IJICTR International Journal of Information & Communication Technology Research

Volume 8 - Number 3- Summer 2016 (63-69)

On Maximizing the Secrecy Rate in a Cooperative Wireless Network using Friendly Jammers

Mohammad Hatami
Department of Electrical Engineering
Sharif University of Technology
Tehran, Iran
hatami_mohammad@ee.sharif.edu

Hamid Behroozi
Department of Electrical Engineering
Sharif University of Technology
Tehran, Iran
behroozi@sharif.edu

Received: March 14, 2016- Accepted: June 21, 2016

Abstract—**In this paper, the security of two-phase relaying system with multiple intermediate nodes in the presence of a malicious eavesdropper is investigated. To enhance the secrecy, a joint cooperative beamforming and jamming combined with relay and jammer selection is proposed. First, the source broadcasts its signal to the relays that are located close to source in a cluster, i.e., the source node uses a small amount of power to broadcast its message locally to other nodes of the cluster, while destination and the eavesdropper are located outside this cluster. In the second phase, two relays transmit re-encoded signal with optimal beamforming such that the secrecy rate is maximized. Simultaneously, two other intermediate nodes (which act as friendly jammers) transmit random jamming signals to degrade the eavesdropper's channel. Our goal in this paper is to maximize the secrecy rate by applying different methods such as cooperative beamforming, cooperative jamming and relay and jammer selection. To avoid operational complexity, we consider the minimum number of intermediate nodes needed for relaying and jamming without losing the performance, i.e., achieving a non-zero secrecy rate. Cooperative beamforming with multiple relays demands high amount of information exchange and therefore increases the operational complexity. Thus, we aim to reduce the number of relays which take part in cooperative beamforming. Limiting the number of relays may have a bad effect on the coding gain which we compensate it with a proposed selection gain scheme. Numerical results demonstrate the advantage of our proposed scheme compared to the scheme with no cooperative jamming. The main contribution of this work is combining cooperative beamforming and jamming with relay and jammer selection to enhance the physical layer security.**

Keywords-physical layer secrecy; secrecy rate; cooperative jamming; beamforming;relay and jammer selection

I. INTRODUCTION

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 early studies, single-input single-output systems with a wiretap channel model were proposed as the fundamental model for investigating physical layer secrecy. Wyner in his pioneering work [1] revealed that perfect secrecy without relying on private (secret) keys, is possible when the eavesdropper channel (source-eavesdropper channel) is a degraded version of the main channel i.e., the source-destination channel. Csiszár and Korner generalized the Wyner's work for broadcast channels with confidential messages [2]. Wyner's approach is applied to Gaussian wiretap channels in [3]. The general idea is to exploit

the physical characteristics of the wireless channel in order to provide secure communications. The security is measured by secrecy capacity, which is defined as the maximum reliable rate under which a perfectly secret communication is possible from the source to the intended destination in the presence of eavesdroppers.

Physical layer security approaches are typically feasible only when the source-eavesdropper channel is weaker than the source-destination channel. Node cooperation and generating artificial noise (also called cooperative jamming) can be used to overcome this challenge and increase the secrecy rate. 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 noise signals to degrade the channel of the eavesdropper [4], [5]. Cooperative jamming was first developed with the motivation that multihop transmissions are preferred in many wireless networks, and it is challenging to keep the source information secure from those intermediate nodes which might be untrusted nodes.

Cooperative beamforming, cooperative jamming and relay selection are three common techniques to overcome the security issues and enhance the secrecy rate. In [6] and [7] cooperative beamforming is used to enhance secrecy. In these works, a set of collaborating nodes act as a distributed antenna system so that the signals are combined constructively at the intended destination. Relay selection is another approach to utilize multiple relays for the physical layer security. Intelligent relay selection policies can also be devised to further increase the achievable secrecy rate. In [8], performance of the opportunistic relay selection is investigated in order to maximize the ratio of SNRs at the destination and at the eavesdropper. Compared to our work, in [8] cooperative jamming and beamforming are not applied and only one relay is selected. In [9] an optimal relay selection and jamming scheme is proposed. For the relay selection, only channel gains are needed while full channel state information (CSI) is necessary for the cooperative beamforming. In [9], two relays are selected to increase security; the first relay for retransmitting confidential message to the destination and the second one for creating interference at the eavesdropper to confuse it. Note that although in [9] the relay selection criterion is based on maximizing the secrecy rate, it is assumed that the first phase is completely secured. Comparing to our work, in [9] beamforming technique is not established and the interference cancellation scheme at the destination is not considered. In [10], the authors investigate the relay and jammer selection problem in the two-way relay networks. Cooperative jamming strategy based on Stackelberg security game is investigated in [11]. They prove the existence and uniqueness of the Stackelberg Equilibrium and develop a distributed iterative power allocation algorithm to reach the Stackelberg Equilibrium point.

In [12], three jamming power allocation strategies are derived to minimize the outage probability of the secrecy rate in two-hop wireless relaying networks with one eavesdropper. In [13] 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 [14]. In [15] 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 source signal. Since the cooperative jamming is not applied in [15], it is similar to “without cooperative jamming” scheme in our work. [16] 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 [17] 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 jamming signal to confuse the eavesdropper. Compared to our work, in [17] relay selection is not applied and the ultimate goal is minimizing the transmit power subject to a secrecy rate constraint. More recently, motivated by multiple-input multiple-output (MIMO) techniques, the issue of secrecy at physical layer in MIMO wiretap channels has attained much interest [18],[19] and [20]. In [21], authors use cooperative relaying techniques to improve the secrecy rate. In [22] cooperative jamming is adopted to enhance security in situations where we have untrusted relays. In [23] 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 [24] the problem of choosing a jammer and a relay per phase is examined. In [25], 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 [26] we investigate the security of two-phase relaying system with multiple intermediate nodes and in the presence of an eavesdropper. In the first phase, the source node broadcasts a signal to relays while three friendly jammers help the source node to confuse the eavesdropper. In the second phase, two relays transmit the source message with beamforming coefficients such that the received signal at the eavesdropper is completely nulled out. It is necessary to mention that the system model we considered in [26] is completely different from the model investigated in this paper. In [26] the relays and the source are not in the same cluster and there is a link between the eavesdropper and the source. In addition, in [26], we use the zero-forcing method, that is a sub-optimal method.

In this paper, we propose a combined cooperative jamming and beamforming with joint relay and jammer selection scheme. In this paper, a wireless network model consisting of one source node (S), M intermediate nodes ($R_1, \ldots, R_M$), a destination (D), and an eavesdropper (E) is considered. In order to send the message from the source to the destination, a two-phase scheme is introduced. In the first phase, the source broadcasts its message signal locally to the intermediate nodes within the cluster and thus, the information rate at the eavesdropper can be ignored. So the first phase is completely secure. In the second phase, we use

cooperative jamming and beamforming to send the message to the destination. Due to the high amount of operational complexity in cooperative beamforming with multiple relays, we involve the minimum intermediate nodes that are necessary to reach the desired performance. We select two relay nodes to act as jammers and confuse the eavesdropper while two other intermediate nodes relay information to the destination. Selection rules are based on maximizing the secrecy rate. The problem of beamforming in relays equals to an optimization problem that can be formulated as maximizing a Rayleigh quotient. We assume that the global CSI is available for the system design (a common assumption as in most of the PHY-based security literature, see e.g., [27],[7],[28],[23],[29] and [30]). In practice, destination related CSI can be obtained by periodic pilots, and eavesdroppers related CSI may be obtained by monitoring the behavior of eavesdropper.

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

Throughout the paper, upper-case letter X denotes a matrix, boldface letter **x** denotes a column vector. We denote the vector of channel gains between the source and intermediate nodes by $\boldsymbol{h}_{SR} = [h_{SR_1}, h_{SR_2}, \dots, h_{SR_M}]$, and the channel gains from the intermediate nodes to the eavesdropper by $\boldsymbol{h}_{RE} = [h_{R_1E}, h_{R_2E}, \dots, h_{R_ME}]$ and the channel gain from the intermediate nodes to the destination by $\boldsymbol{h}_{RD} = [h_{R_1D}, h_{R_2D}, \dots, h_{R_MD}]$.

II. System Model

In this paper, a wireless network model consisting of one source node (S), M intermediate nodes $(R_1, \dots, R_M)$, a destination (D), and an eavesdropper (E) is considered (See Fig.1). All nodes in the network operate in half-duplex mode and equipped with only one single omnidirectional antenna. The eavesdropper is passive which listens to the information transmitted by the source and its goal is interpreting the source information without trying to jam it or modify it. We assume that the channels for different pairs of nodes are modeled using frequency-flat Rayleigh fading with additive white Gaussian noise (AWGN). We also assume that the direct links from the source to the destination and to the eavesdropper, S→D and S→E, are not available, i.e., the first phase is taken to be secure. It is note that the source-destination communication is performed via the intermediate nodes. For instance, the source and the intermediate nodes are located in the same cluster, while the destination and the eavesdropper are far away from the source, i.e., they are located in another cluster. This model in also considered in some other papers in the literature, see e.g., [9] and [30].

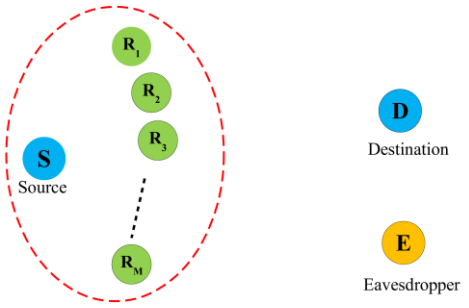

Fig. 1. Our system model, consisting of a source, a destination, an eavesdropper and M intermediate nodes. The source and the intermediate nodes are located in the same cluster, while the destination and the eavesdropper are located outside this cluster.

III. Combined Relay Selection, Cooperative Jamming and Beamforming

In order to send the message from the source to the destination a two-phase scheme is introduced. In the first phase, the source broadcasts its message signal locally to the intermediate nodes within the cluster. The power of the source is chosen such that the message signal can be decoded at intermediate nodes with high probability while the eavesdropper cannot decode the message. In the second phase, we select two relays, out of *M* intermediate nodes. The selected relays decode the source message and then employ optimal beamforming such that the secrecy rate is maximized. Simultaneously, two preselected intermediate nodes (which act as jammers) help the source node by generating a weighted artificial noise to interfere with the eavesdropper's received signal while no interference occurs at the destination.

Suppose that P_S is the transmit power of the source in the first phase. So, the received signal at the *i*th intermediate node can be expressed as

$$y_{R_i} = \sqrt{P_S} h_{SR_i} x + n_{R_i}, \quad (1)$$

where n_{R_i} denotes the additive noise at the *i*th intermediate node which is a white complex Gaussian with zero mean and variance σ_n^2, i.e., $n_{R_i} \sim \mathbb{C}\mathcal{N}(0, \sigma_n^2)$. Also we assume that the power of the message signal is normalized to unity, $E\{X^2\} = 1$.

To simultaneously ensure that (a) all intermediate nodes can decode the source signal successfully and (b) an eavesdropper cannot decode the source signal, the channel capacity between the source and each intermediate node must be greater than a threshold, R_{th}^R, and the capacity between the source and the eavesdropper must be lower than a threshold, R_{th}^E. In other words $R_{SR_i} > R_{th}^R$, for $i = 1,2,\dots,M$ and $R_{SE} > R_{th}^E$. So we obtain

$$\begin{cases} \log_2\left(1 + \frac{P_S |h_{SR_i}|^2}{\sigma_n^2}\right) > R_{th}^R; i = 1,2,\dots,M \\ \log_2\left(1 + \frac{P_S |h_{SE}|^2}{\sigma_n^2}\right) < R_{th}^E \end{cases} \quad (2)$$

Combining the inequalities in Eq. (2), we get

$$\frac{(2^{R_{th}^{R}}-1)\sigma_n^2}{\left|h_{SR_{(\min)}}\right|^2} < P_S < \frac{(2^{R_{th}^{E}}-1)\sigma_n^2}{|h_{SE}|^2} \quad (3)$$

here $h_{SR_{(\min)}} = \min\{h_{SR_i}\}_{i=1,2,\ldots,M}$. Since we have supposed that the source and the intermediate nodes are in the same cluster, i.e., the intermediate nodes are closer to the source than the eavesdropper, there exists a feasible set for appropriate transmit power of the source (due to Eq. (3)). Therefore, the source message is sent to all intermediate nodes confidentially.

In the second phase, we select four nodes. Two of them $\{R_m, R_n\}$ send the message to the destination by using optimal beamforming, while the rest, $\{R_p, R_j\}$, act as jammers and generate weighted artificial noise, i.e., apply beamforming. Suppose that $\mathbf{w} = \{w_m, w_n\}$ is the beamforming vector for relays and $\mathbf{u} = \{u_p, u_j\}$ is the beamforming vector for jammers.

The received signals at the destination and at the eavesdropper can be expressed as

$$y_D = \sqrt{P_R}\mathbf{w}\mathbf{h}_{RD_{(m,n)}}^T x + \sqrt{P_J}\mathbf{u}\mathbf{h}_{RD_{(p,j)}}^T z + n_D, \quad (4)$$

$$y_E = \sqrt{P_R}\mathbf{w}\mathbf{h}_{RE_{(m,n)}}^T x + \sqrt{P_J}\mathbf{u}\mathbf{h}_{RE_{(p,j)}}^T z + n_E, \quad (5)$$

where $\boldsymbol{h}_{RD_{(m,n)}} = \left[h_{R_mD}, h_{R_nD}\right]$, $\mathbf{h}_{RE_{(m,n)}} = [h_{R_mE}h_{R_nE}]$, $\boldsymbol{h}_{RD_{(p,j)}} = \left[h_{R_pD}, h_{R_jD}\right]$, $\mathbf{h}_{RE_{(p,j)}} = [h_{R_pE}h_{R_jE}]$, P_R is the total transmit power of relays, and P_J is the total transmit power of jammers. n_D and n_E denote the white complex Gaussian noise at the destination and at the eavesdropper, respectively. The jamming signal is represented by z and has unity power, i.e., $E\{|Z|^2\} = 1$. The goal of jammers is to interfere with the eavesdropper's received signal. Thus, in order to completely null out the jamming signal at the destination, $\mathbf{u} = \{u_p, u_j\}$ must be in the null space of $\boldsymbol{h}_{RD_{(p,j)}} = \left[h_{R_pD}, h_{R_jD}\right]$. This means that

$$\begin{cases} \mathbf{u}\mathbf{h}_{RD_{(p,j)}}^T = 0. \\ s.t. \quad \mathbf{u}\mathbf{u}^H = 1 \end{cases} \quad (6)$$

Solving Eq. (6), the optimal beamforming vector at the jammers is obtained as

$$\mathrm{u}_p = \alpha h_{R_jD}, \quad (7)$$

$$\mathrm{u}_j = -\alpha h_{R_pD}, \quad (8)$$

where $\alpha = \frac{1}{\left|h_{R_pD}\right|^2 + \left|h_{R_jD}\right|^2}$. Rewriting Eq. (4) and Eq. (5), we have

$$y_D = \sqrt{P_R}\mathbf{w}\mathbf{h}_{RD_{(m,n)}}^T x + n_D, \quad (9)$$

$$y_E = \sqrt{P_R}\mathbf{w}\mathbf{h}_{RE_{(m,n)}}^T x + \sqrt{P_J}\mathbf{u}\mathbf{h}_{RE_{(p,j)}}^T z + n_E, \quad (10)$$

Now, we obtain the beamforming vector at the relays such that the achievable secrecy rate is maximized. The achievable secrecy rate is defined as [31]:

$$R_S = \max\{R_D - R_E, 0\}, \quad (11)$$

where

$$R_D = \frac{1}{2}\log_2(1+\gamma_D), \quad (12)$$

$$R_E = \frac{1}{2}\log_2(1+\gamma_E), \quad (13)$$

According to Eq. (9) and Eq. (10), we have

$$\gamma_D = \frac{P_R\left|\mathbf{w}\mathbf{h}_{RD_{(m,n)}}^T\right|^2}{\sigma_n^2} = \frac{P_R}{\sigma_n^2}\mathbf{w}\mathbf{H}_{RD_{(m,n)}}\mathbf{w}^H, \quad (14)$$

$$\gamma_E = \frac{P_R\left|\mathbf{w}\mathbf{h}_{RE_{(m,n)}}^T\right|^2}{\sigma_n^2 + \left|\mathbf{u}\mathbf{h}_{RE_{(p,j)}}^T\right|^2} = \frac{P_R\mathbf{w}\mathbf{H}_{RE_{(m,n)}}\mathbf{w}^H}{\sigma_n^2 + \mathbf{u}\mathbf{G}_{RE_{(p,j)}}\mathbf{u}^H}, \quad (15)$$

where

$$\mathbf{H}_{RD_{(m,n)}} = \mathbf{h}_{RD_{(m,n)}}^T\mathbf{h}_{RD_{(m,n)}}^*$$

$$\mathbf{H}_{RE_{(m,n)}} = \mathbf{h}_{RE_{(m,n)}}^T\mathbf{h}_{RE_{(m,n)}}^*$$

$$\mathbf{G}_{RE_{(p,j)}} = \mathbf{h}_{RE_{(p,j)}}^T\mathbf{h}_{RE_{(p,j)}}^*.$$

Replacing Eq. (14) and Eq. (15) in Eq. (11), the achievable secrecy rate is obtained as

$$\mathrm{R}_S = \left[\log_2\left(\frac{1+\gamma_D}{1+\gamma_E}\right)\right]^+, \quad (16)$$

where $[x]^+ = \max\{0, x\}$.

For a fixed power budget, we want to have the maximum secrecy rate. As we said before, suppose that the selected relays are (R_m, R_n) and the selected jammers are (R_p, R_j) . Since the logarithm is an increasing function of its argument, the problem of secrecy rate maximization is equivalent to

$$\begin{cases} \max\left(\frac{1+\gamma_D}{1+\gamma_E}\right) \\ s.t. \quad \mathbf{w}\mathbf{w}^H = 1 \end{cases} \quad (17)$$

By a simple calculation, we have

$$\frac{1+\gamma_D}{1+\gamma_E} = \frac{1+\gamma_{0D}\mathbf{w}\mathbf{H}_{RD_{(m,n)}}\mathbf{w}^H}{1+\gamma_{0E}\mathbf{w}\mathbf{H}_{RE_{(m,n)}}\mathbf{w}^H} =$$

$$\frac{\mathrm{w}\left(\mathrm{I}_{2\times2} + \gamma_{0D}\mathrm{H}_{\mathrm{RD}_{(\mathrm{m,n})}}\right)\mathrm{w}^{\mathrm{H}}}{\mathrm{w}\left(\mathrm{I}_{2\times2} + \gamma_{0E}\mathrm{H}_{\mathrm{RE}_{(\mathrm{m,n})}}\right)\mathrm{w}^{\mathrm{H}}}, \quad (18)$$

where $\gamma_{0D} = \frac{P_R}{\sigma_n^2}$ and $\gamma_{0E} = \frac{P_R}{\sigma_n^2 + \mathbf{u}\mathbf{G}_{RE_{(p,j)}}\mathbf{u}^H}$. By replacing Eq. (18) in Eq. (17), the optimization problem can be reformulated as

$$\begin{cases} \max & \{\frac{\mathbf{w}\tilde{A}\mathbf{w}^H}{\mathbf{w}\tilde{B}\mathbf{w}^H}\} \\ s.t. & \mathbf{w}\mathbf{w}^H = 1 \end{cases} \quad (19)$$

where

$$\tilde{A} = I_{2\times 2} + \gamma_{0D}\mathbf{H}_{RD_{(m,n)}}$$
$$\tilde{B} = I_{2\times 2} + \gamma_{0E}\mathbf{H}_{RE_{(m,n)}}$$

The above optimization problem can be formulated as maximizing a Rayleigh quotient. By a simple modification, it can be solved using Lagrange multipliers. The solution of this problem is the eigenvector corresponding to the largest eigenvalue of the symmetric matrix $\tilde{B}^{-1}\tilde{A}$. As a result, the optimal beamforming vector can be written as

$$\mathbf{w} = \mathrm{V}_{max}\left(\left(I_{2\times 2} + \gamma_{0D}\mathbf{H}_{RD_{(m,n)}}\right)^{-1}\left(I_{2\times 2} + \gamma_{0E}\mathbf{H}_{RE_{(m,n)}}\right)\right). \quad (20)$$

where $\mathrm{V}_{max}(\mathrm{X})$ denotes the eigenvector corresponding to the largest eigenvalue of the matrix X.

Note that in order to maximize the secrecy rate, **w**, the beamforming vector for relays and **u**, the beamforming vector for jammers should be obtained jointly. Since we found these beamforming vectors sequentially, our solution can be considered as a sub-optimal solution.

Now, we can find the best relays and jammers, this means that, the relay pairs and jammer pairs are selected according to

$$\{(R_m, R_n), (R_p, R_j)\} = \arg\max_{R_i}\left(\frac{1+\gamma_D}{1+\gamma_E}\right) \quad (21)$$

Note that finding a closed form solution does not seem to be tractable, thus the secrecy capacity will be evaluated numerically using simulations in Section IV.

IV. Numerical Results

In this Section, we evaluate the performance of our proposed scheme and compare the proposed scheme with the existing ones. The 2D topology of the system is demonstrated in Fig. 2, where the network consists of a source, a destination, an eavesdropper and M randomly distributed intermediate nodes. The source and the destination are located at fixed points (0,0) and (100,0), respectively. The channels between any two nodes are modeled using frequency-flat Rayleigh fading with a path loss, i.e., $h_{i,j}\sim\mathbb{CN}(0, d_{i,j}^{-\beta})$ 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 power constraint, $P_T = 2.5W$ and the noise power $\sigma_n^2 = -65dBm$. The cluster is a half disk with radius $R = 16$. The cluster nodes (intermediate nodes) are uniformly distributed in the half disk as in Fig. 2. In order to procure the average results, we execute Monte-Carlo experiments consisting of 10^4 independent trials with independent channel realizations.

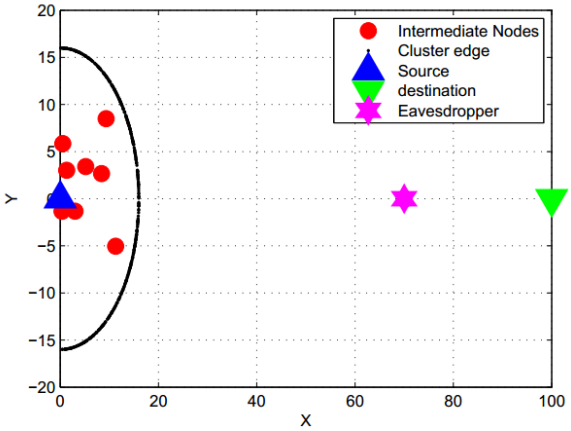

Fig. 2. A 2D topology of the system used for numerical experiments. S(0,0), E(70,0), D(100,0) and M=8 randomly-distributed intermediate nodes.

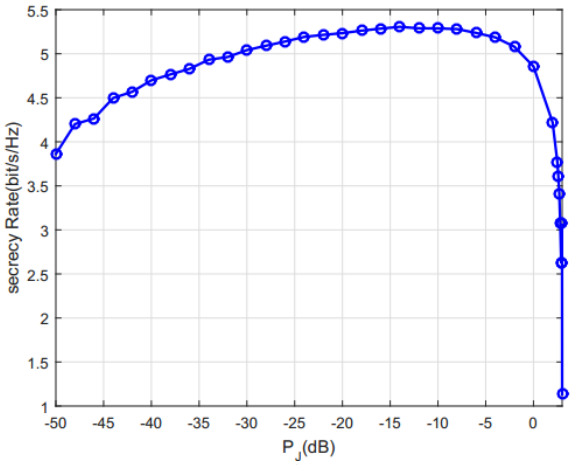

Fig. 3. The average secrecy rates of the proposed scheme versus the power of jammers, when $M = 8$, $x_E = 70, x_D = 100$. Power constraints of the system are $P_T = 2.5$W, $P_S = 0.5$W, $P_R = P_T - P_S - P_J = 2 - P_J$.

The average secrecy rate of the proposed cooperative scheme versus the power of jammers is depicted in Fig. 3 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.

A fair comparison between our proposed system that uses cooperative jamming and a system without cooperative jamming can be performed, since we suppose that the total power is fixed in two scenarios. In Fig. 4, Fig. 5 and, the average secrecy rate of the proposed cooperative scheme versus the eavesdropper's locations is plotted when the eavesdropper moves from (50,0) to (110,0) and we have $M = 6$, $M = 8$ and $M = 10$ intermediate nodes, respectively. The system without cooperative jamming is also simulated for comparison. In the latter case, the total power is allocated to the source and the relays. As it can be observed from these figures, the secrecy rate of the proposed scheme with cooperative jamming outperforms the system without cooperative jamming,

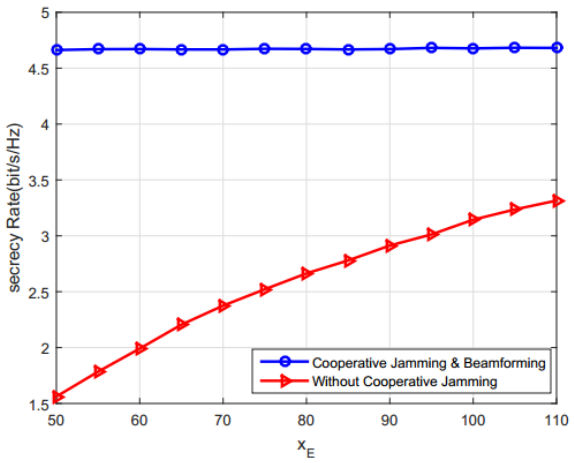

Fig. 4 .The average secrecy rates versus the eavesdropper's locations when $M = 6$. The eavesdropper moves from (50,0) to (110,0), and the jammer power is fixed, $P_J = 0\ dB$.

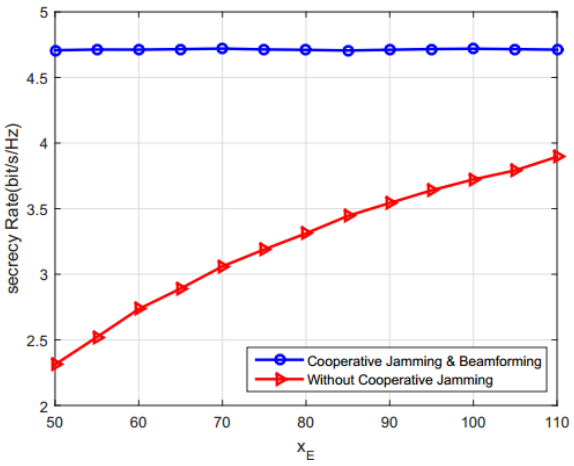

Fig. 5. The average secrecy rates versus the eavesdropper's locations when $M = 8$. The eavesdropper moves from (50,0) to (110,0), and the jammer power is fixed, $P_J = 0\ dB$.

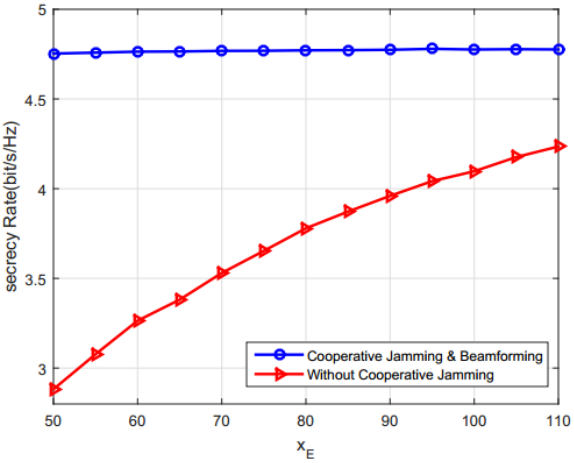

Fig. 6. The average secrecy rates versus the eavesdropper's locations when $M = 10$. The eavesdropper moves from (50,0) to (110,0), and the jammer power is fixed, $P_J = 0\ dB$.

especially when the eavesdropper is located close to the source.

In [15], combined relay selection and beamforming (that we call it "without cooperative jamming") is compared to other schemes. It is shown that [15], their proposed scheme outperforms the others. The scheme that we introduce in this paper performs better than "without cooperative jamming" scheme. As we can see from Fig. 4, Fig. 5 and, with increasing the distance between the relays and the eavesdropper, the improvement of using cooperative jamming will be marginal compare to the scheme "without cooperative jamming". Thus, in the cases that the distances between the relays and the eavesdropper are too high, it is suggested to use beamforming method without cooperative jamming.

V. Conclusion

In this paper, a joint beamforming and cooperative jamming via relay and jammer selection scheme presented to address the secrecy issue at the physical layer. As discussed thoroughly, to handle the operational complexity problem and synchronization among the relays, we only use four intermediate nodes, two DF-based relays for transmitting the source message to the destination and two jammers for generating artificial noise. Our proposed scheme significantly improves the secrecy rate, compared to the scheme using beamforming via relay selection and without cooperative jamming, as we evaluated via numerical examples. The secrecy rate is improved in the case that eavesdropper is closer to the source rather than destination. As future work, we would like to consider the effect of imperfect CSI on the achievable secrecy rate. In addition, the case of multiple eavesdroppers instead of one eavesdropper would be investigated in our future work.

References

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

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

[3] 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.

[4] 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.

[5] 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.

[6] 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.

[7] 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.

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

[9] 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.

[10] 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.

[11] A. Wang, Y. Cai, W. Yang, and Z. Hou, "A stackelberg security game with cooperative jamming over a multiuser

OFDMA network," in *Wireless Communications and Networking Conference (WCNC), IEEE*, 2013, pp. 4169–4174.

[12] 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. Sel. Areas Commun.*, vol. 31, no. 9, pp. 1741–1750, 2013.

[13] 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.

[14] 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.

[15] 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.

[16] 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.

[17] 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.

[18] A. Mukherjee *et al.*, "Robust beamforming for security in MIMO wiretap channels with imperfect CSI," *IEEE Trans. Signal Process.*, vol. 59, no. 1, pp. 351–361, 2011.

[19] S. Yan, N. Yang, R. Malaney, and J. Yuan, "Transmit antenna selection with alamouti coding and power allocation in MIMO wiretap channels," *IEEE Trans. Wireless Commun.*, vol. 13, no. 3, pp. 1656–1667, 2014.

[20] T. Lv, H. Gao, and S. Yang, "Secrecy transmit beamforming for heterogeneous networks," *IEEE J. Sel. Areas Commun.*, vol. 33, no. 6, pp. 1154 –1170, 2015.

[21] 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.

[22] 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.

[23] 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.

[24] 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.

[25] 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.

[26] M. Hatami, M. Jahandideh, and H. Behroozi, "Two-phase cooperative jamming and beamforming for physical layer secrecy," in *23rd Iranian Conference on Electrical Engineering (ICEE)*, IEEE, 2015, pp. 456–461.

[27] 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.

[28] 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.

[29] 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.

[30] 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.

[31] 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.

Mohammad Hatami received the B.Sc. degree in Electronic Engineering from Iran University of Science and Technology (IUST), Tehran, Iran, in 2013, and the M.Sc. degree in Communication Engineering (System) from the Sharif University of Technology, Tehran, Iran, in 2015. His research interests include wireless communication systems, physical layer secrecy and system design and simulation.

Hamid Behroozi received the B.Sc. degree from the University of Tehran, Tehran, Iran, in 2000, the M.Sc. degree from the Sharif University of Technology, Tehran, in 2003, and the Ph.D. degree from Concordia University, Montreal, QC, Canada, in 2007, all in electrical engineering. From 2007 to 2010, he was a Post-Doctoral Fellow with the Department of Mathematics and Statistics, Queens University. He is currently an Assistant Professor with the Electrical Engineering Department, Sharif University of Technology. His research interests include information theory, joint source-channel coding, and cooperative communications. Dr. Behroozi is a recipient of several academic awards, including the Ontario Postdoctoral Fellowship by the Ontario Ministry of Research and Innovation, the Quebec Doctoral Research Scholarship by the Government of Quebec (FQRNT), the Hydro Quebec Graduate Award, and the Concordia University Graduate Fellowship.

This Page intentionally left blank.