Two-Phase Cooperative Jamming and Beamforming for Physical Layer Secrecy

Mohammad Hatami[1], Mojtaba Jahandideh[2], Hamid Behroozi[3]
[1,3]Department of Electrical Engineering, Sharif University of Technology, Tehran, Iran
[2]Electrical and Computer Engineering Department, Tarbiat Modares University, Tehran, Iran
Email: hatami_mohammad@ee.sharif.edu, m.jahandideh@modares.ac.ir, behroozi@sharif.edu

***Abstract*—The broadcast nature of wireless communications makes the propagation medium vulnerable to security attacks such as eavesdropping and jamming from adversarial or unauthorized users. Applying physical layer secrecy approaches will enable the exchange of confidential messages over a wireless medium in the presence of unauthorized eavesdroppers, without using any secret keys. However, physical layer security approaches are typically feasible only when the source-eavesdropper channel is weaker than the source-destination channel. Cooperative jamming can be used to overcome this challenge and increase the secrecy rate. In this paper, the security of two-phase relaying system with multiple intermediate nodes and in the presence of an eavesdropper is investigated. To enhance the system secrecy rate, a joint cooperative beamforming and jamming combined with relay and jammer selections is proposed. In *phase I*, the source node broadcasts a signal to relays while three intermediate nodes (which act as jammers) help the source node by transmitting random jamming signals to confuse the eavesdropper. Since the friendly (cooperative) jammers create interference for both the intended relays and the eavesdropper, optimal beamforming is applied such that no interference is caused at two preselected desired relays (that are going to receive the confidential massage in *phase I*). In *phase II*, two preselected relays transmit the source message with beamforming coefficients such that the received signal at the eavesdropper is completely nulled out. Our goal in this paper is to minimize the received SNR at the eavesdropper while increasing it at the destination as much as possible by applying different methods such as cooperative beamforming, cooperative jamming and relay selection. To avoid operational complexity, we consider the minimum number of intermediate nodes that are necessary without losing the performance. Numerical results demonstrate the advantage of our proposed scheme compared with the scheme with no cooperative jamming.**

***Index Terms*—cooperative jamming; beamforming; relay selection; physical layer security**

I. Introduction

The broadcast characteristic of wireless communications imposes major concerns to the security of these systems. Physical layer security has recently attracted a lot of attention and it has been regarded as a promising approach to address reliability and security issues in wireless communication systems without upper-layer encryption. In [1] Wyner introduced the wiretap channel and established the fundamental results of creating perfect secrecy without relying on private (secret) keys. In later works [2], [3], Wyner's approach was applied to Gaussian wiretap channels and broadcast channels.

In wireless communications, interference is generally regarded as an undesired phenomenon. In contrast with the conventional belief, cooperative jamming is a beneficial technique for the physical layer security, where some relay nodes transmit independent identically distributed (i.i.d.) Gaussian jamming signals to degrade the channel of the eavesdropper [4], [5], [6], [7], [8]. Cooperative jamming was originally proposed in [4] for a multiple access wiretap channel, where multiple users wish to have simultaneous secure communications with a legitimate receiver in the presence of an illegitimate receiver (referred to as the eavesdropper). Although the friendly (cooperative) jammer creates interference for both the intended receiver and the eavesdropper, its jamming might be more detrimental to the eavesdropper than the illegitimate receiver, thus increasing the achievable secrecy rate between the legitimate TX-RX pair.

In cooperative beamforming, a set of collaborating nodes act as a distributed antenna system so that the signals are combined constructively at the intended destination [9], [10].

Relay selection is another approach to utilize multiple relays for the physical layer security. In [11] the performance of opportunistic relay selection to maximize the ratio of SNRs at the destination and at the eavesdropper is investigated. In [12] an optimal selection and jamming scheme is proposed. For the relay selection, only channel gains are needed while full channel state information (CSI) is necessary for cooperative beamforming. [13] investigates the relay and jammer selection problem in the two-way relay networks. In [14] multiple relay cooperative beamforming combined with jamming is adopted to maximize the secrecy rate. To enhance the security of two-way relay network, a joint cooperative beamforming and jamming scheme is proposed in [15]. In [16] authors use beamforming and relay selection techniques to maximize the secrecy rate where a two-step scheme is introduced. In the first step where the source transmits signal to the relays, it is assumed that the eavesdropper is not able to receive the signal. [17] considers the problem of secret communication through cognitive relay assisted interference channels where the secrecy rate of cognitive interference channels is improved via beamforming and cooperative jamming. The authors in [18] propose a joint decode-and-forward and cooperative jamming scheme where the relay nodes transmit a scaled version of the source signal and the jamming nodes just transmit a common

978-1-4799-1972-7/15/$31.00

jamming signal to confuse the eavesdropper. The ultimate goal in [18] is minimizing the transmit power subject to a secrecy rate constraint, but the relay selection is not applied. In[19], cooperative jamming with the multiple-input multiple-output (MIMO) relay is analyzed to enhance the security. In [20], authors use cooperative relaying techniques to improve the secrecy rate. In [21] cooperative jamming is adopted to enhance security in situations where we have untrusted relays. In[22] a cooperative jamming scheme is proposed to overcome the attackers in the networks where a relay node might be compromised to become an eavesdropper. In [23] the problem of choosing a jammer and a relay per phase is examined. In [24], the problem of secure communications in a four-node network, consisting of one source, one destination, one eavesdropper and one helper is investigated where the authors verify the question"to jam or to relay?" for the helper to improve the secrecy.

In this paper we propose a two-phase cooperative jamming with joint relay selection and cooperative beamforming scheme. Cooperative beamforming with multiple relays requires high amount of operational complexity; To avoid that, we involved minimum intermediate nodes that are necessary to reach the desired performance. We set three relay nodes to act as jammers and confuse the eavesdropper while two other intermediate nodes relay information to the destination. We assume that the global CSI is available for the system design (a common assumption as in most of PHY-based security literature, see e.g., [7], [10], [19], [22], [25], [26]).

The rest of this paper is organized as follows: Section II presents the system model. In Section III, the cooperative jamming with cooperative beamforming and relay selection are analyzed. Numerical results are given in Section IV. Section V concludes this paper.

Throughout the paper, upper-case letter X denotes a random variable, boldface letter $\mathbf{x}$ denotes a column vector. We denote the channel gain from the source to the eavesdropper by h_{SE} , the vector of channel gains between the source and intermediate nodes by $\mathbf{h}_{SR} = [h_{SR_1}, h_{SR_2}, ..., h_{SR_M}]$, and the channel gains from the intermediate nodes to the eavesdropper by $\mathbf{h}_{RE} = [h_{R_1E}, h_{R_2E}, ..., h_{R_ME}]$.

II. System Model

We consider a wireless network model consisting of one source node (S), M intermediate nodes $(\mathrm{R}_1, ..., R_M)$, a destination (D), and an eavesdropper (E). The system model is depicted in Fig.1. All nodes operate in the half-duplex mode and equipped with only one single omni-directional antenna. The eavesdropper is assumed to be passive with the aim of interpreting the source information (decoding the received signal from the transmitter but not to jam it or modify it). We also assume that there is no direct link between the source and the destination, i.e., $h_{SD} \approx 0$, while there exists a direct link between the source and the eavesdropper. Some intermediate nodes can be used as cooperative jamming sources to confuse

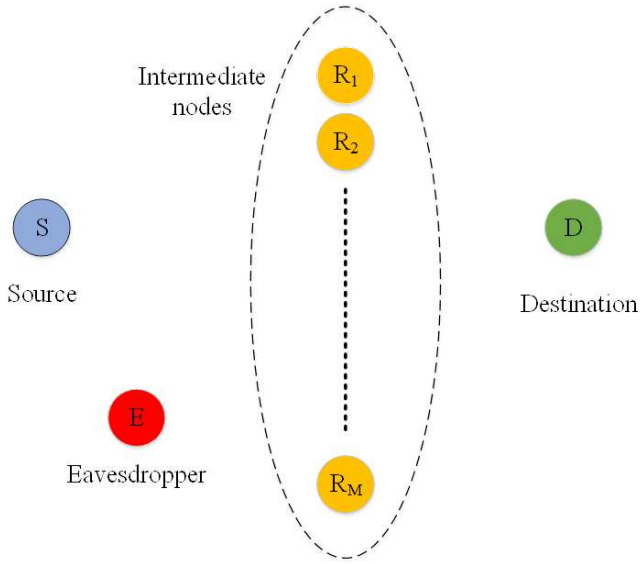

Figure 1. A wireless network model consisting of one source node (S), M intermediate nodes $(\mathrm{R}_1, ..., R_M)$, and a destination node (D). We assume that there is a potential eavesdropper (E) in vicinity.

the eavesdropper while the other intermediate nodes might help as relays to send the source message to the decoder. The source, the relays and the jammers are subject to power constraints P_S, P_R and P_J, respectively. Here, the figure of merit is the secrecy rate defined as the rate at which information can be transmitted secretly from a source to its intended legitimate destination node.

We assume that channels for different pairs of nodes are independent and identically distributed (i.i.d.) with quasi-static Rayleigh fading and additive white Gaussian noise (AWGN) with mean zero and variance σ_n^2, i.e., $\mathbb{CN}(0, \sigma_n^2)$, where $\mathbb{CN}(\mu, \sigma^2)$ denotes the complex Gaussian distribution with mean μ and variance σ^2.

III. Cooperative Jamming and Beamforming

In this paper, we propose a two-phase cooperative jamming and cooperative beamforming protocol, which can be described as follows:

Phase I: As illustrated in Fig. 2, the source node transmits the information carrying codewords intended for the destination to M relays. Meanwhile, three preselected intermediate nodes (which act as jammers) help the source node by sending jamming signals to confuse the eavesdropper, using desired beamforming. Since the friendly (cooperative) jammers create interference for both the intended relays and the eavesdropper, optimal beamforming is applied such that the jammers only confuse the eavesdropper while no interference is caused at two preselected desired relays (that are going to receive the confidential massage in *phase I*).

Phase II: As shown in Fig. 3, two selected relays, out of M intermediate nodes, decode the source message and then perform beamforming by transmitting scaled versions of the same signal to the destination node (D).

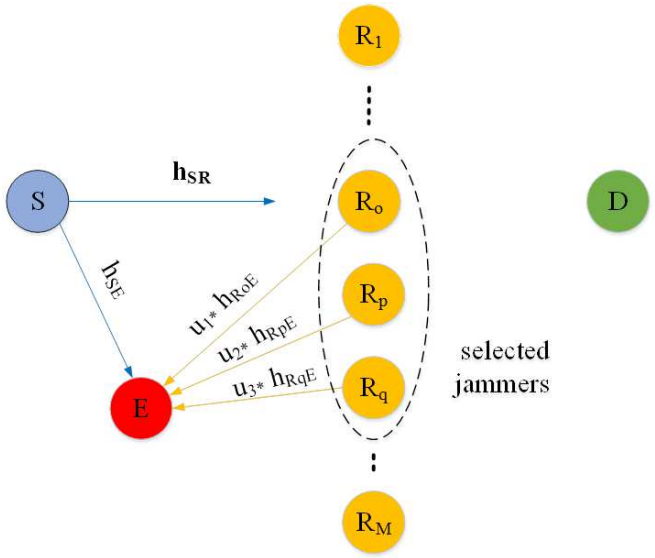

Figure 2. *Phase I* of the proposed *two-phase* transmission scheme: The source node wants to communicate with a destination through M relays. Meanwhile, three preselected intermediate nodes transmit jamming signals.

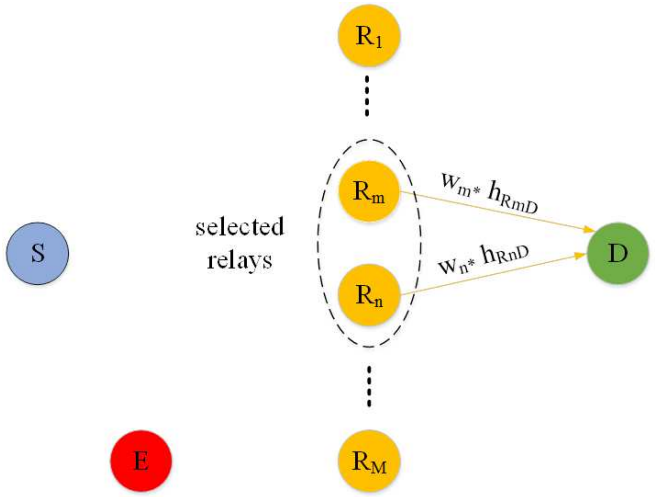

Figure 3. *Phase II* of the proposed *two-phase* transmission scheme: Two selected intermediate relay nodes, R_m and R_n, perform beamforming by transmitting scaled versions of the decoded source message to the destination node (D).

Suppose that nodes R_m and R_n are the selected relays at *phase II* . The received signals at the destination and at the eavesdropper in *phase II* can be expressed as

$$y_D^{(2)} = \sqrt{P_R}\mathbf{w}^T\mathbf{h}_{RD,(m,n)}x + n_D^{(2)}, \quad (1)$$
$$y_E^{(2)} = \sqrt{P_R}\mathbf{w}^T\mathbf{h}_{RE,(m,n)}x + n_E^{(2)}, \quad (2)$$

where P_R is the transmit power of relays, x is the transmitted signal, $\mathbf{w} = [\ w_m \quad w_n\ ]^T$, $\mathbf{h}_{RD,(m,n)} = [\ h_{RD,m} \quad h_{RD,n}\ ]$, and $\mathbf{h}_{RE,(m,n)} = [\ h_{RE,m} \quad h_{RE,n}\ ]$. $n_D^{(2)}$ and $n_E^{(2)}$ are white complex Gaussian noise at the destination and at the eavesdropper, respectively. Also we assume that $E\left\{|x|^2\right\} = 1$. The corresponding SNRs at the destination and at the eavesdropper are

$$\gamma_D^{(2)} = \frac{P_R\left|\mathbf{w}^T\mathbf{h}_{RD,(m,n)}\right|^2}{\sigma_n^2}, \quad (3)$$
$$\gamma_E^{(2)} = \frac{P_R\left|\mathbf{w}^T\mathbf{h}_{RE,(m,n)}\right|^2}{\sigma_n^2}, \quad (4)$$

where σ_n^2 is the noise power. For a Gaussian channel, the achievable secrecy rate equals to [27]

$$R_S = \max\{R_D - R_E, 0\}, \quad (5)$$

where

$$R_D = \frac{1}{2}\log_2(1+\gamma_D), \quad (6)$$
$$R_E = \frac{1}{2}\log_2(1+\gamma_E), \quad (7)$$

in which γ_D and γ_E, , respectively, denote the received SNRs at the destination and at the eavesdropper. Using beamforming, the signal transmitted to the legitimate receiver can be maximized while jointly minimizing the signal power received by the illegitimate receiver, i.e., the eavesdropper. In this phase, the beamforming vector is calculated such that no information carrying signal is received at the eavesdropper, i.e., $\gamma_E^{(2)}$ given in (4) equals to zero, which results in

$$\mathbf{w}^T\mathbf{h}_{RE,(m,n)} = 0,$$
$$s.t.\ \mathbf{w}^H\mathbf{w} = 1. \quad (8)$$

Writing in a vector form we have

$$\begin{bmatrix} w_m & w_n \end{bmatrix}\begin{bmatrix} h_{RE,m} \\ h_{RE,n} \end{bmatrix} = 0.$$
$$s.t.\ \mathbf{w}^H\mathbf{w} = 1 \quad (9)$$

Solving the above problem we have

$$w_m = \alpha h_{RE,n}, \quad (10)$$
$$w_n = -\alpha h_{RE,m}, \quad (11)$$

where

$$\alpha = \frac{1}{|h_{RE,m}|^2 + |h_{RE,n}|^2}. \quad (12)$$

Now we calculate the SNR at the destination. By replacing the beamforming vector, (10) and (11), in the received SNR at the destination, (3), we obtain

$$\gamma_{D,(m,n)}^{(2)} = \alpha^2\frac{P_R}{\sigma_n^2}\left|h_{RE,n}h_{RD,m} - h_{RE,m}h_{RD,n}\right|^2. \quad (13)$$

Relay nodes R_m and R_n are selected to maximize the SNR at the destination, $\gamma_D^{(2)}$. Therefore, the relay selection rule can be written as

$$(m^*, n^*) = \underset{\substack{m,n\in\{1,...,M\}\\ m\neq n}}{\arg\max}\,\gamma_{D,(m,n)}^{(2)}. \quad (14)$$

In *phase I,* we select three intermediate nodes to act as jammers, in order to create interference and confuse the eavesdropper. Suppose that the selected jammers are $\mathbf{J} = (R_o\ R_p\ R_q)$, and the corresponding beamforming vector is $\mathbf{u} = [u_1\ u_2\ u_3]^T$.

In *phase I*, the received signals at R_m and R_n, can be expressed as

$$y_{R_m}^{(1)} = \sqrt{P_S} h_{SR_m} x + \sqrt{P_J} \mathbf{u}^T \mathbf{h}_{JR_m} z + n_{R_m}^{(1)}, \quad (15)$$

$$y_{R_n}^{(1)} = \sqrt{P_S} h_{SR_n} x + \sqrt{P_J} \mathbf{u}^T \mathbf{h}_{JR_n} z + n_{R_n}^{(1)}, \quad (16)$$

where x is the transmitted signal, z is the jamming signal, $\mathbf{h}_{JR_m} = [h_{R_oR_m}\ h_{R_pR_m}\ h_{R_qR_m}]^T$,$\mathbf{h}_{JR_n} = [h_{R_oR_n}\ h_{R_pR_n}\ h_{R_qR_n}]^T$, $h_{SR_m}$and h_{SR_n} are the channel coefficients between the source and the relay R_m and R_n, respectively. $n_{R_m}^{(1)}$ and $n_{R_n}^{(1)}$ denote the complex white Gaussian noise at R_m and R_n, respectively. We are assuming that the jamming signal has unit power, i.e, $E\left\{|z|^2\right\} = 1$. The received signal at the eavesdropper in *phase I* can be expressed as

$$y_E^{(1)} = \sqrt{P_S} h_{SE} x + \sqrt{P_J} \mathbf{u}^T \mathbf{h}_{JE} z + n_E^{(1)}, \quad (17)$$

where $\mathbf{h}_{JE} = [\ h_{R_oE}\ \ h_{R_pE}\ \ h_{R_qE}\ ]^T$. In order to make sure that the relay nodes (R_m, R_n) can correctly decode the source message, the source power is chosen such that rates between the source and each intermediate node should be greater than a threshold R_{th}. In order to have successful decoding at the relay nodes, the following conditions need to be satisfied:

$$\log_2(1 + \frac{P_S \left|h_{SR_i}\right|^2}{\sigma_n^2}) > R_{th}. \quad (18)$$

By simple calculation, we get

$$P_S > \frac{\left(2^{R_{th}} - 1\right)\sigma_n^2}{\left|h_{SR_{(\min)}}\right|^2}, \quad (19)$$

where $h_{SR_{(\min)}} = \min_{i=m,n} \{h_{SR_i}\}$. Then, we want to eliminate the effect of jammers on the relay pair (R_m, R_n), that are going to send the source message to the destination in *phase II.* To reach this goal, we should have

$$\mathbf{u}^T \mathbf{h}_{\mathbf{J}R_m} = 0, \quad (20)$$

$$\mathbf{u}^T \mathbf{h}_{\mathbf{J}R_n} = 0, \quad (21)$$

$$\mathbf{u}\mathbf{u}^H = 1. \quad (22)$$

Rewriting above equations in the matrix form, we obtain

$$\begin{pmatrix} h_{R_oR_m} & h_{R_pR_m} & h_{R_qR_m} \\ h_{R_oR_n} & h_{R_pR_n} & h_{R_qR_n} \\ u_1^* & u_2^* & u_3^* \end{pmatrix} \begin{pmatrix} u_1 \\ u_2 \\ u_3 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 1 \end{pmatrix}. \quad (23)$$

By a simple calculation, the beamforming vector be obtained as Equations (24,25,26), which are presented on top of page 5.

As a result, the desired beamforming vector in *phase I* is obtained. Now, we select the intermediate nodes (R_o, R_p, R_q) out of $M-2$ intermediate nodes such that the received SNR at the eavesdropper is minimized. According to (17) the received

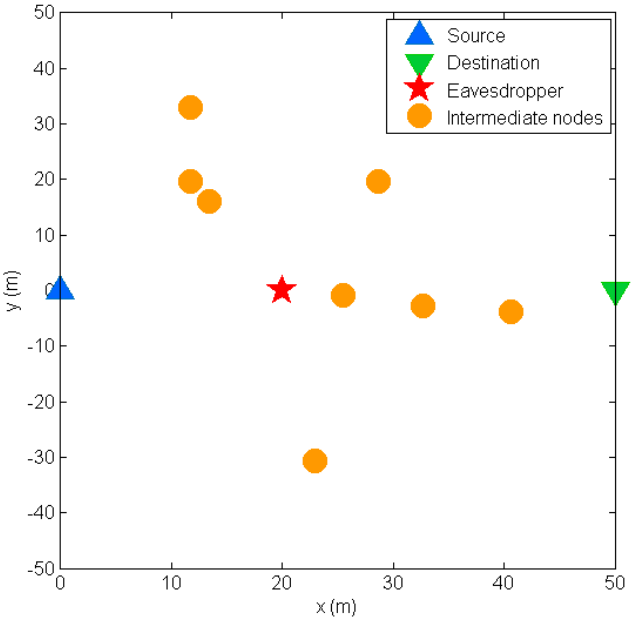

Figure 4. A 2D topology of the system used for numerical experiments. S(0,0), E(20,0), D(50,0) and M=8 randomly-distributed intermediate nodes.

SNR at the eavesdropper in *phase I* is

$$\gamma_E^{(1)} = \frac{P_S \left|h_{SE}\right|^2}{\sigma_n^2 + P_J \left|\mathbf{u}^T \mathbf{h}_{JE}\right|^2}. \quad (27)$$

Therefore, the jammer selection rule can be written as

$$(o^*, p^*, q^*) = \begin{array}{l} \arg\max \left|\mathbf{u}^T \mathbf{h}_{RE}\right|^2 \\ .(o,p,q) \in \{1, ..., M\} \\ o,p,q \neq m,n \end{array} \quad (28)$$

Since the eavesdropper receives the source signal in both phases, it can benefit from the maximum ratio combining (MRC) technique. So the achievable secrecy rate is

$$R_S = \max\left\{\frac{1}{2}\log_2(\frac{1+\gamma_D^{(2)}}{1+\gamma_E^{(1)}+\gamma_E^{(2)}}), 0\right\}. \quad (29)$$

Since we use beamforming such that $\gamma_E^{(2)} = 0$, the achievable secrecy rate for our system can be obtained as follows

$$R_S = \max\left\{\frac{1}{2}\log_2(\frac{1+\gamma_D^{(2)}}{1+\gamma_E^{(1)}}), 0\right\}. \quad (30)$$

IV. Numerical Results

In this Section, we evaluate the performance of our proposed scheme. The 2D topology of the system is demonstrated in Fig. 4, where the network consists of a source, a destination, an eavesdropper and 8 randomly distributed intermediate nodes. Channels between any two nodes are modeled using frequency-flat Rayleigh fading with a path loss, i.e., $h_{i,j} \sim \mathcal{CN}(0, d_{i,j}^{-\beta})$ where $d_{i,j}$ is the distance between node i and node j, and the path loss exponent is $\beta = 3.5$. We also consider the total

$$u_1 = \frac{h_{R_pR_m}h_{R_qR_n} - h_{R_pR_n}h_{R_qR_m}}{\sqrt{(h_{R_pR_m}h_{R_qR_n} - h_{R_pR_n}h_{R_qR_m})^2 + (h_{R_oR_n}h_{R_qR_m} - h_{R_oR_m}h_{R_qR_n})^2 + (h_{R_oR_m}h_{R_pR_n} - h_{R_pR_m}h_{R_oR_n})^2}}, \quad (24)$$

$$u_2 = \frac{h_{R_oR_n}h_{R_qR_m} - h_{R_oR_m}h_{R_qR_n}}{\sqrt{(h_{R_pR_m}h_{R_qR_n} - h_{R_pR_n}h_{R_qR_m})^2 + (h_{R_oR_n}h_{R_qR_m} - h_{R_oR_m}h_{R_qR_n})^2 + (h_{R_oR_m}h_{R_pR_n} - h_{R_pR_m}h_{R_oR_n})^2}}, \quad (25)$$

$$u_3 = \frac{h_{R_oR_m}h_{R_pR_n} - h_{R_pR_m}h_{R_oR_n}}{\sqrt{(h_{R_pR_m}h_{R_qR_n} - h_{R_pR_n}h_{R_qR_m})^2 + (h_{R_oR_n}h_{R_qR_m} - h_{R_oR_m}h_{R_qR_n})^2 + (h_{R_oR_m}h_{R_pR_n} - h_{R_pR_m}h_{R_oR_n})^2}}. \quad (26)$$

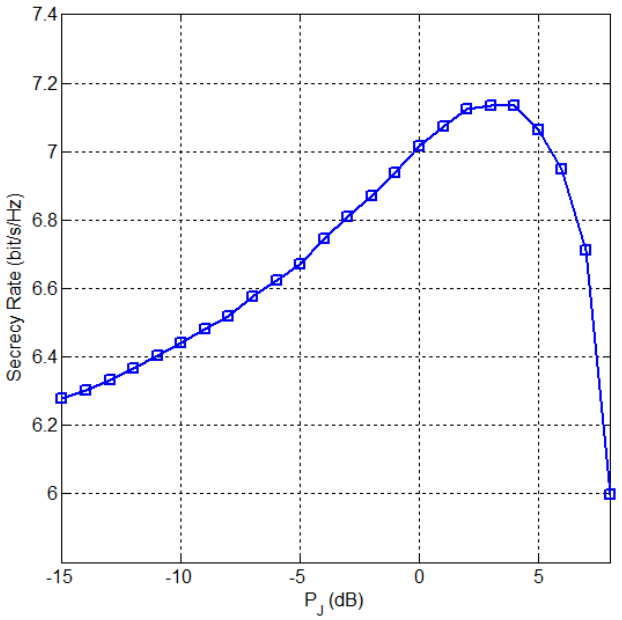

Figure 5. The average secrecy rates of the proposed scheme versus the power of jammers. Power constraints of the system are P_T=10W, P_S=3W, P_R= $P_T - P_S - P_J$.

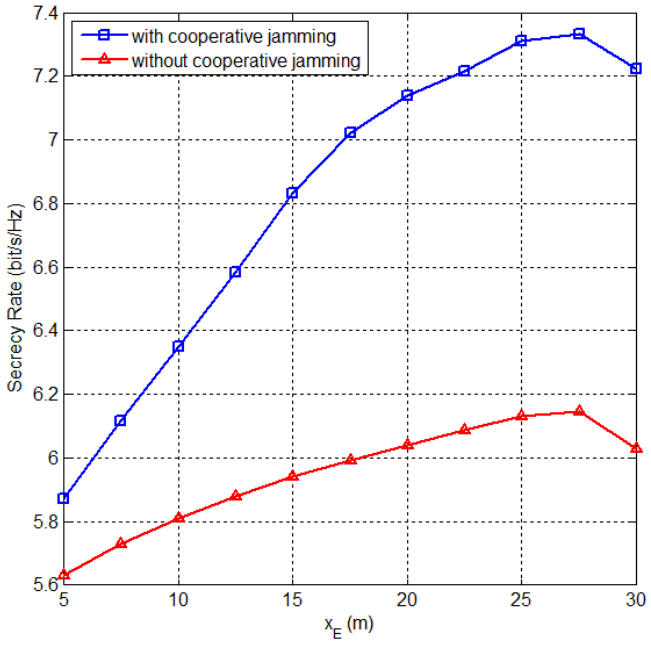

Figure 6. The average secrecy rates versus the eavesdropper's locations. The eavesdropper moves from (5,0) to (30,0), and the jammer power is fixed, $P_J = 3dB$.

power constraint, $P_T = 10W$. By performing Monte-Carlo experiments consisting of 10^4 independent trials with independent channel realizations, the average results are obtained. Due to the assumption that all intermediate nodes can decode the received signal properly we can assign a relatively large value $P_S = 3W$ to satisfy this condition.

Fig. 5 represents the average secrecy rate of the proposed cooperative scheme versus the power of jammers. Based on allocating different powers to jammers or relays, we get different secrecy rates. As it can be observed, the system's secrecy rate increases until reaches a maximum point and then falls down drastically because all the power is allocated to jammers and there is no more power left for the relays to transmit the source signal. Since the total power is fixed we can have a fair comparison between our system that uses cooperative jamming and a system without cooperative jamming.

In Fig. 6, the average secrecy rate of the proposed cooperative scheme versus the eavesdropper's locations is plotted when the eavesdropper moves from (5,0) to (30,0). The system without cooperative jamming is also simulated for comparison. In the later case, the total power is allocated to the source and the relays. As in can be observed from Fig.6, the secrecy rate of the proposed scheme with cooperative jamming outperforms the system without cooperative jamming at all points.

V. Conclusion

In this paper, a cooperative jamming, cooperative beamforming and relay selection scheme is proposed to enhance the secrecy rate in the presence of an eavesdropper. In the proposed scheme, some relay nodes are selected to act as jammers in the first phase in order to create interference for the eavesdropper by sending jamming signals; while we select two other nodes to relay information of the source to the destination in second phase. Cooperative beamforming is performed in this system in both phases. Since we only use five intermediate nodes, two of them for relaying and the others for jamming, the system has low operational complexity. Numerical results demonstrate the superiority of the proposed scheme compared with the scheme with no cooperative jamming. As the future work, we would

work on optimal power allocation for jammers and relays to get the maximum secrecy rate under a total power constraint.

REFERENCES

[1] A. D. Wyner, "The wire-tap channel," *Bell System Technical Journal, The*, vol. 54, no. 8, pp. 1355–1387, 1975.

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

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

[4] E. Tekin and A. Yener, "The general gaussian multiple-access and two-way wiretap channels: Achievable rates and cooperative jamming," *IEEE Trans. Inf. Theory*, vol. 54, no. 6, pp. 2735–2751, 2008.

[5] R. Bassily, E. Ekrem, X. He, E. Tekin, J. Xie, M. Bloch, S. Ulukus, and A. Yener, "Cooperative security at the physical layer: a summary of recent advances," *Signal Processing Magazine, IEEE*, vol. 30, no. 5, pp. 16–28, 2013.

[6] J. Yang, I. M. 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, 2013.

[7] L. Dong, Z. Han, A. P. Petropulu, and H. V. Poor, "Cooperative jamming for wireless physical layer security," in *Proc. 15th Workshop on Statistical Signal Processing (SSP)*. IEEE, 2009, pp. 417–420.

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

[9] J. Zhang and M. C. Gursoy, "Relay beamforming strategies for physical-layer security," in *Proc. 44th Ann. Conf. Inf. Sci. Syst. (CISS)*. IEEE, 2010, pp. 1–6.

[10] R. Zhang, L. Song, Z. Han, B. Jiao, and M. Debbah, "Physical layer security for two way relay communications with friendly jammers," in *Proc. Global Telecommunications Conference (GLOBECOM)*. IEEE, 2010, pp. 1–6.

[11] I. Krikidis, "Opportunistic relay selection for cooperative networks with secrecy constraints," *IET Communications*, vol. 4, no. 15, pp. 1787–1791, 2010.

[12] I. Krikidis, J. S. Thompson, and S. McLaughlin, "Relay selection for secure cooperative networks with jamming," *IEEE Trans. Wireless Commun.*, vol. 8, no. 10, pp. 5003–5011, 2009.

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

[14] 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, 2013.

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

[16] J. Kim, A. Ikhlef, and R. Schober, "Combined relay selection and cooperative beamforming for physical layer security," *Journal of Communications and Networks*, vol. 14, no. 4, pp. 364–373, 2012.

[17] W. Liu, M. Z. I. Sarkar, and T. Ratnarajah, "Combined approach of zero forcing precoding and cooperative jamming: A secrecy tradeoff," in *Proc. Wireless Communications and Networking Conf. (WCNC)*. IEEE, 2013, pp. 1825–1829.

[18] S. Huang, J. Wei, Y. Cao, and C. Liu, "Joint decode-and-forward and cooperative jamming for secure wireless communications," in *Proc. 7th Int. Conf. Wireless Communications, Networking and Mobile Computing (WiCOM)*. IEEE, 2011, pp. 1–4.

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

[20] 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, 2012.

[21] H. Long, W. Xiang, J. Wang, Y. Zhang, and W. Wang, "Cooperative jamming and power allocation with untrusty two-way relay nodes," *IET Communications*, vol. 8, no. 13, pp. 2290–2297, 2014.

[22] L. Wang, C. Cao, M. Song, and Y. Cheng, "Joint cooperative relaying and jamming for maximum secrecy capacity in wireless networks," in *Proc. Int. Conf. Communications (ICC)*. IEEE, 2014, pp. 4448–4453.

[23] C. Xing, N. Wang, J. Ni, Z. Fei, and J. Kuang, "MIMO beamforming designs with partial CSI under energy harvesting constraints," *IEEE Signal Process. Lett.*, vol. 20, no. 4, pp. 363–366, 2013.

[24] H. Deng, H. M. Wang, W. Guo, and W. Wang, "Secrecy transmission with a helper: To relay or to jam," *IEEE Trans. Inf. Forensics Security*, vol. PP, no. 99, pp. 1–1, 2014.

[25] J. Li, A. P. Petropulu, and S. Weber, "On cooperative relaying schemes for wireless physical layer security," *IEEE Trans. Signal Process.*, vol. 59, no. 10, pp. 4985–4997, 2011.

[26] 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, 2010.

[27] M. Bloch, J. Barros, M. R. D. Rodrigues, and S. W. McLaughlin, "Wireless information-theoretic security," *IEEE Trans. Inf. Theory*, vol. 54, no. 6, pp. 2515–2534, 2008.