Physical Layer Security: Friendly Jamming in an Untrusted Relay Scenario

Bakhtiar Ali, Nida Zamir, Muhammad Fasih Uddin Butt
COMSATS Institute of Information Technology
Islamabad, Pakistan
Email: {bakhtiar_ali, nida.zamir, fasih}@comsats.edu.pk

Soon Xin Ng
University of Southampton
Department of Electronics and Computer Science
Southampton SO17 1BJ, United Kingdom

***Abstract*—This paper investigates the achievable secrecy regions when employing a friendly jammer in a cooperative scenario employing an untrusted relay. The untrusted relay which helps to forward the source signal towards the destination, could also be regarded as a potential eavesdropper. Our system employs a friendly jammer which sends a known noise signal towards the relay. In this paper, we investigate the effect of jammer and relay locations on the achievable secrecy rate. We consider two scenarios where in the first case we consider no direct transmission between the source and destination, while in the second case we include a source to destination direct link in our communication system.**

I. Introduction

With the exponential growth of wireless devices, privacy of the link becomes a major challenge. When many devices are cooperating to help each other out especially in an unsecure network, where relays may have poor security authorization, privacy becomes a major challenge. To deal with this situation, cooperative jamming is a promising technique, which uses cooperating nodes to transmit artificial noise [1]. Most of the algorithms discussed in the literature consider that the relays are reliable and the eavesdropper is assumed to be an outside entity which wants to tap the signal [1], [2]. However in many situations like heterogenous networks, the relays have a poor security authorization as compared to the source-destination link. Therefore the relays could become a potential eavesdropper and hence untrusted.

Untrusted relays were first studied by He and Yener in [3], in which a source destination pair was assisted by the relays. These authors discussed the prospects of whether using an untrusted relay can be beneficial at all. They provided the secrecy rates for an untrusted relay by using destination as a jammer to keep their messages secret from the relay. The authors in [4], presented a joint source and relay beamforming for untrusted relay MIMO systems. They proposed two transmission strategies for transmitting confidential data between source and destination, namely noncooperative and cooperative secure beamforming. Noncooperative scheme considers relay as an outside entity which does not take part in communication, hence it is considered as an eavesdropper. The relay is employed for relaying signals from the source to the destination in a cooperative system and a joint source and relay beamforming is designed for maximizing the secrecy. The secrecy outage probability for different relaying protocols were studied in [5] and the effect of number of relay nodes on the secrecy capacity performance was investigated. In [6], the author proposed a power allocation strategy for Amplify and Forward (AF) based untrusted relay systems. They analyzed the ergodic secrecy capacity (ESC) and presented compact expressions for ESC in high Signal to Noise Ratio (SNR) system.

Various algorithms on untrusted relay systems have been stated, however most of the recent works considered single relay model. For multiple relay models, [7] investigated that as the number of untrusted relays increase, the secrecy capacity decreases. A Destination-Based Jamming (DBJ) technique was proposed in [7] for achieving positive secrecy rate. They provided an ESC lower bound closed form expression for a single relay scenario, which was extended to multiple relay case. They proposed a relay selection algorithm, which maximized the achievable secrecy rate. In [8] another DBJ in an AF based secure transmission in an untrusted relay scenario is proposed. They provided an optimal power allocation strategy and gave closed form expressions for three different scenarios i.e. having large scale antenna array at the source, destination and both source and destination, respectively. In [9] the authors consider a multihop scenario with some untrusted relays. Secrecy is examined by employing random linear network coding at the relays. They analyzed the feasibility of employing untrusted relays with enough untrusted relays. The authors in [10] suggested relay assignment and link adaptation for both security and spectral-efficiency. High performance rate adaptive channel coding schemes with efficient power allocation is used to provide both reliability and security in the presence of untrusted relays. Within this framework, several schemes were proposed to achieve spectrally efficient link adaptation and relay selection [10]. Their results indicated the superiority of the proposed systems and it was found that power adaptation at the source plays an important part in improving spectral efficiency. Furthermore, [11] proposed a security aware relaying scheme, where the transmissions of both the first and the second phases in a two hop scenario are secured.

In this contribution, we first consider a two hop system where the direct link is not available between the source node and the destination node, and then provide the results for achievable secrecy rates at different positions of the jammer.

Then we include the source to destination direct link in our system for our second scenario and present the results for achievable secrecy rates.

The organization of the paper is as follows. Section II outlines the system model for our proposed scenario. Section III furnishes the results for our proposed scenario, while the conclusion is offered in Section IV.

II. System Model

We consider an AF based network consisting of a source (S), a destination (D), an untrusted relay (R) and a cooperative jammer (CJ) which assists in jamming the signal at the relay by transmitting a noise signal that is known at the destination. The two scenarios that we have incorporated in our paper are described below.

A. Cooperative Jamming without S-D Direct Link

Here we consider a scenario where the direct link is not available between the S and the D, as shown in Fig. 1. Each node employs a single antenna and operates in a half-duplex mode with h_{ij} being the rayleigh fading channel between node i and node j. Total transmit power is reserved as P. Noise at each receiver is characterised by a zero-mean, complex Gaussian with variance N_0. As seen in Fig. 1, S transmits

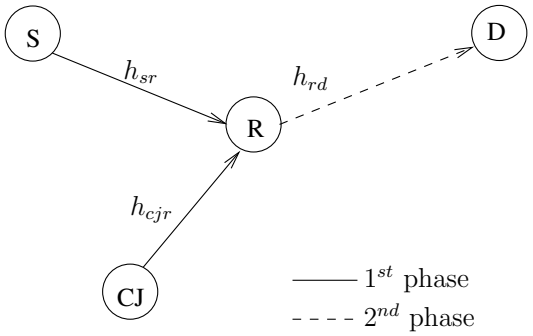


Fig. 1: Cooperative Jamming System Model

the source signal x_s with power αP and a single selected CJ sends artificial noise η_{CJ}, with power $(1-\alpha)P$ which is known to the D, where $\{0 \leq \alpha \leq 1\}$ is power distribution variant. Therefore we can write the signal received at R as:

$$y_r = h_{sr}\sqrt{\alpha P}x_s + h_{CJr}\sqrt{(1-\alpha)P}\eta_{CJ} + w_r, \quad (1)$$

where w_r is the additive noise with variance N_0 at R. After this, R amplifies and forwards the received signal y_r towards D, where the signal received at D can be expressed as

$$y_d = h_{rd}\eta_r y_r + w_d, \quad (2)$$

where w_d is the Additive White Gaussian Noise (AWGN) at D and the amplification factor is given by

$$\eta_r = \sqrt{\frac{P}{\alpha P|h_{sr}|^2 + (1-\alpha)P|h_{CJr}|^2 + N_0}}. \quad (3)$$

By substituting (1) and (3) into (2), we get

$$\begin{aligned} y_d &= h_{rd}\eta_r(h_{sr}\sqrt{\alpha P}x_s + h_{CJr}\sqrt{(1-\alpha)P}\eta_{CJ} + w_r) + w_d \\ &= \eta_r h_{rd}h_{sr}\sqrt{\alpha P}x_s + \eta_r h_{rd}h_{CJr}\sqrt{(1-\alpha)P}\eta_{CJ} \\ &\quad + \eta_r h_{rd}w_r + w_d. \quad (4) \end{aligned}$$

Since η_{CJ} is known at D, the term $\eta_r h_{rd}h_{CJr}\sqrt{(1-\alpha)P}\eta_{CJ}$ can be removed from y_d before decoding the source information. The amplification factor in Eq. (3) can be inserted to the received signal to obtain

$$\begin{aligned} y_d = &\sqrt{\frac{\alpha}{\alpha P|h_{sr}|^2 + (1-\alpha)P|h_{CJr}|^2 + N_0}}Ph_{rd}h_{sr}x_s + \\ &\sqrt{\frac{P}{\alpha P|h_{sr}|^2 + (1-\alpha)P|h_{CJr}|^2 + N_0}}h_{rd}w_r + w_d. \quad (5) \end{aligned}$$

We can calculate the SNR γ_D at D as follows:

$$\begin{aligned} \gamma_D &= \frac{\left|\sqrt{\frac{\alpha}{\alpha P|h_{sr}|^2+(1-\alpha)P|h_{CJr}|^2+N_0}}Ph_{rd}h_{sr}\right|^2}{\left|\sqrt{\frac{P}{\alpha P|h_{sr}|^2+(1-\alpha)P|h_{CJr}|^2+N_0}}h_{rd}\right|^2 N_0 + N_0} \\ &= \frac{\alpha\frac{P^2}{N_0^2}|h_{rd}|^2|h_{sr}|^2}{\frac{P}{N_0}|h_{rd}|^2 + \alpha\frac{P}{N_0}|h_{sr}|^2 + (1-\alpha)\frac{P}{N_0}|h_{CJr}|^2 + 1}. \quad (6) \end{aligned}$$

Therefore,

$$\gamma_D = \frac{\alpha\gamma_{rd}\gamma_{sr}}{\gamma_{rd} + \alpha\gamma_{rd} + (1-\alpha)\gamma_{CJr} + 1} \quad (7)$$

Similarly, from Eq. (1) we can derive the SNR γ_r at R as follows:

$$\begin{aligned} \gamma_r &= \frac{|\sqrt{\alpha P}h_{sr}|^2}{|\sqrt{(1-\alpha P)}h_{CJr}|^2 + 1} \\ &= \frac{\alpha\gamma_s r}{(1-\alpha)\gamma_{CJr} + 1}. \quad (8) \end{aligned}$$

Consequently, the achievable rates $\bar{R}_D$ at D and $\bar{R}_r$ at R will be calculated as

$$\begin{aligned} \bar{R}_D &= \frac{1}{2}\log(1+\gamma_D) \\ &= \frac{1}{2}\log\left(1 + \frac{\alpha\gamma_{rd}\gamma_{sr}}{\gamma_{rd} + \alpha\gamma_{rd} + (1-\alpha)\gamma_{CJr} + 1}\right) \quad (9) \end{aligned}$$

$$\bar{R}_r = \frac{1}{2}\log(1+\gamma_r) = \frac{1}{2}\log\left(1 + \frac{\alpha\gamma_s r}{(1-\alpha)\gamma_{CJr} + 1}\right) \quad (10)$$

Finally, the secrecy rate $\bar{R}_s$ of the system is given by:

$$\bar{R}_s = \bar{R}_D - \bar{R}_r \quad (11)$$

B. Cooperative Jamming with S-D Direct Link

The transmission of the message signal comprises of two phases in this scenario, namely the broadcast phase (1^{st} phase) and the relaying phase (2^{nd} phase), as shown in Fig. 2.

During the 1^{st} phase, S transmits the source signal x_s with power αP and a single selected jammer CJ sends artificial noise η_{CJ}, with power $(1-\alpha)P$ which is known to the D,

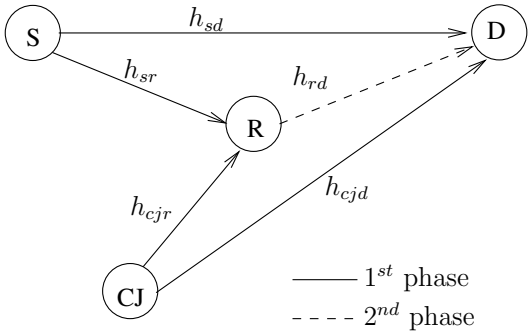


Fig. 2: Cooperative Jamming System Model

where $\{0 \leq \alpha \leq 1\}$ is the power distribution factor. Therefore the signals received at R and D are, given by

$$y_r = h_{sr}\sqrt{\alpha P}x_s + h_{CJr}\sqrt{(1-\alpha)P}\eta_{CJ} + w_r, \quad (12)$$

and

$$y_d^{(1)} = h_{sd}\sqrt{\alpha P}x_s + h_{CJd}\sqrt{(1-\alpha)P}\eta_{CJ} + w_d^{(1)}, \quad (13)$$

where w_r and $w_d^{(1)}$ represent the AWGN at R and D during the 1^{st} phase, respectively. Then, R amplifies and forwards the received signal y_r during the 2^{nd} phase, where the received signal at D can be expressed as

$$y_d^{(2)} = h_{rd}\eta_r y_r + w_d^{(2)}, \quad (14)$$

where $w_d^{(2)}$ represents the AWGN at D during this phase and the amplification factor may be written as

$$\eta_r = \sqrt{\frac{P}{\alpha P|h_{sr}|^2 + (1-\alpha)P|h_{CJr}|^2 + N_0}}. \quad (15)$$

By substituting Eqs. (12) and (15) into Eq. (14), we get

$$\begin{aligned} y_d^{(2)} &= h_{rd}\eta_r(h_{sr}\sqrt{\alpha P}x_s + h_{CJr}\sqrt{(1-\alpha)P}\eta_{CJ} + w_r) \\ &\quad + w_d^{(2)} \\ &= \eta_r h_{rd}h_{sr}\sqrt{\alpha P}x_s + \eta_r h_{rd}h_{CJr}\sqrt{(1-\alpha)P}\eta_{CJ} \\ &\quad + \eta_r h_{rd}w_r + w_d^{(2)}. \end{aligned} \quad (16)$$

By adding two received signals $y_d^{(1)}$ and $y_d^{(2)}$, we get

$$y_d = a y_d^{(1)} + b y_d^{(2)}, \quad (17)$$

where a and b are the amplification constants. By substituting Eqs. (13) and (16) into Eq. (17) (assuming a = 1 and b = 1), we have

$$\begin{aligned} y_d &= h_{sd}\sqrt{\alpha P}x_s + h_{CJd}\sqrt{(1-\alpha)P}\eta_{CJ} + w_d^{(1)} + \\ &\quad \eta_r h_{rd}h_{sr}\sqrt{\alpha P}x_s + \eta_r h_{rd}h_{CJr}\sqrt{(1-\alpha)P}\eta_{CJ} \\ &\quad + \eta_r h_{rd}w_r + w_d^{(2)}. \end{aligned} \quad (18)$$

Since η_{CJ} is known by D, both $\eta_r h_{rd}h_{CJr}\sqrt{(1-\alpha)P}\eta_{CJ}$ and $h_{CJd}\sqrt{(1-\alpha)P}\eta_{CJ}$ terms can be removed from y_d to yield:

$$\begin{aligned} y_d &= h_{sd}\sqrt{\alpha P}x_s \\ &\quad + \sqrt{\frac{\alpha}{\alpha P|h_{sr}|^2 + (1-\alpha)P|h_{CJr}|^2 + N_0}}Ph_{rd}h_{sr}x_s \\ &\quad + \sqrt{\frac{P}{\alpha P|h_{sr}|^2 + (1-\alpha)P|h_{CJr}|^2 + N_0}}h_{rd}w_r + w_d. \end{aligned} \quad (19)$$

where $w_d = w_d^{(1)} + w_d^{(2)}$, we can calculate the SNR at D as:

$$\gamma_D = \frac{\alpha^2\gamma_{sd}\gamma_{sr} + \alpha(1-\alpha)\gamma_{CJr}\gamma_{sd} + \alpha\gamma_{sd} + \alpha\gamma_{rd}\gamma_{sr}}{\gamma_{rd} + \alpha\gamma_{rd} + (1-\alpha)\gamma_{CJr} + 1}, \quad (21)$$

Similarly, from Eq. (12) we can derive the SNR at R as:

$$\begin{aligned} \gamma_r &= \frac{|\sqrt{\alpha P}h_{sr}|^2}{|\sqrt{(1-\alpha P)}h_{CJr}|^2 + 1} \\ &= \frac{\alpha\gamma_{sr}}{(1-\alpha)\gamma_{CJr} + 1}, \end{aligned} \quad (22)$$

Consequently, the achievable rates at D and R is given as:

$$\begin{aligned} \bar{R}_D &= \frac{1}{2}\log(1+\gamma_D) \\ &= \frac{1}{2}\log\left(1 + \frac{\alpha^2\gamma_{sd}\gamma_{sr} + \alpha(1-\alpha)\gamma_{CJr}\gamma_{sd} + \alpha\gamma_{sd} + \alpha\gamma_{rd}\gamma_{sr}}{\gamma_{rd} + \alpha\gamma_{sr} + (1-\alpha)\gamma_{CJr} + 1}\right) \end{aligned} \quad (23)$$

and

$$\bar{R}_r = \frac{1}{2}\log(1+\gamma_r) = \frac{1}{2}\log\left(1 + \frac{\alpha\gamma_{sr}}{(1-\alpha)\gamma_{CJr} + 1}\right). \quad (24)$$

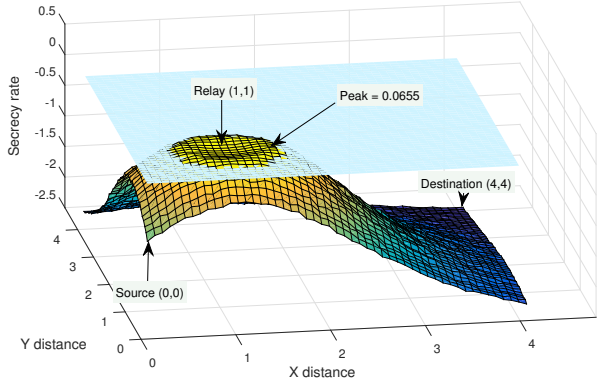
The secrecy rate $\bar{R}_s$ of the system can be calculated as

$$\bar{R}_s = \bar{R}_D - \bar{R}_r \quad (25)$$

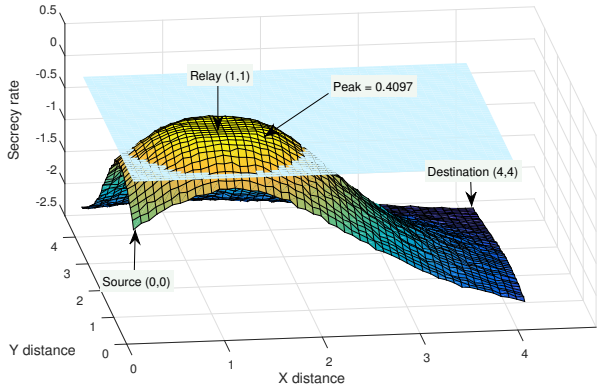
III. Results and Discussions

Figs. 3, 4 and 5 show the secrecy rates for the two cases discussed with relay being employed close to the source, in the center and close to the destination, respectively. The X and Y axis give the location of the jammer on the plane and for a specific jammer the secrecy rate is represented by the Z axis on that specific location of the jammer. The X and Y axis range from 0 - 4 km in distance. Note that the reduced distance related to path gain [12] is given by: $G_{ij} = \left(\frac{d_{sd}}{d_{ij}}\right)^{\alpha}$, where d_{ij} is the distance between node i and node j. Furthermore we have $h_{ij} = \sqrt{G_{ij}}\bar{h}_{ij}$. We consider a pathloss exponent of $\gamma = 4$, while α is set to 0.8. Fig. 3 shows the secrecy rate performance when the relay is closer to the source. We can see that the secrecy rate improves if there is a direct link between source and destination in addition to the relay link for its transmission. In addition, at a closer look we can see that the secrecy rate is maximum if the CJ is at a certain distance from the relay which can be seen as a ring shaped region in Fig. 3(a). If the CJ is closer to relay than this point, the secrecy rate drops because the signal received at destination is

$$\gamma_D = \frac{|h_{sd}\sqrt{\alpha P}|^2 + |\sqrt{\frac{\alpha}{\alpha P|h_{sr}|^2+(1-\alpha)P|h_{CJr}|^2+N_0}}Ph_{rd}h_{sr}|^2}{|\sqrt{\frac{P}{\alpha P|h_{sr}|^2+(1-\alpha)P|h_{CJr}|^2+N_0}}h_{rd}|^2N_0 + N_0^2} = \frac{\alpha P|h_{sd}|^2(\alpha P|h_{sr}|^2 + (1-\alpha)P|h_{CJr}|^2 + N_0) + \alpha P^2|h_{rd}|^2|h_{sr}|^2}{P|h_{rd}|^2N_0 + \alpha P|h_{sr}|^2N_0 + (1-\alpha)P|h_{CJr}|^2N_0 + N_0}$$
$$= \frac{\alpha^2\frac{P^2}{N_0^2}|h_{sd}|^2|h_{sr}|^2 + \alpha(1-\alpha)\frac{P^2}{N_0^2}|h_{sd}|^2|h_{CJr}|^2 + \frac{P}{N_0}|h_{sd}|^2 + \alpha\frac{P^2}{N_0^2}|h_{rd}|^2|h_{sr}|^2}{\frac{P}{N_0}|h_{rd}|^2 + \alpha\frac{P}{N_0}|h_{sr}|^2 + (1-\alpha)\frac{P}{N_0}|h_{CJr}|^2 + 1} \quad (20)$$

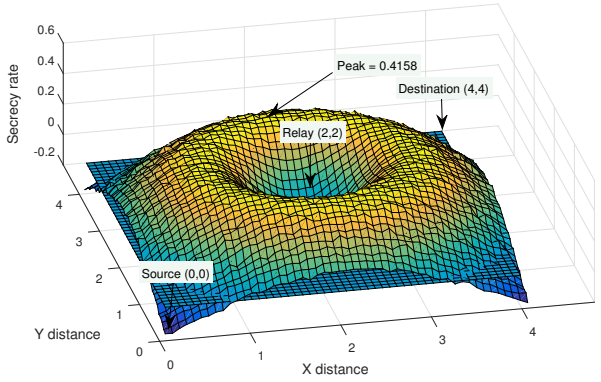


(a) Without S-D link

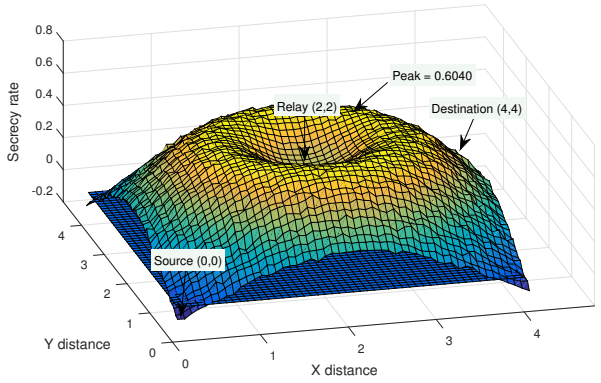


(b) With S-D link

Fig. 3: Relay at (x,y)=(1,1), and Source power is 90% of the total power



(a) Without S-D link



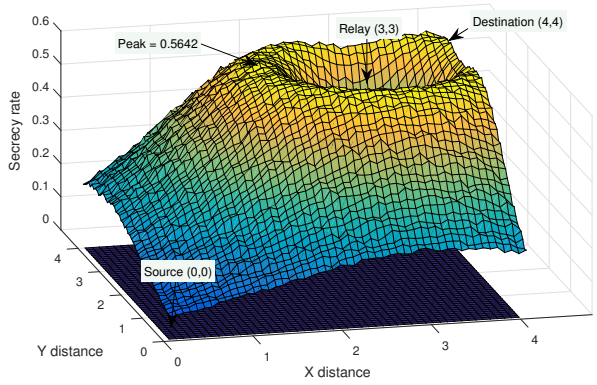
(b) With S-D link

Fig. 4: Relay at (x,y)=(2,2), and Source power is 90% of the total power

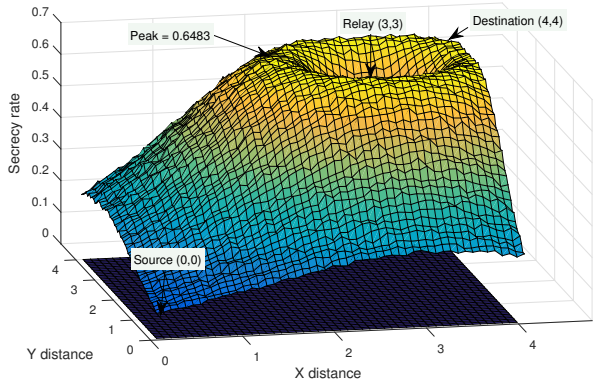
more distorted due to a higher interference at relay. The drop in secrecy rate can be seen more prominently in Fig. 4(a), where the relay is at the center between the source and the destination nodes. As seen in Fig. 4(b), the S-D direct link provides a higher secrecy rate compared to that without the S-D link seen in Fig. 4(a). Another observation that we can make from the Figs. 3, 4 and 5 is that the secrecy rate depends on the location of the relay as well. If a relay is closer to the source then we can see that peak secrecy rates of 0.0655 and 0.4097 can be achieved for the CJ without S-D scenario and the CJ with S-D scenario respectively, as shown in Fig. 3. Furthermore in Fig. 4 the peak secrecy rates are 0.4158 and 0.6040 for the CJ without S-D and the CJ with S-D scenario, respectively. Finally in Fig. 5, where the relay is located closer to the destination, we observe that the peak secrecy rates of 0.5642 and 0.6483 can be attained for the CJ without S-D case and the CJ with S-D case, respectively.

IV. Conclusions

In this paper, we have investigated the secrecy regions for friendly jamming in two-hop as well as the cooperative scenarios employing an untrusted relay. Our results show that the secrecy rate regions for different scenarios depends heavily on the positions of both the relay (a potential eavesdropper) and the cooperative jammer. We show that the secrecy rates are higher if the jammer is positioned closer to the relay. Our



(a) Without S-D link



(b) With S-D link

Fig. 5: Relay at (x,y)=(3,3), and Source power is 90% of the total power

results also indicate that if the relay is closer to the destination then we can ensure a higher secrecy rate in comparison to the case when the relay is closer to the source. Secondly, our results confirm that the secrecy rates would improve when we have a direct S-D link in our transmission.

REFERENCES

[1] X. Zhou, M. Tao, and R. Kennedy, "Cooperative jamming for secrecy in decentralized wireless networks," in *Communications (ICC), 2012 IEEE International Conference on*, June 2012, pp. 2339–2344.

[2] A. Bletsas, A. Khisti, D. Reed, and A. Lippman, "A simple cooperative diversity method based on network path selection," *Selected Areas in Communications, IEEE Journal on*, vol. 24, no. 3, pp. 659–672, March 2006.

[3] X. He and A. Yener, "Cooperation with an untrusted relay: A secrecy perspective," *Information Theory, IEEE Transactions on*, vol. 56, no. 8, pp. 3807–3827, Aug 2010.

[4] C. Jeong, I.-M. Kim, and D. I. Kim, "Joint secure beamforming design at the source and the relay for an amplify-and-forward mimo untrusted relay system," *Signal Processing, IEEE Transactions on*, vol. 60, no. 1, pp. 310–325, Jan 2012.

[5] J. Huang, A. Mukherjee, and A. Swindlehurst, "Secure communication via an untrusted non-regenerative relay in fading channels," *Signal Processing, IEEE Transactions on*, vol. 61, no. 10, pp. 2536–2550, May 2013.

[6] L. Wang, M. Elkashlan, J. Huang, N. Tran, and T. Duong, "Secure transmission with optimal power allocation in untrusted relay networks," *Wireless Communications Letters, IEEE*, vol. 3, no. 3, pp. 289–292, June 2014.

[7] L. Sun, T. Zhang, Y. Li, and H. Niu, "Performance study of two-hop amplify-and-forward systems with untrustworthy relay nodes," *Vehicular Technology, IEEE Transactions on*, vol. 61, no. 8, pp. 3801–3807, Oct 2012.

[8] A. Kuhestani and A. Mohammadi, "Destination-based cooperative jamming in untrusted amplify-and-forward relay networks: resource allocation and performance study," *IET Communications*, vol. 10, no. 1, pp. 17–23, 2016.

[9] T. Y. Liu, S. C. Lin, and Y. W. P. Hong, "Multicasting with untrusted relays: A noncoherent secure network coding approach," in *Information Forensics and Security (WIFS), 2015 IEEE International Workshop on*, Nov 2015, pp. 1–6.

[10] H. Khodakarami and F. Lahouti, "Link adaptation with untrusted relay assignment: Design and performance analysis," *Communications, IEEE Transactions on*, vol. 61, no. 12, pp. 4874–4883, December 2013.

[11] L. Sun, P. Ren, Q. Du, Y. Wang, and Z. Gao, "Security-aware relaying scheme for cooperative networks with untrusted relay nodes," *Communications Letters, IEEE*, vol. 19, no. 3, pp. 463–466, March 2015.

[12] H. Ochiai, P. Mitran, and V. Tarokh, "Design and analysis of collaborative diversity protocols for wireless sensor networks," in *Vehicular Technology Conference, 2004. VTC2004-Fall. 2004 IEEE 60th*, vol. 7, Sept 2004, pp. 4645–4649 Vol. 7.