Joint Cooperative Beamforming, Jamming and Power Allocation to Secure AF Relay Systems

Hui-Ming Wang, *Member, IEEE*, Feng Liu, and Mengchen Yang

***Abstract*—The idea of multi-user (nodes) cooperation is an efficient way to improve the physical-layer security of a wireless transmission in the presence of passive eavesdroppers. However, due to the half-duplex constraint of the practical transceivers, *two* phases are required for one round of data transmission, which grants the eavesdroppers two opportunities to wiretap the information. Therefore, protecting the data transmissions in *both* phases is critical. Towards this end, we propose a *joint* cooperative beamforming, jamming and power allocation scheme to enhance the security of an amplify-and-forward (AF) cooperative relay network in this correspondence. Different from the existing works assuming that the source node always uses its total power, we show that the secrecy rate is a quasi-concave function of the power of the source node so that allocating its total power may not be optimal. The beamformer design and power optimization problem can be solved by a bisection method together with a generalized eigenvalue decomposition, which has a semi-closed form and is computationally very convenient. Simulations show the joint scheme greatly improves the security.**

I. Introduction

Exploiting multiple-nodes cooperation to improve the physical layer security of wireless communications has attracted increasing interest very recently [1]-[15]. For a cooperative system where all terminals are 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 [1]-[5] helps to improve the channel quality to the legitimate destination, while cooperative jamming (also called artificial noise) degrades the channel condition of the eavesdroppers [6]-[10]. 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). This grants the potential eavesdroppers two opportunities to intercept the information. Therefore, protecting the data transmissions in *both* phases is critical to guarantee the security of the data transmission.

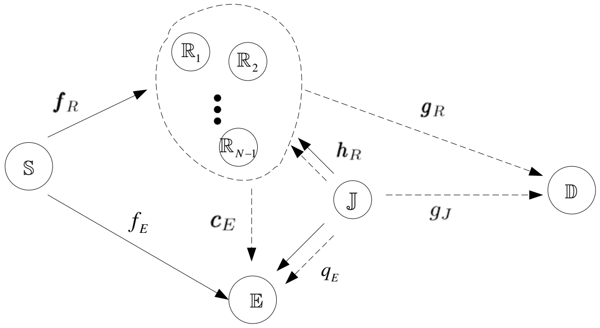

Fig. 1. Joint cooperative beamforming and jamming scheme, where the solid lines, and dash lines are the transmissions in phase I and II, respectively.

However, most previous works only consider to take cooperative beamforming or jamming in phase II to protect the transmission [1]-[5]. In phase I, they assume that the source node broadcasts with its total power and all the relay nodes listen. Some even simply assume that the transmission in phase I is perfectly secured [2], [3], [10], which is obviously over optimistic. In our previous works [12]-[13], we already have shown that the joint cooperative beamforming and jamming in both phases will greatly improve the secrecy rate. However, power allocation of the source node has still not been considered.

In this correspondence, we aim to enhance the security of an amplify-and-forward (AF) cooperative relay network. Based on the joint cooperative beamforming and jamming scheme in [12], we optimize the power allocation of the source node to improve the secrecy rate further. We show that the secrecy rate is a quasi-concave function of the transmission power of the source node so that allocating its total power may even harm the secrecy. This is intuitively reasonable since increasing the source transmission power will increase both the rate to the legitimate destination and that to the eavesdropper. Therefore, the power allocation should balance these two effects. The beamformer design and power optimization problem can be solved by a bisection method together with a generalized eigenvalue decomposition, which has a semi-closed form and is computationally very convenient. Simulations show the joint scheme greatly improves the security.

II. System Model

We consider an AF wireless network in which a source $\mathbb{S}$ wants to send information to the destination $\mathbb{D}$ under the

† The authors are with the School of Electronic and Information Engineering, and also with the MOE Key Lab for INNS, Xi'an Jiaotong University, Xi'an, 710049, Shaanxi, P. R. China. Email: xjbswhm@gmail.com. This work was partially supported by the NSFC under Grants No. 61102081, and No. 61221063, the Specialized Research Fund for the Doctoral Program of Higher Education of China under Grant 20110201120013, the New Century Excellent Talents Support Fund of China under Grant NCET-13-0458, the Industrial Research Fund of Shaanxi Province under Grant 2012GY2-28, the Fok Ying Tong Education Foundation under Grant 141063, and the Fundamental Research Funds for the Central University under Grant No. 2013jdgz11.

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 that there is no direct connection between $\mathbb{S}$ and $\mathbb{D}$. Our joint beamforming and jamming scheme is to divide the intermediate nodes into two groups: one node is jammer $\mathbb{J}$ and all the other $N-1$ are relay nodes, as shown in Fig. 1. The relay nodes will forward the received signal using cooperative beamforming, and the jammer transmits interference signals to confuse the eavesdropper. The quasi-stationary flat-fading channels between $\mathbb{S}$, $\mathbb{R}$, $\mathbb{J}$ and $\mathbb{E}$ are also shown in Fig. 1.

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 listen 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 $\boldsymbol{y}_R \triangleq [y_{R,1}, y_{R,2}, \cdots, y_{R,N-1}]^T$, $\boldsymbol{f}_R \triangleq [f_{R,1}, f_{R,2}, \cdots, f_{R,N-1}]^T$, and similarly for $\boldsymbol{h}_R$, P_s, and $P_J^{(1)}$ are the transmit powers of the source 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 also receive the signal

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

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 $\boldsymbol{x}_R = \boldsymbol{W}\boldsymbol{y}_R$, where $\boldsymbol{W}$ is the weight matrix in the form of $\boldsymbol{W} = \text{diag}([w_1^*, w_2^*, \cdots, w_{N-1}^*])$, and $\text{diag}(\cdot)$ is a diagonal matrix. 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:

$$y_D = \sqrt{P_s}\boldsymbol{g}_R^T \boldsymbol{W}\boldsymbol{f}_R s + \sqrt{P_J^{(1)}}\boldsymbol{g}_R^T \boldsymbol{W}\boldsymbol{h}_R z^{(1)} + \bar{n}_D, \tag{3}$$

$$y_E^{(2)} = \sqrt{P_s}\boldsymbol{c}_E^T \boldsymbol{W}\boldsymbol{f}_R s + \sqrt{P_J^{(1)}}\boldsymbol{c}_E^T \boldsymbol{W}\boldsymbol{h}_R z^{(1)} + \bar{n}_E^{(2)}, \tag{4}$$

where $\bar{n}_D \triangleq \sqrt{P_J^{(2)}} g_J z^{(2)} + \boldsymbol{g}_R^T \boldsymbol{W}\boldsymbol{n}_R + n_D$, and $\bar{n}_E^{(2)} \triangleq \sqrt{P_J^{(2)}} q_E z^{(2)} + \boldsymbol{c}_E^T \boldsymbol{W}\boldsymbol{n}_R + n_E^{(2)}$, respectively. $\boldsymbol{c}_E \triangleq [c_{E,1}, c_{E,2}, \cdots, c_{E,N-1}]^T$ and n_D, $n_E^{(2)}$ are additive noises at $\mathbb{D}$, $\mathbb{E}$ during phase II, respectively. (3) can be reformulated as

$$y_D = \sqrt{P_s}\boldsymbol{w}^H \boldsymbol{a}_{fg} s + \sqrt{P_J^{(1)}}\boldsymbol{w}^H \boldsymbol{a}_{gh} z^{(1)} + \bar{n}_D, \tag{5}$$

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 (4) yields the receiving model of the eavesdropper in the whole procedure as

$$\boldsymbol{y}_E = \boldsymbol{H}_E s + \boldsymbol{n}_E, \tag{6}$$

where

$$\begin{aligned} \boldsymbol{H}_E &= \begin{bmatrix} \sqrt{P_s} f_E \\ \sqrt{P_s}\boldsymbol{w}^H \boldsymbol{a}_{cf} \end{bmatrix}, \\ \boldsymbol{n}_E &= \begin{bmatrix} \bar{n}_E^{(1)} \\ \sqrt{P_J^{(1)}}\boldsymbol{c}_E^T \boldsymbol{W}\boldsymbol{h}_R z^{(1)} + \bar{n}_E^{(2)} \end{bmatrix}, \end{aligned} \tag{7}$$

with $\boldsymbol{a}_{cf} \triangleq [c_{E,1}f_{R,1}, c_{E,2}f_{R,2}, \cdots, c_{E,N-1}f_{R,N-1}]^T$, $\boldsymbol{a}_{cg} \triangleq [c_{E,1}g_{R,1}, c_{E,2}g_{R,2}, \cdots, c_{E,N-1}g_{R,N-1}]^T$, 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.

III. Joint Secrecy Scheme with Optimal Power Allocation

The achievable *maximum secrecy rate* is the measurement of the physical layer security:

$$R_s = \max\left[I\left(y_D; s\right) - I\left(\boldsymbol{y}_E; s\right)\right]^+, \tag{8}$$

where $[a]^+ = \max(0, a)$, and $I(\cdot, \cdot)$ is the mutual information. In our considered problem, specifically, the destination and the eavesdropper see an equivalent SISO and 1×2 SIMO channel with correlated equivalent noise, respectively, so we have $I\left(y_D; s\right)$ and $I\left(\boldsymbol{y}_E; s\right)$ at the top of the next page, where $\boldsymbol{R}_{ff} \triangleq \text{diag}(|f_{R,1}|^2, |f_{R,2}|^2, \cdots, |f_{R,N-1}|^2)$, and similarly for $\boldsymbol{R}_{gg}$, and $\boldsymbol{R}_{cc}$, respectively, $\boldsymbol{R}_{fg} \triangleq \boldsymbol{a}_{fg}\boldsymbol{a}_{fg}^H$, and similarly 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 $P_J^{(2)}$, and P_s.

Remark: Most works only consider the fixed P_s case [2]-[13], i.e., the source node broadcasts its data with its total power[1]. However, we will show that this may harm the secrecy, and the power allocation should be optimized. We will find that this will further improve the secrecy rate of the system greatly, compared to the case utilizing all its power.

Substituting (9) and (10) into (8), it has been shown in [12] that the problem is a non-convex problem even with fixed P_s. When taking P_s as a new optimization argument, the problem will be more difficult to solve. Therefore, we propose a *heuristic* scheme to achieve a suboptimal but reasonably good solution. Observing (8)-(10) 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 (7) 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., $P_J^{(2)} = 0$.

[1] Although in [1] the authors have investigated the source power allocation problem, the proposed scheme is a "hill-climbing" method, which has no optimality guarantee.

$$I\left(y_D;s\right)=\frac{1}{2}\log\left(1+\frac{P_s\boldsymbol{w}^H\boldsymbol{R}_{fg}\boldsymbol{w}}{\sigma^2(1+\boldsymbol{w}^H\boldsymbol{R}_{gg}\boldsymbol{w})+P_J^{(1)}\boldsymbol{w}^H\boldsymbol{R}_{gh}\boldsymbol{w}+P_J^{(2)}|g_J|^2}\right), \tag{9}$$

$$I\left(\boldsymbol{y}_E;s\right)=\frac{1}{2}\log\det\left(\boldsymbol{I}+\boldsymbol{H}_E\boldsymbol{H}_E^H\boldsymbol{Q}_E^{-1}\right),\boldsymbol{Q}_E\triangleq\begin{bmatrix}\sigma^2+P_J^{(1)}|q_E|^2 & P_J^{(1)}q_E\boldsymbol{h}_R^H\boldsymbol{W}^H\boldsymbol{c}_E^*\\ P_J^{(1)}q_E^H\boldsymbol{c}_E^T\boldsymbol{W}\boldsymbol{h}_R & P_J^{(1)}\boldsymbol{c}_E^T\boldsymbol{W}\boldsymbol{h}_R\boldsymbol{h}_R^H\boldsymbol{W}^H\boldsymbol{c}_E^*\end{bmatrix}, \tag{10}$$

With all these considerations, (9)-(10) can be re-written as

$$I\left(y_D;s\right)=\frac{1}{2}\log\left(1+\frac{P_s}{\sigma^2}\frac{\boldsymbol{w}^H\boldsymbol{R}_{fg}\boldsymbol{w}}{1+\boldsymbol{w}^H\boldsymbol{R}_{gg}\boldsymbol{w}}\right), \tag{11}$$

$$I\left(\boldsymbol{y}_E;s\right)=\frac{1}{2}\log\left(1+\frac{P_s|f_E|^2}{\sigma^2+P_J^{(1)}|q_E|^2}\right). \tag{12}$$

We can see (12) is a decreasing function of $P_J^{(1)}$, and to make information leakage as small as possible, we should let $P_J^{(1)}=\bar{P}_J$ where $\bar{P}_J$ is the maximum power constraint of the jammer. Substituting (11) and (12) into (8) and after some simply manipulations, we obtain the optimization problem as

$$\begin{aligned}\max_{\boldsymbol{w},P_s}\quad & \frac{\sigma^2+P_s\frac{\boldsymbol{w}^H\boldsymbol{R}_{fg}\boldsymbol{w}}{1+\boldsymbol{w}^H\boldsymbol{R}_{gg}\boldsymbol{w}}}{a+bP_s},\\ s.t.\quad & \boldsymbol{w}^H\boldsymbol{a}_{cf}=0,\quad \boldsymbol{w}^H\boldsymbol{a}_{gh}=0,\\ & \boldsymbol{w}^H\boldsymbol{T}(P_s)\boldsymbol{w}\le P_R,\\ & P_s\le P_T,\end{aligned} \tag{13}$$

where $a\triangleq\sigma^2+\bar{P}_J|q_E|^2$, $b\triangleq|f_E|^2$, $\boldsymbol{T}(P_s)\triangleq P_s\boldsymbol{R}_{ff}+\bar{P}_J\boldsymbol{R}_{hh}+\sigma^2\boldsymbol{I}$, P_T is the source power constraint and P_R is the sum power constraint of the relay nodes.

The Selection of the Jammer: From (12), the leakage rate is inverse to the jamming level. To improve the security further, we can select the node with the largest $|q_E|^2$ as the jammer.

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 constraints can be transformed into $\boldsymbol{w}=\boldsymbol{H}_\perp\boldsymbol{v}$ where $\boldsymbol{v}$ is any vector. On the other hand, note that at the optimum, the power constraint $\boldsymbol{w}^H\boldsymbol{T}(P_s)\boldsymbol{w}\le P_R$ should be active, i.e., $\boldsymbol{w}^{oH}\boldsymbol{T}(P_s)\boldsymbol{w}^o=P_R$. This is because $\frac{\boldsymbol{w}^H\boldsymbol{R}_{fg}\boldsymbol{w}}{1+\boldsymbol{w}^H\boldsymbol{R}_{gg}\boldsymbol{w}}$ is an increasing function of the norm of $\boldsymbol{w}$. However, the objective function is not an increasing function of P_s, which implies that utilizing total power of the source may not be optimal. The problem (13) now becomes

$$\begin{aligned}\max_{\boldsymbol{v},P_s}\quad & \frac{\sigma^2+P_s\frac{\boldsymbol{v}^H\bar{\boldsymbol{R}}_{fg}\boldsymbol{v}}{1+\boldsymbol{v}^H\bar{\boldsymbol{R}}_{gg}\boldsymbol{v}}}{a+bP_s},\\ s.t.\quad & \boldsymbol{v}^H\bar{\boldsymbol{T}}(P_s)\boldsymbol{v}=P_R,\quad P_s\le P_T,\end{aligned} \tag{14}$$

where $\bar{\boldsymbol{R}}_{fg}\triangleq\boldsymbol{H}_\perp^H\boldsymbol{R}_{fg}\boldsymbol{H}_\perp$, $\bar{\boldsymbol{R}}_{gg}\triangleq\boldsymbol{H}_\perp^H\boldsymbol{R}_{gg}\boldsymbol{H}_\perp$, $\bar{\boldsymbol{T}}(P_s)\triangleq P_s\bar{\boldsymbol{R}}_{ff}+\bar{P}_J\bar{\boldsymbol{R}}_{hh}+\sigma^2\boldsymbol{I}$, $\bar{\boldsymbol{R}}_{ff}\triangleq\boldsymbol{H}_\perp^H\boldsymbol{R}_{ff}\boldsymbol{H}_\perp$, and $\bar{\boldsymbol{R}}_{hh}\triangleq\boldsymbol{H}_\perp^H\boldsymbol{R}_{hh}\boldsymbol{H}_\perp$. This problem can be decoupled into two concatenate subproblems as follows

$$\begin{aligned}\max_{P_s}\quad & \frac{\sigma^2+P_s\max_{\boldsymbol{v}}\left(\frac{\boldsymbol{v}^H\bar{\boldsymbol{R}}_{fg}\boldsymbol{v}}{1+\boldsymbol{v}^H\bar{\boldsymbol{R}}_{gg}\boldsymbol{v}}\right)}{a+bP_s},\\ s.t.\quad & \boldsymbol{v}^H\bar{\boldsymbol{T}}(P_s)\boldsymbol{v}=P_R,\quad P_s\le P_T,\end{aligned} \tag{15}$$

where the inner optimization is performed over $\boldsymbol{v}$ solely taking P_s as a constant, and the solution of which is a function of P_s (Note that P_s is an argument in $\bar{\boldsymbol{T}}(P_s)$), and the outer optimization problem is taken over P_s. Let's first focus on the inner optimization.

From the definition, $\bar{\boldsymbol{T}}(P_s)$ is a positive definite matrix, and there exists an invertible matrix $\boldsymbol{A}(P_s)$ satisfying $\boldsymbol{A}(P_s)^H\boldsymbol{A}(P_s)=\bar{\boldsymbol{T}}(P_s)$. Let $\bar{\boldsymbol{v}}\triangleq\frac{1}{\sqrt{P_R}}\boldsymbol{A}(P_s)\boldsymbol{v}$, and $\boldsymbol{v}=\sqrt{P_R}\boldsymbol{A}(P_s)^{-1}\bar{\boldsymbol{v}}$. Substituting $\bar{\boldsymbol{v}}$ into (15), we can rewrite the inner optimization as

$$\begin{aligned}\max_{\bar{\boldsymbol{v}}}\quad & \frac{\bar{\boldsymbol{v}}^H\boldsymbol{B}(P_s)\bar{\boldsymbol{v}}}{\bar{\boldsymbol{v}}^H\boldsymbol{D}(P_s)\bar{\boldsymbol{v}}},\\ s.t.\quad & \bar{\boldsymbol{v}}^H\bar{\boldsymbol{v}}=1,\end{aligned} \tag{16}$$

where $\boldsymbol{B}(P_s)=P_R\boldsymbol{A}(P_s)^{-H}\bar{\boldsymbol{R}}_{fg}\boldsymbol{A}(P_s)^{-1}$, and $\boldsymbol{D}(P_s)=\boldsymbol{I}+P_R\boldsymbol{A}(P_s)^{-H}\bar{\boldsymbol{R}}_{gg}\boldsymbol{A}(P_s)^{-1}$. Obviously, the optimization problem (16) is a generalized eigenvalue problem. The optimal value is the largest eigenvalue of $\boldsymbol{D}(P_s)^{-1}\boldsymbol{B}(P_s)$ achieved at the eigenvector associated with the largest eigenvalue. Mathematically, we have the optimal $\bar{\boldsymbol{v}}^o$ as

$$\bar{\boldsymbol{v}}^o=\alpha\mathcal{E}\left(\boldsymbol{D}(P_s)^{-1}\boldsymbol{B}(P_s)\right), \tag{17}$$

where α is a scalar to normalize $\bar{\boldsymbol{v}}^o$ to satisfy $\bar{\boldsymbol{v}}^{oH}\bar{\boldsymbol{v}}^o=1$, and $\mathcal{E}\left[\mathbf{X}\right]$ is one eigenvector of matrix $\mathbf{X}$ associated with the largest eigenvalue. Note that $\bar{\boldsymbol{R}}_{fg}$ is a rank-1 matrix, thus the matrix $\boldsymbol{B}(P_s)$ is rank-1 as well. Therefore, the matrix $\boldsymbol{D}(P_s)^{-1}\boldsymbol{B}(P_s)$ has only one nonzero eigenvalue, which is the largest one. Since equation (18) at the top of next page holds, where in the first equation we just substitute $\boldsymbol{B}(P_s)$ in and in the second equation we change the positions of the productions, the only nonzero eigenvalue is $\lambda\triangleq P_R\boldsymbol{a}_{fg}^H\boldsymbol{H}_\perp\boldsymbol{A}(P_s)^{-1}\boldsymbol{D}(P_s)^{-1}\boldsymbol{A}(P_s)^{-H}\boldsymbol{H}_\perp^H\boldsymbol{a}_{fg}$, and the associated eigenvector is $\mathcal{E}\left(\boldsymbol{D}(P_s)^{-1}\boldsymbol{B}(P_s)\right)=\boldsymbol{D}(P_s)^{-1}\boldsymbol{A}(P_s)^{-H}\boldsymbol{H}_\perp^H\boldsymbol{a}_{fg}$.

We now have

$$\alpha=\left|\left|\boldsymbol{D}(P_s)^{-1}\boldsymbol{A}(P_s)^{-H}\boldsymbol{H}_\perp^H\boldsymbol{a}_{fg}\right|\right|, \tag{19}$$

$$\boldsymbol{v}^o=\alpha\sqrt{P_R}\boldsymbol{A}(P_s)^{-1}\boldsymbol{D}(P_s)^{-1}\boldsymbol{A}(P_s)^{-H}\boldsymbol{H}_\perp^H\boldsymbol{a}_{fg}, \tag{20}$$

and the maximum objective function of (16) is

$$\begin{aligned}f(P_s)&\triangleq P_R\boldsymbol{a}_{fg}^H\boldsymbol{H}_\perp\boldsymbol{A}(P_s)^{-1}\boldsymbol{D}(P_s)^{-1}\boldsymbol{A}(P_s)^{-H}\boldsymbol{H}_\perp^H\boldsymbol{a}_{fg}\\ &=P_R\boldsymbol{a}_{fg}^H\boldsymbol{H}_\perp(\bar{\boldsymbol{T}}(P_s)+P_R\bar{\boldsymbol{R}}_{gg})^{-1}\boldsymbol{H}_\perp^H\boldsymbol{a}_{fg}.\end{aligned} \tag{21}$$

Substituting (21) into (15), we get the outer optimization

$$\begin{aligned}\max_{P_s}\quad & g(P_s)\triangleq\log\left(\frac{\sigma^2+h(P_s)}{a+bP_s}\right)\\ & \qquad=\log(\sigma^2+h(P_s))-\log(a+bP_s),\\ s.t.\quad & 0\le P_s\le P_T.\end{aligned} \tag{22}$$

where $h(P_s)\triangleq P_sf(P_s)=P_RP_s\boldsymbol{h}^H\boldsymbol{J}(P_s)\boldsymbol{h}$, $\boldsymbol{h}\triangleq\boldsymbol{H}_\perp^H\boldsymbol{a}_{fg}$, and $\boldsymbol{J}(P_s)\triangleq(P_s\bar{\boldsymbol{R}}_{ff}+\bar{P}_J\bar{\boldsymbol{R}}_{hh}+\sigma^2\boldsymbol{I}+P_R\bar{\boldsymbol{R}}_{gg})^{-1}$. The

$$\begin{aligned}&\left(\boldsymbol{D}(P_s)^{-1}\boldsymbol{B}(P_s)\right)\left(\boldsymbol{D}(P_s)^{-1}\boldsymbol{A}(P_s)^{-H}\boldsymbol{H}_\perp^H\boldsymbol{a}_{fg}\right)\\&=\boldsymbol{D}(P_s)^{-1}P_R\boldsymbol{A}(P_s)^{-H}\boldsymbol{H}_\perp^H\boldsymbol{a}_{fg}\left(\boldsymbol{a}_{fg}^H\boldsymbol{H}_\perp\boldsymbol{A}(P_s)^{-1}\boldsymbol{D}(P_s)^{-1}\boldsymbol{A}(P_s)^{-H}\boldsymbol{H}_\perp^H\boldsymbol{a}_{fg}\right)\\&=\left(P_R\boldsymbol{a}_{fg}^H\boldsymbol{H}_\perp\boldsymbol{A}(P_s)^{-1}\boldsymbol{D}(P_s)^{-1}\boldsymbol{A}(P_s)^{-H}\boldsymbol{H}_\perp^H\boldsymbol{a}_{fg}\right)\left(\boldsymbol{D}(P_s)^{-1}\boldsymbol{A}(P_s)^{-H}\boldsymbol{H}_\perp^H\boldsymbol{a}_{fg}\right).\end{aligned}\tag{18}$$

objective function is a difference of two logarithm functions, which is neither convex nor concave, and generally difficult to solve. However, in the following, we will show that it is a quasi-concave function of P_s. Towards this end, let us first evaluate the convexity of $h(P_s)$. The first and second derivatives of $h(P_s)$ to P_S are

$$\begin{aligned}h'(P_s)&=P_R\left(\boldsymbol{h}^H\boldsymbol{J}(P_s)\boldsymbol{h}-P_s\boldsymbol{h}^H\boldsymbol{J}^2(P_s)\bar{\boldsymbol{R}}_{ff}\boldsymbol{h}\right),\\h''(P_s)&=-2P_R\boldsymbol{h}^H\boldsymbol{J}^3(P_s)(\bar{P}_J\bar{\boldsymbol{R}}_{hh}+\sigma^2\boldsymbol{I}+P_R\bar{\boldsymbol{R}}_{gg})\bar{\boldsymbol{R}}_{ff}\boldsymbol{h},\end{aligned}\tag{23}$$

respectively. The detailed derivations are given in the appendix. Since $\boldsymbol{J}(P_s)$ is a positive definite matrix and so as to $\boldsymbol{J}^3(P_s)$, we have $h''(P_s)<0$, i.e., $h(P_s)$ is a concave function of P_s.

The first derivative of $g(P_s)$ is

$$\begin{aligned}g'(P_s)&=\frac{1}{\ln 2}\left(\frac{h'(P_s)}{\sigma^2+h(P_s)}-\frac{b}{a+bP_s}\right)\\&=\frac{(a+bP_s)h'(P_s)-b\sigma^2-bh(P_s)}{\ln 2(\sigma^2+h(P_s))(a+bP_s)}.\end{aligned}\tag{24}$$

Note that $f(P_s)$ is the non-zero eigenvalue of a rank 1 positive semi-definite matrix, it is obvious that $f(P_s)\geq 0$, and then $h(P_s)\geq 0$. Recalling that $a>0$ and $b\geq 0$, the denominator of (24) is always positive in the range of P_s. Therefore, the positivity-negativity of $g'(P_s)$ depends on the numerator only. Let $m(P_s)=(a+bP_s)h'(P_s)-b\sigma^2-bh(P_s)$. Since $h(P_s)$ is a real polynomial function of P_s, it is continuous and its first derivative is $m'(P_s)=bh'(P_s)+(a+bP_s)h''(P_s)-bh'(P_s)=(a+bP_s)h''(P_s)<0$ due to $h''(P_s)<0$. This indicates that the numerator $m(P_s)$ is a strictly decreasing function. The positivity-negativity of $g'(P_s), P_s\in[0,P_T]$ has the following cases.

If $m(0)\leq 0$, then $g'(P_s)$ is always negative, and the maximum objective value is $g(0)=\log\left(\frac{\sigma^2}{a}\right)<0$, which suggests that the secrecy rate is 0 and it is impossible to communicate safely.

If $m(P_T)\geq 0$, then $g'(P_s)$ is always positive so that $g(P_s)$ is an increasing function, and the maximum happens to be $g(P_T)$.

Finally, if $m(0)>0$ and $m(P_T)<0$, which implies that $g'(0)>0$, and $g'(P_T)<0$. Since $m(P_s)$ is a strictly decreasing continuous real function, there must be a unique point, say $P_c\in(0,P_s)$, such that $m(P_c)=0$, and for $P_s\leq P_c$, $m(P_s)>0$ and for $P_s\geq P_c$, $m(P_s)<0$. Then we conclude that for $P_s\leq P_c$, $g(P_s)$ is strictly increasing and for $P_s\geq P_c$, $g(P_s)$ is strictly decreasing. According to the definition [17], $g(P_s)$ is a quasi-concave function P_s. In this situation, $P_s=P_c$ achieves the maximum $g(P_c)$ of the problem (22). Since P_c is the unique real root of the equation $m(P_s)=0$, we can calculate P_c by using the bisection method.

From the above discussion, we can see that the optimal P_s depends on the positivity-negatively of $m(0)$, and $m(P_T)$.

TABLE I
PROPOSED ALGORITHM

- Power allocation:
  - · Calculate $m(0)$ and $m(P_T)$.
  - · If $m(0)\leq 0$, set $P_s^o=0$.
  - · Else if $m(P_T)\geq 0$, set $P_s^o=P_T$.
  - · Otherwise, use bisection method to solve $m(P_c)=0$ and find $P_s^o=P_c>0$.
- Beamfomrer design:
  - · Substitute the obtained P_s^o into (20) to obtain $\boldsymbol{v}^o$ and $\boldsymbol{w}^o=\boldsymbol{H}_\perp\boldsymbol{v}^o$.
- Secrecy rate calculation:
  - · Substitute the so obtained P_s^o and $\boldsymbol{w}^o$ into (11) and (12) to get the secrecy rate.

Only when $m(P_T)\geq 0$, allocating the total power of the source is optimal. In the case that $m(0)>0$ and $m(P_T)<0$, only a part of its total power should be allocated. This can be intuitively explained as follows. Since the legitimate channel from the source to the destination is a two hop relay channel, both the power P_s and P_R will impact the secrecy rate. From a traditional two hop AF relay network without security consideration, we know that if P_R is fixed, increasing P_s will first increase the rate but it will achieve a limit and will not increase any more no matter how large the P_s is since then the fixed P_R becomes a bottleneck of the two hop channel, as shown by the authors in [16]. In the security transmission of the AF two hop network, however, increasing P_s too much not only will not increase the rate of the legitimate channel but will increase the leakage rate to the eavesdropper (from (12)), and thus harms the secrecy rate. This is the reason that P_s should not always be the maximal available power P_T.

After the optimal $P_s^o=P_c$ has been obtained, the optimal cooperative beamformer $\boldsymbol{w}^o$ has a closed-form $\boldsymbol{w}^o=\boldsymbol{H}_\perp\boldsymbol{v}^o$ where $\boldsymbol{v}^o$ is in the form of (20). Finally, we substitute the so obtained P_s^o and $\boldsymbol{w}^o$ into (11) and (12) to get the secrecy rate. We summarize the whole algorithm in Tab. I.

IV. 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. 5000 Monte Carlo runs were done for each point in the figures. The jammer power

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TVT.2014.2370754, IEEE Transactions on Vehicular Technology

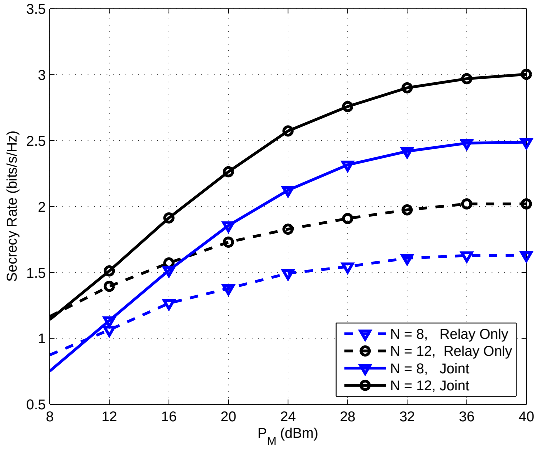

Fig. 2. Secrecy rate comparison of the proposed joint scheme and the relay only scheme.

$\bar{P}_J$ is assumed to be $\frac{P_R}{(N-1)}$, where N is the number of the intermediate nodes.

In Fig. 2, we illustrate the secrecy rate of the proposed joint optimization scheme, and compare it with the scheme where all N nodes do null-space beamforming in phase II without jamming in phase I (labeled as "Relay only" in the figure). We illustrate cases with different $N = 8, 12$, respectively. The total power of the source is $P_T = 10\text{dBm}$. The x-axis P_M is the total power consumed by all the relay nodes and the jammer $P_M = P_R + \bar{P}_J$. To make the comparison fair, for the "Relay only" scheme, N relay nodes have the same total power. We can see that as the total power increases, the secrecy rate of the proposed joint scheme has significant improvement to the "Relay only" scheme. This is because in the proposed joint scheme the jammer plays an important role and greatly reduces the information leakage in phase I while in the "Relay only" scheme, the transmission in phase I is revealed to the eavesdropper without any protection. Also we can see that although the total power is fixed, as N increases, the achievable secrecy rate increases as well. This is obviously due to the power gain provided by the more relay nodes.

Fig. 3 shows the secrecy rate enhancement of the optimized source power allocation (labeled as "Optimal P_s") to the total power allocation (labeled as "Full P_s") of the joint scheme. We illustrate the cases when $P_M = 10, 20, 30\text{dBm}$, respectively. It is obvious that when P_T is small, the optimal value of P_s should be the source power constraint P_T. As P_T being larger and larger, transmitting with the full power will harm the secrecy rate, which consists with the aforementioned interpretations. In this situation, increasing P_T will not increase the secrecy rate anymore, and the optimal P_s should be a constant, which leads to a fixed secrecy rate. Fig. 4 shows this enhancement versus the sum power P_M when $P_T = 10, 20, 30\text{dBm}$, respectively. We can find that when P_M is small, the secrecy rate of the "Optimal P_s" is larger, indicating that in this situation, using full source power is not the optimal choice. However, when P_M is large enough, the total power allocation is optimal.

In Fig. 5, we illustrate the advantage of the jammer selection. The x-axis is still the total power. We can see that selecting the node with the largest $|q_E|^2$ as the jammer improves the secrecy rate further. As the total power increases, the improvement gets smaller. This is also reasonable since with more power, the function of jammer selection becomes insignificant.

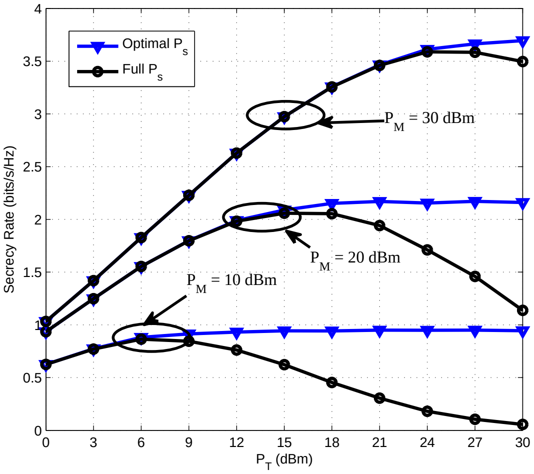

Fig. 3. Secrecy rate enhancement of the optimized source power allocation to the total power allocation of the joint scheme, where $P_M = 10, 20, 30\text{dBm}$.

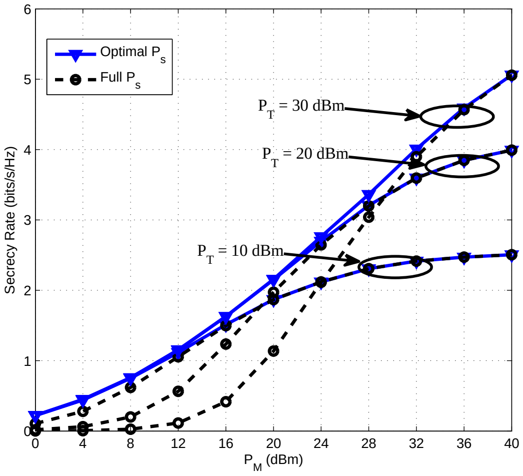

Fig. 4. Secrecy rate enhancement of the joint scheme versus the sum power P_M, where $P_T = 10, 20, 30\text{dBm}$.

V. Conclusions

In this correspondence we propose a joint cooperative beamforming, jamming and power allocation scheme to enhance the security of an AF cooperative relay network. The scheme takes both phases of the cooperative transmissions into protection, so that the secrecy rate will be greatly improved. We show that the secrecy rate is a quasi-concave function of the power of the source so that allocating its total power may not be optimal. The beamformer design and power optimization problem can be solved by a bisection method together with a generalized

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TVT.2014.2370754, IEEE Transactions on Vehicular Technology

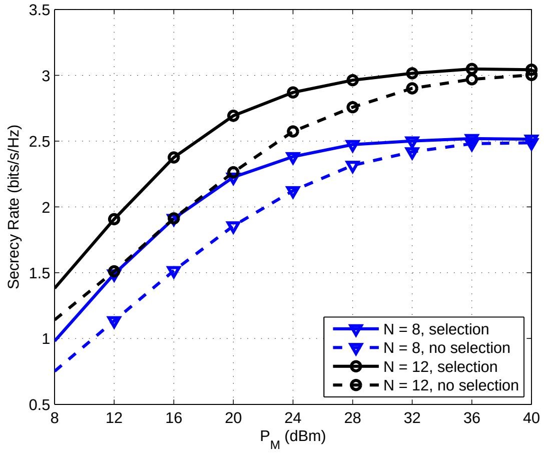

Fig. 5. The secrecy rate improvement of the jammer selection.

eigenvalue decomposition, which has a semi-closed form and is computationally very convenient.

Appendix

In the appendix, we will give the detailed derivation of (23). First, we have $h(P_s) = P_s f(P_s) = P_R P_s \boldsymbol{h}^H \boldsymbol{J}(P_s)\boldsymbol{h}$, and its first derivative is

$$\begin{aligned} h'(P_s) &= P_R \boldsymbol{h}^H \boldsymbol{J}(P_s)\boldsymbol{h} - P_R P_s \boldsymbol{h}^H \boldsymbol{J}'(P_s)\boldsymbol{h} \\ &= P_R \left(\boldsymbol{h}^H \boldsymbol{J}(P_s)\boldsymbol{h} - P_s \boldsymbol{h}^H \boldsymbol{J}^2(P_s)\bar{\boldsymbol{R}}_{ff}\boldsymbol{h}\right), \end{aligned}$$

where $\boldsymbol{J}^2(P_s) \triangleq \boldsymbol{J}(P_s)\boldsymbol{J}(P_s)$. The second derivative of $h(P_s)$ is

$$\begin{aligned} h''(P_s) &= P_R \left(\boldsymbol{h}^H \boldsymbol{J}'(P_s)\boldsymbol{h} - \boldsymbol{h}^H \boldsymbol{J}^2(P_s)\bar{\boldsymbol{R}}_{ff}\boldsymbol{h}\right) \\ &\quad - P_R \left(P_s \boldsymbol{h}^H (\boldsymbol{J}^2(P_s))'\bar{\boldsymbol{R}}_{ff}\boldsymbol{h}\right) \\ &= P_R \left(-2\boldsymbol{h}^H \boldsymbol{J}^2(P_s)\bar{\boldsymbol{R}}_{ff}\boldsymbol{h} + 2P_s \boldsymbol{h}^H \boldsymbol{J}^3(P_s)\bar{\boldsymbol{R}}_{ff}^2\boldsymbol{h}\right) \\ &= -2P_R \boldsymbol{h}^H \boldsymbol{J}^3(P_s)(\bar{P}_J \bar{\boldsymbol{R}}_{hh} + \sigma^2 \boldsymbol{I} + P_R \bar{\boldsymbol{R}}_{gg})\bar{\boldsymbol{R}}_{ff}\boldsymbol{h} \end{aligned}$$

where $\boldsymbol{J}^3(P_s) = \boldsymbol{J}(P_s)\boldsymbol{J}(P_s)\boldsymbol{J}(P_s)$, and $\bar{\boldsymbol{R}}_{ff}^2 = \bar{\boldsymbol{R}}_{ff}\bar{\boldsymbol{R}}_{ff}$.

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] 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.

[5] Y. Yang, Q. Li, W.-K. Ma, J. Ge, and P. C. Ching, "Cooperative secure beamforming for AF relay networks with multiple eavesdroppers," *IEEE Signal Process. Lett.*, vol.20, no.1, pp.35-39, Jan. 2013.

[6] M. Bloch, J. Barros, J. P. Vilela, and S. W. McLaughlin, "Friendly jamming for wireless secrecy," in *IEEE International Conference on Communications (ICC)*, Cape Town, South Africa, 2010.

[7] 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

[8] 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

[9] 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.

[10] K.-H. Park, T. Wang, and M.-S. Alouini, "On the jamming power allocation for secure amplify-and-forward relaying via cooperative jamming," *IEEE. J. Selec. Area. Commu.*, vol, 31, no. 9, pp. 1741-1750, Sept. 2013.

[11] Z. Ding, M. Peng, H.-H. Chen, "A general relaying transmission protocol for MIMO secrecy communications," *IEEE Trans. Commun.*, vol. 60, no. 11, pp. 3461-3471, Nov. 2012.

[12] H.-M. Wang, M. Luo, X.-G. Xia, and Q. Yin, "Joint cooperative beamforming and jamming to secure AF relay systems with individual power constraint and no eavesdropper's CSI, " *IEEE Signal Process. Lett.*, vol. 20, no. 1, pp. 39-42, Jan. 2013.

[13] H.-M. Wang, M. Luo, Q. Yin, and X.-G. Xia, "Hybrid cooperative beamforming and jamming for physical-layer security of two-way relay networks," *IEEE Trans. on Infor. Forensics & Secu.*, vol. 8, no. 12, pp. 2007-2020, Dec. 2013.

[14] H.-M. Wang, F. Liu, and X.-G. Xia, "Joint source-relay precoding and power allocation for secure amplify-and-forward MIMO relay networks," *IEEE Trans. on Infor. Forensics & Secu.*, vol. 9, no. 8, pp.1240-1250, Aug. 2014.

[15] M. Lin, J. Ge, and Y. Yang, "An effective secure transmission scheme for AF relay networks with two-hop information leakage," *IEEE Commun. Lett.*, vol. 17, no. 8, pp. 1676-1679, Aug. 2013.

[16] X. Tang and Y. Hua, "Optimal design of non-regenerative MIMO wireless relays," *IEEE Trans. Wireless Commun.*, vol. 6, no. 4, pp. 1398-1407, Apr. 2007.

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