Joint Cooperative Relaying and Jamming for Maximum Secrecy Capacity in Wireless Networks

Li Wang*, Chunyan Cao*, Mei Song* and Yu Cheng†
*Beijing Key Laboratory of Work Safety Intelligent Monitoring
School of Electronic Engineering, Beijing University of Posts and Telecommunications, Beijing, P.R. China
Email: {*liwang@bupt.edu.cn*, *chunyancao@bupt.edu.cn*, *songm@bupt.edu.cn*}
†Department of Electrical and Computer Engineering Illinois Institute of Technology
3301 S. Dearborn Street, Siegel Hall 320 Chicago, IL 60616
Email: *cheng@iit.edu*

***Abstract*—This paper proposes a joint cooperative relaying and jamming scheme based on distributed beamforming to enhance the secrecy rate of a wireless channel in the presence of an eavesdropper. Specifically, we consider the scenario that a source node transmits messages to a destination with the help of multiple cooperative relays, where a relay might be compromised to become an eavesdropper as an inside attacker. Our joint relaying and jamming approach is to assign some relay nodes to act as jammers to interfere the eavesdropper, while the remaining ones continue relaying information to the destination. We propose a protocol to implement the joint cooperative relaying and jamming. Our protocol further considers the particular challenge brought by the inside attacker: it may know the jamming signal and can use it to remove the interference from the jammers. The issue of phase and frequency synchronization in the distributed beamforming is also taken into account. A mixed integer programming problem is formulated to maximize the secrecy rate with the proposed joint relaying and jamming, by which the optimal role assignment to a relay and the associated optimal power assignment can be solved. Numerical results are presented to demonstrate the efficiency of the proposed joint relaying and jamming in improving the secrecy rate, with comparison to existing approaches.**

***Index Terms*—Cooperative relaying and jamming, distributed beamforming, synchronization, inside attacker, secrecy rate.**

I. Introduction

Recently, physical layer security has been regarded as a promising approach to address security issues in wireless networks without upper-layer encryption, which exploits the physical characteristics of the wireless channels to ensure secure communications. *Secrecy rate* is defined as the rate at which information can be transmitted secretly from the source to its intended destination in the presence of eavesdroppers, and the maximum achievable secrecy rate is named the *secrecy capacity*. In [1], Aaron Wyner introduced the wiretap channel and established the fundamental results of creating perfect secure communications without cryptographic techniques involved. Wyner's approach was extended to Gaussian wiretap channels and broadcast channels in later works [2]-[3].

Cooperative transmission has attracted a lot of attention to enhance the capacity of a wireless channel as a virtual MIMO system [4]-[5]. 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. For cooperative beamforming, all relays resort to the distributed beamforming technique to concentrate the signal towards the intended destination, trying to mitigate the information leakage to the eavesdropper as much as possible [6]-[7], [8]. The philosophy of cooperative jamming is that some relay nodes concentrate certain jamming signal to interfere the eavesdropper (normally by the distributed beamforming technique too) while not impact the destination [9]-[10], [11]. A relay equipped with multiple antennas for jamming was studied in [10]. However, the cost of a multiple antenna system is normally high. The work in [12] presented a systematic study of cooperative beamforming and cooperative jamming. The cooperative jamming situation considered in [12] only applies to the one-hop source to destination transmission though. Hybrid relaying and jamming schemes to secure the networks were proposed in [13]-[14], where some nodes adopt distributed beamforming to relay the message and others jam the eavesdroppers. It is worth noting that most of existing works, in all the three categories, considered a given set of relay(s), jammer(s) and the eavesdropper(s), which may not be the case in practice: a normal node could be compromised to turn into an attacker and the role of a relay node could be dynamically assigned.

This paper considers a practical scenario where a transmission with multiple cooperative relays starts at the normal state and the relays can apply distributed beamforming technique for high capacity. A relay node might be compromised to become an eavesdropper, which is an inside attacker. We assign some relay nodes to act as jammers to interfere the eavesdropper, while the rest continue relaying information to the destination. The unique issue in our scenario is the optimal role assignment to each relay, as a data relay or a jammer, for maximum secrecy rate. We formulate a mixed integer programming problem. Furthermore, we consider the particular challenge brought by the inside attacker: all the jammers need to transmit the same jamming symbols and use the distributed beamforming technique for effective jamming, however, the inside attacker may also know the jamming symbols (if preloaded) and can use it to remove the interferences from the jammers. We thus design a protocol to address such an issue. In addition, our protocol incorporates operations for

978-1-4799-2003-7/14/$31.00 ©2014 IEEE

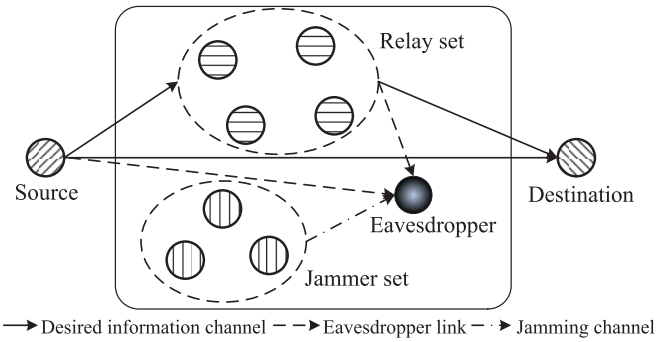

Fig. 1. System model for secure transmission.

synchronization in distributed beamforming, which is ignored in most of the existing studies on secrecy rate for cooperative communications. To make our scheme more efficient and practical, we introduce two hop distributed beamforming for joint cooperative relaying and jamming.

The paper is organized as follows. Section II presents the system model. Section III presents the protocol design for joint cooperative relaying and jamming. Section IV formulates a mixed integer programming problem to maximize the secrecy rate. Numerical results are provided in Section V to demonstrate the performance. Section VI gives conclusion remarks.

II. System Model

In this section, we will first present the system model and then give a brief description of the secure transmission between the source and the destination.

As shown in Fig. 1, we consider the scenario where a source needs to communicate with a destination under the help of some cooperative relays in the DF manner. Each node is equipped with a single omni-directional antenna and operates in a half-duplex mode. We assume that channels for different pairs of nodes are independent and identically distributed (i.i.d.) with flat Rayleigh fading, and the noise is the additive white Gaussian noise (AWGN) with a mean of zero and a variance of σ^2. In the system, a relay node might be compromised to become an eavesdropper, as an inside attacker, which can be detected by its malicious behavior. Some relay nodes will be assigned as jammers to interfere the eavesdropper, while the remaining ones continue relaying information to the destination. Here we assume the eavesdropper can be located by some existing techniques [15], and all candidate nodes can successfully decode the message transmitted by the source as assumed in [12].

The secure transmission process between the source and the destination can be divided into two transmitting phases. In the first phase, the source broadcasts the message, $\mathcal{S}$, which is also listened by the eavesdropper. To decrease the interception, the jammers send jamming signals, $\mathcal{Z}$, at the same time. Distributed beamforming is employed at the jammers so that the jamming signals confuse the eavesdropper only, without impacting the destination. In the second phase, the relays utilize distributed beamforming to forward the data to the destination, while the jammers continue sending jamming signals to interfere the eavesdropper. When useful message sent by the relays can be completely nulled out at the eavesdropper using null space cooperative beamforming at the relays [8], the jamming is not needed and the transmit power of the jammer set can be set zero. While if cooperative beamforming at the relays does not work well, the jammers interfere the eavesdropper and decrease its interception. Optimal power allocation to jammers and relays will be studied in Section IV.

We denote the channel gain form the source to the destination by h_{sd}, the channel gain form the source to the eavesdropper by h_{se}, the row channel gain vector $(1 \times N)$ from the source to all the candidate nodes by $\mathbf{h}_{sN}^T$, the column channel gain vector $(N \times 1)$ from all the candidate nodes to the eavesdropper by $\mathbf{h}_{Ne}$, the column channel gain vector $(N \times 1)$ from all the candidate nodes to the destination by $\mathbf{h}_{Nd}$, the channel gain matrix $(N \times N)$ between all the candidate nodes by $\mathbf{H}_N$. N is the number of candidate nodes. $(\bullet)^T$ is the transpose of a matrix or a vector. $[x]^+ = \max(0, x)$.

III. Joint Cooperative Relaying and Jamming

In this section, we design a protocol to implement the proposed cooperative relaying and jamming scheme.

The technique underpinning of the joint relaying and jamming is the distributed beamforming. An important issue with distributed beamforming is the synchronization of the carrier signals in phase and frequency. The study in [16] presented an effective synchronization technique for distributed beamforming and indicated that the beamforming gain still remains good even with imperfect synchronization. We develop our protocol based on that used in [16].

Furthermore, the severe impact of inside attacks from the eavesdropper can not be ignored. Cooperative jamming relies on distributed beamforming where the jammers need to transmit the same jamming symbols for effective jamming, however, the eavesdropper may also know the predefined jamming symbols and can use it to remove the interference. Our protocol utilizes on-line selection of the jamming signals rather than pre-installation to be against the inside attacker. Although we involve some cryptographic techniques here to deliver the on-line selected jamming signal from the source to the jamming nodes, the cryptographic technique just incurs some overhead to our cooperative relaying and jamming, and the secrecy rate still depends on the physical layer security technique.

The proposed protocol works as follows.

• First, the source generates a sinusoid signal $c_0(t)$ with a frequency f_c based on its local oscillator and broadcasts it. Here we assume that the source has one pair of public/private keys. The sinusoid signal $c_0(t)$ can be modulated with the public key of the source. The jammers use PLL (Phase Locking Loop) to lock on the frequency f_c and the received signal at the κth jammer node is $c_{\kappa,0}(t)$ with a phase shift θ_κ. The jammers apply phase error correction techniques to deal with phase shift θ_κ [16]. Then the κth jammer node obtains the calibrated signal $c_\kappa(t)$ used for channel estimation and beamforming. All the jammers also demodulate the public key

of the source to be used later for jamming signal transmission. An easier (but not that general) implementation is that the public key of the source is pre-installed into each relay node.

• Second, all the candidate nodes and the destination then take turns to broadcast a carrier signal so that each node can estimate the channel gain between itself and the broadcasting one. These channel gains can later be used for distributed beamforming, either for cooperative relaying to the destination or for jamming to the eavesdropper.

• Third, if each jammer obtains the public key of the source in the first step, it then uses this key to encrypt its session key to the source (here we use the local phase error as a session key, which is related to the propagation delay of the wireless channel between the source and this jammer). The source can later use the session key to send updated jamming signals used for distributed beamforming to the jammers, which is similar to the method in [17] by exploiting the wireless channel for building cryptographic services.

• Last, at a certain moment, if the source announces the eavesdropper, it will send the updated jamming signals to each jammer, encrypted by their session keys, respectively. The jammers then start to jam the eavesdropper with distributed beamforming. Since the on-line selected jamming signal is encrypted by the session key, the eavesdropper (the inside attacker) cannot obtain it.

Please be noted that the proposed protocol can be implemented with a time-divided system, by extending the frame structure presented in [16]. As the focus of this paper is to demonstrate the effectiveness of the joint cooperative relaying and jamming and the associated optimal relay role assignment, we will fully develop the implementation details and conduct related overhead study in our future work.

IV. Secrecy Capacity Maximization

In this section, we will first formulate the secrecy rate of the whole transmission, and present a mixed integer programming problem to maximize the secrecy rate, which relates to the optimal assignment of the roles to candidate nodes. Distributed beamforming is utilized in the model, where each relay node and jammer node apply a weight to the signal transmitted. With proper selection of the weights, the received signal at a certain node can be nulled out to achieve jamming through distributed beamforming.

A. Secrecy Rate Formulation

As indicated before, to improve the secrecy rate of the whole transmission, a two-phase transmission between the source and the destination is established.

Each candidate node can be regarded as a relay or a jammer. We present an optimal relay and jammer selection to maximize the secrecy rate.

Denote the set of all the candidate nodes $\mathcal{N} = \{1, 2, , ..., N\}$. For each candidate node, we set two parameters to indicate its role as a relay or jammer. The specifical description can be expressed as

$$n_i = \begin{cases} \text{relay} \quad if\ x_i = 1 \text{ and } u_i = 0, \\ \text{jammer}\ \ if\ x_i = 0 \text{ and } u_i = 1, \end{cases}$$

where n_i is the ith candidate node ($i = 1, ..., N$), the value of x_i and u_i can be 0 or 1, and $x_i + u_i = 1$.

According to the definition, for convenience of description and explicit physical meaning, we denote the roles of all N candidate nodes by two vectors $\mathbf{x} = [x_1, x_2, ..., x_N]^T$ and $\mathbf{u} = [u_1, u_2, ..., u_N]^T$. Therefore, we can obtain the role of the ith candidate node by the values of x_i and u_i, which are relative to the secrecy rate maximization problem.

1) The first transmitting phase: The source broadcasts the message, $\mathcal{S}$, and certainly the eavesdropper can hear the message. To disturb the eavesdropping, the jammers at the same time send the jamming signals, $\mathcal{Z}$, by distributed beamforming without affecting the destination.

For the candidate nodes acting as relays, the values corresponding to them in vector $\mathbf{x}$ must be 1, and the values corresponding to the candidate nodes acting as jammers in vector $\mathbf{u}$ must be 1. In this phase, the received signals at the candidate nodes, the destination and the eavesdropper can be written as

$$\mathbf{y}_N = \sqrt{P_s}\mathbf{h}_{sN}^T\mathcal{S} + \mathbf{n}_N, \tag{1}$$

$$y_d^{(1)} = \sqrt{P_s}h_{sd}\mathcal{S} + n_d^{(1)}, \tag{2}$$

$$y_e^{(1)} = \sqrt{P_s}h_{se}\mathcal{S} + \sqrt{P_1}\mathbf{u}^T\mathbf{W}_1\mathbf{h}_{Ne}\mathcal{Z} + n_e^{(1)}, \tag{3}$$

respectively, where P_s is the transmit power of the source, P_1 is the total transmit power of the candidate nodes in the first phase, $\mathbf{W}_1 = diag([\mathrm{w}_1^{(1)}, \mathrm{w}_2^{(1)}, ..., \mathrm{w}_N^{(1)}])$ is a $N \times N$ power allocation weight matrix of the candidate nodes in the first phase, $\mathbf{w}_1^T\mathbf{w}_1$=1 where $\mathbf{w}_1 = [\mathrm{w}_1^{(1)}, \mathrm{w}_2^{(1)}, ..., \mathrm{w}_N^{(1)}]^T$, $\mathbf{n}_N$ is the AWGN at the candidate nodes, $n_d^{(1)}$ is the AWGN at the destination and $n_e^{(1)}$ is the AWGN at the eavesdropper.

The received SNRs at the destination and the eavesdropper in the first phase can be described as

$$\gamma_d^{(1)} = \frac{P_s|h_{sd}|^2}{\sigma^2}, \tag{4}$$

$$\gamma_e^{(1)} = \frac{P_s|h_{se}|^2}{P_1|\mathbf{u}^T\mathbf{W}_1\mathbf{h}_{Ne}|^2 + \sigma^2}, \tag{5}$$

respectively.

2) The second transmitting phase: The relays utilize distributed beamforming to forward the weighted message to the destination while the jammers continue sending jamming signals to interfere the eavesdropper without impacting the destination.

In this phase, the received signals at the destination and the eavesdropper can be written as

$$y_d^{(2)} = \sqrt{P_2}\mathbf{x}^T\mathbf{W}_2\mathbf{h}_{Nd}\mathcal{S} + n_d^{(2)}, \tag{6}$$

$$y_e^{(2)} = \sqrt{P_2}\mathbf{x}^T\mathbf{W}_2\mathbf{h}_{Ne}\mathcal{S} + \sqrt{P_2}\mathbf{u}^T\mathbf{W}_2\mathbf{h}_{Ne}\mathcal{Z} + n_e^{(2)}, \tag{7}$$

respectively, where P_2 is the total transmit power of the candidate nodes in the second phase, $\mathbf{W}_2 = diag([\mathrm{w}_1^{(2)}, \mathrm{w}_2^{(2)}, ..., \mathrm{w}_N^{(2)}])$ is a $N \times N$ power allocation weight matrix of the candidate nodes in the second phase, $\mathbf{w}_2^T\mathbf{w}_2$=1 where $\mathbf{w}_2 = [\mathrm{w}_1^{(2)}, \mathrm{w}_2^{(2)}, ..., \mathrm{w}_N^{(2)}]^T$, $n_d^{(2)}$ is the AWGN at the destination and $n_e^{(2)}$ is the AWGN at the eavesdropper.

The received SNRs at the destination and the eavesdropper in the second phase can be described as

$$\gamma_d^{(2)} = \frac{P_2|\mathbf{x}^T\mathbf{W}_2\mathbf{h}_{Nd}|^2}{\sigma^2}, \tag{8}$$

$$\gamma_e^{(2)} = \frac{P_2|\mathbf{x}^T\mathbf{W}_2\mathbf{h}_{Ne}|^2}{P_2|\mathbf{u}^T\mathbf{W}_2\mathbf{h}_{Ne}|^2+\sigma^2}, \tag{9}$$

respectively.

In the second phase, when the desired message sent by the relays can be completely nulled out at the eavesdropper by using cooperative beamforming at the relays, i.e., $\mathbf{x}^T\mathbf{W}_2\mathbf{h}_{Ne} = 0$, the eavesdropper can wiretap nothing about the desired message, then the jamming is not necessary.

We combine the signals from the first and second phases adopting maximal ratio combining (MRC) method [18], and the received SNRs at the destination and the eavesdropper in the whole transmission can be described as

$$\gamma_d = \gamma_d^{(1)} + \gamma_d^{(2)} = \frac{P_s|h_{sd}|^2}{\sigma^2} + \frac{P_2|\mathbf{x}^T\mathbf{W}_2\mathbf{h}_{Nd}|^2}{\sigma^2}, \tag{10}$$

$$\begin{aligned}\gamma_e &= \gamma_e^{(1)} + \gamma_e^{(2)} \\ &= \frac{P_s|h_{se}|^2}{P_1|\mathbf{u}^T\mathbf{W}_1\mathbf{h}_{Ne}|^2+\sigma^2} + \frac{P_2|\mathbf{x}^T\mathbf{W}_2\mathbf{h}_{Ne}|^2}{P_2|\mathbf{u}^T\mathbf{W}_2\mathbf{h}_{Ne}|^2+\sigma^2},\end{aligned} \tag{11}$$

respectively. When $\mathbf{x}^T\mathbf{W}_2\mathbf{h}_{Ne} = 0$, the second part of the above equation is zero, i.e., $\gamma_e^{(2)} = 0$.

The corresponding maximum information rates at the destination and the eavesdropper are

$$R_d = \frac{1}{2}\log_2(1+\gamma_d) = \log_2(1+\gamma_d^{(1)}+\gamma_d^{(2)}), \tag{12}$$

$$R_e = \frac{1}{2}\log_2(1+\gamma_e) = \log_2(1+\gamma_e^{(1)}+\gamma_e^{(2)}), \tag{13}$$

respectively, where the factor $1/2$ is due to the fact that the two phases share the transmission time.

Therefore, the secrecy rate of the whole transmission can be written as

$$\begin{aligned}SC &= \{R_d - R_e\}^+ \\ &= \frac{1}{2}\left\{\log_2(1+\gamma_d) - \log_2(1+\gamma_e)\right\}^+.\end{aligned} \tag{14}$$

B. Maximization Problem

From the above discussion, we can see that changing the number of relays and jammers will impact the secrecy rate, i.e., different values of the vectors $\mathbf{x}$ and $\mathbf{u}$ influence the security of the transmission. Thus, a mixed integer programming problem for secrecy rate maximization with the optimal values of the vectors $\mathbf{x}$ and $\mathbf{u}$ is presented.

In the first transmitting phase, distributed beamforming is adopted at the jammers to avoid the interference at the relays and the destination while confusing the eavesdropper. Thus, there are two null space constraints in this phase, i.e., $\mathbf{u}^T\mathbf{W}_1\mathbf{H}_N\mathbf{X} = \mathbf{0}_{1\times N}$ and $\mathbf{u}^T\mathbf{W}_1\mathbf{h}_{Nd} = 0$, where $\mathbf{X} = diag([\mathrm{x}_1, \mathrm{x}_2, ..., \mathrm{x}_N])$. The necessary condition for the null space constraints in this phase is that the number of jammers is larger than that of relays and destination, i.e., $N_J > N_R+1$, where N_J and N_R are the numbers of jammers and relays, respectively. Otherwise, if $N_J \le N_R+1$, we cannot avoid interference caused by the jammers at the relays and the destination completely.

If cooperative beamforming at the relays does not work well in the second transmitting phase, the jammers interfere the eavesdropper without affecting the destination, that is, $\mathbf{u}^T\mathbf{W}_2\mathbf{h}_{Nd} = 0$ and $N_J > 1$. When null space cooperative beamforming employed at the relays can completely null out the desired message at the eavesdropper, then $\mathbf{x}^T\mathbf{W}_2\mathbf{h}_{Ne} = 0$ and $N_R > 1$.

Our objective is to select optimal relays and jammers with power allocation to maximize the secrecy rate subject to a total transmit power constraint. Depending on whether $\mathbf{x}^T\mathbf{W}_2\mathbf{h}_{Ne}$ is zero or not, we can formulate the secrecy rate maximization problem as following.

1) $\mathbf{x}^T\mathbf{W}_2\mathbf{h}_{Ne} \neq 0$ *(without nulling out):* The desired message sent by the relays cannot be completely nulled out at the eavesdropper in the second phase. Under the null space constraints in the first phase, the optimization problem for maximum secrecy rate can be formulated as follows.

$$\begin{aligned}&\arg\max_{\mathbf{W}_1,\mathbf{W}_2} SC \\ &= \arg\max_{\mathbf{W}_1,\mathbf{W}_2} \{R_d - R_e\} \\ &= \arg\max_{\mathbf{W}_1,\mathbf{W}_2} \frac{1}{2}\left\{\log_2(1+\gamma_d) - \log_2(1+\gamma_e)\right\},\end{aligned} \tag{15}$$

subject to

$$P_s + P_1 + P_2 = P_0, \tag{15a}$$

$$\mathbf{u}^T\mathbf{W}_1\mathbf{h}_{Nd} = 0, \tag{15b}$$

$$\mathbf{u}^T\mathbf{W}_2\mathbf{h}_{Nd} = 0, \tag{15c}$$

$$\mathbf{u}^T\mathbf{W}_1\mathbf{H}_N\mathbf{X} = \mathbf{0}_{1\times N}, \tag{15d}$$

where P_0 is the total transmit power constraint. It is obviously a mixed integer programming problem.

Specifically, when SNR $\gg 1$, the objective function can be expressed as

$$\begin{aligned}&\arg\max_{\mathbf{W}_1,\mathbf{W}_2} \frac{1}{2}\left\{\log_2(1+\gamma_d) - \log_2(1+\gamma_e)\right\} \\ &\simeq \arg\max_{\mathbf{W}_1,\mathbf{W}_2} \left(\frac{\frac{P_s|h_{sd}|^2}{\sigma^2} + \frac{P_2|\mathbf{x}^T\mathbf{W}_2\mathbf{h}_{Nd}|^2}{\sigma^2}}{\frac{P_s|h_{se}|^2}{P_1|\mathbf{u}^T\mathbf{W}_1\mathbf{h}_{Ne}|^2+\sigma^2} + \frac{P_2|\mathbf{x}^T\mathbf{W}_2\mathbf{h}_{Ne}|^2}{P_2|\mathbf{u}^T\mathbf{W}_2\mathbf{h}_{Ne}|^2+\sigma^2}}\right).\end{aligned} \tag{16}$$

2) $\mathbf{x}^T\mathbf{W}_2\mathbf{h}_{Ne} = 0$ *(nulling out):* The desired message sent by the relays can be completely nulled out at the eavesdropper in the second phase. In this case, the secrecy rate maximization problem can be formulated as follows.

$$\begin{aligned}&\arg\max_{\mathbf{W}_1,\mathbf{W}_2} SC \\ &= \arg\max_{\mathbf{W}_1,\mathbf{W}_2} \frac{1}{2}\left\{\log_2(1+\gamma_d) - \log_2(1+\gamma_e)\right\},\end{aligned} \tag{17}$$

subject to

$$P_s + P_1 + P_2 = P_0, \tag{17a}$$

$$\mathbf{u}^T\mathbf{W}_1\mathbf{h}_{Nd} = 0, \tag{17b}$$

$$\mathbf{x}^T\mathbf{W}_2\mathbf{h}_{Ne} = 0, \tag{17c}$$

$$\mathbf{u}^T\mathbf{W}_1\mathbf{H}_N\mathbf{X} = \mathbf{0}_{1\times N}. \tag{17d}$$

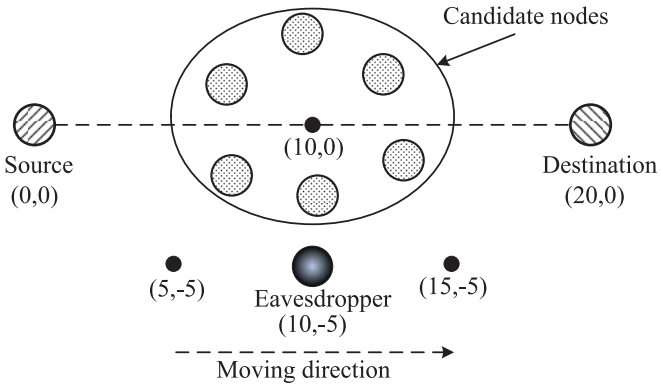

Fig. 2. Scenario used for numerical experiments.

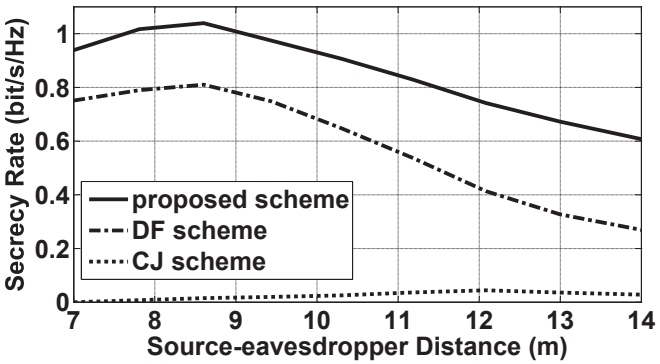

Fig. 3. Secrecy rate versus source-eavesdropper distance.

Similarly, when SNR $\gg 1$, the objective function will be

$$\begin{aligned}
&\arg \max_{\mathbf{W}_1,\mathbf{W}_2} \frac{1}{2}\left\{\log_2\left(1+\gamma_d\right)-\log_2\left(1+\gamma_e\right)\right\} \\
&\simeq \arg \max_{\mathbf{W}_1,\mathbf{W}_2} \left(\frac{\frac{P_s|h_{sd}|^2}{\sigma^2}+\frac{P_2|\mathbf{x}^T\mathbf{W}_2\mathbf{h}_{Nd}|^2}{\sigma^2}}{\frac{P_s|h_{se}|^2}{P_1|\mathbf{u}^T\mathbf{W}_1\mathbf{h}_{Ne}|^2+\sigma^2}} \right) \\
&= \arg \max_{\mathbf{W}_1,\mathbf{W}_2} \\
&\left(P_s|h_{sd}|^2+P_2|\mathbf{x}^T\mathbf{W}_2\mathbf{h}_{Nd}|^2\right)\cdot\frac{P_1|\mathbf{u}^T\mathbf{W}_1\mathbf{h}_{Ne}|^2+\sigma^2}{P_s|h_{se}|^2}. \quad (18)
\end{aligned}$$

We can see that the secrecy rate maximization problem is a mixed integer programming problem, which is NP-hard in general. In this paper, our focus is to demonstrate the efficiency of the proposed joint relaying and jamming and the optimal relay assignment, and we use exhaustive search to solve the problem which is an easy approach to obtain the solution when the network scale is small, while it becomes difficult for a large network scale.

Therefore, in the future work, we will study how to develop efficient approximate algorithms to solve this mixed integer programming problem when the network scale gets larger, such as the branch-and-bound and cutting plane methods.

V. Numerical Results

In this section, numerical results are provided to demonstrate the performance of our proposed scheme. In our simulation, the path-loss exponent of wireless channels is $\beta = 3$ and the additive white Gaussian noise power is $\sigma^2 = 1$ mW. In addition, we set the total transmit power constraint, $P_0 = 1000$ mW. The 2D square topology of the scenario is shown as in Fig. 2, where there is a source, a destination, an eavesdropper and several randomly distributed candidate nodes whose center is at $(10, 0)$.

To demonstrate the performance of our proposed scheme, two cooperative schemes, decode-and-forward (DF) scheme and cooperative jamming (CJ) scheme mentioned in [12] have been involved. The relays transmit a weighted version of a re-encoded noise-free message signal for the DF scheme while the relays transmit a jamming signal for the CJ scheme.

According to our assumption that all candidate nodes can properly decode the signals from the source, we can assign a fixed large value of $P_s = 200$ mW to satisfy the assumption, and thus our established model is applied to solve the power allocation and weight factors for the relays and jammers. In addition, the number of candidate nodes is $N = 6$.

As in Fig. 2, the eavesdropper location is first fixed at $(10, -5)$. When move the position of the eavesdropper from $(5, -5)$ to $(15, -5)$, we can obtain the relationship between the secrecy rate of the whole transmission and the distance from the eavesdropper to the source. From Fig. 3, when the distance between the eavesdropper and the source becomes larger, the secrecy rates for the DF scheme, the CJ scheme and our proposed scheme first increase and then decrease. The secrecy rates for all three schemes increase since the received signal power at the eavesdropper decreases when the eavesdropper moves away from the source, while when the distance between the eavesdropper and the source continues to increase, the secrecy rate decreases since the eavesdropper approaches the destination, which has a negative impact on the secrecy rate. Furthermore, the secrecy rate for the CJ scheme is much lower than the other two schemes, since the CJ scheme can only decrease the rate at the eavesdropper but it cannot improve the rate at the destination.

Fig. 4 shows the secrecy rate for different numbers of candidate nodes. The eavesdropper location is fixed at $(10, -5)$. From the figure, with the number of candidate nodes increasing, the secrecy rate of the whole transmission for each scheme becomes larger, which indicates that increasing the number of candidate nodes improves the secrecy rate. However, when the number of candidate nodes continues to increase, the secrecy rates for three schemes increase slowly and are almost saturated, which shows that there is a limitation for improving the secrecy rate through increasing the number of candidate nodes. In addition, the secrecy rate for the CJ scheme is also much lower than the other two schemes which is limited by the distance between the source and the destination. Furthermore, the secrecy rate for our scheme has a better performance than the other two schemes since we consider the optimal selection of relays and jammers to simultaneously enhance the rate at the destination and reduce the rate at the eavesdropper.

VI. Conclusion

In this paper, a joint cooperative relaying and jamming scheme has been presented to enhance the secrecy rate of a

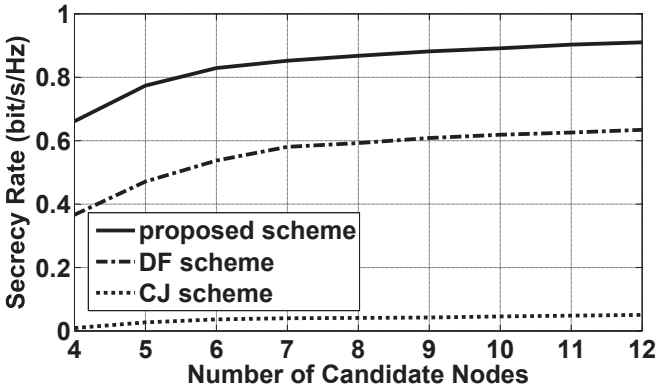

Fig. 4. Secrecy rate versus number of candidate nodes.

wireless channel in the presence of an eavesdropper, which is an inside attacker. We have proposed to assign some relay nodes to act as jammers while the rest continue relaying information to the destination. A mixed integer programming problem for maximum secrecy rate has been formulated. Furthermore, our scheme also considers some special challenges, such as dealing with both the impact of the inside attacker and the phase and frequency synchronization in distributed beamforming. Numerical results have demonstrated the merits of our scheme in terms of secrecy rate, with comparison to DF and CJ schemes.

ACKNOWLEDGMENT

This work was supported in part by the National Natural Science Foundation of China (Grant No. 61201150), the Science Technology Innovation Foundation for Young Teachers in BUPT (Grant No. 2013RC0202), the State Major Science and Technology Special Projects (Grant No. 2012ZX03004001), and the Beijing Higher Education Young Elite Teacher Project (Grant No. YETP0442).

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] I. Csiszar and J. Korner, "Broadcast channels with confidential messages," *IEEE Trans. Inf. Theory*, vol. 24, no. 3, pp. 339-348, May 1978.

[4] Q. Guan, F.R. Yu and S. Jiang, "Capacity-optimized topology control for MANETs with cooperative communications," *IEEE Trans. Wireless Commun.*, vol. 10, no. 7, pp. 2162-2170, Jul. 2011.

[5] D.W.K. Ng, E.S. Lo and R. Schober, "Energy-efficient resource allocation in multi-cell OFDMA systems with limited backhaul capacity," *IEEE Trans. Wireless Commun.*, vol. 11, no. 10, pp. 3618-3631, Oct. 2012.

[6] J. Kim, A. Ikhlef and R. Schober, "Combined relay selection and cooperative beamforming for physical layer security," *J. Commun. Netw.*, vol. 14, no. 4, pp. 364-373, Aug. 2012.

[7] Y. Liu and W. Nie, "Selection based cooperative beamforming and power allocation for relay networks," *J. Commun. Netw.*, vol. 13, no. 4, pp. 377-384, Aug. 2011.

[8] 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. 35-38, Jan. 2013.

[9] J. Yang, I. Kim and D. I. Kim, "Optimal cooperative jamming for multiuser broadcast channel with multiple eavesdroppers," *IEEE Trans. Wireless Commun.*, vol. 12, no. 6, pp. 2840-2852, Jun. 2013.

[10] L. Dong, Z. Han, A.P. Petropulu and H.V. Poor, "Cooperative jamming for wireless physical layer security," in *2009 IEEE SSP Workshops*, Sept. 2009, pp. 417-420.

[11] R. Zhang, L. Song, Z. Han and B. Jiao, "Physical layer security for two-way untrusted relaying with friendly jammers," *IEEE Trans. Vehicular Tech.*, vol. 61, no. 8, pp. 3693-3704, Oct. 2012.

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

[13] 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.

[14] J. Chen, R. Zhang, L. Song, Z. Han and B. Jiao, "Joint relay and jammer selection for secure two-way relay networks," *IEEE Trans. Inf. Forensics and Security*, vol. 7, no. 1, pp. 310-320, Feb. 2012.

[15] Hong L., M. McNeal and C. Wei, "Secure cooperative MIMO communications under active compromised nodes," *2011 IEEE Int'l. Pervasive Computing and Commun. Workshops (PERCOM Workshops)*, Mar 2011, pp. 184-189.

[16] R. Mudumbai, G. Barriac and U. Madhow, "On the feasibility of distributed beamforming in wireless networks," *IEEE Trans. Wireless Commun.*, vol. 6, no. 5, pp. 1754-1763, May 2007.

[17] R. Liu and W. Trappe, *Securing Wireless Communications at the Physical Layer*, Springer, 2009.

[18] T. S. Rappaport, *Wireless Communications Principles and Practice*, 2nd ed. Prentice Hall, 2002.