New Secret Key Agreement Scheme over Relay Communication Channel

Li-Juan Xing[1,a] , Feng Pan [1,b] , Xue-Qin Jiang [1,c], Kaizhi Peng[2,d] and Miaowen Wen[3,e]

[1]School of Information Science and Technology, Donghua University, Shanghai, China
[2] Wuhan Maritime Communication Research Institute, Wuhan, China
[3] School of Electronic and Information Engineering, South China University of Technology, Guangzhou, China

Email: [a]xinglijuan625@163.com, [b]fpan@dhu.ehu.cn, [c]xqjiang@dhu.edu.cn, [d]32114199@dhu.edu.cn, [e]eemwwen@scut.edu.cn

Abstract. The novel advantage distillation (AD) scheme for secret key agreement (SKA) scheme over relay communication system for the wiretap channel model is proposed. For the case where there are noiseless both the main channel and the eavesdropper's channel, the SKA scheme for the noiseless relay communication (SKA-NRC) system is proposed. In this scheme, random sequences $\boldsymbol{q}_A$ and $\boldsymbol{q}_B$ are used as artificial interference to prevent eavesdropping. Simulation results show that with the proposed SKA schemes, the bit error ratio (BER) of eavesdropper Eve maintains stably at 0.5, while legitimate users Alice and Bob are able to get much lower BERs.

1. Introduction

Traditional communication secrecy is achieved mainly relying on cryptography-based encryption technology, which always relies upon computational hardness of mathematical problems [1-2] to make the schemes unbreakable. However, security of traditional encryption is compromised with the dramatic improvement of computational power [3]. Secret key agreement (SKA) appears as an approach that supports physical-layer security with no limitation on the eavesdropper's computational power and also serves as a supplement or replacement of upper layer encryption schemes.

In SKA, the legitimate users, Alice and Bob, intend to generate sequences of agreed bits (key) which are secret to the eavesdropper, Eve. In a SKA scheme three phases are included typically: (a) advantage distillation (AD), (b) information reconciliation (IR), and (c) privacy amplification [4]. The purpose of AD is to offer Alice and Bob a superiority over the Eve. Alice and Bob are supposed to generate an identical random sequence in the reconciliation phase, from which a secret key is extracted in the privacy amplification phase [5].

There have been a lot of researches focused on AD schemes. For example, an AD scheme for SKA was proposed for additive white Gaussian noise (AWGN) [4]. An AD scheme was proposed over a wiretap channel [5], which can achieve the purpose of secret sharing.

The wiretap channel model was defined [6] applying Shannon's perfect secrecy model [7], where there existed an eavesdropper who can obtain information by wiretapping. According to Wyner wiretap channel model [6], perfect secrecy can be realized on condition that the eavesdropper’s channel is noisier

than the main channel. The condition of perfect secrecy can be achieved through the AD phase. A novel scheme was proposed for wiretap channel I [6] by using feedback and low density parity check (LDPC) codes [8-9]. In this scheme, the legitimate users can be free of error after multi-round-trip two-way communication.

We consider the case where there are noiseless both in all the channels and propose a new AD scheme over two-way wiretap channel model, which consists of two legitimate users and one eavesdropper [8]. In this scheme, random sequences $\boldsymbol{q}_A$ and $\boldsymbol{q}_B$ are used to prevent eavesdropping. The security gap [10] is defined as the quality ratio between the main channel and the eavesdropper's channel required to guarantee the security level, while ensuring that the legitimate user reliably receives the information. Security gap can be increased by proposed scheme, and it is estimated by the bit error ratio (BER).

In a communication system, the relay is widely used for the situation where the communication distance is out of the transmission range [11]. In a relay communication system, traditional transmission schemes [12-13] required four time slots to achieve two-way communication. A distributed scheme was introduced for exchanging independent information mutually in wireless networks [14]. In this scheme, time slots was saved and transmission efficiency was improved by using network coding and physical-layer broadcast.

In summary, our contributions are as follows:

- An AD schemes for SKA schemes over relay communication systems is proposed. The AD schemes can provide the legitimate users a superiority over the eavesdropper.
- Simulations have been performed, and performance of the SKA-NRC scheme is evaluated by BER. With the proposed scheme, the BER of eavesdropper maintains at 0.5, while legitimate users are able to get much lower BERs.

2. System model

We consider two legitimate users, say Alice and Bob, communicating with the help of a relay in the presence of a powerful eavesdropper, Eve. We assume that Eve can listen to all the communications between Alice and Bob and try to compromise the key generation between them. Eve can also measure both the channels between herself and Alice and Bob. The phase and amplitude of the signals are assumed to be ideally synchronized and matched.

2.1. The noiseless wiretap channel with relay (NLR-WT)

The NLR-WT model handles the noiseless situations. The signals transmitted between the legitimate users are random sequences $\boldsymbol{q} \in (0,1)^n$. Hamming code is taken for IR. $\boldsymbol{s}_X$ denotes the sequence sent by the user *X*. $\boldsymbol{c}_X$ denotes the sequence received by the user *X*. All channels in this model are assumed to be noiseless.

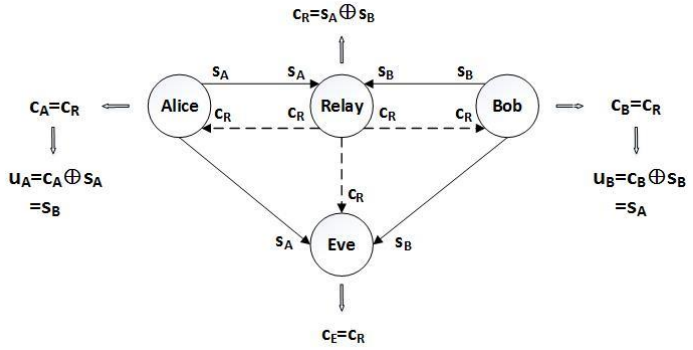

Figure. 1 The noiseless wiretap channel with relay (NLR-WT)

Figure 1 shows the key agreement process of the NLR-WT model. First, Alice sends the sequence $\boldsymbol{s}_A$ and Bob sends the sequence $\boldsymbol{s}_B$ to the relay simultaneously. The relay receives the superimposed sequences

$$\boldsymbol{s}_R = \boldsymbol{s}_A + \boldsymbol{s}_B, \tag{1}$$

and maps it via PNC by $\boldsymbol{c}_R = f(\boldsymbol{s}_R)$. Equivalently, $\boldsymbol{c}_R$ can be represented by

$$\boldsymbol{c}_R = \boldsymbol{s}_A \oplus \boldsymbol{s}_B. \tag{2}$$

Then, the relay broadcasts $\boldsymbol{c}_R$ to all the users. Alice receives the sequence

$$\boldsymbol{c}_A = \boldsymbol{c}_R \tag{3}$$

and Bob receives the sequence

$$\boldsymbol{c}_B = \boldsymbol{c}_R. \tag{4}$$

Alice (Bob) can extract the sequence $\boldsymbol{s}_B$ ($\boldsymbol{s}_A$) from $\boldsymbol{c}_R$ by using the local sequence she (he) sent before, $\boldsymbol{s}_A$ ($\boldsymbol{s}_B$). After extraction, Alice gets

$$\begin{aligned} \boldsymbol{u}_A &= \boldsymbol{c}_A \oplus \boldsymbol{s}_A \\ &= \boldsymbol{s}_A \oplus \boldsymbol{s}_B \oplus \boldsymbol{s}_A \\ &= \boldsymbol{s}_B \end{aligned} \tag{5}$$

and Bob gets

$$\begin{aligned} \boldsymbol{u}_B &= \boldsymbol{c}_B \oplus \boldsymbol{s}_B \\ &= \boldsymbol{s}_A \oplus \boldsymbol{s}_B \oplus \boldsymbol{s}_B \\ &= \boldsymbol{s}_B. \end{aligned} \tag{6}$$

At the meantime, for the nature of broadcast and the synchronization of the signals sent by Alice and Bob, Eve can only obtain the superimposed sequence

$$\boldsymbol{s}_E = \boldsymbol{s}_A + \boldsymbol{s}_B. \tag{7}$$

Eve maps it by PNC by $\boldsymbol{c}_E = f(\boldsymbol{s}_E)$ or simply wiretaps to get the sequence

$$\boldsymbol{c}_E = \boldsymbol{s}_A \oplus \boldsymbol{s}_B \tag{8}$$

from the relay.

3. Proposed secrete key agreement schemes

3.1. SKA scheme for noiseless relay communication system

SKA scheme for the noiseless relay communication (SKA-NRC) system introduces the random sequences $\boldsymbol{q}_A$ and $\boldsymbol{q}_B$ as artificial interference, which are generated by Alice and Bob, respectively. $\boldsymbol{q}_A$ and $\boldsymbol{q}_B$ are both $1 \times N$ vectors, in which the number of 1's and 0's can be set. At the beginning, Alice (Bob) sends $\boldsymbol{s}_A^1$ ($\boldsymbol{s}_B^1$) to the relay, respectively, as

$$\boldsymbol{s}_A^1 = h(\boldsymbol{x}^1) \oplus \boldsymbol{q}_A^1 \tag{9}$$

and

$$\boldsymbol{s}_B^1 = h(\boldsymbol{y}^1) \oplus \boldsymbol{q}_B^1, \tag{10}$$

where $\mathrm{h}(\cdot)$ denotes the Hamming coding function and $\boldsymbol{x}^1$ ($\boldsymbol{y}^1$) is the sequence Alice (Bob) wants to send in the first round. From the second round on, Alice and Bob code the sequences to be sent both

with random sequences $\boldsymbol{q}_A^n$, $\boldsymbol{q}_B^n$ and $\boldsymbol{u}_A^{n-1}$, $\boldsymbol{u}_B^{n-1}$. $\boldsymbol{u}_A^{n-1}$ ($\boldsymbol{u}_B^{n-1}$) is the sequence Alice (Bob) receives in round $n-1$. When $n \geq 2$, we have

$$\boldsymbol{s}_A^n = h(\boldsymbol{x}^n \oplus \boldsymbol{u}_A^{n-1}) \oplus \boldsymbol{q}_A^n, \tag{11}$$

$$\boldsymbol{s}_B^n = h(\boldsymbol{y}^n \oplus \boldsymbol{u}_B^{n-1}) \oplus \boldsymbol{q}_B^n. \tag{12}$$

The relay receives the superimposed sequence $\boldsymbol{s}_R^n = \boldsymbol{s}_A^n + \boldsymbol{s}_B^n$ and maps it via PNC by $\boldsymbol{c}_R^n = f(\boldsymbol{s}_R^n)$, which is equivalent to

$$\begin{aligned} \boldsymbol{c}_R^n &= \boldsymbol{s}_A^n \oplus \boldsymbol{s}_B^n \\ &= h(\boldsymbol{x}^n \oplus \boldsymbol{u}_A^{n-1}) \oplus \boldsymbol{q}_A^n \oplus h(\boldsymbol{y}^n \oplus \boldsymbol{u}_B^{n-1}) \oplus \boldsymbol{q}_B^n \end{aligned} \tag{13}$$

After that, $\boldsymbol{c}_R^n$ is broadcast to all users. When Alice receives the sequence $\boldsymbol{c}_A^n$=$\boldsymbol{c}_R^n$, she use $\boldsymbol{x}^{n-1}$ and the random sequence $\boldsymbol{q}_A^n$ generated by herself to decode the sequence as

$$\begin{aligned} \boldsymbol{u}_A^n &= h^{-1}(\boldsymbol{c}_A^n \oplus \boldsymbol{s}_A^n) \oplus \boldsymbol{x}^{n-1} \\ &= h^{-1}(\boldsymbol{s}_B^n) \oplus \boldsymbol{x}^{n-1} \\ &= \boldsymbol{y}^n \oplus \boldsymbol{u}_B^{n-1} \oplus \boldsymbol{x}^{n-1} \\ &= \boldsymbol{y}^n, \end{aligned} \tag{14}$$

where $h^{-1}(\cdot)$ denotes Hamming decoding function. Similarly, Bob receives the sequence $\boldsymbol{c}_B^n$=$\boldsymbol{c}_R^n$ and he can also obtain

$$\begin{aligned} \boldsymbol{u}_B^n &= h^{-1}(\boldsymbol{c}_B^n \oplus \boldsymbol{s}_B^n) \oplus \boldsymbol{y}^{n-1} \\ &= h^{-1}(\boldsymbol{s}_A^n) \oplus \boldsymbol{y}^{n-1} \\ &= \boldsymbol{x}^n \oplus \boldsymbol{u}_A^{n-1} \oplus \boldsymbol{y}^{n-1} \\ &= \boldsymbol{x}^n. \end{aligned} \tag{15}$$

At the same time, due to the nature of broadcast and the synchronization of the signals sent by Alice and Bob, Eve can get the superimposed sequence

$$\begin{aligned} \boldsymbol{s}_E^n &= \boldsymbol{s}_A^n + \boldsymbol{s}_B^n \\ &= h(\boldsymbol{x}^n \oplus \boldsymbol{u}_A^{n-1}) \oplus \boldsymbol{q}_A^n + h(\boldsymbol{y}^n \oplus \boldsymbol{u}_B^{n-1}) \oplus \boldsymbol{q}_B^n. \end{aligned} \tag{16}$$

Eve can map $\boldsymbol{s}_E^n$ via PNC by $\boldsymbol{c}_E^n = f(\boldsymbol{s}_E^n)$ or simply wiretaps to get the sequence

$$\begin{aligned} \boldsymbol{c}_E^n &= \boldsymbol{s}_A^n \oplus \boldsymbol{s}_B^n \\ &= h(\boldsymbol{x}^n \oplus \boldsymbol{u}_A^{n-1}) \oplus \boldsymbol{q}_A^n \oplus h(\boldsymbol{y}^n \oplus \boldsymbol{u}_B^{n-1}) \oplus \boldsymbol{q}_B^n. \end{aligned} \tag{17}$$

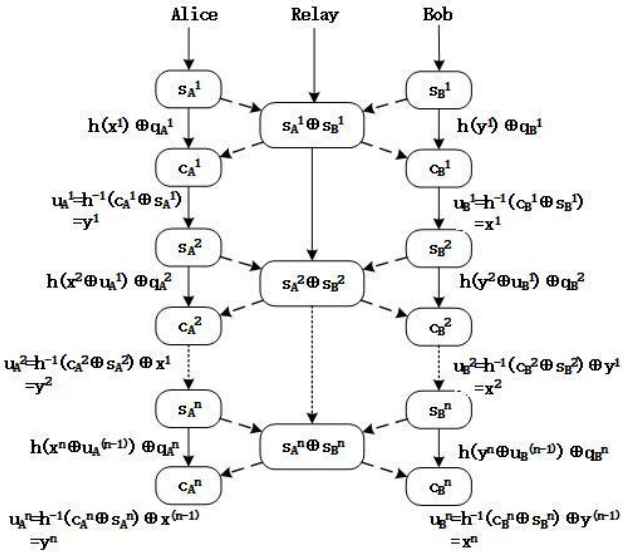

Figure. 2 Flow chart of SKA-NRC scheme

However, on one hand, Eve cannot decode in the same way as she does not know the sequences $\boldsymbol{q}_A^n$ and $\boldsymbol{q}_B^n$, and the sequences $\boldsymbol{u}_A^{n-1}$ and $\boldsymbol{u}_B^{n-1}$. On the other hand, Eve cannot distinguish between what Alice sends and what Bob sends from Eq. (16) and Eq. (17). Therefore, neither the superimposed sequence $\boldsymbol{s}_E^n$ nor the sequence $\boldsymbol{c}_E^n$ can be used for extracting to get $\boldsymbol{x}^n$ or $\boldsymbol{y}^n$. It is clear that the correct sequence $\boldsymbol{x}^n$ or $\boldsymbol{y}^n$ can be extracted by Alice and Bob while Eve cannot. The proposed SKA scheme for the noiseless relay communication system (SKA-NRC) is illustrated in figure 2.

4. Results and simulations

With SKA-RC scheme, the probability that Eve get the right bit is 0.5 since Eve cannot distinguish which user the sequence comes from. The BER of Alice is

$$p_r(\boldsymbol{u}_A^n) = p_r(\boldsymbol{y}^n) \tag{18}$$

and the BER of Bob is

$$p_r(\boldsymbol{u}_B^n) = p_r(\boldsymbol{x}^n). \tag{19}$$

BER simulation results of the proposed SKA-NRC scheme are shown in figure 3-figure 6. The number of rounds n is 1,000.

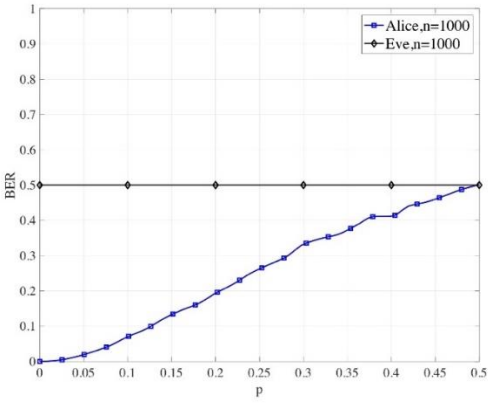

Figure 3. BER of secret keys received by Alice and Eve

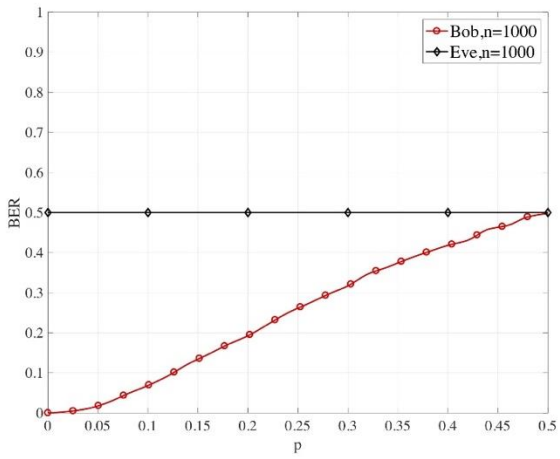

Figure 4. BER of secret keys received by Bob and Eve

The BER simulation results of Alice and Eve are shown in figure 3. It is shown that with the increasing crossover probability p, BER of Alice increases, which does not exceed 0.5. While BER of Eve remains at 0.5, a value which is always higher than that of Alice. The BER simulation results of Bob and Eve are shown in figure 4. It is shown that with the increasing crossover probability p, BER of Bob increases as well, which does not exceed 0.5. While BER of Eve remains at 0.5, a value which is always higher than that of Bob. When p is between 0 and 0.12, the BER of Alice (Bob) is slowly rising and when $p \geq 0.13$, the BER starts to rise sharply. This indicates that the BER performance of the main channel is superior to that of the eavesdropper's channel under the same number of rounds n. The BER simulation results of Alice and Bob are shown in figure 5. It is shown that the legitimate users Alice and Bob have almost the same BER for the same p. That indicates Alice and Bob have the same superiority over Eve. BER simulation results of Eve are shown in figure 6. It is shown that BER from Alice to Eve and BER from Bob to Eve are stably maintained at 0.5 with the increasing p, which is the same as the theoretical analysis.

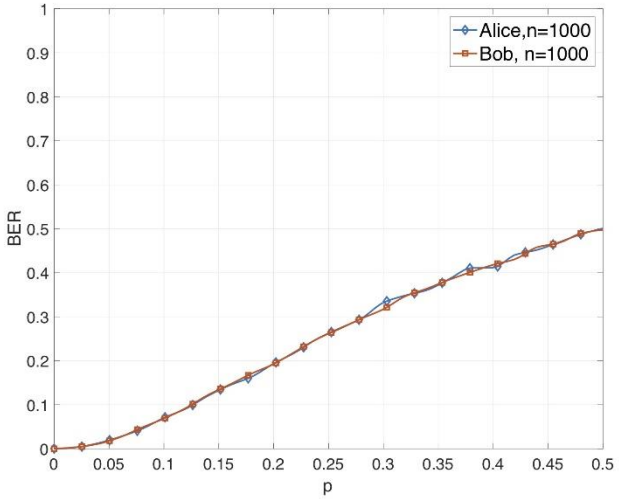

Figure 5. BER of secret keys received by Alice and Bob

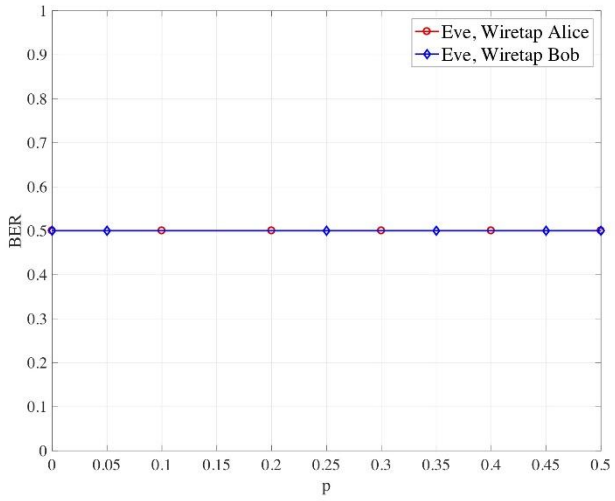

Figure 6. BER of secret keys received by Eve

In summary, BER of Alice and Bob could be as low as possible while BER of Eve remains a BER of 0.5.

5. Conclusion

In this paper, a novel AD schemes for SKA over the relay communication system was proposed. The proposed SKA-NRC scheme handled with the noiseless conditions. We proved that with the proposed SKA scheme, after the AD phase the legitimate users, Alice and Bob, had a superiority over the eavesdropper, Eve. The secret keys were extracted after executing the privacy amplification on the obtained identical sequences. Simulations were performed for the SKA-NRC scheme to analyse the proposed scheme in terms of BER. The simulation results of SKA-NRC showed that BER of Alice and Bob could be as low as possible while BER of Eve remains a BER of 0.5.

Acknowledgment

This work was supported by National Natural Science Foundation of China (61671143).

References

[1] Huang Y, Jin L and Wei H. Fast Secret Key Generation based on Dynamic Private Pilot from Static Wireless Channels. *China Commun.*, 2018, 15(11), 171–183.
[2] Shen W, Hong W and Cao X. Secure Key Establishment for Device-to-device Communications. *Global Commun. Conf. (GLOBECOM)*, Austin, TX, USA, Dec. 2014, 336–340.
[3] Shimizu T, Iwai H and Sasaoka H. Physical-layer Secret Key Agreement in Two-way Wireless Relaying Systems. *IEEE Trans. Inf. Forensics Security*, 2011, 6(3), 650–660.
[4] Tomasin S, Trentini F and Laurenti N. Secret Key Agreement by LLR Thresholding and Syndrome Feedback over AWGN Channel. *IEEE Commun. Lett.* 2014, 18(1), 26–29.
[5] Cao Y, Jiang X Q and Wang H M. Advantage Distillation over MIMO Wiretap Channels based on Generalized Extended Orthogonal Space-time Block Codes. *Int. Conf. Comput. Inf. Telecommun. Syst.* Kunming, China, Aug. 2016, pp. 1–5.
[6] Wyner A D. The Wire-tap Channel. *Bell Syst. Tech. J.* 1975, 54(8), 1355–1387.
[7] Shannon C E. Communication Theory of Secrecy Systems. *Bell Syst. Tech. J.* 1949, 28(4), 656–715.
[8] Wen H, Gong G and Ho P H. Build-in Wiretap Channel I with Feedback and LDPC Codes. *J. Commun. Netw*. 2009, 11(6), 538–643.

[9] Zhang G, Wen H and Pu J. Build-in Wiretap Channel I with Feedback and LDPC Codes by Soft Decision Decoding. *IET Commun.,* 2017, 11(11), 1808–1814.
[10] Baldi T, Bianchi M and Chiaraluce F. Coding with Scrambling, Concatenation, and HARQ for the AWGN Wiretap Channel: A Security Gap Analysis. *IEEE Trans. Inf. Forensics Security*, 2012, 7(3), 883–894.
[11] Fragouli C, Le Boudec J Y and Widmer J. Network Coding: an Instant Primer. *ACM SIGCOMM Computer Communication Review*, 2006, 36(1), 63–68.
[12] Cover T and M Gamal A E. Capacity Theorems for the Relay Channels. *IEEE Trans. Inf. Theory,* 1979, 25(5), 572–584.
[13] Laneman J, Tse N D and Wornell G. Cooperative Diversity in Wireless Networks: Efficient Protocols and Outage Behavior. *IEEE Trans. Inf. Theory*. 2004, 50(12), 3062–3080.
[14] Wu Y, Chou P A and Kung S Y. Information Exchange in Wireless Networks with Network Coding and Physical-layer Broadcast. *Microsoft, Tech. Rep. MSR-TR-2004-78*, 2004.