# Decode-and-forward plus cooperative jamming based cooperation for wireless physical layer security

Shuanglin Huang* and Jianjun Tan*
*School of Information Engineering, Hubei University for Nationalities, EnShi, China, 445000

*Abstract*—**In this paper, the case of one source-destination pair with the help of multiple cooperating nodes in the presence of one eavesdropper was considered to improve the performance of secure wireless communications. A novel cooperative scheme decode-and-forward plus cooperative jamming(DFCJ) was proposed. In this scheme, the relay nodes transmit a weighted version of the source signals plus a common weighted jamming signal to confound the eavesdropper. For DFCJ, the optimal power allocation is obtained in closed-form in the condition of the complete nulling of jamming signals at the destination subject to a secrecy rate constraint. The numerical evaluation of the transmit power and the obtained secrecy rate results shows that the proposed scheme can significantly improve the performance of wireless physical layer security, as compared to the decode-and-forward(DF) scheme.**

***Index Terms*—Secrecy rate, cooperation, power allocation, wireless networks.**

## I. Introduction

In wireless networks, information theoretic security has recently received much interest due to its capability to realize perfect secrecy transmission without relying on traditional encryption mechanisms [1], [2]. Note that the achievable secrecy rate is typically zero if the channel conditions between the legitimate transceiver is worse than that of source and eavesdroppers, which motivates the use of node cooperation [3]-[8].

The use of cooperation node can be grouped into three categories. In the first category, the relays or the helpers transmit artificial noise to jam the eavesdropper; in the second one, the relays or the helpers help the source-destination transmission; in the third one, each relay or the helper not only helps the source-destination transmission, but also transmits artificial noise to jam the eavesdropper. A basic approach to ensuring confidentiality were proposed in [3]. The basic idea is to schedule downlink base station transmissions at the same time as the concurrent uplink transmissions of interest, so as to create intentional interference on the possible eavesdroppers. In [4], the authors proposed a two-relay scheme to increase security against eavesdroppers, where the first relay uses a DF strategy and assists source to deliver its data to destination and the second relay is used to create intentional interference at the eavesdropper nodes. However, only single cooperation node was considered for a secure link, multiple relays or helpers can be used to enjoy the benefits of multiple-antenna systems[5]-[8]. Three cooperative schemes, DF, amplify-and-forward (AF) and cooperative jamming (CJ), were considered to improve the achievable secrecy rate, or minimize the total transmit power in [5]. The DF and AF, in [6], were also studied to obtain the optimal beamforming structure and maximize the secrecy rates under both total and individual power constraints. In [7], some friendly jammers charge the sources with a certain price for interfering the unauthenticated malicious relay. The authors in [8] proposed two opportunistic secrecy transmission schemes: opportunistic cooperative jamming and relay chatting. In the two schemes, a part of relays and the destination are grouped to transmit jamming signals to confuse the eavesdropper.

However, in the previous works, only first two uses are explored and utilized. Actually, each relay can be potentially used for both helping the source-destination transmission and transmitting artificial noise to jam the eavesdropper. In this paper, a novel cooperative scheme: DFCJ is proposed, and focuses on the single eavesdropper case, which is obviously different from the DF and CJ. For DFCJ, the use of each relay is not only for forwarding the messages from source but also for transmitting jamming signal with the purpose of confounding the eavesdropper. Furthermore, under special circumstance, a part of relays follow the proposed DFCJ strategy and other part of relays just transmit jamming signals to confuse the eavesdropper. Therefore, more cooperation node may be involved into cooperation in the DFCJ scheme. By inviting more relays into cooperation, in general, the security performance will be further improved in the proposed system. We wish to design the cooperative node weights and the transmit power of each node, so that the total cooperative power is minimized subject to a secrecy capacity constraint.

## II. System Model and Cooperative Schemes

We study a wireless network model consisting of one source node, $N$ trusted relay nodes, one destination node, and one eavesdropper. The source wishes to transmit its own data to the destination in the presence of a single eavesdropper. The $N$ relays, $r_1, ..., r_N$, simultaneously follow DF protocols and the CJ protocols. Furthermore, each node has a single omni-directional antenna for both transmission and reception and operates in half-duplex mode. We assume that global channel state information(CSI) is available(This is a common assumption in the physical layer security literature).

This work was supported by Research Fund for the Doctoral Program of Higher Education of China(No.20090142110018) and National Natural Science Foundation of China(No.61261016)

We adopt the following notation. Bold uppercase letters denote matrices and bold lowercase letters denote column vectors. Conjugate, transpose and conjugate transpose are represented by $(\cdot)^*$, $(\cdot)^T and(\cdot)^\dagger$, and respectively. All channels are assumed to undergo flat fading and are quasi-static. We denote by $P_s$ the transmit power of the source, by $P_D$ the transmit power of the re-encoded signal sent from relays for helping the source-destination transmission and by $P_J$ the transmit power of the jamming signal sent from relays for confounding the eavesdropper. Let us define the relay message signal weight vector $\mathbf{w}_D(N \times 1)$ and the relay jamming signal weight vector $\mathbf{w}_J(N \times 1)$. Also, let $\sigma^2$ denote the noise power, $\mathbf{h}(N \times 1)$ represent the channel vector between the $N$ relays and the destination, $\mathbf{g}(N \times 1)$ represent the channel vector between the $N$ relays and the eavesdropper, respectively. Furthermore, define matrix $\mathbf{R}_h = \mathbf{h}\mathbf{h}^\dagger$ and $\mathbf{R}_g = \mathbf{g}\mathbf{g}^\dagger$.

There are two stages in DFCT. In Stage 1, the source broadcasts its $n$ encoded symbols to its trusted relay nodes using the first transmission slot. The source's transmit power is chosen so that the signal $x$ can be decoded at the relays with high probability. For simplicity we assume that the transmit power in Stage 1 is known a priori and the cooperative jamming is not selected. In Stage 1, when transmitting the symbol $x$, the received signal at the destination is

$$y_d^{(1)} = \sqrt{P_s} h_0 x + n_d^{(1)} \tag{1}$$

and the received signal at the eavesdropper is given by

$$y_e^{(1)} = \sqrt{P_s} g_0 x + n_e^{(1)} \tag{2}$$

where $n_d^{(1)}$ and $n_e^{(1)}$ are the noises at the destination and the eavesdropper, $h_0$ and $g_0$ represent the source-destination channel and the source-eavesdropper channel, respectively.

In Stage 2, all the trusted relay nodes that successfully decode the message, re-encode the message and cooperatively transmit the re-encoded symbols to the destination, using the second transmission slot. For notational convenience, we here assume that all the relay nodes successfully decode the source message. Specifically, each relay node transmits a weighted version of the re-encoded symbol. In DFCJ, while the $N$ relay nodes are transmitting the re-encoded symbol, they also transmit weighted jamming signals that are independent of the source message, with the purpose of confounding the eavesdropper. Let the weights of all relay nodes be stacked in vector and let $\tilde{x}$ be the re-encoded symbol and $z$ is the jamming signal at the relay nodes.

In the stage 2, the received signal at the destination is

$$y_d^{(2)} = \mathbf{h}^\dagger \mathbf{w}_D \tilde{x} + \mathbf{h}^\dagger \mathbf{w}_J z + n_d^{(2)} \tag{3}$$

and the received signal at the eavesdropper is given by

$$y_e^{(2)} = \mathbf{g}^\dagger \mathbf{w}_D \tilde{x} + \mathbf{g}^\dagger \mathbf{w}_J z + n_e^{(2)} \tag{4}$$

where $n_d^{(2)}$ and $n_e^{(2)}$ are the noises at the destination and the eavesdropper, respectively.

The rate[5] at the destination, $R_d$, and the eavesdropper, $R_e$, is,

$$R_d = \frac{1}{2}\log(1 + \frac{P_s|h_0|^2}{\sigma^2} + \frac{\mathbf{w}_D^\dagger \mathbf{R}_h \mathbf{w}_D}{\sigma^2 + \mathbf{w}_J^\dagger \mathbf{R}_h \mathbf{w}_J}) \tag{5}$$

$$R_e = \frac{1}{2}\log(1 + \frac{P_s|g_0|^2}{\sigma^2} + \frac{\mathbf{w}_D^\dagger \mathbf{R}_g \mathbf{w}_D}{\sigma^2 + \mathbf{w}_J^\dagger \mathbf{R}_g \mathbf{w}_J}) \tag{6}$$

The secrecy rate in the presence of a single eavesdropper in stage 2 is given by[5]-[8]

$$R_s = \max\{0, R_d - R_e\} \tag{7}$$

## III. Formulations for Transmit Power Minimization

In this section, we firstly provide lemma 1 and lemma 2, which will be the basis of the following results. Then, we assume that $\mu = \mathbf{w}_J^\dagger \mathbf{g}$ and fix it to obtain the weights $\mathbf{w}_D$ and $\mathbf{w}_J$ to minimize the total power of cooperative nodes. And find the optimal value of $\mu$ in the end.

**Lemma 1:** Let $\mathbf{w}_J^\dagger \mathbf{g} = \mu$ and $\mathbf{w}_J^\dagger \mathbf{h} = 0$. The solution[9] of problem minimizing $\mathbf{w}_J^\dagger \mathbf{w}_J$, is given by

$$\mathbf{w}_J = \mu \begin{bmatrix} \mathbf{g} & \mathbf{h} \end{bmatrix} \begin{bmatrix} \mathbf{g}^\dagger\mathbf{g} & \mathbf{g}^\dagger\mathbf{h} \\ \mathbf{h}^\dagger\mathbf{g} & \mathbf{h}^\dagger\mathbf{h} \end{bmatrix}^{-1} \begin{bmatrix} \mathbf{1} \\ \mathbf{0} \end{bmatrix} \tag{8}$$

**Lemma 2:** Let $\mathbf{s}$ and $\mathbf{t}$ be (known) linearly uncorrelated vectors. The matrix $\mathbf{s}\mathbf{s}^\dagger - \mathbf{t}\mathbf{t}^\dagger$ has only two nonzero eigenvalues, i.e., $\eta_1 > 0$ and $\eta_2 < 0$, given by

$$\eta_1 = \frac{\| \mathbf{s} \|^2 - \| \mathbf{t} \|^2 + \sqrt{(\| \mathbf{s} \|^2 + \| \mathbf{t} \|^2)^2 - 4|\mathbf{s}^\dagger \mathbf{t}|^2}}{2} \tag{9}$$

$$\eta_2 = \frac{\| \mathbf{s} \|^2 - \| \mathbf{t} \|^2 - \sqrt{(\| \mathbf{s} \|^2 + \| \mathbf{t} \|^2)^2 - 4|\mathbf{s}^\dagger \mathbf{t}|^2}}{2} \tag{10}$$

The proof of lemma 2 is simple and is omitted for brevity.

Given the secrecy rate constraint $R_s = R_s^0$ and the source power $P_s$, the optimization problem of minimizing the transmit power in Stage 2 can be formulated as

$$\min P_0 = P_s + ||\mathbf{w}_D||^2 + ||\mathbf{w}_J||^2, s.t. R_s = R_s^0 \tag{11}$$

Nulling signals at the undesired nodes is sometimes referred to as null-steering beamforming in array signal processing. By nulling the jamming signals at the destination [5][8]. Without loss of generality, we assume that $\mu$ is a positive real number and $\mathbf{w}_J^\dagger \mathbf{g} = \mu$. This is because the transmit power remains the same when the weight vector $\mathbf{w}_J$ is rotated an arbitrary phase. So $\mathbf{w}_J^\dagger \mathbf{R}_g \mathbf{w}_J = \mu^2$. Then, (11) can be rewritten as

$$\begin{aligned} &\min P_0 = P_s + P_D + P_J \\ &s.t. \begin{cases} \mathbf{w}_J^\dagger \mathbf{h} = 0 \\ \mathbf{w}_J^\dagger \mathbf{g} = \mu \\ \mathbf{w}_D^\dagger \widetilde{\mathbf{R}} \mathbf{w}_D = \zeta \end{cases} \end{aligned} \tag{12}$$

where $\zeta = \frac{P_s}{\sigma^2}(4^{R_s^0}|g_0|^2 - |h_0|^2) + 4^{R_s^0} - 1$ and $\widetilde{\mathbf{R}} = \mathbf{R}_h/\sigma^2 - 4^{R_s^0}\mathbf{R}_g/(\sigma^2 + \mu^2)$.

*Theorem 1:* For a given source's power $P_s$, the optimal cooperative power consumption $P_0$ is a function of $\mu^2$ and $P_0(\mu^2)$ is convex with respect to $\mu^2 (\mu^2 \geq 0)$. The optimum of $\mu^2$ is existent and unique.

Proof: From Lemma 1, we firstly know that the $||\mathbf{w}_J||^2$ can be represented as a function of $\mu$:

$$P_J(\mu^2) = k\mu^2 \tag{13}$$

where $k > 0$ and $k$ is coefficient independent of $\mu$.

Then, the second objective becomes to find the relationship between $P_D$ and $\mu^2$. Without loss of generality, let us first assume that $\zeta > 0$ and $\widetilde{\mathbf{R}}$ is positive definite. Let $\lambda$ is one of the eigenvectors of the matrix $\widetilde{\mathbf{R}}$. So we have $\lambda \mathbf{w}_D = \widetilde{\mathbf{R}} \mathbf{w}_D$, and further yields

$$\mathbf{w}_D^{\dagger} \mathbf{w}_D = \frac{1}{\lambda} \mathbf{w}_D^{\dagger} \widetilde{\mathbf{R}} \mathbf{w}_D = \frac{\zeta}{\lambda} \tag{14}$$

Then, minimizing $\mathbf{w}_D^{\dagger} \mathbf{w}_D$ is equivalent to maximize $\lambda$, so $\lambda$ corresponds to the largest eigenvalue of $\widetilde{\mathbf{R}}$, and thus $\mathbf{w}_D$ should be the largest eigenvector of $\widetilde{\mathbf{R}}$.

On the other hand, if $\zeta \leq 0$, it means that $P_s \geq \frac{\sigma^2(4^{R_s^0}-1)}{|h_0|^2 - 4^{R_s^0}|g_0|^2}$. However, when $P_s \geq \frac{\sigma^2(4^{R_s^0}-1)}{|h_0|^2 - 4^{R_s^0}|g_0|^2}$, the destination can directly achieved the secrecy rate $R_s^0$ in stage 1. The node cooperation is no needed in stage 2. Thus, it is meaningless for $\zeta \leq 0$.

For simplicity, we define $p = \sigma^2 + \mu^2 (p \geq \sigma^2)$, $u = \parallel \mathbf{h} \parallel^2 / \sigma^2$, $v = 4^{R_s^0} \parallel \mathbf{g} \parallel^2$ and $m = 4^{R_s^0} |\mathbf{h}^{\dagger} \mathbf{g}|^2 / \sigma^2$. It is obvious that $uv - m > 0$. From Lemma 2, $\widetilde{\mathbf{R}}$ has only two nonzero eigenvalues, and the positive eigenvalue is given by

$$\lambda = \frac{u}{2} - \frac{v}{2p} + \frac{1}{2}\sqrt{(u + \frac{v}{p})^2 - \frac{4m}{p}} \tag{15}$$

Thus the $P_D$ can be represented as a function of $\mu^2$:

$$P_D(\mu^2) = \frac{2\zeta}{u - \frac{v}{\mu^2+\sigma^2} + \sqrt{(u + \frac{v}{\mu^2+\sigma^2})^2 - \frac{4m}{\mu^2+\sigma^2}}} \tag{16}$$

According to (13) and (16), the $P_0$ can be represented as a function of $\mu^2$:

$$P_0(\mu^2) = \frac{2\zeta}{u - \frac{v}{\mu^2+\sigma^2} + \sqrt{(u + \frac{v}{\mu^2+\sigma^2})^2 - \frac{4m}{\mu^2+\sigma^2}}} + k\mu^2 + P_s \tag{17}$$

Taking the second-order derivatives of $P_0(\mu^2)$ with respect to $\mu^2$, we can get

$$\frac{\partial^2 P_0}{\partial(\mu^2)^2} = \frac{2\zeta m}{[\sqrt{(u(\mu^2+\sigma^2) - v)^2 + 4(uv - m)(\mu^2+\sigma^2)}]^3} \tag{18}$$

It is straightforward to verify that $\frac{\partial^2 P_0}{\partial(\mu^2)^2} > 0$. So $P_0(\mu^2)$ is convex with respect to $\mu^2$. And, it is obvious that the constraints $\mu \geq 0$ is convex. Thus, the optimum of $\mu^2$ is existent and unique. Up to this point, the theorem 1 is proved.

Firstly, if $\frac{\partial P_0}{\partial(\mu^2)}|_{\mu^2=0} \geq 0$, $\mu^2 = 0$, which corresponds to the case of DF scheme. Secondly, if $\frac{\partial P_0}{\partial(\mu^2)}|_{\mu^2=0} < 0$, taking the first-order derivative of $P_0(\mu^2)$ and setting it to zero, we can have a quadratic equation of $p$.

$$Ap^2 + Bp + C = 0 \tag{19}$$

with $A = u^2(u^2 - L^2)$, $B = (2uv - 4m)(u^2 - L^2)$, $C = (uv - 2m)^2 - v^2 L^2$ and $L = \frac{\zeta u - 2k(uv-m)}{\zeta}$. Since $\mu^2$ is a nonnegative real number, $B^2 - 4AC \geq 0$. Then, the optimal value of $\mu^2$ can be expressed

$$\mu^2 = \frac{\sqrt{B^2 - 4AC} - B}{2A} - \sigma^2 \tag{20}$$

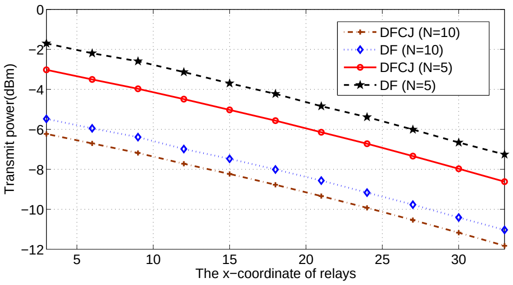

Fig. 1. The transmit power $P_D + P_J$ versus the x-coordinate of relays. The position of the relays varies from (3, 5) to (33, 5) and $P_s = 10^{-4}$W.

## IV. Numerical Results

In this section, some numerical simulations are conducted to illustrate the proposed scheme. In this paper, we use the same system configuration as that in [5], where the source, the destination and the eavesdropper are placed along a line. To emphasize the effects of distances, the channel model between any two nodes are modeled as a line-of-sight channel model $d^{-c/2} e^{i\theta}$, where $d$ is the distance between any two nodes, $c = 3.5$ is the path loss exponent, and $\theta$ is the phase uniformly distributed within $[0, 2\pi)$. We assume that the distances between relay nodes are much smaller than the distances between relay nodes and source/destination/eavesdropper, so that the path losses between different relay nodes and source/destination can be regarded as approximately the same. The source, destination and eavesdropper are located at fixed two-dimensional coordinates (0, 0), (100, 0) and (60, 0), respectively (unit: meters). The noise power is $\sigma^2 = -90$dBm. In order to obtain the average results, the Monte Carlo experiments consisting of 1000 independent trials are performed.

The performance of transmit power for different location of the relays is shown in Fig.1, in which the secrecy capacity constraint is fixed at $R_0 = 1 bits/s/Hz$. The number of relay nodes is $N = 5, 10$. As can be seen from Fig. 1, there is a significant gap between the power consumption by the two schemes. This is due to the fact that relays use only a little of power to confuse the eavesdropper and can obviously reduce the rate $R_e$. When the relays are close to the source and eavesdropper, the total power consumption is decreased. This is because the relays can use less power to help the source-destination transmission for the same $R_d$, and less power to confuse the eavesdropper for the same $R_e$. An interesting observation from the figure is that the performance of both schemes can be improved by inviting more relays into cooperation.

In Fig.2, simulations for relays $r_1, r_2, \cdots, r_{10}$ at (10,5), (20,5) and (30,5) are conducted respectively. The total transmit power is increasing as the transmit power of source increases.

Now, we conduct some simulations, in which the source's transmit power is not a constant and its optimum is used. In Fig.3 and Fig.4, a part of relays $r_1, r_2, \cdots, r_5$ are fixed at (5,5) and another part of relays $r_6, r_7, \cdots, r_{10}$ are moved from point (5, 5) to point (95, 5) along a line.

The total transmit power is shown in Fig.3. As observed in Fig.3, at the beginning, when relays $r_6, r_7, \cdots, r_{10}$ are the

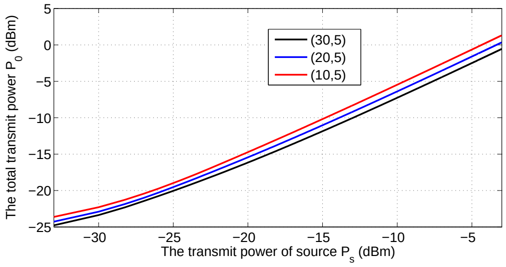

Fig. 2. The total transmit power versus $P_s$. The value of $P_s$ varies from $5 \times 10^{-7}$W to $5 \times 10^{-4}$W.

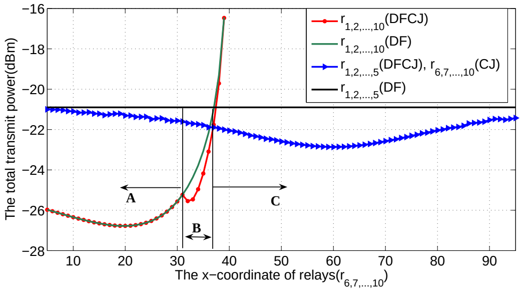

Fig. 3. The total transmit power versus the x-coordinate of relays. $R_s^0 = 1bits/s/Hz$.

left of double vertical line which is marked by arrow ”A”, the optimal performance(the minimal total transmit power) can be achieved if all relays perform DF scheme. This is because the the relays $r_6, r_7, \cdots, r_{10}$ are very close to the source and quite far away from the eavesdropper, the source can just use a little power to achieve the secrecy rate $R_s^0$ at relays $r_6, r_7, \cdot \cdot \cdot, r_{10}$ in stage 1 and it is not worthy spending a lot of power on transmitting the jamming signal in this situation, since the received power of the message signal at the eavesdropper is always small (regardless of jamming) due to the large path loss in stage 2. Then, when relays $r_6, r_7, \cdot \cdot \cdot, r_{10}$ are in the middle of double vertical line which is marked by arrow ”B”, the optimal performance can be achieved, if all relays perform DFCJ scheme. In this situation, relays $r_6, r_7, \cdots, r_{10}$ are close enough to the eavesdropper and it is worthy spending some power on transmitting the jamming signal, so that more power on transmitting the message signal can be saved, this fact has explained the advantage of DFCJ as compare to DF. In the end, when relays $r_6, r_7, \cdots, r_{10}$ are the right of double vertical line which is marked by arrow ”C”, the optimal performance can be achieved, if relays $r_1, r_2, \cdot \cdot \cdot, r_5$ perform DFCJ scheme and relays $r_6, r_7, \cdot \cdot \cdot, r_{10}$ just perform CJ scheme. In this area, it is not worthy spending a large mount of power on achieving the secrecy rate $R_s^0$ at relays $r_6, r_7, \cdots, r_{10}$ in stage 1, since relays $r_6, r_7, \cdot \cdot \cdot, r_{10}$ are far away from the source and are correspondingly close to the eavesdropper, such that relays $r_6, r_7, \cdot \cdot \cdot, r_{10}$ should not follow the DF scheme and more power is saved if relays $r_6, r_7, \cdots, r_{10}$ just transmit the jamming signal to confound the eavesdropper in stage 2.

The results show that the JDFCJ scheme can significantly improve the system performance as compared to the DF scheme in [5], since DF is a special case of DFCJ for $P_J = 0$, the performance of DFCJ is no worse than that of DF. Furthermore, more cooperation node may be involved into cooperation in the DFCJ scheme.

## V. Conclusion

In this paper, a novel system designs have been proposed to allocate transmit power among source and relays and determine the relay weights, such that the performance of secure wireless communications can be improved in the presence of one eavesdropper. This cooperative scheme, DFCJ, has been considered to minimize the total transmit power subject to a secrecy rate constrain. Via analysis and numerical evaluations, we have shown that the proposed DFCJ scheme can overcome the traditional limitation on channel conditions and significantly improve the system performance, as compared to the DF scheme. The future research includes system design of cooperative schemes that uses partial CSI or channel statistics about the eavesdropper’s channels. The ergodic secrecy rate and outage probability could be employed. Further study is also needed for the case in which the number of eavesdroppers is more than one.

## References

[1] M. Bloch, J. Barros, M. R. D. Rodriques, and S. W. McLaughlin, *Wireless information-theoretic security*, IEEE Trans. Information Theory, vol. 54, pp. 2515-2534, June. 2008.

[2] L. Lai and H. El Gamal, *The relay-eavesdropper channel: Cooperation for secrecy*, IEEE Trans. Inf. Theory, vol. 54, no. 9, pp. 4005-4019, Sep. 2008.

[3] Popovski Petar, Simeone Osvaldo, *Wireless Secrecy in Cellular Systems With Infrastructure-Aided Cooperation*, IEEE Transaction on Information Forensics and Security, vol. 4 no. 2, pp. 242-256, Jun. 2009.

[4] I. Krikidis, J. S. Thompson, and S. McLaughlin, *Relay selection for secure cooperative networks with jamming*, IEEE Transaction on Wireless Communications, vol. 51, pp. 5003-5011, Oct. 2009.

[5] L. Dong, Z. Han, A. Petropulu and H. V. Poor, *Improving wireless physical layer security via Cooperative relays*, IEEE Trans. Signal Processing. vol. 58, no. 3, pp. 1875-1888 march. 2010.

[6] J. Zhang and M. Gursoy, *Collaborative relay beamforming for secrecy*, in Proc. the IEEE International Conference on Communications (ICC10), Jun. 2010, pp. 1-5.

[7] R. Zhang, L. Song, Z. Han, and B. Jiao, *Physical layer security for two way relay communications with friendly jammers*, in Proc. IEEE Global Communications Conference, Dec. 2010.

[8] Ding ZG, Leung KK, Goeckel DL, Towsley D, *Opportunistic Relaying for Secrecy Communications: Cooperative Jamming vs. Relay Chatting*, IEEE Transaction on Wireless Communications, vol. 10, no. 6, pp. 1725-1729 Jun. 2011.

[9] S. Boyd and L. Vandenberghe, *Convex Optimization*, Cambridge U.K.: Cambridge Univ. Press, 2004.