Study on Physical Layer Security Performance of Wireless Relay Communication System Based on PLNC

Yang Baofeng[1,a], Zhu Youfan[1], Gao Yuanyuan[1] and Zhang Xiaobing[2]

[1]Institution of Communications Engineering, PLA University of Science and Technology, Nanjing, 210007, China

[2] Nanjing University of Science and Technology, Nanjing, 210001, China

[a]770809@126.com

Keywords: Physical Layer Security; Network Coding; Security Capacity; Wireless Relay Communication System.

Abstract. Due to the broadcast nature of wireless communications, security performance of conventional wireless relay communication system is difficult to be guaranteed. In this paper, security performance of the wireless relay communication system based on physical layer network coding (PLNC) is studied. The theoretical analyses and simulations show that the physical layer security performance of wireless relay communication system can be improved effectively by using PLNC technique.

Introduction

Wireless relay communication system can reduce costs, expand the coverage of communications, and increase the transmission rate of the mobile communication systems with relay technology. However, due to the broadcast nature and openness of electromagnetic signals, the enemy's passive eavesdropping becomes a major threat to the security of the wireless relay communication system.

In 1975, Wyner[1] proposed the basic model of physical layer security - tapping channel model, and proved that when capacity of tapping channel was inferior to capacity of the main channel, any eavesdropper could not obtain the information. At this time, the rate of information between the source and the destination was defined as security information rate, and the maximum rate of security information rate is called security capacity (Cs). When information rate was not greater than Cs, communication security could be guaranteed and any eavesdropper could not get any useful information from the received message.

In 2006, Zhang Shengli creatively put forward PLNC technology [2]. The traditional relay system aimed to avoid interference with each other, and it required four slots. NC(Network layer) Network Coding was proposed to reduce 4 slots to 3 slots required by a two-way communication. PLNC was proposed to solve the problem of signal interference, which reduced 3 slots to 2 slots by using a two-way communication. This method was applied to make the eavesdropper subject to interference, so that interference of eavesdropper was much greater than that of receiver, then improving the security performance of physical layer.

Based on Wyner's eavesdropping channel model, this paper studies security performance of wireless relay communication system based on physical layer network coding when the wiretap channel information is unknown.

The Security performance of Wireless Relay Communication System

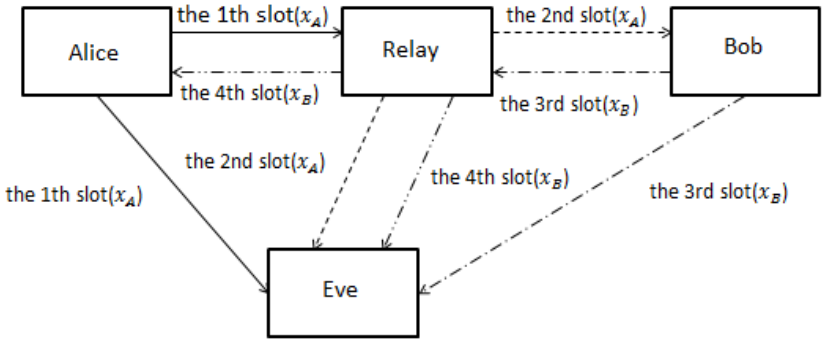


Fig.1 Traditional relay transmission mechanism with eavesdropper

We suppose the wireless relay communication system has three nodes[4], and valid communication sides are Alice and Bob respectively, which is shown in Fig.1. Relay adopts amplify-and-forward strategies. In this model, a passive eavesdropper Eve is also considered. Eve's location is unknown. Here we suppose Alice is denoted as A, Bob is denoted as B, Eve as E, Relay as R. Assuming that loss factor α (0<α< 1) in Additive White Gaussian Noise (AWGN) channel path and communication is inversely proportional to the square of the distance on both sides. Loss factor of AR, BR, AE, BE and RE is $\alpha_A,\alpha_B,\alpha_1,\alpha_2,\alpha_3$. Amplification coefficient of R is $1/\alpha_A$. e_A^n, e_B^n, e_1^n, e_2^n and e_3^n represent the AWGN of AR, BR, AE, BE and RE in the n slot respectively, and $e_A^n \ \left(0, s_A^{\ 2}\right), e_B^n \ \left(0, s_B^{\ 2}\right), e_1^n \ \left(0, s_1^{\ 2}\right), e_2^n \ \left(0, s_2^{\ 2}\right), e_3^n \ \left(0, s_3^{\ 2}\right)$. Given that A sends a signal of to B is x_A, and B will send a signal to A is x_B, x_A^n represents the n-th symbol sent by A, and x_B^n represents the n-th symbol sent by B.

According to Shannon formula[5], the channel capacity from B to A(C_{BA}), from A to B(C_{AB}), from A to E(C_{AE}) and the channel capacity of A(C_{BE}) is:

$$C_{BA} = \frac{1}{2}\log_2\left(1+\frac{\alpha_B^2 * P}{\sigma_A^2+\sigma_B^2}\right) \tag{1}$$

$$C_{AB} = \frac{1}{2}\log_2\left(1+\frac{\alpha_B^2 * P}{(\alpha_B/\alpha_A)^2\sigma_A^2+\sigma_B^2}\right) \tag{2}$$

$$C_{AE} = \frac{1}{2}\log_2\left(1+\max\left[\frac{\alpha_3^2 * P}{(\alpha_3/\alpha_A)^2\sigma_A^2+\sigma_3^2}, \frac{\alpha_1^2 * P}{\sigma_1^2}\right]\right) \tag{3}$$

$$C_{BE} = \frac{1}{2}\log_2\left(1+\max\left[\frac{(\alpha_3\alpha_B/\alpha_A)^2 * P}{(\alpha_3/\alpha_A)^2\sigma_B^2+\sigma_3^2}, \frac{\alpha_2^2 * P}{\sigma_2^2}\right]\right) \tag{4}$$

Wyner has proved that[6] : As long as hacking channel capacity is inferior to that of the main channel (C_w<C_M, Cs> 0), theoretically there must be some kind of communication scheme that can ensure communication security. When the system information transmission rate satisfies R<=Cs, the legitimate communication node can achieve secure communication. So the security capacity is defined as the difference between the main channel capacity C_M and wiretap channel capacity C_W, namely, Cs = [C_M - C_W].

Therefore, security capacity of A can be expressed as:

$$C_{SA} = C_{RA} - C_{RE} = \frac{1}{2}\log_2\left(1+\frac{\alpha_B^2 * P}{\sigma_A^2+\sigma_3^2}\right) - \frac{1}{2}\log_2\left(1+\max\left[\frac{(\alpha_3\alpha_B/\alpha_A)^2 * P}{(\alpha_3/\alpha_A)^2\sigma_B^2+\sigma_3^2}, \frac{\alpha_2^2 * P}{\sigma_2^2}\right]\right) \tag{5}$$

Similarly, security capacity of B can be expressed as:

$$C_{SB} = C_{AR} - C_{AE} = \frac{1}{2}\log_2\left(1+\frac{\alpha_B^2 * P}{(\alpha_B/\alpha_A)^2\sigma_A^2+\sigma_B^2}\right) - \frac{1}{2}\log_2\left(1+\max\left[\frac{\alpha_2^2 * P}{(\alpha_3/\alpha_A)^2\sigma_A^2+\sigma_3^2}, \frac{\alpha_1^2 * P}{\sigma_1^2}\right]\right) \tag{6}$$

Study on Physical Layer Security Performance of Wireless Relay Communication System Based on PLNC

The communication process of the wireless relay system based on PLNC is shown as Fig.2.

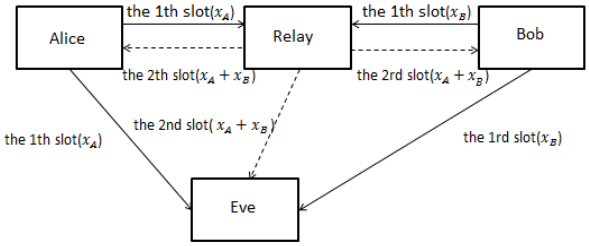


Fig.2 PLNC transport mechanism with eavesdropper

Similarly, the channel capacity from B to A(C_{BA}) , from A to B(C_{AB}) , from A to E(C_{AE}) and from B to E(C_{BE}) are:

$$C_{BA} = \frac{1}{2}\log_2\left(1 + \frac{\alpha_B^{\,2} * P}{\alpha_A^2 n_D^2 + n_D^2}\right) \tag{7}$$

$$C_{AB} = \frac{1}{2}\log_2\left(1 + \frac{\alpha_B^{\,2} * P}{(\alpha_B/\alpha_A)^2 n_A^2 + [1+(\alpha_B/\alpha_A)^2] n_D^2}\right) \tag{8}$$

$$C_{AE} = \frac{1}{2}\log_2\left(1 + \max\left[\frac{\alpha_3^{\,2} * P}{(\alpha_B\alpha_3/\alpha_A)^2 * P + (\alpha_3/\alpha_A)^2\sigma_A^2 + (\alpha_3/\alpha_A)^2\sigma_B^2 + \sigma_3^2}, \frac{\alpha_1^{\,2} * P}{\alpha_2^{\,2} * P + \sigma_1^2 + \sigma_1^2}\right]\right) \tag{9}$$

$$C_{BE} = \frac{1}{2}\log_2\left(1 + \max\left[\frac{(\alpha_B\alpha_3/\alpha_A)^2 * P}{\alpha_3^{\,2} * P + (\alpha_3/\alpha_A)^2 n_A^2 + (\alpha_3/\alpha_A)^2 n_D^2 + n_3^2}, \frac{\alpha_2^{\,2} * P}{\alpha_1^{\,2} * P + n_1^2 + n_1^2}\right]\right) \tag{10}$$

So the security capacity of A is:

$$C_{SA} = C_{BA} - C_{BE} = \frac{1}{2}\log_2\left(1 + \frac{\alpha_B^{\,2} * P}{2\sigma_A^2 \mid \sigma_B^2}\right) - \frac{1}{2}\log_2(1 + N) \tag{11}$$

Where $N = \max\left[\frac{(\alpha_B\alpha_3/\alpha_A)^2 * P}{\alpha_3^{\,2} * P + (\alpha_3/\alpha_A)^2 n_A^2 + (\alpha_3/\alpha_A)^2 n_D^2 + n_3^2}, \frac{\alpha_2^{\,2} * P}{\alpha_1^{\,2} * P + n_1^2 + n_1^2}\right]$

Similarly, the security capacity of B is:

$$C_{SB} = C_{AB} - C_{AE} = \frac{1}{2}\log_2\left(1 + \frac{\alpha_B^{\,2} * P}{(\alpha_B/\alpha_A)^2\sigma_A^2 \mid [1 \mid (\alpha_B/\alpha_A)^2]\sigma_B^2}\right) - \frac{1}{2}\log_2(1 + N) \tag{12}$$

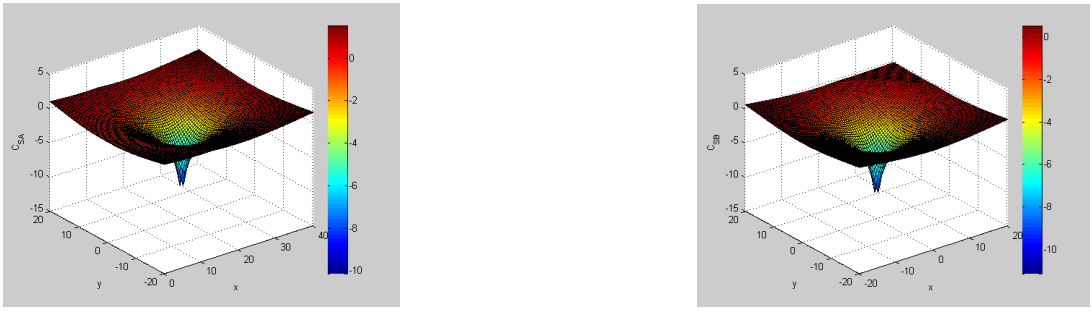
Where $N = \max\left[\frac{\alpha_3^{\,2} * P}{(\alpha_B\alpha_3/\alpha_A)^2 * P + (\alpha_3/\alpha_A)^2\sigma_A^2 + (\alpha_3/\alpha_A)^2\sigma_B^2 + \sigma_3^2}, \frac{\alpha_1^{\,2} * P}{\alpha_2^{\,2} * P + \sigma_1^2 + \sigma_1^2}\right]$

Simulations and Analysis

Assuming the distance between A and B is 20 meters. Given the position of R is (10,10), E is any point in the space. A and B are on an article line, in which A is on origin of coordinates, B's coordinate is (20,0), and R's coordinate is (10,10). The range of E is ($-20 \le x \le 20, -20 \le y \le 20$). When B is the transmitting terminal, the range of E is ($0 \le x \le 40, -20 \le y \le 20$). According to the analysis of two data sets selected from various parameters in the model:

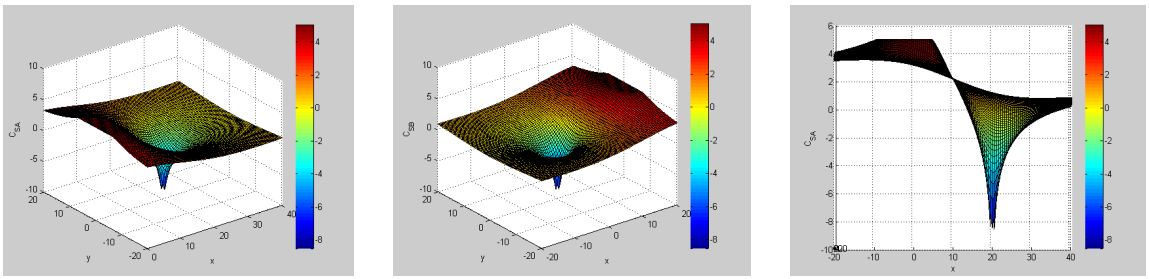
Low signal to noise ratio: $e_A^n = 2\times10^{-4}$W, $e_B^n = 2\times10^{-4}$W, $e_1^n = 10^{-4}$W, $e_2^n = 10^{-4}$W, transmit power of A and B reach 10W.

High signal to noise ratio: $e_A^n = 10^{-4}$W, $e_B^n = 10^{-4}$W, $e_1^n = 10^{-4}$W, $e_2^n = 10^{-4}$W, transmit power of A and B reach 10W.



(a) (b)

Fig.3 traditional models with low SNR (a) C_{SA}; (b) C_{SB}



(a) (b) (c)

Fig.4 PLNC model with low SNR (a) C_{SA}; (b) C_{SB}; (c) C_{SA}(side view)

Fig. 3(a) and (b) show that in traditional communications mode, when eavesdropper gradually leaves away from transmitting terminal, security capacity increases. Fig.4 (a) and (b) show that security capacity has been improved by using PLNC technique. For example, in Fig.3 (a) x=0 and y=20, C_S=-0.3389bit/symbol. When PLNC is adopted (in Fig. 4(a)), x=0,y=20, C_S=3.162 bit/symbol. This indicates that PLNC technique greatly enhances the physical security performance of the system, thereby effectively deterring eavesdroppers to access to information.

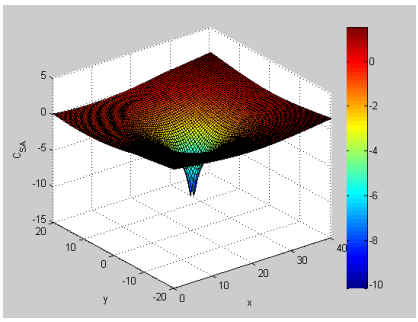


Fig. 5 traditional model C_{SA} with high SNR

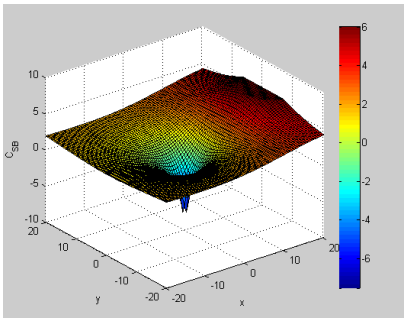


Fig. 6 PLNC mode C_{SB} with high SNR

From Fig. 3(a) and Fig. 5, Fig. 4(b) and Fig. 6, it can be drawn, with high signal to noise ratio, security capacity improves but not significantly. For example, in traditional model C_{SA} with low SNR (x=10,y=20), security capacity improve is about -0.178bit/symbol, while in traditional model C_{SA} with high SNR (x=30,y=20),security capacity is about 0.8218bit/symbol.

Conclusions

This paper studies three-node wireless relay communication system based on PLNC, and provides theoretical expression of security capacity in the condition of unknown information about wiretap channel. In accordance with theoretical analysis and simulation results, compared with the traditional wireless relay communication system, either with high SNR and low SNR, PLNC technology can improve the physical layer security performance of wireless relay communication system. In addition, when the eavesdropping position has a longer distance to the transmitter but a shorter distance to the receiver, its physical layer security performance is better.

References

[1]A.D.Wyner. The Wire-tap Channel [J]. Bell System Technical Journal, 1975, 54(8):1355-1387.

[2] S. Zhang, S. C. Liew, and P. P. Lam, *Physical-layer network coding[C]*, in Proc.Int.Conf.on Mobile Computing and Networking (MOBICOM), Los Angeles, CA, Sept. 2006, pp. 358-365.

[3] BinShi, LiangJin, ZhouZhong, JiangJi, *To Improve Security Performance of Physical Layer of Wireless Relay System by Network Coding*, Journal of Information Engineering University, 2011 No. 06.

[4] T.M .Cover and A .A .E .Carnal, *Capacity Theorems for the Relay Channel[J]*, IEEE Trans.Info.Theory, vol.25 ,no5, Sept. 1979:572-584.

[5] YuehongShen,YuanyuanGao, YiminWei, *Communication Theory[m]*, Mechanical Industry Publishing, Beijing, Second Edition, September 2008.
[6] YuanFeng, XiaoyunHou, etc.*The Influence of Node Location on Security Capacity of Wiretap Channel*, Development of Computer Technology December 2014, 12th, 24.
[7] M Hay, B Saeed，CH Lung，A Srinivasan.*Co-Located Physical-Layer Network Coding to Mitigate Passive Eavesdropping*, International Conference on Privacy Security &Trust, 2010-1-2.