes are helpers to relay the signal using distributed beamforming and the others are jamming nodes to confuse the potential eavesdropper. Under such a scheme, both phases are secured. We consider the scenario when the eavesdropper's CSI is known. It corresponds to the case when the "eavesdropper" is actually a legitimate user in the network but not the target one. We propose a null-space beamforming based approach, subjected to the more practical individual power constraint of each node. We optimize the beamformer weights by using a bisection method together with an SOCP programming.

In [5], the authors proposed joint relay and jammer *selection* schemes to improve the security of a decode-and-forward (DF) one-way relay network. The idea is generalized into AF and DF TWRN, respectively, in [10] and [11]. However, in all of these works, out of a bunch of intermediate nodes, only one node is *selected* as relay to help transmit signal, which may not take full advantage of the multiple nodes. On the other hand, the jammer will also interfere the relay node and degrade the receiving performance. However, in our scheme, all the intermediate nodes are exploited so that these two problems have been overcome by cooperative beamforming.

2. SYSTEM MODEL

We consider a wireless network in which a source $\mathbb{S}$ wants to send information to the destination $\mathbb{D}$ under the existence of an eavesdropper $\mathbb{E}$. There are N intermediate relay nodes $\mathbb{R}_n, n = 1, 2, \cdots, N$, between $\mathbb{S}$ and $\mathbb{D}$. 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 $\mathbb{S}$ and $\mathbb{D}$. In this paper we propose a joint cooperative beamforming and jamming scheme, where the intermediate nodes are divided into two groups: the relay nodes and the jammers. The relay nodes will forward the received signal using cooperative beamforming while the jammer transmit interference signals to confuse the eavesdropper. For convenience, we assume that only one node is jammer $\mathbb{J}$ and all the other $N-1$ are relay nodes, as shown in Fig. 1. However, it can be generalized to more than one jammer case easily. The quasi-stationary flat-fading channel between $\mathbb{S}$, $\mathbb{R}$, $\mathbb{J}$ and $\mathbb{E}$ are also shown in Fig. 1.

Signal transmission under AF protocol requires two phases. During phase I, $\mathbb{S}$ broadcasts its data. In conventional schemes [1]-[3], all N relay nodes will listen to the signal while in our scheme, the $N-1$ relay nodes listens and the jammer sends interference signal to cover the information transmission. The signal vector received at

the relays is

$$\boldsymbol{y}_R = \sqrt{P_s}\boldsymbol{f}_R s + \sqrt{P_J^{(1)}}\boldsymbol{h}_R z^{(1)} + \boldsymbol{n}_R, \tag{1}$$

where $\boldsymbol{y}_R \triangleq [y_{R,1}, \cdots, y_{R,N-1}]^T$, $\boldsymbol{f}_R \triangleq [f_{R,1}, \cdots, f_{R,N-1}]^T$, and similarly for $\boldsymbol{h}_R$, P_s and $P_J^{(1)}$ are the transmit powers of the signal and the jammer, respectively, $z^{(1)}$ is the jamming signal, $\boldsymbol{n}_R$ is the additive noise at the relay nodes. We normalize $E\{|s|^2\} = 1$ and $E\{|z^{(1)}|^2\} = 1$. Concurrently, the eavesdropper will receive

$$y_E^{(1)} = \sqrt{P_s} f_E s + \sqrt{P_J^{(1)}} q_E z^{(1)} + n_E^{(1)}, \tag{2}$$

where $n_E^{(1)}$ is the additive noise at the eavesdropper.

In phase II, the $N-1$ relay nodes do a distributed beamforming to forward the received signal to the destination. The transmitted signal $\boldsymbol{x}_R \triangleq [x_{R,1}, x_{R,2}, \cdots, x_{R,N-1}]$ is

$$\boldsymbol{x}_R = \boldsymbol{W}\boldsymbol{y}_R, \tag{3}$$

where $\boldsymbol{W}$ is the weight matrix in the form of $\boldsymbol{W} = \text{diag}([w_1^*, w_2^*, \cdots, w_{N-1}^*])$, and diag is a diagonal matrix. Due to the individual power constraint of each relay node, we should have $E\{|x_{R,n}|^2\} \leq \bar{P}_n, n = 1, \cdots, N-1$.

Concurrently, the jammer transmits interference signal again as $z^{(2)}$ with power $P_J^{(2)}$. The received signals at the destination $\mathbb{D}$ and the eavesdropper $\mathbb{E}$ are, respectively:

$$y_D = \sqrt{P_s}\boldsymbol{g}_R^T\boldsymbol{W}\boldsymbol{f}_R s + \sqrt{P_J^{(1)}}\boldsymbol{g}_R^T\boldsymbol{W}\boldsymbol{h}_R z^{(1)} + \bar{n}_D, \tag{4}$$

$$y_E^{(2)} = \sqrt{P_s}\boldsymbol{c}_E^T\boldsymbol{W}\boldsymbol{f}_R s + \sqrt{P_J^{(1)}}\boldsymbol{c}_E^T\boldsymbol{W}\boldsymbol{h}_R z^{(1)} + \bar{n}_E^{(2)}, \tag{5}$$

where $\bar{n}_D \triangleq \sqrt{P_J^{(2)}} g_J z^{(2)} + \boldsymbol{g}_R^T\boldsymbol{W}\boldsymbol{n}_R + n_D$, $\bar{n}_E^{(2)} \triangleq \sqrt{P_J^{(2)}} q_E z^{(2)} + \boldsymbol{c}_E^T\boldsymbol{W}\boldsymbol{n}_R + n_E^{(2)}$, $\boldsymbol{c}_E \triangleq [c_{E,1}, c_{E,2}, \cdots, c_{E,N-1}]^T$. n_D, $n_E^{(2)}$ are additive noises at $\mathbb{D}$, $\mathbb{E}$ during phase II, respectively. (4) can be reformulated as

$$y_D = \sqrt{P_s}\boldsymbol{w}^H\boldsymbol{a}_{fg} s + \sqrt{P_J^{(1)}}\boldsymbol{w}^H\boldsymbol{a}_{gh} z^{(1)} + \bar{n}_D, \tag{6}$$

where $\boldsymbol{a}_{fg} \triangleq [f_{R,1}g_{R,1}, f_{R,2}g_{R,2}, \cdots, f_{R,N-1}g_{R,N-1}]^T$, and similarly for $\boldsymbol{a}_{gh}$, and $\boldsymbol{w} \triangleq [w_1, w_2, \cdots, w_{N-1}]^T$.

For the eavesdropper, each transmission phase grants it an opportunity to get the information. Combining (2) and (5) yields the receiving model of the eavesdropper in the whole procedure as

$$\boldsymbol{y}_E = \boldsymbol{H}_E s + \boldsymbol{n}_E, \tag{7}$$

where

$$\boldsymbol{H}_E = \begin{bmatrix} \sqrt{P_s} f_E \\ \sqrt{P_s}\boldsymbol{w}^H\boldsymbol{a}_{cf} \end{bmatrix}, \boldsymbol{n}_E = \begin{bmatrix} \bar{n}_E^{(1)} \\ \sqrt{P_J^{(1)}}\boldsymbol{c}_E^T\boldsymbol{W}\boldsymbol{h}_R z^{(1)} + \bar{n}_E^{(2)} \end{bmatrix}, \tag{8}$$

with $\boldsymbol{a}_{cf} \triangleq [c_{E,1}f_{R,1}, c_{E,2}f_{R,2}, c_{E,3}f_{R,3}, \cdots, c_{E,N-1}f_{R,N-1}]^T$, $\boldsymbol{a}_{cg} \triangleq [c_{E,1}g_{R,1}, c_{E,2}g_{R,2}, c_{E,3}g_{R,3}, \cdots, c_{E,N-1}g_{R,N-1}]^T$, and $\bar{n}_E^{(1)} = \sqrt{P_J^{(1)}} q_E z^{(1)} + n_E^{(1)}$. We assume that all the noise terms $n_D, n_E^{(1)}, n_E^{(2)}$, and $\boldsymbol{n}_R$ are zero-mean and time-spatially white independent complex Gaussian random variables with variance σ^2. We also assume that the jamming signals $z^{(1)}$ and $z^{(2)}$ are both complex Gaussian random variables.

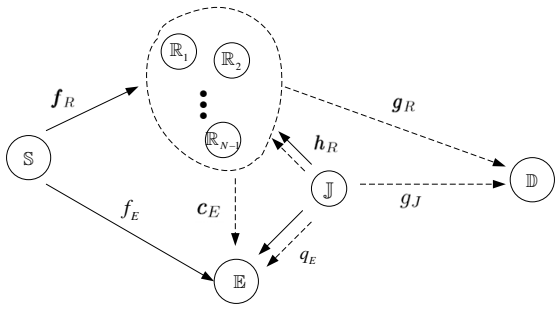

Fig. 1. The proposed joint security scheme, where the solid lines, and dash lines are the transmissions in phase I and II, respectively.

3. SECRECY SCHEME WITH EAVESDROPPER'S CSI

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

$$C_s = \max\left[I\left(y_D; s\right) - I\left(\boldsymbol{y}_E; s\right)\right]^+, \tag{9}$$

where $[a]^+ = \max(0, a)$, and $I(\cdot,\cdot)$ is the mutual information. Specifically, since the eavesdropper sees an equivalent 1×2 SIMO system, it can do maximum ratio combination (MRC) so we have $I\left(y_D; s\right)$ and $I\left(\boldsymbol{y}_E; s\right)$ at the top of the next page with $\boldsymbol{R}_{ff} \triangleq \text{diag}(|f_{R,1}|^2, |f_{R,2}|^2, \cdots, |f_{R,N-1}|^2)$, and similar for $\boldsymbol{R}_{gg}$, and $\boldsymbol{R}_{cc}$, respectively, $\boldsymbol{R}_{fg} \triangleq \boldsymbol{a}_{fg}\boldsymbol{a}_{fg}^H$, and similar for $\boldsymbol{R}_{cf}$, $\boldsymbol{R}_{gh}$, $\boldsymbol{R}_{ch}$. We hope to achieve the maximum secrecy rate by searching the optimal $\boldsymbol{w}$, $P_J^{(1)}$, and $P_J^{(2)}$ (We assume that P_s is fixed).

However, it can be shown that the objective function is a product of two correlated generalized Rayleigh quotients problem. Furthermore, there are multiplicative terms of the arguments in the objective function, such as $P_J^{(1)}\boldsymbol{w}^H$, $P_J^{(1)}P_J^{(2)}$, which makes the problem more difficult to solve. In the following, we propose a suboptimal secure scheme assuming the eavesdropper's CSI is known. It corresponds to the case when the "eavesdropper" is actually a legitimate but not the target user.

Observing (9)-(11) we can see that we hope to increase $I\left(y_D; s\right)$ as large as possible while keeping $I\left(\boldsymbol{y}_E; s\right)$ as small as possible. Therefore, we can do the following.

a) Design $\boldsymbol{w}$ in the null space of $\boldsymbol{a}_{cf}$ to completely eliminate the information leakage in phase II, i.e., let $\boldsymbol{\omega}^H\boldsymbol{a}_{cf} = 0$ so that the second row of $\boldsymbol{H}_E$ in (8) can be eliminated;

b) Design $\boldsymbol{w}$ in the null space of $\boldsymbol{a}_{gh}$ to eliminate the interference to the destination by the jamming signal in phase I, i.e., $\boldsymbol{\omega}^H\boldsymbol{a}_{gh} = 0$ (it has been forwarded by the relay nodes in phase II);

c) Since no information leakage happens in phase II (by a)), the jammer should stop sending interference so that $\mathbb{D}$ will not be jammed in phase II, i.e., $P_J^{(2)} = 0$.

With all these considerations, (10)-(11) can be re-written as

$$I\left(y_D; s\right) = \frac{1}{2}\log\left(1 + \frac{P_s}{\sigma^2}\frac{\boldsymbol{w}^H\boldsymbol{R}_{fg}\boldsymbol{w}}{1 + \boldsymbol{w}^H\boldsymbol{R}_{gg}\boldsymbol{w}}\right), \tag{12}$$

$$I\left(\boldsymbol{y}_E; s\right) = \frac{1}{2}\log\left(1 + \frac{P_s|f_E|^2}{\sigma^2 + P_J^{(1)}|q_E|^2}\right). \tag{13}$$

We can see (13) is only related to $P_J^{(2)}$, and to make information leakage as small as possible, we should let $P_J^{(1)} = \bar{P}_J$ where $\bar{P}_J$

$$I\left(y_D;s\right)=\frac{1}{2}\log\left(1+\frac{P_s\boldsymbol{w}^H\boldsymbol{R}_{fg}\boldsymbol{w}}{\sigma^2(1+\boldsymbol{w}^H\boldsymbol{R}_{gg}\boldsymbol{w})+P_J^{(1)}\boldsymbol{w}^H\boldsymbol{R}_{gh}\boldsymbol{w}+P_J^{(2)}|g_J|^2}\right), \tag{10}$$

$$I\left(\boldsymbol{y}_E;s\right)=\frac{1}{2}\log\left(1+\frac{P_s|f_E|^2}{\sigma^2+P_J^{(1)}|q_E|^2}+\frac{P_s\boldsymbol{w}^H\boldsymbol{R}_{cf}\boldsymbol{w}}{\sigma^2+\boldsymbol{w}^H\left(P_J^{(1)}\boldsymbol{R}_{ch}+\sigma^2\boldsymbol{R}_{cc}\right)\boldsymbol{w}+P_J^{(2)}|q_E|^2}\right), \tag{11}$$

is the maximum power constraint of the jammer. Then $I\left(\boldsymbol{y}_E;s\right)$ is fixed so the objective now is to maximize $I\left(y_D;s\right)$ over $\boldsymbol{w}$ under the conditions of a), b), and the individual power constraint. The consumed power of each relay node is

$$\begin{aligned}&E\{|x_{R,n}|^2\}\\=&E\left\{\left|w_n^*\left(\sqrt{P_s}f_{R,n}s+\sqrt{P_J^{(1)}}h_{R,n}z^{(1)}+n_{R,n}\right)\right|^2\right\}\\=&\left[\boldsymbol{w}\boldsymbol{w}^H\right]_{n,n}[\boldsymbol{T}]_{n,n},n=1,2,\cdots,N-1\end{aligned} \tag{14}$$

where $\boldsymbol{T}\triangleq P_s\boldsymbol{R}_{ff}+\bar{P}_J\boldsymbol{R}_{hh}+\sigma^2\boldsymbol{I}$, and $[\cdot]_{m,n}$ is the (m,n)-th element of a matrix. Mathematically, our optimization problem can be expressed as

$$\begin{aligned}\max_{\boldsymbol{w}}\quad&\frac{P_s}{\sigma^2}\frac{\boldsymbol{w}^H\boldsymbol{R}_{fg}\boldsymbol{w}}{1+\boldsymbol{w}^H\boldsymbol{R}_{gg}\boldsymbol{w}},\\ s.t.\quad&\boldsymbol{w}^H\boldsymbol{a}_{cf}=0,\quad\boldsymbol{w}^H\boldsymbol{a}_{gh}=0,\\&\left[\boldsymbol{w}\boldsymbol{w}^H\right]_{n,n}[\boldsymbol{T}]_{n,n}\le\bar{P}_n,\ n=1,2,\cdots,N-1.\end{aligned} \tag{15}$$

Let $\boldsymbol{H}\triangleq[\boldsymbol{a}_{cf},\boldsymbol{a}_{gh}]$, and $\boldsymbol{H}_\perp$ is the projection matrix onto the null space of $\boldsymbol{H}$. Then the equation constraint can be transformed into $\boldsymbol{w}=\boldsymbol{H}_\perp\boldsymbol{v}$ where $\boldsymbol{v}$ is any vector. Substituting this into (15) yields

$$\begin{aligned}\max_{\boldsymbol{v}}\quad&\frac{\boldsymbol{v}^H\bar{\boldsymbol{R}}_{fg}\boldsymbol{v}}{1+\boldsymbol{v}^H\bar{\boldsymbol{R}}_{gg}\boldsymbol{v}},\\ s.t.\quad&\left[\boldsymbol{H}_\perp\boldsymbol{v}\boldsymbol{v}^H\boldsymbol{H}_\perp^H\right]_{n,n}[\boldsymbol{T}]_{n,n}\le\bar{P}_n/\left[\boldsymbol{T}\right]_{n,n},\end{aligned} \tag{16}$$

where $\bar{\boldsymbol{R}}_{fg}\triangleq\boldsymbol{H}_\perp^H\boldsymbol{R}_{fg}\boldsymbol{H}_\perp$, and $\bar{\boldsymbol{R}}_{gg}\triangleq\boldsymbol{H}_\perp^H\boldsymbol{R}_{gg}\boldsymbol{H}_\perp$.

We can see that without the individual power constraint, this is a Rayleigh quotient problem and can be elegantly solved by taking the generalized eigenvalue decomposition (GED) of a matrix pair $(\bar{\boldsymbol{R}}_{fg},\bar{\boldsymbol{R}}_{gg})$. However, under individual power constraint, this does not work any more. To address this, we transform (16) into an equivalent form

$$\begin{aligned}\max_{\boldsymbol{v},t}\quad&t\\ s.t.\quad&\boldsymbol{v}^H\bar{\boldsymbol{R}}_{fg}\boldsymbol{v}\ge t\left(1+\boldsymbol{v}^H\bar{\boldsymbol{R}}_{gg}\boldsymbol{v}\right),\\&\left[\boldsymbol{H}_\perp\boldsymbol{v}\boldsymbol{v}^H\boldsymbol{H}_\perp^H\right]_{n,n}\le\bar{P}_n/\left[\boldsymbol{T}\right]_{n,n},\end{aligned} \tag{17}$$

Note that now the problem (17) is quasi-convex. In fact, for any fixed t, the feasible set in (17) is convex. To see this, we rewrite (17) as

$$\begin{aligned}\max_{\boldsymbol{v},t}\quad&t\\ s.t.\quad&\left\|\begin{array}{c}\sqrt{\boldsymbol{R}_{gg}}\boldsymbol{H}_\perp\boldsymbol{v}\\1\end{array}\right\|^2\le\frac{1}{t}|\boldsymbol{v}^H\bar{\boldsymbol{a}}_{fg}|^2,\\&\left|\boldsymbol{H}_\perp^{(n)}\boldsymbol{v}\right|\le\sqrt{\bar{P}_n/\left[\boldsymbol{T}\right]_{n,n}},n=1,2,\cdots,N-1,\end{aligned} \tag{18}$$

where $\bar{\boldsymbol{a}}_{fg}\triangleq\boldsymbol{H}_\perp^H\boldsymbol{a}_{fg}$, $\boldsymbol{H}_\perp^{(n)}$ is the n-th row of $\boldsymbol{H}_\perp$, and $\sqrt{\boldsymbol{R}_{gg}}$ means taking the element-wise square root of $\boldsymbol{R}_{gg}$. Note that the constraint functions are based on Euclidean vector norm. Multiplying the optimal $\boldsymbol{v}^o$ by an arbitrary phase shift $e^{j\phi}$ will not affect the constraints. Thus we can assume that $\boldsymbol{v}^H\bar{\boldsymbol{a}}_{fg}$ is a positive real number, without loss of generality. Therefore, when t is fixed, the first constraint is a second-order convex cone, and the second constraint is always an ellipsoid, both of which are convex.

Based on this observation, for any given $t>0$, if the following convex feasibility problem

$$\begin{aligned}\text{find}\quad&\boldsymbol{v}\\ s.t.\quad&\left\|\begin{array}{c}\sqrt{\boldsymbol{R}_{gg}}\boldsymbol{H}_\perp\boldsymbol{v}\\1\end{array}\right\|^2\le\frac{1}{t}|\boldsymbol{v}^H\bar{\boldsymbol{a}}_{fg}|^2,\\&\left|\boldsymbol{H}_\perp^{(n)}\boldsymbol{v}\right|\le\sqrt{\bar{P}_n/\left[\boldsymbol{T}\right]_{n,n}},n=1,2,\cdots,N-1,\end{aligned} \tag{19}$$

is feasible, it means t has not reached its maximum $t_{\max}$, i.e., $t<t_{\max}$. Conversely, if the problem (19) is not feasible, we have $t>t_{\max}$. The feasibility problem (19) is an SOCP [12] problem. Due to the convexity, the optimal $\boldsymbol{v}^o$ is unique and global, which can be efficiently solved using interior point methods [12].

Therefore, we can solve the quasi-convex problem (18) using bisection method. Starting with an interval $[0,\bar{t}_{\max}]$ known to contain the optimal value, we solve (19) at its midpoint to determine whether the optimal value is larger or smaller. We shrink the interval until the required precision is met. The algorithm is shown in Tab. I, where $\bar{t}_{\max}$ can be obtained by solving (16) using GED, ignoring the power constraints. After we get $\max I\left(y_D;s\right)$, we calculate the achievable secrecy rate under the proposed scheme according to (9).

The Selection of the Jammer: Since the information leakage can be completely eliminated in phase II while the security in phase I depends only on the jamming level, to improve the security further, we can select the node with the largest $|q_E|^2$ as the jammer.

4. 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 σ^2 is normalized to be at 0dBm and P_s is fixed as 10dBm. We use CVX toolbox [13] to solve the SOCP problem.

In Fig. 2, we compare the achievable secrecy rate of the proposed joint beamforming and jamming scheme with the scheme using all N nodes to do null-space beamforming without jamming in phase I (labeled as "relay only" in the figure). We illustrate cases with different $N=8,12,16$, respectively. To make the comparison fair, the x-axis is the total power consumed by all the relay nodes and the jammer, and each node has the equal individual power constraint $\bar{P}_n=P_M/N,n=1,2,\cdots,N$. We can see in the joint scheme, the jammer plays an important role in phase I and greatly reduces the information leakage so the secrecy has been significantly improved. Also we can see although the total power is equal, as N increases,

Table 1. The proposed algorithm

- Initialize $t_{low} = 0$, $t_{up} = \bar{t}_{\max}$.
- Repeat the following until $t_{up} - t_{low} < \varepsilon$.

1) Set $t \leftarrow \frac{1}{2}(t_{low} + t_{up})$.

2) Solve SOCP problem (19) with t using interior point method.

3) Update t: If (19) is feasible, set $t_{low} = t$; otherwise, $t_{up} = t$.

the achievable secrecy rate increases as well. This is obviously due to the power gain provided by the more relay nodes.

In Fig. 3, we illustrate the advantage of the jammer selection. The x-axis is still the total power and each node has the equal individual power constraint. We can see the jammer selection improves the secrecy rate further. However, as the total power increases, the improvement gets smaller. This is also reasonable since with more power, the function of jammer selection becomes insignificant.

5. CONCLUSION

In this paper, we propose a joint null-space beamforming and jamming scheme to enhance the security of an AF cooperative relay network so that both two phases of the cooperative transmissions are well protected. Subjected to the more practical individual power constraint, we optimize the secrecy rate of the system using bisection method and SOCP convex optimization techniques. We show the security of the joint scheme is greatly improved compared to the conventional relay only scheme.

The scheme can be generalized to the scenarios when the eavesdropper has more than one antennas, or when more intermediate nodes are used as jammers, which will be investigated in the future.

6. REFERENCES

[1] 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.

[2] J. Zhang, M. C. Gursoy, "Collaborative relay beamforming for secure broadcasting," in *Proc. IEEE WCNC*, pp.1-6, Princeton, NJ, Apr. 2010.

[3] J. Zhang, M. C. Gursoy, "Relay beamforming strategies for physical-layer security," in *Proc. CISS*, pp.1-6, Syndeney, Australia, Mar. 2010.

[4] M. Bloch, J. Barros, J. P. Vilela, and S. W. McLaughlin, "Friendly jamming for wireless secrecy," in *IEEE ICC*, Cape Town, South Africa, 2010.

[5] 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

[6] G. Zheng, L.-C. Choo, K.-K. Wong, "Optimal cooperative jamming to enhance physical layer security using relays," *IEEE Trans. Signal Process.*, vol.59, no.3, pp.1317-1322, Mar. 2011

[7] J. Huang, A. L. Swindlehurst, "Cooperative jamming for secure communications in MIMO relay networks," *IEEE Trans. Signal Process.*, vol.59, no.10, pp.4871-4884, Oct. 2011

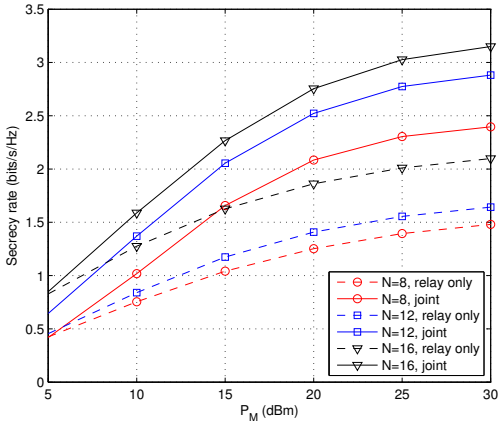

Fig. 2. Comparisons of the proposed and the relay only schemes.

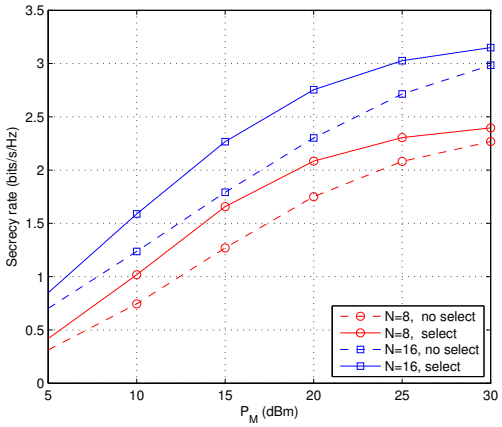

Fig. 3. The improvement of jammer selection.

[8] A. Mukherjee and A. L. Swindlehurst, "Securing multi-antenna two-way relay channels with analog network coding against eavesdroppers," in *Proc. 11th IEEE SPAWC*, Jun. 2010.

[9] H.-M. Wang, Q. Yin, and X.-G. Xia, "Distributed beamforming for physical-layer security of two-way relay networks, " *IEEE Trans. Signal Process.*, vol.60, no.7, pp.3532-3545, Jul. 2012.

[10] J. Chen, R. Zhang, L. Song, et al, "Joint relay and jammer selection for secure two-way relay networks," in *Proc. IEEE ICC*, Jun. 2011.

[11] J. Chen, L. Song, Z. Han, et al, "Joint relay and jammer selection for secure decode-and-forward two-way relay communications," in *Proc. GLOBECOM*, Houston, TX, Dec. 2011.

[12] S. Boyd and L. Vandenberghe, *Convex Optimization*. Cambridge, U.K.: Cambridge Univ. Press, 2004.

[13] G. Michael and B. Stephen, "CVX Users' Guide for CVX ver. 1.21." http://cvxr.com/, April 2011.