Improving Secrecy Rate via Cooperative Jamming based on Nash Equilibrium

Nida Zamir[1], Bakhtiar Ali[1], Muhammad Fasih Uddin Butt[1] and Soon Xin Ng[2]

1. Department of Electrical Engineering, COMSATS Institute of Information Technology (CIIT), Islamabad 44000, Pakistan

(Email: {nida.zamir, bakhtiar_ali, fasih}@comsats.edu.pk).

2. School of Electronics and Computer Science, University of Southampton, SO17 1BJ, Southampton, U.K.

(Email: sxn@ecs.soton.ac.uk).

***Abstract*— This paper investigates a power control scheme for cooperative cognitive communication system which employs an untrusted relay. More explicitly, a friendly jammer transmits a jamming signal enabling secure communication between the source and the destination, in the presence of an untrusted relay. In return, the source compensates the potential jammer with an access to its bandwidth for a fraction of its time period. In addition, cooperative jammer defines its jamming power through Nash-Equilibrium for improving the secrecy rate. In our proposed scheme, we employ only one jammer and place it on different locations in order to analyze the secrecy rate achieved and the utility of the jammer. Additionally, we fix the positions of the source and the destination while the relay is moved at different locations.**

I. Introduction

For the last few decades, it has become important to ensure confidentiality of the transmitted signal communicating over the wireless medium as wireless medium is highly vulnerable to eavesdropping. Shannon was the first to investigate the secret communication between legitimate parties over a noiseless channel [1]. Wyner formally defined the discrete memoryless wiretap channel, revealing that legitimate parties can communicate secretly as well as reliably over the noisy communication medium [2]. Reliable communication alongwith confidentiality was established by [3] considering a broadcast channel with two receivers, i.e., a pair of discrete memoryless wiretap channels.

Broadcast and superposition are the fundamental challenges of the wireless medium in terms of ensuring security and reliability of a communication system in the presence of unauthorized users. Recently, Physical-Layer Security (PLS) techniques have gained considerable attention especially in military networks to enable secret communication [4]. In addition, traditional cryptographic (key-based enciphering) techniques have been used to achieve the confidentiality of a transmitted signal [5]. Physical layer security techniques can prevent eavesdropping in wireless communication without data encryption on upper layer. The basic principle behind physical layer security is to take the advantage of the random nature of noise and communication channels in order to minimize the amount of information that can be retrieved at the bit level by an unintended receiver. Cooperating Jammer (CJ) is one of the important PLS enhancement scheme in which legitimate parties secretly communicate with each other by having external helper(s) that transmit jamming signal to confuse the unauthorized recipient(s) at the time of data transmission [6], [7]. Relay can be considered as a trusted or as an untrusted node in cooperative communication network. In trusted relaying scenario, source and destination secretly communicate with the help of cooperative relay in the presence of an eavesdropper [8]–[10]. The untrusted relaying system was first investigated by [11], where source and destination have achieved non-zero secrecy rate with the help of destination which transmit the jamming signal. In [12], an Amplify-and-Forward (AF) multiple-input multiple-output (MIMO) untrusted relay system has been considered in which source and relay beamforming was jointly designed to maximize the secrecy rate. Reference [13] investigated secure communication for a multiple untrusted relay network and concluded that secrecy capacity will be degraded with the increase in number of untrusted relays. Since relay is considered untrusted in some applications [14]–[17] so it is important to secure the confidential data from it via some cooperative jamming techniques. Cooperative jammers protect the transmitted confidential signal by transmitting noise [6] or sending codewords [18], [19] to combat eavesdropping. Inspite of using dedicated nodes, reference [20] used non-altruistic jamming nodes to facilitate secure transmission between the legitimate parties where jammers are compensated by using legitimate parties' spectrum for their own data transmission to their destination.

In this work, we have proposed the power control scheme for cooperative communication system in which cooperative jammer transmits jamming signal to enable secret communication between source and destination in the presence of untrusted relay. Source compensates the potential jammer with an access to fraction of its transmission bandwidth. In addition, cooperative jammer defines its jamming power through Nash-Equilibrium to improve the secrecy rate. In our proposed scheme, we are employing only one jammer and place it on different locations in order to analyze the behaviour of secrecy rate curve. The position of the source and destination are fixed in our model and the position of the relay is changed from a location closer to the source towards the destination.

978-0-9928-6265-7/16/$31.00 ©2016 IEEE

II. System Model

We consider amplify-and-forward (AF) network consisting of a source (S), a destination (D), an untrusted relay (R), K cooperative jammers (CJ_i), i=$\{1,...,K\}$) and their destinations (DJ_i). The transmission of the message signal is composed of three phases, namely the broadcast phase (1^{st} phase), the relaying phase (2^{nd} phase) and the jammer's transmission phase (3^{rd} phase), as shown in Fig. 1. Each node is employed with a single antenna and operates in a half-duplex mode. The channel between any node pair (l, m) is denoted by $h_{lm} = \sqrt{G_{lm}}.\overline{h}_{lm}$, where $\overline{h}_{lm}$ is the Rayleigh fading coefficient and $G_{lm} = (\frac{d_{sd}}{d_{lm}})^{\gamma}$ is the reduced distance related path gain [21], while d_{lm} is the distance between node l and node m. The received signal-to-noise ratio at node m is defined as $\gamma_{lm} = \frac{|h_{lm}|^2}{N_0}$, with variance N_0. P_s is the source's power and P_J is the jammer's power which is being calculated by the Nash Equilibrium. To prevent the source message from being eavesdropped at the untrusted relay, we propose the following jamming method.

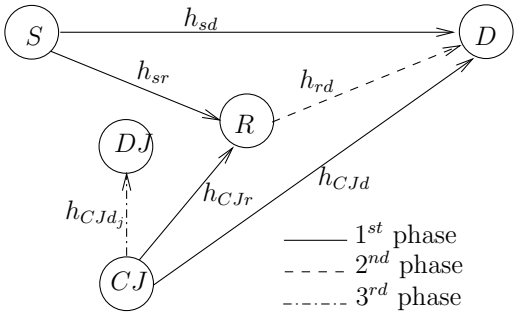


Fig. 1. Cooperative Jamming System Model

To prevent the source message from being eavesdropped, we investigate the following jamming method. The legitimate parties, a source S and its destination D, communicate through untrusted relay R and a jammer CJ sends an artificial noise η_{CJ}, known by D, with the power P_J. The source provides the cooperative jammer with an access to the fraction of its transmission interval/bandwidth in order to compensate it for its participation in cooperative jamming. The source's objective is to maximize its secrecy rate. The interaction between source and the cooperative jammer can be defined in the form of a *leader-follower* game framework [22], [23], i.e., source is the leader and the jammer is the follower. In particular, the source preserves only a fraction ($\alpha \leq 1$) of its bandwidth to establish secret communication aided by cooperative jamming. The legitimate pair determines the value of β which is the ratio of the average power used by the jammer during the cooperative jamming phase in which it transmits the Gaussian noise, while it transmits its own data during the transmission phase. The source also communicates the power ratio β and fraction α to the jammers, as well as the set of chosen jammers $\mathcal{J} \in \{1,..,N\}$, where N is the number of choosen jammers. The outcome of the game the jammers play is the set of powers that is the jammer's response, in the form of *Nash equilibrium* which is given by the following equation [6], [24]:

$$P^*_{J_{i\in\mathcal{J}}}(\alpha,\beta;\mathcal{J}) = \left[\frac{1-\alpha}{c_i \ln(2)} - \frac{\sigma^2}{h_{J_{ii}}}(\alpha\beta+1-\alpha) - \sum_{j\in\mathcal{J},j\neq i}\frac{h_{J_{ji}}}{h_{J_{ii}}}P^*_{J_j}(\alpha,\beta;\mathcal{J})\right]^{\overline{P}_{J_i}}_{0} \quad (1)$$

where c is the cost per unit transmission power, h_{ji} represents the channel interference between jammers and the jammer's power P_{J_i} is limited by the power budget i.e $P_{J_i} \leq \overline{P}_{J_i}$. NE always exists and is unique for weak interference cases. For example, if the interference matrix ($[\mathbf{H}]_{ji} = h_{ji}$) is strictly diagonally dominant, then $\sum_{j\in\mathcal{J},j\neq i}\frac{h_{ji}}{h_{ii}} < 1$.

During the 1^{st} phase, the received signals at relay R and destination D can be expressed respectively as

$$y_r = h_{sr}\sqrt{P_s}x_s + h_{CJr}\sqrt{P_J}\eta_{CJ} + w_r \quad (2)$$

and

$$y_d^{(1)} = h_{sd}\sqrt{P_s}x_s + h_{CJd}\sqrt{P_J}\eta_{CJ} + w_d^{(1)} \quad (3)$$

where w_r and $w_d^{(1)}$ represent the additive noises at relay and destination during 1^{st} phase, respectively. After this, R amplifies and forwards the received signal y_r. At the end of 2^{nd} phase, the received signal at D can be expressed as

$$y_d^{(2)} = h_{rd}\eta_r y_r + w_d^{(2)} \quad (4)$$

where $w_d^{(2)}$ represents the additive noise at D during this phase and the amplification factor

$$\eta_r = \sqrt{\frac{P_s}{P_s|h_{sr}|^2 + P_J|h_{CJr}|^2 + N_0}}. \quad (5)$$

By substituting (2) and (5) into (4), we get

$$\begin{aligned} y_d^{(2)} &= h_{rd}\eta_r(h_{sr}\sqrt{P_s}x_s + h_{CJr}\sqrt{P_J}\eta_{CJ} + w_r) + w_d^{(2)} \\ &= \eta_r h_{rd}h_{sr}\sqrt{P_s}x_s + \eta_r h_{rd}h_{CJr}\sqrt{P_J}\eta_{CJ} + \eta_r h_{rd}w_r \\ &\quad + w_d^{(2)}. \end{aligned} \quad (6)$$

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

$$y_d = a y_d^{(1)} + b y_d^{(2)} \quad (7)$$

where a and b are the amplification constants. By substituting (3) and (6) into (7) (assuming a = 1 and b = 1), we have

$$\begin{aligned} y_d = h_{sd}\sqrt{P_s}x_s + h_{CJd}\sqrt{P_J}\eta_{CJ} + \eta_r h_{rd}h_{sr}\sqrt{P_s}x_s \\ + \eta_r h_{rd}h_{CJr}\sqrt{P_J}\eta_{CJ} + \eta_r h_{rd}w_r + w_d^{(1)} + w_d^{(2)}. \end{aligned} \quad (8)$$

Since η_{CJ} is known by the destination so D can subtract the term $\eta_r h_{rd}h_{CJr}\sqrt{P_J}\eta_{CJ}$ and $h_{CJd}\sqrt{P_J}\eta_{CJ}$ from y_d and then decode the source information based on the remainder. Now replacing η_r, we get

$$y_d = h_{sd}\sqrt{P_s}x_s + \sqrt{\frac{1}{P_s|h_{sr}|^2 + P_J|h_{CJr}|^2 + N_0}}P_s h_{rd}h_{sr}x_s + \sqrt{\frac{P_s}{P_s|h_{sr}|^2 + P_J|h_{CJr}|^2 + N_0}}h_{rd}w_r + w_d \quad (9)$$

where $w_d = w_d^{(1)} + w_d^{(2)}$, we can calculate γ_D signal-to-noise ratio at D as

$$\gamma_D = \frac{|h_{sd}\sqrt{P_s}|^2 + |\sqrt{\frac{1}{P_s|h_{sr}|^2+P_J|h_{CJr}|^2+N_0}}P_s h_{rd}h_{sr}|^2}{|\sqrt{\frac{P_s}{P_s|h_{sr}|^2+P_J|h_{CJr}|^2+N_0}}h_{rd}|^2 + 1}$$

$$= \frac{P_s|h_{sd}|^2(P_s|h_{sr}|^2 + P_J|h_{CJr}|^2 + N_0) + P_s^2|h_{rd}|^2|h_{sr}|^2}{P_s|h_{rd}|^2 + P_s|h_{sr}|^2 + P_J|h_{CJr}|^2 + N_0}$$

$$\gamma_D = \frac{\gamma_{sd}\gamma_{sr} + \gamma_{CJr}\gamma_{sd} + \gamma_{sd} + \gamma_{rd}\gamma_{sr}}{\gamma_{rd} + \gamma_{rd} + \gamma_{CJr} + 1}. \quad (10)$$

Similarly, from (2) we can derive signal-to-noise ratio γ_r at relay.

$$\gamma_r = \frac{|\sqrt{P_s}h_{sr}|^2}{|\sqrt{P_J}h_{CJr}|^2 + 1} = \frac{\gamma_{sr}}{\gamma_{CJr} + 1}. \quad (11)$$

Consequently, the achievable rates $\overline{R_D}$ at destination and $\overline{R_R}$ at relay are given by:

$$\overline{R_D} = \frac{1}{2}\log(1 + \gamma_D) = \frac{1}{2}\log\left(1 + \frac{\gamma_{sd}\gamma_{sr} + \gamma_{CJr}\gamma_{sd} + \gamma_{sd} + \gamma_{rd}\gamma_{sr}}{\gamma_{rd} + \gamma_{sr} + \gamma_{CJr} + 1}\right) \quad (12)$$

$$\overline{R_R} = \frac{1}{2}\log(1 + \gamma_r) = \frac{1}{2}\log\left(1 + \frac{\gamma_{sr}}{\gamma_{CJr} + 1}\right). \quad (13)$$

The secrecy rate of the system, R_s is the communication rate at which untrusted relay is unable to extract secret information being communicated between the source and the destination [6], [20], which can be calculated as

$$\overline{R_s} = \overline{R_D} - \overline{R_R}. \quad (14)$$

The utility of the cooperative jammer is the achievable as well as reliable communication rate for its destination DJ during the fraction (1 - α) which is priced by the overall transmission power cost [22]. The utility of jammer during the 3^{rd} phase is given by

$$U(\alpha, \beta, \mathcal{J}; P_J) = (1-\alpha)\log_2\left(1 + \frac{h_J P_J}{\sigma^2(\alpha\beta + 1 - \alpha)}\right) - cP_J. \quad (15)$$

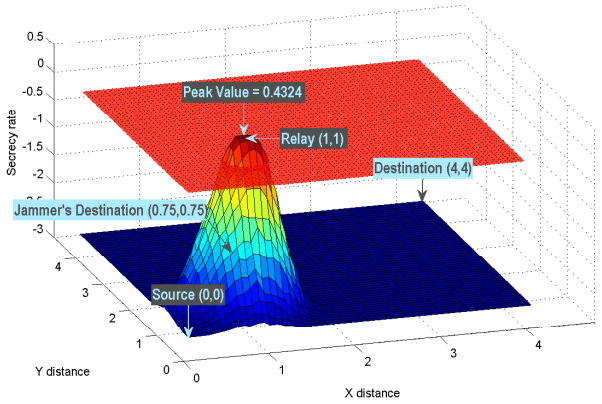
Conditions for Jamming Participation:
Following conditions must be fulfilled in order to yield improvement on the secrecy rate, R_s by employing the cooperative jamming [6]:

$$\frac{h_{SE}h_{JD}}{h_{SD}h_{JE}} < 1 \quad (16)$$

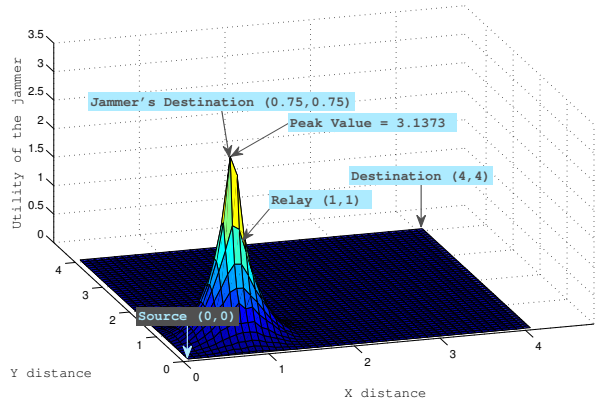
And,

$$\frac{h_{SD}h_{JD}(\sigma^2 + h_{SE}P_s/\alpha)}{h_{SE}h_{JE}(\sigma^2 + h_{SD}P_s/\alpha)} < 1 \quad (17)$$

$$h_J > \sigma^2\left(\frac{\alpha\beta}{1-\alpha} + 1\right)c\ln 2 \quad (18)$$



(a) Secrcey Rate R_s

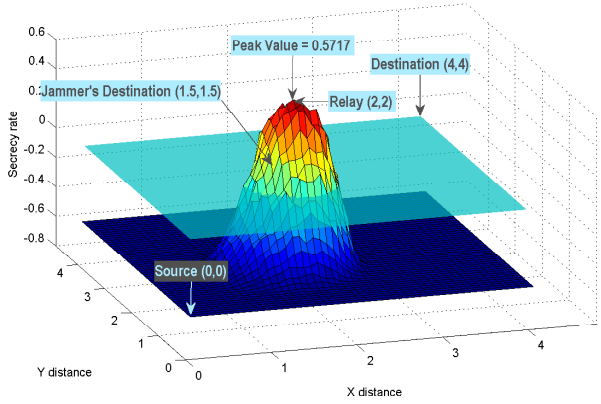


(b) Utility of the Jammer U_j

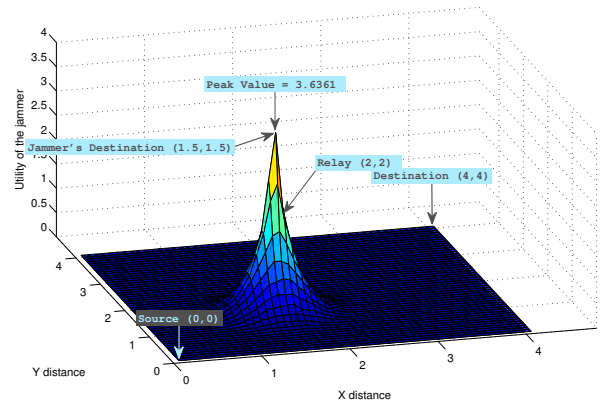
Fig. 2. Relay is at $(x, y) = (1, 1)$ and Jammer's destination is at $D_j = (0.75, 0.75)$.

III. Results and Discussions

This section presents results of the proposed scheme to illustrate the secrecy rate, R_s. Figs. 2(a), 3(a) and 4(a) show R_s in 3D-plots as a function of CJ's location (x, y) where x and y are points on the X and Y coordinates to represent the location of the nodes, while the secrecy rate is plotted on the Z-coordinate. Three scenarios are considered in which secrecy rate is being analysed for different locations of the relay, whereas source S and destination D are fixed at location $(0, 0)$ and $(4, 4)$, respectively. A simple pathloss model with propogation factor $\gamma = 4$ is used, with $\alpha = 0.79$, $\beta = 1$, $c_i = c = 0.25$, $P_s = 30$ and $N = 1$. In Figure 2, relay is placed near the source at point $(1, 1)$, where maximum secrecy rate of 0.4324 is achieved. As the relay's position is moved closer to the middle point $(2, 2)$ between S and D, the secrecy rate increases to 0.5717, as shown in Figure 3. Finally, when the relay is moved near the destination at point $(3, 3)$ the maximum secrecy rate of 0.6697 is achieved, as shown in Figure 4.

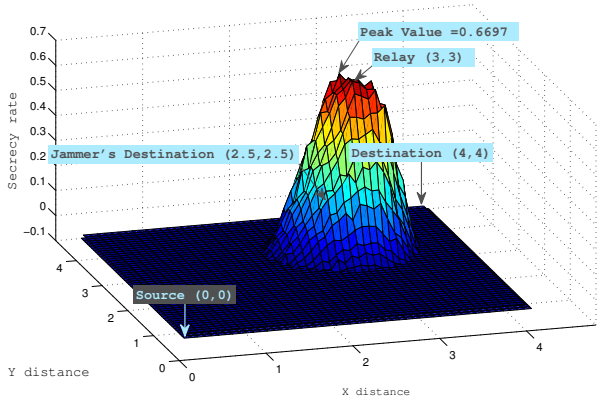


(a) Secrcey Rate R_s

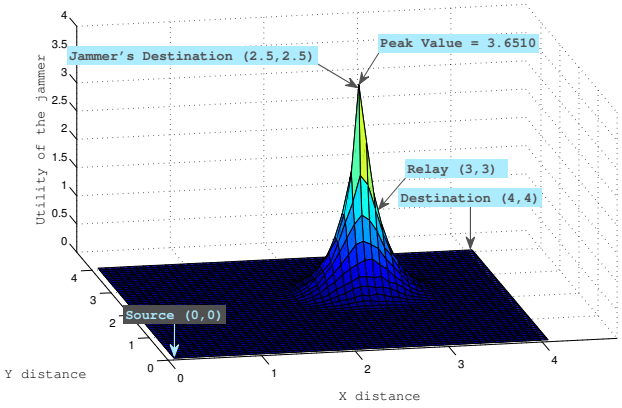


(b) Utility of the Jammer U_j

Fig. 3. Relay is at $(x, y) = (2, 2)$ and Jammer's destination is at $D_j = (1.5, 1.5)$.



(a) Secrcey Rate R_s



(b) Utility of the Jammer U_j

Fig. 4. Relay is at $(x, y) = (3, 3)$ and Jammer's destination is at $D_j = (2.5, 2.5)$.

The utility of the jammer is shown in Figures 2(b), 3(b) and 4(b). We can observe that when the relay R is located at (1,1), (2,2) and (3,3) and the jammer's destination D_j are at (0.75,0.75), (1.5,1.5) and (2.5,2.5) positions the utility of the jammer is at the maximum values of 3.1373, 3.6361 and 3.6510, respectively. Both the utility and secrecy rate plots show that the best response is achieved when D_j is placed closer to the relay.

IV. Conclusions

In this paper, we have investigated the achievable secrecy rates for cooperative cognitive scenarios employing an untrusted relay based on a power control scheme. In our scheme the source compensates the jammer with an access to its bandwidth for a fraction of time period, while the cooperative jammer defines its jamming power through Nash-Equilibrium to improve the secrecy rate. We have investigated the secrecy regions for different scenarios based on the position of both the untrusted relay (a potential eavesdropper) and the friendly (cooperative) jammer. It is observed that if the relay is moved closer to its destination then we can ensure a higher secrecy rate in comparison to when it is placed closer to the source. In addition, it is shown that the secrecy rates are high if the jammer is positioned close to its own destination. Similarly, the utility of the jammer will become maximum when it is placed closer to its own destination and the secrecy rate is the highest when the relay is closer to the destination.

References

[1] C. E. Shannon, "Communication theory of secrecy systems," *Bell Systems Technical Journal*, vol. 28, no. 4, pp. 656–715, Sep. 1949.

[2] A. D. Wyner, "The wiretap channel," *Bell Systems Technical Journal*, vol. 54, no. 8, pp. 1355–1387, Oct. 1975.

[3] J. Csiszar and J. Korner, "Broadcast channels with confidential messages," *IEEE Transactions on Information Theory*, vol. 24, no. 3, pp. 339–348, May 1978.

[4] Mukherjee, A., Fakoorian, S. A. A., Huang, J., Swindlehurst, A. L.:'Principles of physical layer security in multiuser wireless networks: A survey', IEEE Communications Surveys & Tutorials, 2014, 16, (3), pp.1550–1573.

[5] Massey, J. L.: 'An Introduction to Contemporary Cryptology', IEEE Proceeding, 1988, 76, (5), pp.533–549.

[6] E. Tekin and A. Yener, "The general Gaussian multiple-access and two-way wiretap channels: Achievable rates and Cooperative Jamming," *IEEE Transactions on Information Theory*, vol. 54, no. 6, pp. 2735–2751, 2008.

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

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

[9] V. N. Q. Bao, N. Linh-Trung and M. Debbah, "Relay selection schemes for dual-hop networks under security constraints with multiple eavesdroppers," *IEEE Transactions on Wireless Communications*, vol. 12, no. 12, pp. 6076–6085, 2013.

[10] L. Dong, Z. Han, A. P. Petropulu and H. V. Poor, "Improving wireless physical layer security via cooperating relays," *IEEE Transactions on Signal Processing*, vol. 58, no. 3, pp. 1875–1888, 2010.
[11] X. He and A. Yener, "Cooperation with an untrusted relay: A secrecy perspective," *IEEE Transactions on Information Theory*, vol. 56, no. 8, pp. 3807–3827, 2010.
[12] 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," *IEEE Transactions on Signal Processing*, vol. 60, no. 1, pp. 310–325, Jan. 2012.
[13] L. Sun, T. Zhang, Y. Li, H. Niu, "Performance study of two-hop amplify-and-forward systems with untrustworthy relay nodes," *IEEE Transactions on Vehicular Technology*, vol. 61, no. 8, pp. 3801–3807, Oct. 2012.
[14] J. Huang, A. Mukherjee, A.L. Swindlehurst, "Secure communication via an untrusted non-regenerative relay in fading channels," *IEEE Transactions on Signal Processing*, vol. 61, no. 10, pp. 2536–2550, May 2013.
[15] H. Khodakarami and F. Lahouti, "Link Adaptation with Untrusted Relay Assignment: Design and Performance Analysis," *IEEE Transactions on Communications*, vol. 61, no. 12, pp. 4874–4883, Dec. 2013.
[16] L. Wang, M. Elkashlan, J. Huang, N. H. Tran and T.Q. Duong,, "Secure Transmission with Optimal Power Allocation in Untrusted Relay Networks," *IEEE Wireless Communications Letters*, vol. 3, no. 3, pp. 289–292, Jun. 2014.
[17] L. Sun, P. Ren, Q. Du, Y. Wang and Z. Gao, "Security-Aware Relaying Scheme for Cooperative Networks With Untrusted Relay Nodes," *IEEE Communications Letters*, vol. 19, no. 3, pp. 463–466, 2015.
[18] L. Lai and H. L. Gamal, "The relay–eavesdropper channel: Cooperation for secrecy," *IEEE Transactions on Information Theory*, vol. 54, no. 9, pp. 4005–4019, 2008.
[19] E. Ekrem and S. Ulukus, "Secrecy in cooperative relay broadcast channels," *IEEE Transactions on Information Theory*, vol. 57, no. 1, pp. 137–155, 2011.
[20] I. Stanojev and A. Yener, "Improving secrecy rate via spectrum leasing for friendly jamming," *IEEE Transactions on Wireless Communications*, vol. 12, no. 1, pp. 134–145, 2013.
[21] H. Ochiai, P. Mitran and V. Tarokh, "Design and analysis of collaborative diversity protocols for wireless sensor networks," in *IEEE Vehicular Technology Conference, VTC-'04 Fall*, Los Angeles, USA, September 2004, pp. 4645–4649.
[22] O. Simeone, I. Stanojev, S. Savazzi, Y. Bar-Ness, U. Spagnolini and R. Pickholtz, "Spectrum leasing to cooperating secondary ad hoc networks," *IEEE Journal on Selected Areas in Communications*, vol. 26, no. 1, pp. 203–213, 2008.
[23] G. Scutari, D. P. Palomar and S. Barbarossa, "Optimal linear precoding/multiplexing for wideband optimal linear precoding strategies for wideband noncooperative systems based on game theory-part I: Nash equilibria," *IEEE Transaction Signal Process*, vol. 56, no. 3, pp. 1230–1249, 2008.
[24] M. J. Osborne and A. Rubenstein, *A Course in Game Theory*. MIT press, 1994.