Physical layer security enhanced system with novel LDPC decoder and artificial noise

Yongfang Zhang[a]

School of Computer Science and Engineering, Northeastern University, Shenyang 110819, China

Abstract. Physical layer security is one of the most important issues in the design of communication system, especially in the scenario of wireless communication where the information transmission is exposed to the risk of eavesdropping. Previous works focus on the physical layer security by information scrambling and Low Density Parity Check (LDPC) coding. However, most of these works consider less the impact of physical layer security design on the performance of LDPC decoding, which may impair the system reliability. In this paper, we propose a new physical layer security enhanced system. A novel artificial noise is proposed to enhance the physical layer security of the system by worsening the wiretap channel, while an effective LDPC decoder based on tree structure of expectation propagation is proposed to guarantee the system reliability by solving the loop of decoding errors. Simulation results demonstrate that the proposed system is effective in enhancing the physical layer security with the improved reliability than the traditional systems.

Keywords: physical layer security; LDPC; artificial noise.

1 Introduction

As an emerging technique to significantly improve the security of wireless communication system, physical layer security aims to improve the secrecy of information transmission by exploiting the physical layer properties of the communication system, such as thermal noise, interference, and the time-varying nature of fading channels. Thus, physical layer security is a fundamentally different technique compared to the traditional cryptographic approach.

Artificial noise is one of the promising methods to realize wireless physical layer security. Different from the traditional interference cancellation, the artificial noise technique realizes the secure communication by the information security theory. According to the general principle of artificial noise, the information is protected from eavesdropping by introducing the artificial noise to deteriorate the channel conditions, and thus increase the Bit Error Rate (BER) of the eavesdropper.

Although the artificial noise technique is effective in guaranteeing the system security, it also degrades the system reliability performance due to the undesirable elimination of artificial noise from useful information. In some related works, Low Density Parity Check (LDPC) coding is combined into the physical layer security enhanced system for purpose of compensating the performance loss in reliability. Due to the sparsity of checking matrix in LDPC, the information bits that are far apart from

[a] Corresponding author : yfzhangneu@sina.com

each other are checked in the unified mode, which makes the burst of continuous errors have little effect on decoding [1]. Furthermore, the LDPC coding scheme can be easily implemented in parallel operation, thus contribute to the transmission efficiency of communication system.

There have been some researches on the LDPC coded physical layer security. Klinc presented a drilling LDPC coded system [2], in which the private information is not directly transmitted but hidden in the drilling bit transmission. The optimal drilling distribution is derived with the minimum safety gap. Baldi proposed a combination of private information scrambling and channel coding [3]. A non-singular random scrambling matrix is cascaded before the channel coding. In such a way, the decoding error can be dispersed, and thus increasing the decoding error probability of eavesdropper.

Most of the LDPC coded systems above adopt the Belief Propagation (BP) algorithm for decoding. BP can reduce the decoding complexity greatly by making full use of the sparse parity check matrix. However, the decoding loop is inevitable in the BP algorithm when the code length is finite. Due to the existence of decoding loop, the information iterates between checking nodes and variables nodes repeatedly, which leads to the information redundancy and increases the decoding error.

In this paper, we propose a new physical layer security enhanced system and consider the impact of physical layer security design on the performance of LDPC decoding [4]. The novel contributions can be summarized as follows: (1) An effective artificial noise technique is first proposed to enhance the security of information transmission by deteriorating the wiretap channel and increasing the BER of eavesdropper; (2) A novel LDPC decoder based on Tree structure of Expectation Propagation (TEP) algorithm is further proposed to guarantee the information reliability by eliminating the decoding loop inherent in the traditional BP algorithm without extra computational complexity.

2 Proposed system structure

The structure of the proposed physical layer security enhanced system is shown in Fig. 1. Without of generality, we use Alice, Bob and Eve to represent the transmitter, legitimate receiver and eavesdropper, respectively. At the transmitting end, Alice splits the information into two branches and scrambles either one, and then recombines the two branches. The recombined signal will be encoded via LDPC and transmitted into the wireless channel. At the receiving end, Bob can recover the data through the TEP decoder and scrambling solver. However, since the artificial noise deteriorates the Signal Noise Ratio (SNR) and causes the decoding errors, Eve cannot recover the information even if it eavesdrops the signal. In such a way, the proposed system can enhance the physical layer security with the improved decoding performance.

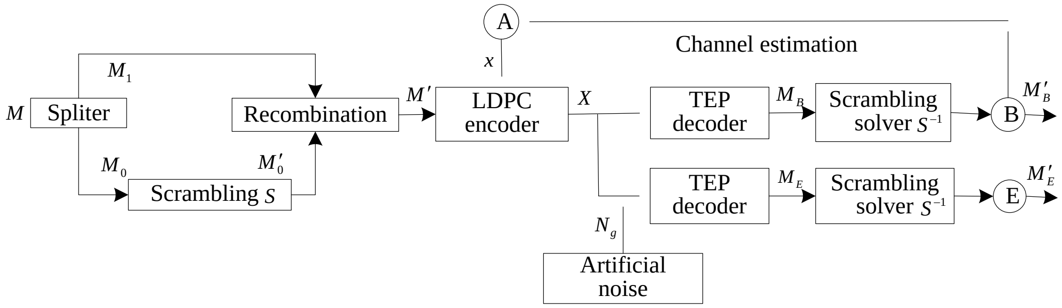


Figure 1. Structure of the proposed physical layer security enhanced system

In summary, the primary components in the proposed system include information scrambling, LDPC encoder, TEP decoder, scrambling solver and channel estimation.

1) *Information scrambling*. At the transmitting end, the original information *M* splits into two branches M_0 and M_1. According to the length of the secret information, Alice needs to construct

randomly a non-singular matrix *S* with the density of 0.5. Then, the secret information M_0 is scrambled by multiplying the matrix *S* to generate M_0'. The information M_0' will be further recombined with the public information M_1 to generate M'.

2) *LDPC encoder*. The information M' will be sent into LDPC encoder and output X. Before the LDPC encoding, the transmitter (i.e., Alice) should send to the receiver (i.e., Bob) the training sequence which will be used for the following channel estimation.

3) *TEP decoder*. At the receiving end, Bob can decode the information X as M_B by the TEP algorithm. However, due to the artificial noise, the eavesdropper Eve obtains the different information M_E through the TEP decoder.

4) *Scrambling solver*. Bob can solve the scrambling and obtain the information M_B' from M_B by multiplying a matrix S^{-1}.

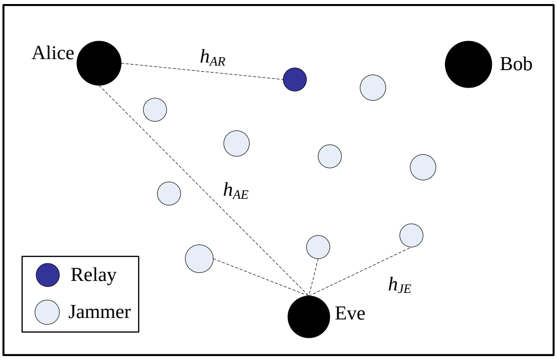
5) *Channel estimation*. The channel is estimated by using the training sequence, and then Bob can recover the original information *M* from M_B' with the estimated channel condition.

3 Artificial noise

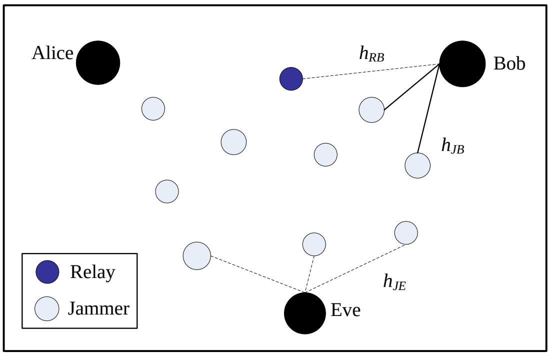
In the proposed system, the artificial noise is realized by the optimal relay selection and cooperative jamming [5-7]. We choose *K* jamming nodes to form a cooperative system. Assuming all nodes work in half duplex mode, the communication process is divided into the following two stages.

Stage 1: When Alice wants to communicate with Bob, it first sends the information to the relay node. To prevent the information from eavesdropping by Eve, the jamming nodes need to transmit in cooperation with relay node the artificial noise.

Stage 2: The relay node will forward the received information to Bob, meanwhile the jamming nodes transmit in cooperation with relay node the artificial noise to deteriorate the signal quality of the eavesdropper Eve.



(a) the first phase



(b) the second phase

Figure 2. Artificial noise based on optimal relay selection and cooperative jamming

The power of relay node is fixed to half of the total power, i.e., $P_R = 0.5P_{in}$, where P_R and P_{in} are the power of relay node and totoal power, respectively. Our goal is to to maximize the security capacity by first selecting the optimal relay node, and then optimizing the beam forming vectors w_1 of the relay node in the first stage and w_2 of the jamming nodes in the second stage.

For brief of presentation, we introduce the following notations. h_{JR} represents the channel vector between the N jamming nodes and the relay node, and h_{JE} denotes the channel vector between the N jamming nodes and the eavesdropping node, where $N = K-1$. We assume that each node has the Additive White Gaussian Noise (AWGN) with the mean of 0 and the variance of 1. P_S , P_{in} and P_R represent the power of transmitting node, the power of cooperative jamming node and the power of relay node. Thus, the optimization of w_1 can be modeled as follows:

$$\arg\max_{w_1} \left| h_{JE}^T w_1 \right|^2 \qquad s.\ t. \begin{cases} h_{JR}^T w_1 = 0 \\ w_1^H w_1 = P_{in} \end{cases} \tag{1}$$

where $w_1 = \mu_1 \left\| h_{JR} \right\|^2 h_{JE}^* - \mu_1 (h_{JR}^T h_{JE}^*) h_{JR}^*$.

Similarly, in the second stage, the value of w_2 should also ensure the maximum power of Eve, while Bob is free of interference. We denote h_{JB} as the channel vector between the *N* jamming node and the receiving node Bob, and h_{JE} as the channel vector between the *N* jamming nodes and the eavesdropping node Eve. Thus, the optimization of w_2 can be modeled as follows:

$$\arg\max_{w_2} \left| h_{JE}^T w_2 \right|^2 \qquad s.\ t. \begin{cases} h_{JB}^T w_2 = 0 \\ w_2^H w_2 = P_{in}\text{-}P_R \end{cases} \tag{2}$$

where $\mu_2 = \sqrt{\dfrac{P_{in} - P_R}{\left\| h_{JB} \right\|^4 \left\| h_{JE} \right\|^2 - \left\| h_{JB} \right\|^2 \left| h_{JB}^T h_{JE}^* \right|^2}}$.

With the constraint of $h_{JR}^{T}w_1 = 0, h_{JB}^{T}w_2 = 0$, the SINR Γ_{AB} between Alice and Bob and the SINR Γ_E between Alice and Eve are derived as follows:

$$\Gamma_{AB} = \frac{P_R P_A |h_{AR}|^2 |h_{RB}|^2 \alpha^2}{P_R |h_{RB}|^2 \alpha^2 + 1} \qquad \Gamma_E = \frac{P_A |h_{AE}|^2}{|h_{JE}^{T}w_1|^2 + 1} + \frac{\alpha^2 P_A P_R |h_{AR}|^2 |h_{RE}|^2}{P_R |h_{RE}|^2 \alpha^2 + |h_{JE}^{T}w_2|^2 + 1} \tag{3}$$

where $\alpha = \left(\sqrt{1+P_S}\,|h_{AR}|^2\right)^{-1}$. Therefore, the optimal relay node is selected as follows:

$$\arg\max_{R} \frac{1+\Gamma_{AB}}{1+\Gamma_E} \tag{4}$$

4 TEP decoder

Unlike the traditional BP decoding algorithm [8], the proposed TEP algorithm can solve the problem of decoding loop in the case of finite code length without the introduction of extra complexity. The procedure of TEP can be described as follows:

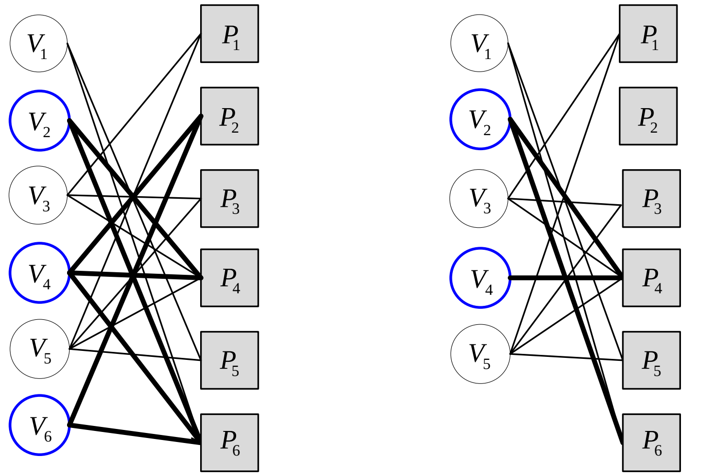
Step 1: To select the checking node with the degree of 1 or 2;

Step 2: If the selected checking node has the degree of 1, to update the information of the variable node that is connected with the selected checking node, and then to update the information of all checking nodes that are connected to the updated variable node.

Step 3: If the selected checking node has the degree of 2, to remove one of the variable nodes that are connected to the selected checking node. Another variable node will afford the connections of the removed variable node. Then, the selected checking node is removed.

Step 4: To repeat the steps 1 to 3 until all the variable nodes are removed.

For example in Fig. 4, the checking node P_2 is connected to the variable nodes V_4 and V_6. If we remove the variable node V_6, another variable node V_4 would afford the connections of V_6, that is, the checking nodes P_2 and P_3 should be connected to V_4. We notice that V_4 has been already connected to the checking nodes P_2 and P_3. To avoid the existence of decoding loop, we should remove the repeated connections between V_4 and the two checking nodes. Thus, in the process of decoding, the same information is prevented from the repeated delivery between the variables nodes and checking nodes, which helps reduce the decoding error induced by the redundant information. Figure 3 illustrates that, when the code length is finite, the TEP algorithm can cope with the decoding loop and outperforms the BP algorithm without the introduction of extra complexity.



(a) Decoding loop of V_2 , V_4 and V_6 (b) Removal of V_6 and P_2

Figure 3. Illustration of TEP algorithm in decoding

5 Simulation analysis

In simulation, we employ the wiretap channel model in [9]. The length of the information transmitted is set to 6000 bits. The coding rate $R = 1/2$. The maximum number of decoding is 40. The information is modulated on BPSK signal and transmitted through the Binary Erasure Channel (BEC) channel. The legal channel and eavesdropping channel are independently and identically distributed. All parameters are set strictly according to the representative scenarios [6-9].

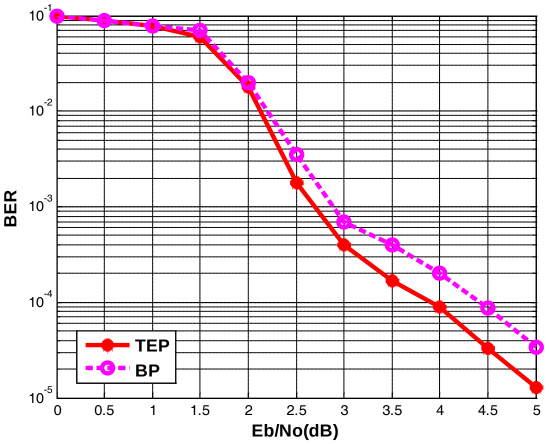


Figure 4. Comparison of TEP and BP

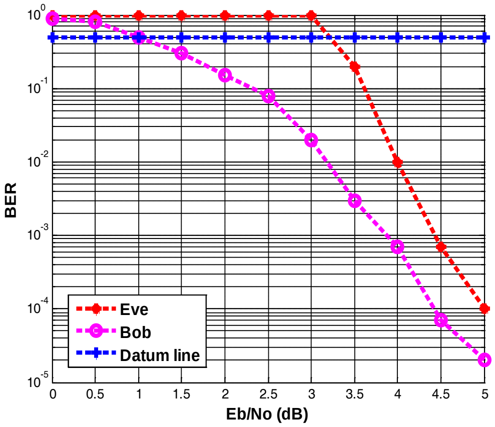


Figure 5. BER without artificial noise

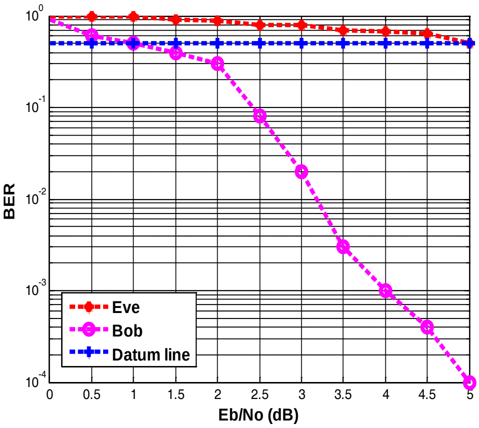


Figure 6. BER with artificial noise

Figure 4 shows the comparison of BP and TEP algorithms in decoding performance over the legal channel. It is obvious that, with the increase of SNR E_b/N_0, the proposed TEP algorithm outperforms the BP algorithm with lower BER. This is because the TEP algorithm can effectively cope with the decoding loop which is a main factor causing the decoding errors in the BP algorithm.

In Fig. 5, we analyze the BER performance of the receiver Bob and the eavesdropper Eve without the artificial noise. Thus, their BER is mainly dependent on the decoding performance. Because the wiretap channel is unknown, the numerical results are used to evaluate the channel condition. When E_b/N_0 is less than 3dB, the BER of Eve is higher than 0.5 (i.e., the Datum line). According to the weak security theorem [10], Eve will always fail to recover the information with such higher BER, thus the security of information transmission is guaranteed.

Figure 6 displays the BER performance of Bob and Eve in order to evaluate the effectiveness of artificial noise. Due to the introduction of artificial noise, the quality of eavesdropping channel is significantly worse than the legal channel. Thus, we can observe that the BER of Eve remains higher than 0.5 (i.e., the Datum line) even when E_b/N_0 reaches to 5 dB, which satisfies the requirement of secure information transmission.

6 Conclusion

In this paper, we have proposed a new physical layer security enhanced system. In the system, an effective artificial noise technique has been proposed to guarantee the security of transmitted information by selecting the optimal relay and cooperative jamming. A novel TEP decoder has also been proposed to mitigate the performance loss in reliability by breaking the decoding loop which is a main reason for decoding errors in traditional methods. Simulation results have demonstrated that the proposed system is effective in enhancing physical layer security with fewer decoding errors.

References

1. K. Andrews, S. Dolinar, J. Thorpe. Encoders for block-circulant LDPC codes, Information Theory, in Proc. IEEE ISIT, 2015: 2300-2304.
2. J. Ha, D. Klinc, J. Kwon, et al. Layered BP decoding for rate-compatible punctured LDPC codes, IEEE Communications Letters, 2007, 11(5): 440-442.

3. M. Baldi. Coding with scrambling, concatenation, and HARQ for the AWGN wire-tap channel: a security gap analysis, IEEE Transactions on Information Forensics and Security, 2012, 7(3): 883-894.
4. M. Baldi, M. Bianchi, F. Chiaraluce. Increasing physical layer security through scrambled codes and ARQ, in Proc. ICC, 2011: 1-5.
5. S. Bellini, M. Ferrari, A. Tomasoni, et al. LDPC design for block differential modulation in optical communications, IEEE/OSA Journal of Lightwave Technology, 2015, 33(1):78 - 88.
6. W. K. Harrison, J. Almeida, S. W. McLaughlin, J. Barros. Physical-layer security over correlated erasure channels, in Proc. IEEE ICC, 2012, pp. 888-892.
7. Y. Zhao, M. Xie, S. Yong. Optimal relay selection and cooperative jamming strategy in physical layer security, Journal of Electronic Science, 2015, 43 (4): 791-794.
8. W. K. Harrison, P. Boyce. Parity modifications and stopping sets in high-rate codes for physical-layer security, in Proc. CNS, 2014: 115-120.
9. K. P. Peppas, N. C. Sagias, A. Maras. Physical layer security for multiple-antenna systems: a unified approach, IEEE Transactions on Communications, 2016, 64(1): 314-328.
10. J. P. Vilela, J. Sa Sousa. Physical-layer security against non-degraded eavesdroppers, in Proc. IEEE Globecom, 2015: 1-6.