A Two-Hop Multi-Relay Secure Transmission with Improved Suboptimal Relay Selection Scheme

Lukman A. Olawoyin[1], Munzali A. Abana[2], Yue Wu[1], and Hongwen Yang[1]
[1] Wireless Communication Center, Beijing University of Posts and Telecommunications, Beijing, 100876, China
[2]Key Laboratory of Wireless Commun. Beijing University of Posts and Telecommunications, Beijing, 100876, China
Email: {lolawoyin, wuyue, yanghong}@bupt.edu.cn; munzal21@gmail.com

Abstract —This work studies the use of relay selection in reducing the capability of a hidden eavesdropper to intercept the confidential message transmitted between information source and legitimate receiver. Specifically, an improved version of the suboptimal selection with jamming scheme (SSJ) is proposed. To achieve a secure transmission system, we propose the choice of best relay node that will forward the confidential message only when the link quality of the selected relay terminal meets some predefined thresholds and the signal is transmitted with low power. The simulation results show that our proposed scheme can significantly improve the system performance in term of average secrecy throughput and intercept probability.

Index Terms—Artificial noise, best and worst relay, channel state information, secrecy throughput, intercept probability

I. Introduction

Due to the inherent nature of wireless medium, openness and broadcast, all users within the coverage area will have equal opportunities to overhear the transmitting messages. Privacy and nonrepudiation of transmitted signal against unlawful access by an unauthorized user have become two important issues, which had received enormous attentions in recent years. The information transmitted over the wireless medium is prone to attack and signal interception from malicious users [1]. Conventionally, cryptography approach is used to address the security challenges at the upper layer of the protocol stack. However, due to difficulties and vulnerabilities associated with secret key distribution and complex algorithm involved in the key distribution and management, cryptography method cannot provide perfect secrecy in wireless networks [2]. Recently, the uses of coding and signal processing techniques were explored as new paradigm to ensure information secrecy at the physical layer since these approaches do not require the exchange of secret keys. The notion of perfect secrecy was first introduced by Shannon [3] and later extended to Gaussian wire-tap channel by Wyner [4], which introduced the notion of secrecy capacity. Secrecy capacity is defined as the rate at which transmitter can reliably communicate a secret message with legitimate receiver without eavesdropper being able to decode the message. Wyner also proved that reliable data transmission at non-zero rate can be achieved provided that the capacity of main channel is larger than the capacity of eavesdropper's channel. Recently, there has been an increased interest about the physical layer security for various wireless systems and various techniques have been proposed to enhance the security [5]-[22].

The authors in [5] examined the secrecy capacity of Gaussian wiretap channel aided by cooperative jammer while [6] discussed the physical-layer secrecy for OFDM transmission over fading channels. The application of artificial noise (AN) was presented by [7]-[8], where the AN was projected towards the null space of the main channel. In their work, it was shown that positive secrecy is achievable in broadcast wireless system even if the eavesdropper has zero noise power at it received terminal. Aggarwal *et al.* in [9] proposed the friendly jammer technique. They showed that the performance of incorporating friendly noise is better than the traditional cooperative jamming technique. The use of joint cooperative techniques to ensure information secrecy in cognitive system was discussed in [10] while the authors in [11], [12] discussed the cooperative relaying and power allocation in wireless networks, respectively.

Cooperative Communication (CC) and artificial noise (AN) have been adjudged as the best techniques to ensure information secrecy in wireless networks. In CC technique, external relay nodes are employed to enhance information secrecy either by forwarding the information signal to the main channel so as to enhance its channel quality [13] or by relaying the AN to eavesdropper channel in order to reduce its channel capacity [14]. The application of beamforming (BF) and precoding were proposed in [15], [16]. Long *et al.* in [15] showed that distributed precoding through multiple relay nodes can be used to enhance the received signal power at the destination and to mitigate the signal leakage to eavesdropper. Qiang *et al.* in [16] introduced robust cooperation between BF and AN where multiple multi-antenna relays collaboratively amplify-and-forward (AF) the information signal from a single antenna source to a single receiver in the presence of multiple eavesdroppers.

The concept of relay selection in secrecy enhancement was discussed in [17]-[20]. Krikidis I *et al.* in [17] proposed the use of three main relay selection techniques

Manuscript received February 19, 2016; revised June 22, 2016.
Corresponding author email: lolawoyin@bupt.edu.cn.
doi:10.12720/jcm.11.6.592-597

which are conventional selection (CS), optimal selection (OS) and suboptimal selection (SS). In their work, the best relay is used to forward information signal while the worst relay is used to forward AN. Application of relay nodes in two-phase communication system was introduced by [18] which proposed the use of three relays over the information transmission which consists of two-phase dual-hop communication. In the first phase, one relay is used to broadcast AN and during the second phase, the other two relays are used in such a way that one of the relays will operate as a conventional relay to help improve the main receiver channel by using decode-forward protocol (DF), and the other relay behaves as jammer to confuse the eavesdropper. The relay selection for secure backscatter wireless communication was discussed in [19]. In [20], the secrecy performance under different diversity techniques were considered. The relay selection for dual-hop networks under security constraints with multiple eavesdroppers was presented in [21] where the authors considered the reduction in overheard information at eavesdropper by choosing the relay having lowest instantaneous signal-to-noise ratio (SNR) to them. In [22], the authors analyzed the tradeoff between the security and reliability in the presence of eavesdropper. They characterized the Security-Reliability Trade off (SRT) of conventional direct transmission from source to the main receiver in the presence of eavesdropper. In general, the use of relay selection in association with AN and BF techniques employed the application of principle of orthogonality, the AN signal is transmitted in all direction but towards the range space of the main receiver while the information signal is beamformed toward the main channel. By doing so, this will prevent the main receiver from receiving the AN, hence will improve the overall system secrecy.

In this work, using SSJ (Suboptimal Selection with Jamming) scheme as a bench mark as presented in [17], we propose an improvement to this technique (ISSJ). We employ the use of relay node that will forward the confidential message only when the link quality of the selected relay node meets some predefined thresholds and then the signal is transmitted with low power. The simulation results show that our proposed scheme can significantly improve the secrecy throughput and intercept probability.

The remaining part of this work is organized as follows. In Section II, the system model is presented while the proposed scheme is discussed in Section III. The simulation results to validate our proposed scheme are presented in Section IV while the paper is concluded in Section V.

II. System Model

Consider a two-hop wireless system model as shown in Fig. 1. Alice has both confidential and non-confidential messages to be communicated to Bob via multiple half-duplex relay nodes while a passive eavesdropper, Eve, is hidden near Bob overhearing the transmitted message. Assume there is no direct link between Alice and Bob/Eve, i.e. neither Bob nor Eve is within the coverage area of Alice. Each node in Fig. 1, is equipped with single antenna. The complex channel gain of the link between Alice to the i-th relay node is denoted by $h_{\mathrm{a},i}=\sqrt{g_{\mathrm{a},i}}\mathrm{e}^{\mathrm{j}\varphi_{\mathrm{a},i}}$, $i=1,2,...,M$ where $g_{\mathrm{a},i}=\left|h_{\mathrm{a},i}\right|^2$ and $\varphi_{\mathrm{a},i}=\angle h_{\mathrm{a},i}$ is, respectively, the power gain and the phase shift of the channel. Similarly, the complex channel gain of the link between the i-th relay node to Bob is denoted by $h_{\mathrm{b},i}=\sqrt{g_{\mathrm{b},i}}\mathrm{e}^{\mathrm{j}\varphi_{\mathrm{b},i}}$, and the channel between the i-th relay node to Eve is denoted by $h_{\mathrm{e},i}=\sqrt{g_{\mathrm{e},i}}\mathrm{e}^{\mathrm{j}\varphi_{\mathrm{e},i}}$. Assuming that $\mathrm{g}_{\mathrm{x},i}$ for all $i=1,2,...,M$, $\mathrm{x}\in\{\mathrm{a},\mathrm{b},\mathrm{e}\}$ are independently and identically distributed (i.i.d.) and are normalized such that $\mathbb{E}\left[g_{\mathrm{x},i}\right]=1$, and the channel is reciprocal and symmetrical, i.e. $g_{\mathrm{x},i}=g_{i,\mathrm{x}}$.

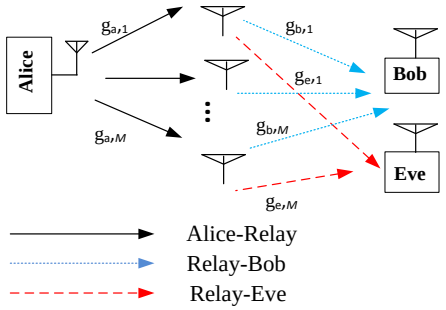


Fig. 1. The system model for two-hop multirelay DF transmission

Alice sends its message with a capacity achieving code of rate R and with power $P_{\max}$. As the capacity achieving code, the signal transmitted by Alice, x is a complex Gaussian variable with zero mean and unit variance $CN(0,1)$. The signal received by the i-th relay node is given by

$$y_i=\sqrt{P_{\max}}h_{a,i}x+n_i \tag{1}$$

where n_i, $i=1,2,\cdots,M$ are i.i.d. complex Gaussian noise with zero mean and variance σ^2. From Shannon's coding theorem, the i-th relay node can only decode the codeword unless its capacity is greater than or equal to the code rate, i.e.

$$R\le\log_2\left(1+\bar{\gamma}\mathrm{g}_{\mathrm{a},i}\right) \tag{2}$$

where $\bar{\gamma}=P_{\max}/\sigma^2$. This is also true for Bob and Eve when they are decoding the relayed signals from the chosen relay terminal. Note that the unit of R is bits per code symbol, so there is no need for the 1/2 coefficient to account for the two-phase half-duplex transmission.

Prior to the message transmission phases is the training period when the nodes estimate the channel coefficients. The channel estimation is based on the training sequences

broadcasted by Alice and Bob. Based on these training sequences, the i-th relay node can estimate $h_{a,i}$ and $h_{b,i}$. Then the relay nodes broadcast $g_{a,i}$ and $g_{b,i}$ over a dedicated control channel such that the Channel State Information (CSI) of all $g_{a,i}$ and $g_{b,i}$ are shared by all nodes, but the complex channel gains $h_{a,i}$ and $h_{b,i}$ are locally known to the i-th relay. Under the operations described above, Eve will have no CSI about the link from any of the relay nodes. This implies that Eve cannot increase its capability by using multiple antennas since typical multi-antenna receiving techniques (such as beamforming) rely on the CSI of each antenna branch, especially on the information of channel phase.

III. Proposed Scheme

In order to achieve information secrecy by protecting the confidential codeword from being decoded by Eve in a multi-relay system, several methods have been proposed in literature [17]. Among them, the most simple and practical one might be the SSJ proposed since it does not require the instantaneous CSI about Eve nor the cooperation between relay nodes. In SSJ, the relay node with best channel quality is selected among the relays as the forwarding node, also another relay with worst channel quality is chosen as the jamming node. Let f and j denote, respectively, the index of forwarding and jamming relay node. The f and j are chosen as

$$f = \arg\max_{i\in\{1,2,\ldots,M\}} \{g_{b,i}\} \tag{3}$$

$$j = \arg\min_{i\in\{1,2,\ldots,M\}} \{g_{b,i}\} \tag{4}$$

and then the f-th relay node will forward the decoded signal x and the j-th relay node will broadcast a jamming signal or artificial noise.

However, the secrecy performance of SSJ is relatively poorer compared with the other schemes which rely on the CSI of Eve (see Fig. 3, Fig. 4 of [17] for example). So in this paper, an improved version of SSJ, namely ISSJ (Improved SSJ), is proposed.

In ISSJ, the forwarding node and the jamming node are selected using (3) and (4), respectively. However, Alice will send confidential messages only under the condition:

$$g_{b,f} > \max\left\{\gamma_{th} g_{b,j}, g_{a,f}\left(g_{b,j}\bar{\gamma}+1\right)\right\} \tag{5}$$

and with code rate given by

$$R = \log_2\left(1+\bar{\gamma} g_{a,f}\right) \tag{6}$$

The transmit power of jamming node is P_{max}. The transmit power of forwarding node is given by

$$P_f = P_{max}\cdot\frac{g_{a,f}}{g_{b,f}}\left(1+\bar{\gamma} g_{b,j}\right) \tag{7}$$

The proposed scheme can be summarized as follows:

1) Based on the CSI, the "forwarding" and "jamming" nodes are selected according to (3) and (4).
2) If condition (5) is met, then during the first data transmission phase, Alice transmit confidential message with code rate given by (6).
3) During the second phase, node f will forward the message with power given by (7) and node j will broadcast AN with full power.

The signals received by forwarding relay node, Bob and Eve are given by

$$y_f = \sqrt{P_{max}} h_{a,f} x + n_f \tag{8}$$

$$y_b = \sqrt{P_f} h_{b,f} x + \sqrt{P_{max}} h_{b,j} w + n_b \tag{9}$$

$$y_e = \sqrt{P_f} h_{e,f} x + \sqrt{P_{max}} h_{e,j} w + n_e \tag{10}$$

where n_f, n_b and n_e are respectively, the noise at forwarding node, Bob and Eve, w is the artificial noise sent by jamming node. n_f, n_b, n_e and w are independent zero mean complex Gaussian variables. The variance of n_f, n_b, n_e is σ^2 while the variance of w is assumed to be 1.

The channel capacities of the links between forwarding node and Bob, forwarding node and Eve can be expressed as

$$C_b = \log_2\left(1+\frac{P_f}{P_{max}}\cdot\frac{g_{b,f}}{1/\bar{\gamma}+g_{b,j}}\right) = R \tag{11}$$

$$C_e = \log_2\left(1+\frac{P_f}{P_{max}}\cdot\frac{g_{e,f}}{1/\bar{\gamma}+g_{e,j}}\right) \tag{12}$$

Eve can decode the codeword of Alice only if $C_e > C_b$, or

$$\frac{g_{e,f}}{1/\bar{\gamma}+g_{e,j}} \geq \frac{g_{b,f}}{1/\bar{\gamma}+g_{b,j}} \tag{13}$$

Assume that $g_{a,i}, g_{b,i}$ for $i = 1,2,\ldots,M$ are i.i.d. random variables. From (3) and (4), $g_{b,f} = \max_i\{g_{b,i}\}$, $g_{b,j} = \min_i\{g_{b,i}\}$. So we have

$$\mathbb{E}[g_{b,f}] \geq \mathbb{E}[g_{e,j}] = \mathbb{E}[g_{e,f}] \geq \mathbb{E}[g_{b,j}] \tag{14}$$

Let X and Y denote, respectively, the left hand side (LHS) and the right hand side (RHS) of (13). Under the condition of (5), X would have much less chance being larger than Y, especially when γ_{th} is large. Hence the proposed scheme can guarantee a positive secure throughput for arbitrary distribution of $g_{x,i}, x\in\{b,e\}, i = 1,2,\ldots,M$.

For the confidential message transmission, the average throughput at Bob and Eve can be expressed as

$$\begin{aligned}\bar{R}_{\mathrm{b}} &= \mathbb{E}[R] \\ \bar{R}_{\mathrm{e}} &= \mathbb{E}[R \cdot I_{C_{\mathrm{e}} \geq C_{\mathrm{b}}}]\end{aligned} \tag{15}$$

where $I_{C_{\mathrm{e}} \geq C_{\mathrm{b}}} \in \{0,1\}$ is an indicator function where $I_{C_{\mathrm{e}} \geq C_{\mathrm{b}}}$ is 1 if $C_e \geq C_b$ and is 0 otherwise.

The secrecy throughput is defined as

$$\bar{R}_{\mathrm{s}} = \bar{R}_{\mathrm{b}} - \bar{R}_{\mathrm{e}} = \mathbb{E}[R \cdot I_{C_{\mathrm{e}} < C_{\mathrm{b}}}] \tag{16}$$

where $I_{C_{\mathrm{e}} < C_{\mathrm{b}}} = 1 - I_{C_{\mathrm{e}} \geq C_{\mathrm{b}}}$.

The interception probability [23] that the confidential message of Alice being intercepted by Eve is given by

$$P_{\text{intercept}} = \Pr\{C_{\mathrm{e}} \geq R\} \tag{17}$$

IV. Simulation Results

Consider Rayleigh fading channel where the power gains $g_{\mathrm{x},i}$, $\mathrm{x} \in \{\mathrm{b},\mathrm{e}\}$, $i = 1,2,\ldots,M$ are i.i.d randomly variables with exponential probability distributions as

$$p(g) = \begin{cases} \mathrm{e}^{-g}, & g \geq 0 \\ 0, & g < 0 \end{cases} \tag{18}$$

Fig. 2 shows an example of the probability density of X and Y which is, respectively, the LHS and RHS of (13). Since X and Y represent the channel quality of the main link and the eavesdropper channel, from the figure it can be seen that the proposed scheme can significantly improve the main channel quality and degrade the wiretap channel.

The secrecy performance in terms of average secrecy throughput as defined in (16) and the intercept probability as defined in (17) are shown in Fig. 3–Fig. 4 where the threshold is set as $\gamma_{\mathrm{th}} = \bar{\gamma}$.

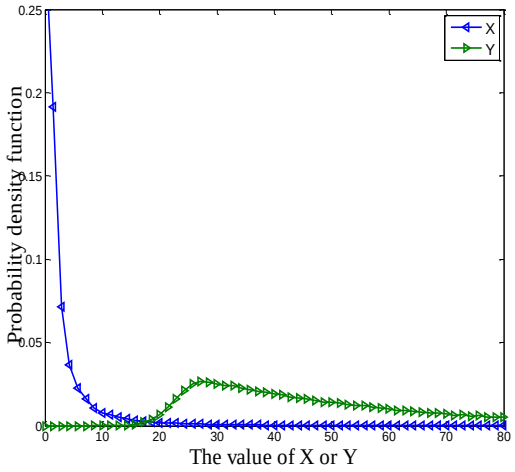
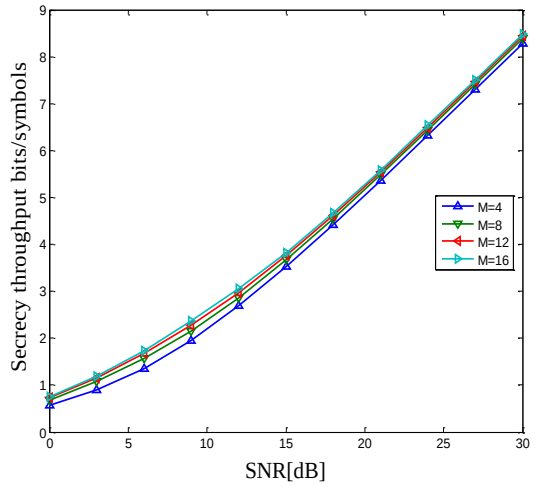
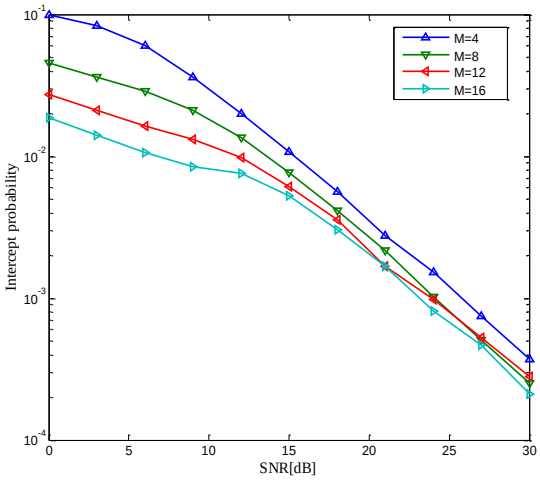


Fig. 2. The probability density of X and Y. $M = 8$, $\gamma_{\mathrm{th}} = \bar{\gamma}$ =15dB

Fig. 3 shows the secrecy performance versus SNR, $\bar{\gamma} = P_{\max}/\sigma^2$. It can be observed that the secrecy throughput is marginally improved as the SNR increases while intercept probability decreases considerably as SNR increases.



(a) Secrecy throughput



(b) Intercept probability

Fig. 3. The secrecy performance versus $\bar{\gamma} = P_{\max}/\sigma^2$. $\gamma_{\mathrm{th}} = \bar{\gamma}$.

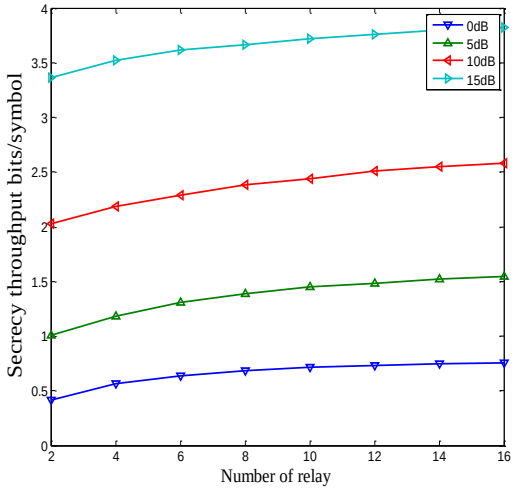
It is worth noting that under condition (5), the code rate R defined in (6) and the average throughput $\mathbb{E}[R]$ increase with SNR monotonically. On the other hand, by substituting (5) and $\gamma_{\mathrm{th}} = \bar{\gamma}$ into (13), we can see that the RHS (i.e. Y) is lower bounded by

$$\begin{aligned} Y &= \frac{g_{\mathrm{b},f}}{1/\bar{\gamma} + g_{\mathrm{b},j}} \geq \frac{\bar{\gamma}}{\left(\bar{\gamma} g_{\mathrm{b},j}\right)^{-1} + 1} \\ &= \bar{\gamma} - \frac{1}{g_{\mathrm{b},j}} + \frac{1}{\bar{\gamma} g_{\mathrm{b},j}^2} - \frac{1}{\left(\bar{\gamma}\right)^2 g_{\mathrm{b},j}^3} \cdots \end{aligned} \tag{19}$$

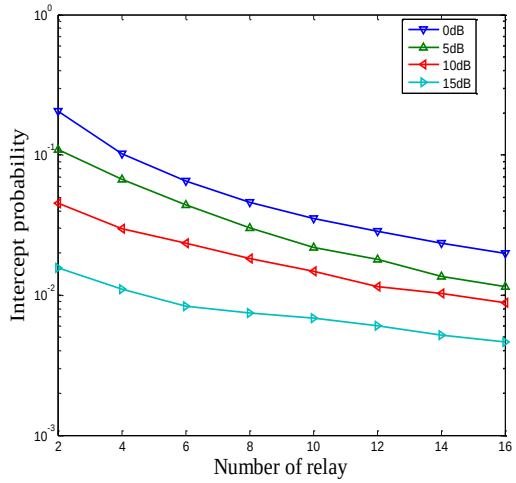
which is approximately equal to $\bar{\gamma}$. However, the LHS (i.e. X) of (13) increase slowly with $\bar{\gamma}$. Therefore, the probability of $X \geq Y$, i.e. the intercept probability $\Pr\{I_{C_{\mathrm{e}} \geq C_{\mathrm{b}}} = 1\}$, will decrease as the increase of SNR. Consequently, the secrecy throughput (16) will increase monotonically with SNR.

Fig. 4 shows the secrecy performance as a function of M, the number of relays. For fixed $\bar{\gamma}$ and $\gamma_{\mathrm{th}} = \bar{\gamma}$, the average throughput $\mathbb{E}[R]$ does not depend on M since R is completely determined by $g_{\mathrm{a},f}$. However, increasing M

has effect on the distribution of $g_{\mathrm{b},f}$ and $g_{\mathrm{b},j}$. As M increases, $\mathbb{E}[g_{\mathrm{b},f}]$ increases while $\mathbb{E}[g_{\mathrm{b},j}]$ decreases, leading to the increases of the RHS of (13). This is the reason that secrecy performance increases with the increase of M. However, by comparing Fig. 4 with Fig. 3 we can see that the secrecy performance is less sensitive to the number of relays.



(a) Secrecy throughput



(b) Intercept probability

Fig. 4. The secrecy performance versus M. $\gamma_{\mathrm{th}} = \overline{\gamma}$.

V. Conclusions

In this paper, we proposed an improved scheme for the secure transmission of confidential messages via two-hop half-duplex multi-relay system. It can be observed that by setting the condition for transmitting confidential message properly, the difference of the link quality of the main channel and of the eavesdropper channel can be made to sufficiently large and hence leading to a significant enhancement in wireless system security.

References

[1] Y. W. P. Hong, P. C. Lan, and C. C. J. Kuo, "Signal processing approaches to secure physical layer communications in multi-antenna wireless systems," *Springer Science & Business Media*. 2013.

[2] M. Nivetha and M. S. Sivaramakrishnan, "A comparative analysis of cryptography algorithms," *Wireless Commun*., vol. 6, no. 8, pp. 304-307, 2014.

[3] C. E. Shannon, "Communication theory of secrecy systems*," *Bell System Technical Journal*, vol. 28, no. 4, pp. 656-715, Oct. 1949.

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

[5] L. Lingxiang, C. Zhi, and F. Jun, "On secrecy capacity of gaussian wiretap channel aided by a cooperative jammer," *IEEE Sig. Process. Lett*., vol. 21, no. 11, pp. 1356-1360, Nov. 2014.

[6] F. Renna, N. Laurenti, and H. V. Poor, "Physical-Layer secrecy for OFDM transmissions over fading channels," *IEEE Trans. Inform. Foren. and Sec.*, vol. 7, no. 4, pp. 1354-1367, Aug. 2012.

[7] S. Goel and R. Negi, "Guaranteeing secrecy using artificial noise," *IEEE Trans. Wirel. Commun*., vol. 7, no. 6 pp. 2180-2189, Jun. 2008.

[8] R. Negi and S. Goel, "Secret communication using artificial noise," in *Proc. 62nd IEEE Conf. Vehic. Techn. VTC-Fall*, 2005.

[9] P. Aggarwal and A. Trivedi, "An approach for secure wireless communication using friendly noise," in *Proc. Interna. Conf. Advan. Comput., Commun. and Inform*, New Delhi, India, 2014. pp. 1578-1584

[10] W. Liu, L. guo, T. Kang, J. Zhang, and J. Lin, "Secure cognitive radio system with cooperative secondary networks," in *Proc. 22nd Internat. Conf. Telecommun*, Sydney, 2015, pp. 6-10

[11] L. Wang, X. Zhang, X. Ma, and M. Song, "Joint cooperative relaying and jamming for maximum secrecy capacity in wireless networks," in *Proc. Interna. Conf. Commun.*, Sydney, 2014, pp. 4448-4453.

[12] H. Long, W. Xiang, Y. Zhang, Y. Liu, and W. Wang, "Cooperative jamming and power allocation in three-phase two-way relaying wiretap systems," in *Proc. IEEE Wirel. Commun. and Network. Conf.*, 2013.

[13] X. Tang, R. Liu, P. Spasojevic, and H. V. Poor, "Interference assisted secret communication," *IEEE Trans. Inform. Theo*., vol. 57, no. 5, pp. 3153-3167, May 2011.

[14] W. Li, M. Ghogho, B. Chen, and C. Xiong, "Secure communication via sending artificial noise by the receiver: Outage secrecy capacity/region analysis," *IEEE Commun. Lett*., vol. 16, no. 10, pp. 1628-1631, Oct. 2012.

[15] H. Long, W. Xiang, Y. Zhang, Y. Liu, and W. Wang, "Secrecy capacity enhancement with distributed precoding in multirelay wiretap systems," *IEEE Trans. Inform. Foren. and Sec*. vol. 8 no. 1, pp. 229-238, Jan. 2013.

[16] L. Qiang, Y. Yang, W. K. Ma, M. Lin, J. Ge, and J. Lin, "Robust cooperative beamforming and artificial noise design for physical-layer secrecy in AF multi-antenna multi-relay networks," *IEEE Trans. Sig. Process*, vol. 63, no. 1, pp. 206-220, Oct. 2015.

[17] I. Krikidis, J. S. Thompson, and S. McLaughlin, "Relay selection for secure cooperative networks with jamming,"

IEEE Trans. Wirel. Commun., vol. 8, no. 10, pp. 5003-5011, Oct. 2009.
[18] D. H. Ibrahim, E. S. Hassan, and S. A. El-Dolil, "A new relay and jammer selection schemes for secure one-way cooperative networks," *Wirel. Pers. Commun.*, vol. 75, no. 1, pp. 665-658, Aug. 2013.
[19] W. Xiaowei, S. Zhou, and W. Guangyi, "Relay selection for secure backscatter wireless communications," *Electro. Lett*., vol. 51, no. 2, pp. 9851-952, Nov. 2015.
[20] F. S. Al-Qahtani, C. Zhong, and H. Alnuweiri, "Opportunistic relay selection for secrecy enhancement in cooperative networks," *IEEE Trans. Commun.*, vol. 63, no. 5, pp. 1756-1770, May 2015.
[21] V. N. Quoc, B. N. Linh-Trung, and M. Debbah, "Relay selection schemes for dual-hop networks under security constraints with multiple eavesdroppers," *IEEE Trans. Wirel. Commun*., vol. 12, no. 12, pp. 6076-6085, Dec. 2013.
[22] Z. Jia, Z. Yulong, C. Benoit, Z. Wei-Ping, and H. Lajos, "Security versus reliability analysis of opportunistic relaying," *IEEE Trans. Vehic. Tech.*, vol. 63, no. 6, pp. 2653-2661, Jul. 2014.
[23] Z. Yulong, Z. Jai, X. Wang, and V. C. M. Leung, "Improving physical-layer security in wireless communications using diversity techniques," *IEEE Network*, vol. 29, no. 1, pp. 42-48, Feb. 2015.

Lukman A Olawoyin received the B.Eng. degree in Electrical and Electronic Engineering from Federal University of Technology, Akure (FUTA), Nigeria in 2003 and M.Sc. degree in Modern Digital Communication Systems (MDCS) from University of Sussex, United Kingdom in 2010.
He is currently pursuing the Ph.D. degree with the Wireless Communication Center, School of Information and Communication Engineering, Beijing University of Posts and Telecommunications, Beijing, China. His research interests include Physical Layer security, signal processing, MIMO and information theory.

Munzali A. Abana received his B.Eng. degree in Electrical & Electronics Engineering from University of Maiduguri, Nigeria in 2006 and MSc. in Network Communications from Loughborough University UK, in 2010.
He is currently pursuing his Ph.D. in the Key Laboratory of Universal Wireless Communications (Ministry of Education) at the Beijing University of Post and Telecommunications (BUPT) China. His research interest includes, Heterogeneous networks, cloud computing based radio access networks, D2D Communications and the applications of stochastic geometry in wireless communications.

Yue Wu is currently a Ph.D. candidate at Beijing University of Posts and Telecommunications. He obtained MSc degree in wireless communication from Chongqing University of Posts and Telecommunication in 2010.
His research interest includes HARQ technology and signal processing in wireless communication system

Hongwen Yang was born in 1964. Prof. Yang is currently the director of the wireless communication center in the school of Information and Communication Engineering, Beijing University of Posts and Telecommunications (BUPT).
His research interest is on wireless aspect of physical layer such as modulation, channel coding, security, signal processing, CDMA, MIMO, OFDM, etc. and information theory.