Physical Layer Security for Two Way Relay Communications with Friendly Jammers

Rongqing Zhang, Lingyang Song, Zhu Han, Bingli Jiao, Merouane Debbah

Physical Layer Security for Two Way Relay Communications with Friendly Jammers

Rongqing Zhang*, Lingyang Song*, Zhu Han†, Bingli Jiao*, and Merouane Debbah‡
*School of Electrical Engineering and Computer Science, Peking University, Beijing, China, 100871.
†Electrical and Computer Engineering Department, University of Houston, Houston, USA.
‡SUPELEC, Alcatel-Lucent Chair in Flexible Radio, 3 rue Joliot-Curie, FR-91192 Gif Sur Yvette, France.

***Abstract*—In this paper, we consider a two-way relay network where two sources can communicate only through an unauthenticated intermediate relay node. We investigate the secure communication of this two-way relay scenario using physical layer security. Specifically, we treat the relay node as an eavesdropper from whom the information transmitted by the sources needs to be kept secret, despite the fact that its cooperation in relaying this information is essential. We first find that a non-zero secrecy rate is indeed achievable in this two-way relay network even without external jammers. Further still, with the help of friendly jammers that transmit the jamming signals to confuse the malicious relay, a positive gain of the secrecy rate can be realized. In order to obtain the maximum secrecy rate, we define and then analyze a source optimization problem. Finally, an optimal solution on the transmit power allocation of all the nodes is provided for the system without and with using friendly jammers.**

I. Introduction

Traditionally, security in wireless networks has been mainly considered at higher layers using cryptographic methods. However, recent advances in wireless decentralized and ad-hoc networking have led to an increasing attention on studying the physical layer based security. The basic idea of physical layer security is to exploit the physical characteristics of the wireless channel to provide secure communication. The security is quantified by the *secrecy capacity*, which is defined as the maximum rate of reliable information sent from the source to the intended destination in the presence of eavesdroppers. This line of work was pioneered by Aaron Wyner, who introduced the wire-tap channel and established the possibility of creating perfectly secure communication links without relying on private keys [1]. Wyner showed that when the eavesdropper channel is a degraded version of the main channel from the source to the destination, they can exchange perfectly secure messages at a non-zero rate. Follow-up work in [2] the secrecy capacity of Gaussian wire-tap channel was studied and in [3] the authors extended Wyner's approach to the transmission of confidential messages over the broadcast channel.

Motivated by the fact that if the source-wiretapper channel is less noisy than the source-destination channel, the perfect secrecy capacity will be zero [3], recently, jamming schemes have been introduced into physical layer security to improve the secret capacity by confusing the eavesdropper with codewords independent of the source message [4]. In [5], the author studied the classical three node one way relay channel by treating the relay as an eavesdropper. In [6], it was established that cooperation even with an unauthenticated relay node could be beneficial in relay channels with orthogonal components. Then in [7], the authors considered a two-hop communication system using an untrusted relay and showed that a cooperative jammer enables a positive secrecy rate which would be otherwise impossible. In [8]–[10], the authors employed the game theory to the physical layer security to study the interaction between the source and the friendly jammers who assist the source by confusing the eavesdropper and got some distributed game solutions.

In this paper, we investigate the physical layer security in a two-way relay network with friendly jammers. The two source nodes could exchange information only through an unauthenticated relay node, as there is no direct communication link between them. The unauthenticated relay node employing amplify-and-forward (AF) protocol, acts as both an essential relay and a malicious eavesdropper who also wants to eavesdrop the transmitted data coming from the sources. As a special case and for convenience, we first study the system without jammers. We find that a non-zero secrecy rate here is indeed available even without the help of jammers confusing the malicious relay. We also derive an optimal power vector of the relay and the sources by maximizing the secrecy rate. Then, we investigate the two-way relay communications with friendly jammers, and we find that a positive gain could be obtained in the secrecy rate. We further derive the optimal power allocation from the friendly jammers through a source optimization problem. In the optimization problem that we formulate here, the sources will have to pay the jammers for interfering the malicious relay, in order to increase the secrecy rate. The friendly jammers charge the sources with a certain price for their service of jamming. The proposed schemes are verified by simulations.

The rest of this paper is organized as follows. In Section II, the system model of two-way relay communication with jammers is described and the corresponding secrecy rate is formulated. In Section III, a two-way relay system without jammers is investigated. In Section IV, we formulate a source optimization problem and analyze the optimizing problem of physical layer security with jammers. Simulation results are shown in Section V and main conclusions are drawn in Section VI.

II. System Model

As shown in Fig. 1, we consider a two-way relay network consisting of two source nodes, one unauthenticated relay

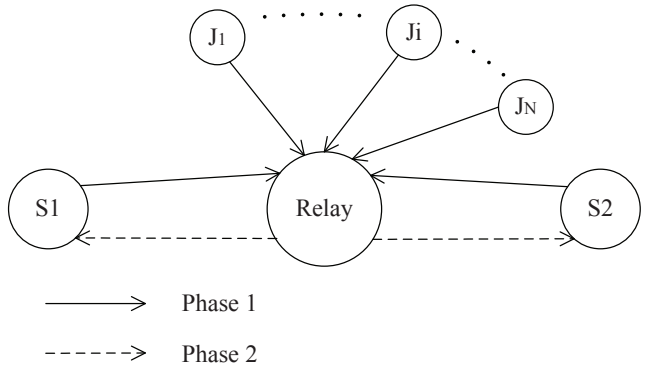

Fig. 1. System model for two-way relay communications with friendly jammers

node, and N friendly jammer nodes, which are denoted by S_k, $k = 1, 2$, R, and J_i, $i = 1, 2, \ldots, N$, respectively. We denote by $\mathcal{N}$ the set of indices $\{1, 2, \ldots, N\}$. All the nodes here are equipped with only a single omni-directional antenna and operate in a half-duplex way, i.e., each node cannot receive and transmit simultaneously. Then the complete transmission can be divided into two phases. During the first phase, shown with solid lines, both source nodes transmit their information to the relay. Simultaneously, the friendly jammers also transmit the jamming signals in order to confuse the malicious relay. In the second phase, shown with dashed lines, the relay broadcasts a combined version of the received signals to both source nodes. We should also note that this two phases' transmission will lead to a loss in spectral efficiency due to the pre-log factor $1/2$ in corresponding expressions for the achievable capacity. A key assumption we make here is that the sources have perfect knowledge of the jamming signals transmitted by the friendly jammers, for they have paid for the service. And global channel state information (CSI) is also available in our assumptions.

Let $s_1 \in \mathcal{A}$, $s_2 \in \mathcal{A}$, and $s_i^J \in \mathcal{A}$, $i \in \mathcal{N}$, denote the signal to be transmitted by the source S_1, S_2, and the jammers J_i, $i \in \mathcal{N}$, respectively, where $\mathcal{A}$ represents a unity power constellation set. Suppose the source nodes S_1 and S_2 transmit with power p_1 and p_2, and the channel gains from the source nodes to the relay node are denoted by $h_{S_k,R}$, $k = 1, 2$. Each friendly jammer node i transmits with power p_i^J, and the channel gain from it to the relay node is denoted by $h_{J_i,R}$, $i \in \mathcal{N}$. The channel gain contains the path loss and the Rayleigh fading coefficient with zero mean and unit variance. For simplicity, we assume that the fading coefficients are constant over one frame, and change independently from one frame to another.

In phase 1, the received signal in the relay can be expressed as

$$y_r = n_r + \sqrt{p_1} s_1 h_{S_1,R} + \sqrt{p_2} s_2 h_{S_2,R} + \sum_i \sqrt{p_i^J} s_i^J h_{J_i,R}, \tag{1}$$

where n_r denotes the thermal noise at the relay note, which is a zero mean Gaussian random variable with two sided power spectral density of σ^2. Furthermore, we assume that S_1, S_2, and R have the same noise variance.

In phase 2, the malicious relay node, who works in AF mode, amplifies the received signal y_r by a factor β and then broadcasts the signal to both S_1 and S_2 with power p_r. For power normalization at the relay we have

$$\beta = \left(p_1 \left| h_{S_1,R} \right|^2 + p_2 \left| h_{S_2,R} \right|^2 + \sum_i p_i^J \left| h_{J_i,R} \right|^2 + \sigma^2 \right)^{-1/2}. \tag{2}$$

Considering the jamming signals transmitted by the jammers in phase 1, the corresponding signal received by S_1 , denoted by y_1, can be written as

$$\begin{aligned} y_1 &= \beta \sqrt{p_r} h_{S_1,R} y_r + \sum_i \sqrt{p_i^J} h_{J_i,S_1} s_i^J + n_1 \\ &= \xi_1 s_1 + \upsilon_1 s_2 + \sum_i \mu_{1,i} s_i^J + \omega_1, \end{aligned} \tag{3}$$

where $\xi_1 \triangleq \beta \sqrt{p_r p_1} h_{S_1,R}^2$, $\upsilon_1 \triangleq \beta \sqrt{p_r p_2} h_{S_1,R} h_{S_2,R}$, $\mu_{1,i} \triangleq \beta \sqrt{p_r p_i^J} h_{J_i,R} h_{S_1,R} + \sqrt{p_i^J} h_{J_i,S_1}$, and $\omega_1 \triangleq \beta \sqrt{p_r} h_{S_1,R} n_r + n_1$.

Similarly, the signal received by S_2 , denoted by y_2, can be written as

$$\begin{aligned} y_2 &= \beta \sqrt{p_r} h_{S_2,R} y_r + \sum_i \sqrt{p_i^J} h_{J_i,S_2} s_i^J + n_2 \\ &= \xi_2 s_1 + \upsilon_2 s_2 + \sum_i \mu_{2,i} s_i^J + \omega_2, \end{aligned} \tag{4}$$

where $\xi_2 \triangleq \beta \sqrt{p_r p_1} h_{S_1,R} h_{S_2,R}$, $\upsilon_2 \triangleq \beta \sqrt{p_r p_2} h_{S_2,R}^2$, $\mu_{2,i} \triangleq \beta \sqrt{p_r p_i^J} h_{J_i,R} h_{S_2,R} + \sqrt{p_i^J} h_{J_i,S_2}$, and $\omega_2 \triangleq \beta \sqrt{p_r} h_{S_2,R} n_r + n_2$.

Assuming that both the source nodes and the jammer nodes are independent, from (1), in phase 1, using the matched filter, the unauthenticated relay node has the capacity with respect to S_1 and S_2 as

$$C_1^m = \frac{W}{2} \log \left(1 + \frac{p_1 g_{S_1,R}}{\sigma^2 + p_2 g_{S_2,R} + \sum_i p_i^J g_{J_i,R}} \right), \tag{5}$$

and

$$C_2^m = \frac{W}{2} \log \left(1 + \frac{p_2 g_{S_2,R}}{\sigma^2 + p_1 g_{S_1,R} + \sum_i p_i^J g_{J_i,R}} \right), \tag{6}$$

where W represents the channel bandwidth, $g_{S_1,R} = |h_{S_1,R}|^2$, $g_{S_2,R} = |h_{S_2,R}|^2$, and $g_{J_i,R} = |h_{J_i,R}|^2$, $i \in \mathcal{N}$.

In phase 2, at S_1, as s_1 and s_i^J is also known to its own source node, and thus we can get

$$y_1 = \upsilon_1 s_2 + \omega_1. \tag{7}$$

Then the corresponding SNR for the transmission from S_2 to S_1, denoted by γ_2, can be expressed as

$$\begin{aligned} \gamma_2 &= \frac{|\upsilon_1|^2}{Var\{\omega_1\}} \\ &= \frac{p_2 g_{S_2,R}}{\sigma^2 + K_2 + \sum_i \frac{\sigma^2 g_{J_i,R}}{p_r g_{S_1,R}} p_i^J}, \end{aligned} \tag{8}$$

where $K_2 \triangleq \frac{\sigma^2(p_1 g_{S_1,R}+p_2 g_{S_2,R}+\sigma^2)}{p_r g_{S_1,R}}$.

Similarly, at S_2, the received signal with s_2 and s_i^J removed can be written as

$$y_2 = \xi_2 s_1 + \omega_2. \tag{9}$$

The corresponding SNR for the transmission from S_1 to S_2, denoted by γ_1, can be expressed as

$$\begin{aligned}\gamma_1 &= \frac{|\xi_2|^2}{Var\{\omega_2\}} \\ &= \frac{p_1 g_{S_1,R}}{\sigma^2 + K_1 + \sum_i \frac{\sigma^2 g_{J_i,R}}{p_r g_{S_2,R}} p_i^J},\end{aligned} \tag{10}$$

where $K_1 \triangleq \frac{\sigma^2\left(p_1 g_{S_1,R}+p_2 g_{S_2,R}+\sigma^2\right)}{p_r g_{S_2,R}}$.

Capacities of two-way relay channel between the source nodes are denoted by C_1 and C_2, then we can get

$$C_1 = \frac{W}{2}\log\left(1+\gamma_1\right), \tag{11}$$

and

$$C_2 = \frac{W}{2}\log\left(1+\gamma_2\right). \tag{12}$$

The secrecy rate for S_1 and S_2 can be defined as

$$C_1^s = (C_1 - C_1^m)^+, \tag{13}$$

and

$$C_2^s = (C_2 - C_2^m)^+. \tag{14}$$

where $(x)^+$ represents $\max\{x, 0\}$.

III. Secrecy Rate of Two-Way Relay Channel Without Jammers

In this section, we investigate a conventional two-way relay communication scenario without the presence of jammers. Compared to the system model described above, this system can be regarded as a reduced one with all the jammers' transmit power p_i^J set to zero, $\forall i \in \mathcal{N}$. We assume that all the system conditions are the same as the previous one except those referring to the jammers. Then from the derivation above, we can get the secrecy rate here as

$$\tilde{C}_1^s = \frac{W}{2}\left(\log\left(1+\frac{p_1 g_{S_1,R}}{\sigma^2+K_1}\right) - \log\left(1+\frac{p_1 g_{S_1,R}}{\sigma^2+p_2 g_{S_2,R}}\right)\right)^+, \tag{15}$$

and

$$\tilde{C}_2^s = \frac{W}{2}\left(\log\left(1+\frac{p_2 g_{S_2,R}}{\sigma^2+K_2}\right) - \log\left(1+\frac{p_2 g_{S_2,R}}{\sigma^2+p_1 g_{S_1,R}}\right)\right)^+. \tag{16}$$

A. Existence of Non-zero Secrecy Rate

When the eavesdropper channels from the two sources to the malicious relay are degraded versions of the main two-way relay channel between S_1 and S_2, the two sources can exchange perfectly secure messages at a non-zero rate. Firstly we consider the transmission from S_1 to S_2. In phase 1, the malicious relay receives the signal s_1 from S_1, which consists of the information for S_2. Meanwhile, S_2 also transmits the signal at the relay, which acts as both the information carrier for S_1 and a jamming signal that makes the eavesdropper channel from S_1 to the malicious relay getting worse. In phase 2, the combined signal consisting of s_1 and s_2 arrives at S_2. As S_2 has a perfect knowledge of its own signal s_2, the signal that jammed the malicious relay in phase 1 has no such an effect on S_2. Therefore it makes possible that the eavesdropper channel is worse than the message transmission channel from S_1 to S_2, which means a non-zero rate for secure communication from S_1 to S_2 is available. It is the same situation in the transmission from S_2 to S_1. From (15) and (16), we can write the probability of the existence of a non-zero secrecy rate as

$$\begin{aligned}\mathrm{P}\left(\tilde{C}_1^s>0, \tilde{C}_2^s>0\right) &= \mathrm{P}\left(K_1 < p_2 g_{S_2,R}, K_2 < p_1 g_{S_1,R}\right) \\ &= \mathrm{P}\left(p_r > \max\left\{\frac{K}{p_2 g_{S_2,R}^2}, \frac{K}{p_1 g_{S_1,R}^2}\right\}\right),\end{aligned} \tag{17}$$

where $K = (p_1 g_{S_1,R} + p_2 g_{S_2,R} + \sigma^2)\sigma^2$.

Considering the power constraint $p_1 \le p_{\max}$, $p_2 \le p_{\max}$, and $p_r \le p_{\max}$, we can get that there exists at least one pair of (p_r, p_1, p_2) that satisfies $p_r > \max\left\{\frac{K}{p_2 g_{S_2,R}^2}, \frac{K}{p_1 g_{S_1,R}^2}\right\}$, under the channel condition of $\frac{g_{S_1,R}+g_{S_2,R}}{g_{S_1,R} g_{S_2,R}} < \frac{p_{\max}}{\sigma^2}$. Therefore we have $\mathrm{P}\left(\tilde{C}_1^s>0, \tilde{C}_2^s>0\right) > 0$ at some power vectors of (p_r, p_1, p_2), which actually indicates that a non-zero secrecy rate in the two-way relay channel is indeed available.

B. Maximizing the Secrecy Rate

In this sub-section, we will try to get an optimal power vector of (p_r, p_1, p_2) which maximizes the secrecy rate of the two-way relay channel. We can formulate the problem subject to the individual secrecy rate constraint and power constraint as

$$\begin{aligned}&\max\ \tilde{C}^s = \max\ \sum_{k=1}^{2} \tilde{C}_k^s, \\ &s.t.\quad \tilde{C}_1^s > 0,\ \tilde{C}_2^s > 0, \\ &\qquad p_1 \le p_{\max},\ p_2 \le p_{\max},\ p_r \le p_{\max}.\end{aligned} \tag{18}$$

From (17), we know that

$$\tilde{C}_1^s > 0,\ \tilde{C}_2^s > 0 \Leftrightarrow p_r > \max\left\{\frac{K}{p_2 g_{S_2,R}^2}, \frac{K}{p_1 g_{S_1,R}^2}\right\}. \tag{19}$$

From (15), (16), and (18), we can get that

$$\tilde{C}^s = \frac{W}{2}\left(\log \tilde{F}\left(p_r, p_1, p_2\right)\right)^+, \tag{20}$$

where

$$\tilde{F}\left(p_r,p_1,p_2\right)=\frac{\left(1+\frac{p_1 g_{S_1,R}}{\sigma^2+K_1}\right)\left(1+\frac{p_2 g_{S_2,R}}{\sigma^2+K_2}\right)}{\left(1+\frac{p_1 g_{S_1,R}}{\sigma^2+p_2 g_{S_2,R}}\right)\left(1+\frac{p_2 g_{S_2,R}}{\sigma^2+p_1 g_{S_1,R}}\right)}. \quad (21)$$

As $\tilde{F}(p_r,p_1,p_2)$ has the same monotonic property as $\tilde{C}^s$ under the conditions of (18), we can transform the optimization problem as

$$\begin{aligned} &\max\ \tilde{F}\left(p_r,p_1,p_2\right),\\ s.t.\quad &p_r>\max\left\{\frac{K}{p_2 g_{S_2,R}^2},\frac{K}{p_1 g_{S_1,R}^2}\right\},\\ &p_1\le p_{\max},\ p_2\le p_{\max},\ p_r\le p_{\max}. \end{aligned} \quad (22)$$

It can be calculated that $\frac{\partial\tilde{F}(p_r,p_1,p_2)}{\partial p_r}>0$ is always established under the conditions in (22), which implies that $\tilde{F}\left(p_r,p_1,p_2\right)$ is a monotonically increasing function of p_r. Therefore when maximizing the secrecy rate $\tilde{C}^s$, the relay should always transmit at the maximum power $p_{\max}$, i.e., $p_{r\_opt}=p_{\max}$, where p_{r_opt} denotes the optimal relay power. As a result, the problem can be further transformed into $\max\ \tilde{F}\left(p_{\max},p_1,p_2\right)$.

From (21), we can observe that how large the value of $\tilde{F}\left(p_{\max},p_1,p_2\right)$ could reach is determined by the gap between K_1 and $p_2 g_{S_2,R}$, as well as K_2 and $p_1 g_{S_1,R}$. And thus, we can obtain that when maximizing the secrecy rate $\tilde{C}^s$, at least one of the sources should transmit at $p_{\max}$, and the one which is chosen to transmit with this maximum power is determined by the channel gains $g_{S_1,R}$ and $g_{S_1,R}$. Hence, the optimal power allocation of S_1 and S_2 can be given as follows:

1) For the case that $g_{S_1,R}>g_{S_2,R}$, we can get that $p_{2\_opt}=p_{\max}$. Meanwhile, if there exists a solution $p_1^*\in(0,p_{\max}]$ that satisfies the equation $\frac{\partial\tilde{F}(p_{\max},p_1,p_{\max})}{\partial p_1}=0$, then we have $p_{1\_opt}=p_1^*$. Otherwise, we have $p_{1\_opt}=p_{\max}$, where p_{1_opt} and p_{2_opt} denote the optimal power transmitted by S_1 and S_2, respectively.
2) For the case that $g_{S_1,R}<g_{S_2,R}$, it yields that $p_{1\_opt}=p_{\max}$. Meanwhile, if there exists a solution $p_2^*\in(0,p_{\max}]$ that satisfies the equation $\frac{\partial\tilde{F}(p_{\max},p_{\max},p_2)}{\partial p_2}=0$, then we have $p_{2\_opt}=p_2^*$. Otherwise, we have $p_{2\_opt}=p_{\max}$.
3) For the case that $g_{S_1,R}=g_{S_2,R}$, we will have that $p_{1\_opt}=p_{\max}$, and $p_{2\_opt}=p_{\max}$.

IV. Physical Layer Security with Jammers

In this section, we investigate the physical layer security for two-way relay communications with friendly jammers. First, we observe that the secrecy rate of the two-way channel could be improved using friendly jammers. These jammers introduce extra interference to the malicious relay while the interference is known to the source nodes. Then, we formulate a source optimization problem and optimize the problem utility function of the two sources.

A. Improved Secrecy Rate using Friendly Jammers

From (13) and (14), we have that

$$C_1^s=\frac{W}{2}\left(\log\left(1+\frac{p_1 g_{S_1,R}}{\sigma^2+K_1+\sum_i\frac{\sigma^2 g_{J_i,R}}{p_r g_{S_2,R}}p_i^J}\right)-\log\left(1+\frac{p_1 g_{S_1,R}}{\sigma^2+p_2 g_{S_2,R}+\sum_i g_{J_i,R}p_i^J}\right)\right)^+, \quad (23)$$

and

$$C_2^s=\frac{W}{2}\left(\log\left(1+\frac{p_2 g_{S_2,R}}{\sigma^2+K_2+\sum_i\frac{\sigma^2 g_{J_i,R}}{p_r g_{S_1,R}}p_i^J}\right)-\log\left(1+\frac{p_2 g_{S_2,R}}{\sigma^2+p_1 g_{S_1,R}+\sum_i g_{J_i,R}p_i^J}\right)\right)^+. \quad (24)$$

Both C_k and C_k^m, $k=1,2$, are decreasing and convex functions of jamming power p_i^J, $i\in\mathcal{N}$. However, if C_k^m decreases faster than C_k as the jamming power p_i^J increases, C_k^s might increase in some region of value p_i^J. But when p_i^J further increases, both C_k and C_k^m will approach zero. As a result, C_k^s approaches zero. By comparing (15) with (16), we can get that if $\frac{\sigma^2}{p_r}<\min\left\{g_{S_1,R},g_{S_2,R}\right\}$, the gain of the secrecy rate will be above zero in some region of the jamming power p_i^J, i.e., the secrecy rate could be improved with the help of friendly jammers.

B. Source Optimization Analysis

We consider the two sources as two buyers who want to optimize their secrecy rate, while the cost paid for the "service", i.e., jamming power p_i^J, should also be taken into consideration. For the sources' side we can define the utility function of source optimization problem as

$$U_s=a\left(C_1^s+C_2^s\right)-M, \quad (25)$$

where a is a positive constant representing the gain per unit rate, and M is the cost to pay for the friendly jammers. Here we have

$$M=\sum_i m_i p_i^J, \quad (26)$$

where m_i is the price per unit power paid for the friendly jammer i by the sources, $i\in\mathcal{N}$.

It can be calculated that $\frac{\partial U_s}{\partial p_r}>0$ is always hold when $p_r\in(0,p_{\max}]$, i.e., when optimizing the secrecy rate, the relay should always transmit at the maximum power $p_{\max}$. As all the nodes transmit with independent power, we can treat the jamming power p_i^J as a constant when considering the optimal power vector of (p_1,p_2). Therefore we can get the same results of the optimal vector as given in the previous section. Hence, our major purpose here is to study how to control the jamming power so as to achieve the maximum utility value.

The source optimization problem can be expressed as

$$\begin{aligned} &\max\ U_s = \max\ \left(a\left(C_1^s + C_2^s\right) - M\right), \\ s.t.\quad & C_1^s > 0, C_2^s > 0, \\ & 0 \le p_i^J \le p_{\max}, p_r = p_{\max}, fixed\, p_1, p_2. \end{aligned} \tag{27}$$

The goal of the sources as buyers is to buy the optimal amount of power from the friendly jammers in order to maximize the secrecy rate. From (23), (24), and (27), we have

$$\begin{aligned} U_s =& \frac{aW}{2}\left(\log\frac{1+\frac{1}{A_1+\sum\limits_i T_{1,i}p_i^J}}{1+\frac{1}{B_1+\sum\limits_i L_{1,i}p_i^J}} + \log\frac{1+\frac{1}{A_2+\sum\limits_i T_{2,i}p_i^J}}{1+\frac{1}{B_2+\sum\limits_i L_{2,i}p_i^J}}\right) \\ & - \sum_i m_i p_i^J, \end{aligned} \tag{28}$$

where $A_1 \triangleq \frac{\sigma^2+K_1}{p_1 g_{S_1,R}}$, $A_2 \triangleq \frac{\sigma^2+K_2}{p_2 g_{S_2,R}}$, $B_1 \triangleq \frac{\sigma^2+p_2 g_{S_2,R}}{p_1 g_{S_1,R}}$, $B_2 \triangleq \frac{\sigma^2+p_1 g_{S_1,R}}{p_2 g_{S_2,R}}$, $T_{1,i} \triangleq \frac{\sigma^2 g_{J_i,R}}{p_r p_1 g_{S_2,R} g_{S_1,R}}$, $T_{2,i} \triangleq \frac{\sigma^2 g_{J_i,R}}{p_r p_2 g_{S_2,R} g_{S_1,R}}$, $L_{1,i} \triangleq \frac{g_{J_i,R}}{p_1 g_{S_1,R}}$, and $L_{2,i} \triangleq \frac{g_{J_i,R}}{p_2 g_{S_2,R}}$.

By differentiating (28) with respect to p_i^J, we get

$$\begin{aligned} \frac{\partial U_s}{\partial p_i^J} =& -\frac{aWT_{1,i}}{2\left(A_1+\sum\limits_i T_{1,i}p_i^J\right)\left(1+A_1+\sum\limits_i T_{1,i}p_i^J\right)} \\ & + \frac{aWL_{1,i}}{2\left(B_1+\sum\limits_i L_{1,i}p_i^J\right)\left(1+B_1+\sum\limits_i L_{1,i}p_i^J\right)} \\ & - \frac{aWT_{2,i}}{2\left(A_2+\sum\limits_i T_{2,i}p_i^J\right)\left(1+A_2+\sum\limits_i T_{2,i}p_i^J\right)} \\ & + \frac{aWL_{2,i}}{2\left(B_2+\sum\limits_i L_{2,i}p_i^J\right)\left(1+B_2+\sum\limits_i L_{2,i}p_i^J\right)} - m_i. \end{aligned} \tag{29}$$

Rearranging the above equation, when $\frac{\partial U_s}{\partial p_i^J} = 0$, we can have a fourth order polynomial equation as

$$\left(p_i^J\right)^4 + F_{i,3}\left(p_i^J\right)^3 + F_{i,2}\left(p_i^J\right)^2 + F_{i,1}p_i^J + F_{i,0} = 0, \tag{30}$$

where $F_{i,l}$, $l = 0,1,2,3$, are formulae of constants A_k, B_k, $T_{i,k}$, $L_{i,k}$, and variables ∂p_j^J, $k = 1,2$, $i \in \mathcal{N}$, $j \in \mathcal{N}$ but $j \ne i$.

The solutions of the quartic equation (30) can be expressed in a closed form [11], but this is not essential here. The solution of our particular interest can be expressed as

$$p_i^{J^*} = p_i^{J^*}\left(m_i, \{A_k\}, \{B_k\}, \{T_{k,i}\}, \{L_{k,i}\}, \left\{p_j^J\right\}_{j\ne i}\right), \tag{31}$$

which is a function of the friendly jammer's price m_i, the other jammers' jamming power $\left\{p_j^J\right\}_{j\ne i}$ and other system parameters. Note that with $0 \le p_i^J \le p_{\max}$ in the optimization problem, we can get the optimal strategy as

$$p_{i\_opt}^J = \min\left(\max\left(p_i^{J^*}, 0\right), p_{\max}\right). \tag{32}$$

V. Simulation Results

To investigate the performances, we conduct the following simulations. For simplicity and without loss of generality, we consider a simple two-way relay system model with only one friendly jammer, where the sources S_1, S_2, and the malicious relay are located at the coordinate $(-1,0)$, $(1,0)$, and $(0,0)$, respectively. Here we study two jammer locations which are $(0.3, 0.4)$ and $(0.6, 0.8)$. The other simulation parameters are set up as follows: The maximum power constraint $p_{\max}$ is 10dB; the transmission bandwidth is 1; the noise variance is $\sigma^2 = 0.1$; Rayleigh fading channel is assumed, where the channel gain consists of the path loss and the Rayleigh fading coefficient; the path loss factor is 2. Here we select $a = 1$ for the source optimization utility in (27).

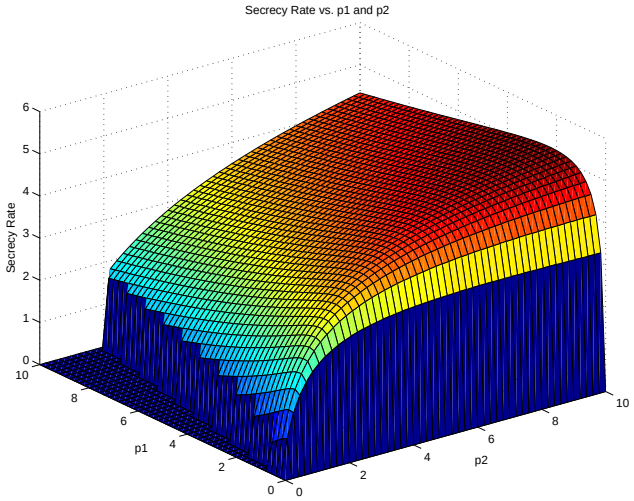

Fig. 2. Secrecy rate vs. p_1 and p_2 for the case without jammers when $g_{S_1,R} > g_{S_2,R}$

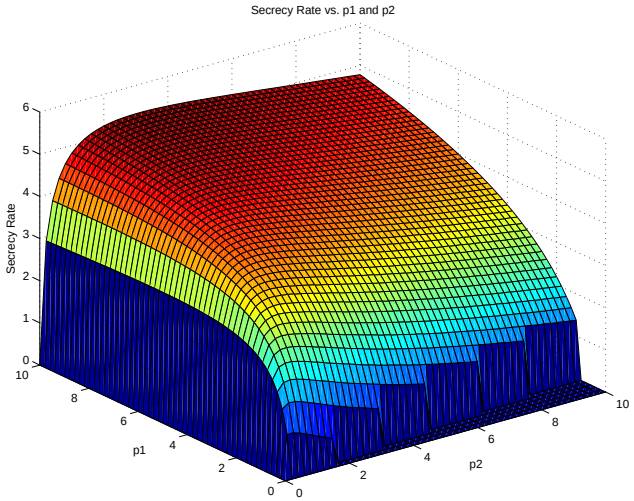

Fig. 3. Secrecy rate vs. p_1 and p_2 for the case without jammers when $g_{S_1,R} < g_{S_2,R}$

For the special case without jammers, we set the jamming power up to zero. In Fig. 2 and Fig. 3, we show the secrecy rate as a function of the two sources transmitting power p_1 and p_2 in this special case. It shows that the optimal power vector of (p_1, p_2) is $(0.22p_{\max}, p_{\max})$ when $g_{S_1,R} = 0.3857$ and $g_{S_2,R} = 0.0443$, and $(p_{\max}, 0.32p_{\max})$ when $g_{S_1,R} = 0.0508$ and $g_{S_2,R} = 0.3018$. After further calculation, we can see that the results fit the optimal power allocation conclusions given in Section III well.

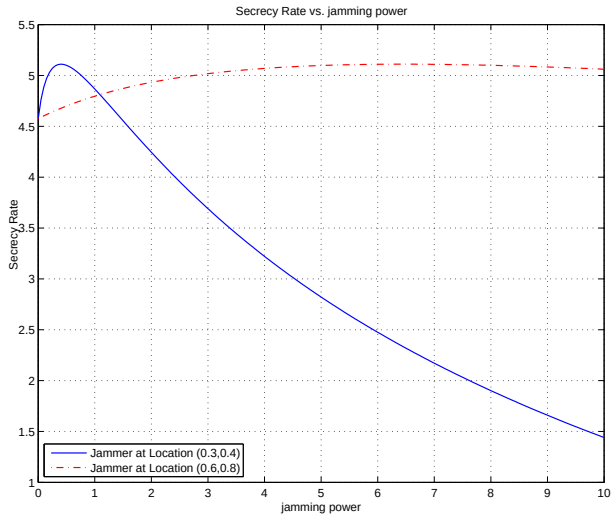

Fig. 4. Secrecy rate vs. jamming power

Fig. 4 shows the secrecy rate as a function of the jamming power when p_1, p_2, and p_r are all set up to $p_{\max}$. We can see that with the increase of the jamming power, the secrecy rate first increases and then decreases. There indeed exists an optimal point for the jamming power. Also the optimal point depends on the location of the friendly jammer, and we can find that the friendly jammer close to the malicious relay is more effective to improve the secrecy capacity.

Fig. 5 shows that the optimal amount of the jamming power bought by the sources depends on the price requested by the jammer. We can see that the amount of bought power gets reduced if the price goes high and the sources would even stop buying after some price point. And thus there is a tradeoff for the jammers to set the price. If the price is set too high, the sources would buy less power or even stop buying. But if the price is given too low, the jammers would benefit very little.

VI. Conclusion

In this paper, we have investigated the physical layer security for two-way relay communications with friendly jammers. As a simple case, a two-way relay system without jammers is studied first, and an optimal power allocation vector of the sources and relay nodes is found. We then analyzed the secrecy rate in the presence of friendly jammers. Furthermore, we defined a source optimization problem and obtained an optimal solution of jamming power. From the simulation results, we can see that a non-zero secrecy rate of two-way

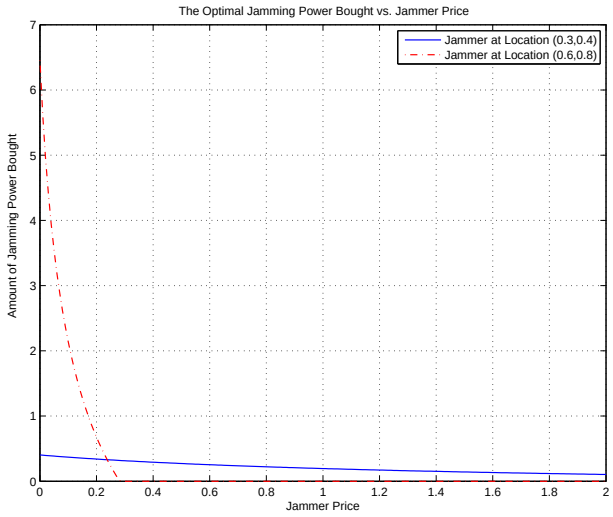

Fig. 5. How much the sources buy as a function of the jammer price

relay channel is indeed available, and it can be improved by proper power allocation between the source nodes or with the help of friendly jammers. In the system with jammers, it has an optimal solution of jamming power allocation. There is also a tradeoff for the price a jammer set, and if the price is too high, the sources would not buy or buy from others. It is worthwhile mentioning that, due to space limitation, we mainly investigated the sources' side optimization problem. But there exists a game between the sources and the friendly jammers, and this will be studied in our future work.

References

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

[2] S. K. Leung-Yan-Cheong and M. E. Hellman, "The Gaussian wiretap channel," *IEEE Transactions on Information Theory*, vol. 24, pp. 451 – 456, Jul. 1978.

[3] I. Csiszar and J. Korner, "Broadcast channels with confidential messages," *IEEE Transactions on Information Theory*, vol. 24, pp. 339 – 348, May 1978.

[4] L. Lai and H. El Gamal, "The relay-eavesdropper channel: Cooperation for secrecy," *IEEE Transactions on Information Theory*, vol. 54, pp. 4005 – 4019, Feb. 2008.

[5] Y. Oohama, "Relay channels with confidential messages," *IEEE Transactions on Information Theory*, Nov. 2006.

[6] X. He and A. Yener, "Cooperation with an untrusted relay: A secrecy perspective," *IEEE Transactions on Information Theory*, Oct. 2008.

[7] X. He and A. Yener, "Two-hop secure communication using an untrusted relay: A case for cooperative jamming," in *Proceedings of IEEE GLOBECOM*, Dec. 2008.

[8] Zhu Han, N. Marina, M. Debbah, and A. Hjørungnes, "Physical layer security game: Interaction between source, eavesdropper and friendly jammer," *EURASIP Journal on Wireless Communications and Networking*, Nov. 2009.

[9] Zhu Han, N. Marina, M. Debbah, and A. Hjørungnes, "Physical layer security game: How to date a girl with her boyfriend on the same table," in *Proceedings of IEEE International Conference on Game Theory for Networks*, Istanbul, Turkey, May 2009.

[10] Zhu Han, N. Marina, M. Debbah, and A. Hjørungnes, "Improved wireless secrecy rate using distributed auction theory," in *Proceedings of IEEE International Conference on Mobile Ad-hoc and Sensor Networks*, Dec. 2009.

[11] I. N. Stewart, *Galois Theory*, 3rd. ed., Chapman & Hall/CRC Mathematics, Boca Raton, FL, 2004.