SECRECY RATE ANALYSIS FOR JAMMING ASSISTED RELAY COMMUNICATIONS SYSTEMS

†*Jingping Qiao* †*Haixia Zhang* ‡*Dalei Wu* †*Dongfeng Yuan*

†School of Info. Sci. & Eng., Shandong University, Jinan, China
‡Mechatronics Research Lab, Massachusetts Institute of Technology, USA

ABSTRACT

The secrecy rate optimization of wireless communication systems with full-duplex (FD) relays and jamming signals is investigated in this work. Cooperated with FD relays, a novel secrecy transmission mechanism is proposed targeting at creating interference at eavesdroppers by adopting jamming signals. In the proposed mechanism, relays work in FD mode to receive information signals and forward them together with extra jamming signals. The global channel state information (CSI) is assumed available at all transmit nodes. Based on the proposed scheme, the secrecy rate of relay communication system is analyzed. Simulation results are also included to support the theoretical analysis. Results show that the proposed scheme can obviously enhance the secrecy rate of relay communication systems.

Index Terms— Physical layer security, secrecy rate, full-duplex, jamming

1. INTRODUCTION

Security has attracted considerable attention because of the broadcast nature of wireless communications. Traditionally, cryptographic approaches are employed in the upper layers for information security. Due to the ever improving computing ability of users, there are more challenges to design secret keys. This therefore will lead to high risk of information security. As a newly booming technique, physical layer security which makes use of channel conditions to improve secrecy rate can avoid such kind of risk and nowadays is of growing interests. Wyner has proved in [1] that if the wiretap channel was a degraded version of the main channel, the security could be guaranteed and eavesdroppers could learn almost nothing about information from the source. Otherwise, the secrecy rate would be zero. To solve this problem, a large amount of work has focused on node cooperation [2–4], such as amplify-and-forward (AF), cooperative jamming (CJ) and decode-and-forward (DF), and all proved that introducing jamming signals into cooperative systems is an efficient way to degrade the channel conditions of eavesdroppers.

To take advantages of jamming signals, jamming nodes are introduced into DF and AF relay systems [5–7]. Although jamming nodes can further increase secrecy rates of cooperative systems, they can also interfere with relays when they interfere with eavesdroppers. In addition, there is no closed form solution for secrecy rate optimization in such kind of systems. To solve this problem, a smart jamming algorithm has been proposed to schedule the interaction between relays and jamming nodes [8–11]. Moreover, [12–14] proposed a novel self-protection scheme, where destinations transmitted jamming signals to interfere with eavesdroppers and protected itself from being interfered. All the previous work made contributions to enhance the physical layer security, yet few of them payed attention to advantages of jamming signals in full-duplex (FD) relay systems. Inspired by [14], jamming signals can also be introduced into FD relay systems to enhance the system security. This paper offers an extension work of [15]. Here, the jamming scheme in our method is cooperated with FD relays. That is, FD relays can transmit information signals with extra jamming signals. As a result, the channel condition of eavesdropper can be degraded by jamming signals, and the secrecy rate performance can be improved.

Notation: x denotes the transmit signal of the source and z represents the jamming signal. $\mathbf{h}_{ij}^*$ denotes the channel between i node and j node, $i = \{S, R\}$, $j = \{R, D, E\}$. $(\cdot)^\dagger$ denotes the conjugate transpose, $(\cdot)^*$ conjugate, $(\cdot)^T$ transpose. And $\mathcal{CN}(0, \sigma^2)$ represents a circularly symmetric complex Gaussian distribution with zero mean and variance σ^2. And $diag\{\mathbf{w}\}$ denotes the operation to construct a diagonal matrix which elements on the main diagonal are the elements of vector $\mathbf{w}$. $\mathbf{I}_N$ is the identity matrix of size N by N, and $\log(\cdot)$ represents the logarithm base 2.

2. SYSTEM MODEL

We consider a cooperative communication system as shown in Fig. 1, where there are one source node S, one destina-

The work presented in this paper was supported in part by the International Science and Technology Cooperation Program of China (2014DFA11640), the National Natural Science Foundation of China (No. 61371109), the Outstanding Youth Fund of Shandong province with No. JQ201315, and the New Century Excellent Talents from the Ministry of Education of China (NCET-11-0316).

tion node D, one eavesdropper node E and N available relay nodes R, all working in FD mode. The source, destination and eavesdropper nodes are all equipped with single antenna, while the relay nodes are all with two antennas, one transmit antenna and one receive antenna. Through out this work, we assume that all the relays work in FD mode. Let the transmission power of the source node be P_s in Watt and assume that the total transmission power constraint for the whole system is P_0. Therefore, relay nodes will transmit signals with power $P_0 - P_s$. Both the destination and the eavesdropper can receive signals from both the source and relays.

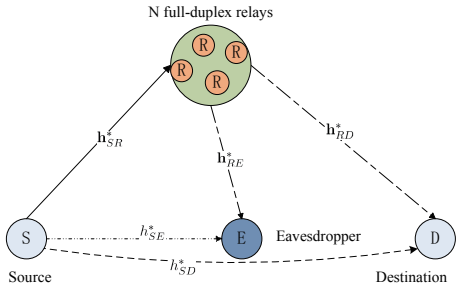

Fig. 1. System model: the eavesdropper is located at somewhere between the source and the destination.

For easy denotation, the power of transmit signal x and jamming signal z are normalized to 1. That is $\mathbb{E}\{|x|^2\} = 1$, $\mathbb{E}\{|z|^2\} = 1$, respectively. Let $\mathbf{h}^*_{SR} \in \mathbb{C}^{N\times 1}$ denote the source-relay channel. It is assumed that each relay can receive signals from itself and other relays. Then the received signal vector at relays can be written as

$$\mathbf{y}'_R = \sqrt{P_s}\mathbf{h}^*_{SR}x + \mathbf{y}_{RR} + \mathbf{n}_R, \tag{1}$$

where $\mathbf{n}_R \in \mathbb{C}^{N\times 1}$ denotes the noise vector at relays, $\mathbf{n}_R \sim \mathcal{CN}(0, \sigma^2\mathbf{I}_N)$. And $\mathbf{y}_{RR}$ represents the received signal vector, which is transmitted from all the relays, $\mathbf{y}_{RR} = [\mathbf{y}_{RR}(1), \ldots, \mathbf{y}_{RR}(k), \ldots, \mathbf{y}_{RR}(N)]^T \in \mathbb{C}^{N\times 1}$, where the parameter $k = 1, 2, \ldots, N$. Since the relay knows its own received signal, $\mathbf{y}_{RR}$ can be cancellated by using interference cancellation algorithm [16]. Thus, the received signal at relays, denoted by $\mathbf{y}_R$, can be written as

$$\begin{aligned}\mathbf{y}_R =& \mathbf{y}'_R - \mathbf{y}_{RR}\\ =& \sqrt{P_s}\mathbf{h}^*_{SR}x + \mathbf{n}_R.\end{aligned} \tag{2}$$

As it is known that the full-duplex relay nodes can retransmit their received signals with very small delay, meaning that the source and relays can almost simultaneously transmit their signals. And the signal transmitted by each relay is the weighted version of the received signal with the jamming signal, i.e., $\mathbf{w}(k)\mathbf{y}_R(k) + \mathbf{w}_J(k)z$. Thus, the signals transmitted by all relays can be denoted as $diag\{\mathbf{w}\}\mathbf{y}_R + \mathbf{w}_J z$, where $\mathbf{w} = [\mathbf{w}(1), \ldots, \mathbf{w}(k), \ldots, \mathbf{w}(N)]^T$ denotes the weight vector at all relays, and $\mathbf{w}_J = [\mathbf{w}_J(1), \ldots, \mathbf{w}_J(k), \ldots, \mathbf{w}_J(N)]^T$ represents the jamming weight vector. Let $\mathbf{h}^*_{Rj_1} \in \mathbb{C}^{N\times 1}$ denote the channel between relays and the j_1 node for transmitting information signals and jamming signals, $j_1 \in \{D, E\}$. Therefore, the destination can receive signals both from the source and all relays. Received signal at the destination can be written as

$$\begin{aligned}y_D =& \sqrt{P_s}h^*_{SD}x + \mathbf{h}^\dagger_{RD}\left(diag\{\mathbf{w}\}\mathbf{y}_R + \mathbf{w}_J z\right) + n_D\\ =& \sqrt{P_s}\mathbf{h}^\dagger_{RD}diag\{\mathbf{h}^*_{SR}\}\mathbf{w}x + \sqrt{P_s}h^*_{SD}x\\ &+ \mathbf{n}^T_R diag\{\mathbf{h}^*_{RD}\}\mathbf{w} + \mathbf{h}^\dagger_{RD}\mathbf{w}_J z + n_D.\end{aligned} \tag{3}$$

Similarly, the version of the received signal at the eavesdropper is

$$\begin{aligned}y_E =& \sqrt{P_s}h^*_{SE}x + \mathbf{h}^\dagger_{RE}\left(diag\{\mathbf{w}\}\mathbf{y}_R + \mathbf{w}_J z\right) + n_E\\ =& \sqrt{P_s}\mathbf{h}^\dagger_{RE}diag\{\mathbf{h}^*_{SR}\}\mathbf{w}x + \sqrt{P_s}h^*_{SE}x\\ &+ \mathbf{n}^T_R diag\{\mathbf{h}^*_{RE}\}\mathbf{w} + \mathbf{h}^\dagger_{RE}\mathbf{w}_J z + n_E,\end{aligned} \tag{4}$$

where $n_D \sim \mathcal{CN}(0, \sigma^2)$ and $n_E \sim \mathcal{CN}(0, \sigma^2)$ represent the additive noise at the destination and eavesdropper, respectively. And according to (3) and (4), the jamming signals interfere with both received signals at the eavesdropper and the destination. If the interference of jamming signals to the eavesdropper is maximized and in the same time the interference to the destination is minimized, the performance of secrecy rate will be optimized.

3. RATE OPTIMIZATION AND SYSTEM DESIGN

In this work, we assume there is only one eavesdropper, and the global channel state information (CSI) is available for all transmitters, including the source node and relay nodes. The definition of the secrecy rate can be denoted as the difference between rate of destination and rate of eavesdropper,

$$R_s = R_D - R_E.$$

From the security point of view, more information received at legitimate receiver is expected, while the less information should be received at the eavesdropper. Thus, the optimal problem to maximize the secrecy rate can be formulated as

$$\arg\max_{\mathbf{w},\mathbf{w}_J} R_s. \tag{5}$$

In the following, this optimal problem for the described model in Fig. 1 will be analyzed. The given total transmit power constraint is P_0, and it is assumed that the power of signal $diag\{\mathbf{w}\}\mathbf{y}_R$ is P_R, i.e., $\mathbf{w}^\dagger\mathbf{T}\mathbf{w} = P_R$, where $\mathbf{T} = P_s diag\{\mathbf{h}^*_{SR}\}diag\{\mathbf{h}_{SR}\} + \sigma^2\mathbf{I}_N$. At receiver sides, including the destination node and the eavesdropper node, in order to simplify the expression of information rate, we define $\mathbf{a} = \sqrt{P_s}diag\{\mathbf{h}_{SR}\}\mathbf{h}_{RD}$. Thus the rate at the destination can be written as

$$R_D = \log\left(1 + \frac{\mathbf{w}^\dagger\mathbf{R}_a\mathbf{w}}{\sigma^2\mathbf{w}^\dagger\mathbf{R}_{RD}\mathbf{w} + \mathbf{w}^\dagger_J\mathbf{h}_{RD}\mathbf{h}^\dagger_{RD}\mathbf{w}_J}\right), \tag{6}$$

where $\mathbf{R}_a = \frac{P_s|h_{SD}|^2}{P_R}\mathbf{T}+\mathbf{a}\mathbf{a}^\dagger$, $\mathbf{R}_{RD} = P_R^{-1}\mathbf{T}+diag\{\mathbf{h}_{RD}\}\cdot diag\{\mathbf{h}_{RD}^*\}$.

Define $\mathbf{b} = \sqrt{P_s}diag\{\mathbf{h}_{SR}\}\mathbf{h}_{RE}$, the rate at the eavesdropper can be represented as

$$R_E = \log\left(1+\frac{\mathbf{w}^\dagger\mathbf{R}_b\mathbf{w}}{\sigma^2\mathbf{w}^\dagger\mathbf{R}_{RE}\mathbf{w}+\mathbf{w}_J^\dagger\mathbf{h}_{RE}\mathbf{h}_{RE}^\dagger\mathbf{w}_J}\right) \quad (7)$$

where $\mathbf{R}_b = \frac{P_s|h_{SE}|^2}{P_R}\mathbf{T}+\mathbf{b}\mathbf{b}^\dagger$, and $\mathbf{R}_{RE} = P_R^{-1}\mathbf{T}+diag\{\mathbf{h}_{RE}\}\cdot diag\{\mathbf{h}_{RE}^*\}$.

Based on (5), the maximization of the secrecy rate is an joint optimization problem of the weight vector $\mathbf{w}_J$ and $\mathbf{w}$, which is very difficult to solve. In order to simplify this problem, we will try to achieve the optimization problem in two steps. Firstly, based on the weight vector $\mathbf{w}_J$, the interference at the eavesdropper can be maximized. The objective function can be described as

$$\arg\max_{\mathbf{w}_J}|\mathbf{w}_J^\dagger\mathbf{h}_{RE}|^2,$$

$$s.t.\begin{cases}\mathbf{w}_J^\dagger\mathbf{h}_{RD}=0\\ \mathbf{w}_J^\dagger\mathbf{w}_J=P_0-P_s-P_R.\end{cases} \quad (8)$$

By solving the above optimization problem, the interference at the destination can be nulled out, and the optimal jamming weight vector can be obtained and written as

$$\mathbf{w}_J = \mu_1\|\mathbf{h}_{RD}\|^2\mathbf{h}_{RE}-\mu_1\mathbf{h}_{RD}^\dagger\mathbf{h}_{RE}\mathbf{h}_{RD}, \quad (9)$$

where $\mu_1 = \sqrt{\frac{P_0-P_s-P_R}{\|\mathbf{h}_{RD}\|^4\|\mathbf{h}_{RE}\|^2-\|\mathbf{h}_{RD}\|^2|\mathbf{h}_{RD}^\dagger\mathbf{h}_{RE}|^2}}$.

Let $Q_J = \mathbf{w}_J^\dagger\mathbf{h}_{RE}\mathbf{h}_{RE}^\dagger\mathbf{w}_J$ represent the interference at the eavesdropper caused by the jamming signals, then the secrecy rate can be rewritten as

$$\begin{aligned}R_s =& \log\left(1+\frac{\mathbf{w}^\dagger\mathbf{R}_a\mathbf{w}}{\sigma^2\mathbf{w}^\dagger\mathbf{R}_{RD}\mathbf{w}}\right)-\\ &\log\left(1+\frac{\mathbf{w}^\dagger\mathbf{R}_b\mathbf{w}}{\sigma^2\mathbf{w}^\dagger\mathbf{R}_{RE}\mathbf{w}+Q_J}\right)\\ =&\log\left(\frac{\mathbf{w}^\dagger\hat{\mathbf{R}}_a\mathbf{w}}{\mathbf{w}^\dagger\mathbf{R}_{RD}\mathbf{w}}\cdot\frac{\mathbf{w}^\dagger\hat{\mathbf{R}}_{RE}\mathbf{w}}{\mathbf{w}^\dagger\hat{\mathbf{R}}_b\mathbf{w}}\right)\end{aligned} \quad (10)$$

where $\hat{\mathbf{R}}_a = \sigma^2\mathbf{R}_{RD}+\mathbf{R}_a$, $\hat{\mathbf{R}}_b = \sigma^2\mathbf{R}_{RE}+\mathbf{R}_b+\frac{Q_J}{P_R}\mathbf{T}$, and $\hat{\mathbf{R}}_{RE} = \mathbf{R}_{RE}+\frac{Q_J}{\sigma^2P_R}\mathbf{T}$. Thus the objective function of the optimization problem of secrecy rate can be simplified as

$$\arg\max_{\mathbf{w}}\frac{\mathbf{w}^\dagger\hat{\mathbf{R}}_{RE}\mathbf{w}}{\mathbf{w}^\dagger\mathbf{R}_{RD}\mathbf{w}}\cdot\frac{\mathbf{w}^\dagger\hat{\mathbf{R}}_a\mathbf{w}}{\mathbf{w}^\dagger\hat{\mathbf{R}}_b\mathbf{w}},$$

$$s.t.\mathbf{w}^\dagger\mathbf{T}\mathbf{w}=P_R. \quad (11)$$

Considering that if $\mathbf{A}\in\mathbb{C}^{n\times n}$ and $\mathbf{B}\in\mathbb{C}^{n\times n}$ are arbitrary n-dimensional diagonal matrix, the sum matrix $\mathbf{A}+\mathbf{B}$ is also diagonal. It is easy to get that $\hat{\mathbf{R}}_{RE}$ and $\mathbf{R}_{RD}$ are both diagonal matrix, therefore the objective function in (11) is a product of two correlated Rayleigh quotients, which is in general intractable [17]. To solve this optimization problem, in this work we propose a sub-optimal solution. As it is known that the maximum value and the minimum value of the ratio $\mathbf{w}^\dagger\hat{\mathbf{R}}_{RE}\mathbf{w}/\mathbf{w}^\dagger\mathbf{R}_{RD}\mathbf{w}$ are corresponding to the maximal eigenvalue $\lambda_{\max}$ and the minimal eigenvalue $\lambda_{\min}$ of the matrix $\mathbf{R}_{RD}^{-1}\hat{\mathbf{R}}_{RE}$, respectively [4]. With this, the lower and upper bounds of the objective function can be written as

$$\lambda_{\min}\frac{\mathbf{w}^\dagger\hat{\mathbf{R}}_a\mathbf{w}}{\mathbf{w}^\dagger\hat{\mathbf{R}}_b\mathbf{w}}\le\frac{\mathbf{w}^\dagger\hat{\mathbf{R}}_{RE}\mathbf{w}}{\mathbf{w}^\dagger\mathbf{R}_{RD}\mathbf{w}}\cdot\frac{\mathbf{w}^\dagger\hat{\mathbf{R}}_a\mathbf{w}}{\mathbf{w}^\dagger\hat{\mathbf{R}}_b\mathbf{w}}\le\lambda_{\max}\frac{\mathbf{w}^\dagger\hat{\mathbf{R}}_a\mathbf{w}}{\mathbf{w}^\dagger\hat{\mathbf{R}}_b\mathbf{w}}. \quad (12)$$

Based on the above derivation, we can get that the weight vector maximizing the lower or upper bounds is

$$\mathbf{w} = \mu_2\mathbf{q}^{unit}, \quad (13)$$

where $\mathbf{q}^{unit}$ is the unit-norm eigenvector of the matrix $\hat{\mathbf{R}}_b^{-1}\hat{\mathbf{R}}_a$ corresponding to its largest eigenvalue. μ_2 can be determined by the power constraint, and is equal to

$$\mu_2 = \sqrt{\frac{P_R}{(\mathbf{q}^{unit})^\dagger\mathbf{T}\mathbf{q}^{unit}}}. \quad (14)$$

With the obtained $\mathbf{w}$, we get the tight rate bounds, as well as the maximized secrecy rate. This scheme has been proved to be sub-optimal and the bounds are also proved to be tight by [5]. These properties keep unchanged for our system with full-duplex relays.

4. NUMERICAL RESULTS

To evaluate the performance of the proposed scheme, we assume that the channel between any two nodes is of line-of-sight transmission, described by $h = d^{-c/2}e^{j\theta}$, d is the distance between two nodes, and c represents the path loss exponent and is set to 3.5, θ denotes the phase offset and follows a uniform distribution in the interval $[0, 2\pi)$. The distance between relay nodes is assumed much smaller than the distance between relays and other nodes. It is also assumed that the path losses between N relays and the source or the destination are almost the same. In this section, the location of source node is always $(0, 0)$, where the unit is meters, and the total transmit power constraint is $P_0 = 10^{-3}$ Watt. All performance results presented in the following are obtained by taking the average over 1000 independent Monte Carlo experiments.

Since locations of nodes in the system are fixed, we assume that the eavesdropper is located between relays and the destination. System performances in terms of the secrecy rate are shown in Fig. 2, from which we can see that increasing the number of relays can improve the secrecy rate. In the lower power regime, the secrecy rate increases rapidly with the source power P_s increase, while when the source power

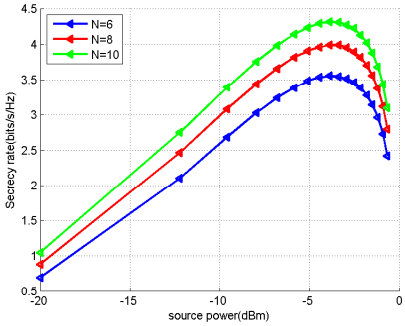

Fig. 2. Secrecy rate versus the source power. The source power varies form -20 dBm to -1 dBm, and relays and the destination are located at $(25, 0)$ and $(50, 0)$, respectively. And the eavesdropper is fixed at $(40, 0)$.

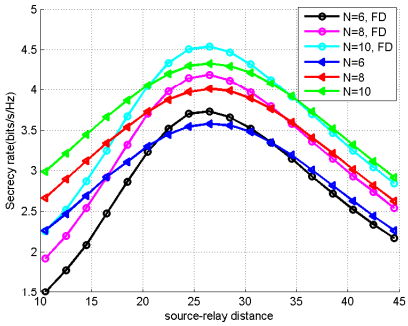

Fig. 3. Secrecy rate versus source-relay distance. The destination is located at $(50, 0)$ and the eavesdropper fixed at $(40, 0)$. The source power is equal to -4 dBm.

is approximately -4 dBm, the secrecy rate reaches its maximum value. However, due to the total power constraint, increasing the source power will result in the power decrease of relays, with the information transmitted by relays decreasing. So it is not beneficial for security if the source power increases continually. Based on the aforementioned experiment, P_s will be set to -4 dBm in the following analysis.

The secrecy rate performance of the FD relay system in [15] and the proposed scheme is displayed in Fig. 3. In the FD relay system described in [15], relays work in FD mode and transmit only information signals. It can be seen as a special case of the proposed scheme, i.e., relays transmit information signals with the total relay power $P_0 - P_s$ and jamming signals with 0 power. The secrecy rate of the FD relay system can be expressed as

$$R_s = \log\left(1 + \frac{\mathbf{w}^\dagger \mathbf{R}_a \mathbf{w}}{\sigma^2 \mathbf{w}^\dagger \mathbf{R}_{RD} \mathbf{w}}\right) - \log\left(1 + \frac{\mathbf{w}^\dagger \mathbf{R}_b \mathbf{w}}{\sigma^2 \mathbf{w}^\dagger \mathbf{R}_{RE} \mathbf{w}}\right).$$

In this work, we compare the secrecy rate of the proposed system with the FD relay system, results are shown in Fig. 3. It can be seen that for the given total power constraint

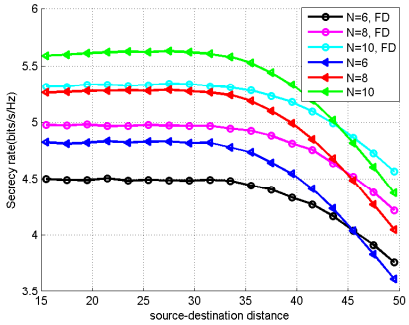

Fig. 4. Secrecy rate versus source-destination distance. The source power is equal to -4 dBm. Relays are fixed at $(25, 0)$. The location of the eavesdropper is $(40, 0)$.

P_0 the proposed scheme achieves better performance than the FD relay system in terms of secrecy rate. Since the FD relay system transmits information signals with higher power than the proposed scheme, its maximal secrecy rate is greater than that of the proposed scheme, which is in agreement with the simulation results shown in Fig. 3.

The secrecy rate performance is also simulated when the source-destination distance varies. Results are included in Fig. 4. For comparison purpose, we also simulate the secrecy rate of the FD relay system. With the help of relays, the secrecy rate of two schemes is almost stable when the destination is located between the source and relays. From the simulation results, we can also see that secrecy rates decrease when the destination moves far away from both the source and relays. Obviously, the secrecy rate of the proposed scheme is much better than that of the simple FD relay system when the destination is close to the source. On the contrary, since they have the same total power constraint, relays in the FD relay system transmit information signals with much more power than that in the proposed scheme. This therefore will lead to better secrecy rate. That is also why the FD relay system performs better than the proposed scheme in the condition that the destination is far away from the source node.

5. CONCLUSION

In this work, by introducing the jamming signals, we proposed a novel transmission mechanism to improve the secrecy rate performance of relay communication systems. With the proposed scheme, secrecy systems can benefit from both the FD relays and jamming signals and thus are of better performance. Theoretical analysis and simulation results have shown that the proposed scheme performs better than the FD relay system when the destination is not much far away from the source or the relays are close to the source. Due to the better performance brought by the jamming signals, it will be widely used in the future studies for secrecy communication.

6. REFERENCES

[1] A. D. Wyner, "The wire-tap channel," *Bell. Syst. Tech. J.*, vol. 54, pp. 1355–1387, October 1975.

[2] L. Dong, Z. Han, A. P. Petropulu, and H. V. Poor, "Secure wireless communications via cooperation," in *in 46th Annual Allerton Conference on Communication, Control, and Computing*. IEEE, 2008.

[3] L. Dong, Z. Han, A. P. Petropulu, and H. V. Poor, "Cooperative jamming for wireless physical layer security," in *IEEE Workshop on Statistical Signal Processing*. IEEE, 2009.

[4] L. Dong, Z. Han, A. P. Petropulu, and H. V. Poor, "Improving wireless physical layer security via cooperating relays," *IEEE Trans. Signal Process.*, vol. 58, pp. 1875–1888, March 2010.

[5] S. Huang, J. Wei, Y. Cao, and C. Liu, "Joint decode-and-forward and cooperative jamming for secure wireless communications," in *Wireless Communications, Networking and Mobile Computing (WiCOM), 7th International Conference on*. IEEE, 2011.

[6] I. Krikids, J. S. Thompson, and S. McLaughlin, "Relay selection for secure cooperative networks with jamming," *IEEE Trans. Wireless Communications*, vol. 8, pp. 5003–5011, October 2009.

[7] G. Zheng, J. Li, K. Wong, and A. P. Petropulu, "Using simple relays to improved physical layer security," in *1th IEEE International Conference on Communication in China*. IEEE, 2012.

[8] B. Han, J. Li, and J. Su, "Secrecy capacity optimization via cooperative relaying and jamming for wanets," *IEEE Trans. Parallel Distributed Systems*, 2014.

[9] J. Chen, R. Zhang, L. Song, Z. Han, and B. Jiao, "Joint relay and jammer selection for secure two-way relay networks," *IEEE Trans. Information Forensics and Security*, vol. 7, pp. 310–320, February 2012.

[10] T. Wang and G. B. Giannakis, "Mutual information jammer-relay games," *IEEE Trans. Information Forensics and Security*, vol. 3, pp. 290–303, June 2008.

[11] J. Huang and A.L. Swindlehurst, "Cooperative jamming for secure communications in mimo relay networks," *IEEE Trans. Signal Processing*, vol. 59, pp. 4871–4884, October 2011.

[12] Y. Liu, J. Li, and A. P. Petropulu, "Destination assisted cooperative jamming for wireless physical-layer security," *IEEE Trans. Information Forensics and Security*, vol. 8, pp. 682–694, April 2013.

[13] S. Luo, J. Li, and A. P. Petropulu, "Uncoordinated cooperative jamming for secret communications," *IEEE Trans. Information Forensics and Security*, vol. 8, pp. 1081–1090, July 2013.

[14] G. Zheng, I. Krikidis, J. Li, A. P. Petropulu, and B. Ottersten, "Improving physical layer secrecy using full-duplex jamming receivers," *IEEE Trans. Signal Processing*, vol. 61, pp. 4962–4974, October 2013.

[15] I. Krikidis, H. A. Suraweera, and C. Yuen, "Amplify-and-forward with full-duplex relay selection," in *Communications (ICC), 2012 IEEE International Conference on*. IEEE, 2012.

[16] W. Li, M. Ghogho, B. Chen, and C. Xiong, "Secure communication via sending artificial noise by the receiver: outage secrecy capacity/region analysis," *IEEE Communications Letters*, vol. 16, pp. 1628–1631, October 2012.

[17] L. Dong, Z. Han, A. P. Petropulu, and H. V. Poor, "Amplify-and-forward based cooperation for secure wireless communications," in *Acoustics, Speech and Signal Processing, 2009. ICASSP 2009. IEEE International Conference on*. IEEE, 2009.