A Novel Scheme for Joint Error Control and Dynamic Security Coding Using Puncturing Mechanism

Dinh Van Linh[1,2] and Vu Van Yem[1]
[1] Hanoi University of Science and Technology, Hanoi 11615, Vietnam
[2] Academy of Cryptography Techniques, Hanoi 12511, Vietnam
Email: vanlinh@actvn.edu.vn; yem.vuvan@hust.edu.vn

Abstract —Reliability and confidentiality are two crucial aspects of digital wireless communications. Due to open-air communication, wireless communication is easy to be eavesdropped on. This paper proposes a scheme allowing a joint error control and dynamic security coding. This scheme consists of combining encryption and Turbo coding in only one step. The secret key derived from channel parameters between legitimate users is used as a seed for Data Encryption Standard (DES) generator and Advanced Encryption Standard (AES) generators with different key lengths to generate a pseudo-random bit sequence. The pseudo-random bit sequence is used to control the puncturing mechanism in the Turbo code. The simulations are carried out in Additive White Gaussian Noise (AWGN) and Rayleigh channels. The simulation results show that the proposed scheme in the AES generator with a high key length outperforms the conventional Turbo code in error correction capability. Moreover, the proposed scheme allows dynamic security coding without changing the hardware structure of the transceiver devices.

Index Terms—Secret key, turbo code, error control coding, puncturing mechanism, DES, AES

I. Introduction

Cryptography is used to protect information from interception by illegal users in communication channels. Traditionally, a cryptosystem is required for data confidentiality. In general, communication devices secure messages using either symmetric-key encryption schemes such as Data Encryption Standard (DES), Advanced Encryption Standard (AES), or asymmetric-key encryption schemes such as Rivest–Shamir–Adleman (RSA) to provide high security for information communications. Symmetric encryption can be more appropriate for devices with limited resources [1], especially in wireless communication systems. However, current encryption techniques are usually sensitive to noise, a few transmission errors may cause the encryption system to collapse. Therefore, in conventional secure communication systems, channel coding is employed at the physical layer for error correction before transmission [2].

Turbo code is an error control coding introduced by Berrou *et al* [3]. By the mean of an iterative soft input soft output decoder, involving a maximum a posteriori probability (MAP) algorithm, the Turbo-code performances are close to the Shannon limit (0.5 dB). The main components of the Turbo encoder consist of two Recursive Systematic Convolutional (RSC) encoders: RSC1 and RSC2, which are connected by an interleaving block. In the puncturing mechanism of a normal Turbo code, the deleted bits are usually located periodically.

The encryption systems have been designed independently with error correction coding. In recent years, there have been some studies on encryption and error correction coding techniques [4]–[12] in a single step, most of the studies have been based on controlling the interleaver and the puncturing mechanism of Turbo code. The authors in [4] proposed a scheme of joint error correction and encryption, but the error correction code in the scheme is based on hard decision and the error-correcting capability is low. The approaches proposed in [5], [6] were based on controlling the puncturing mechanism, their performances are as good as that of using the normal Turbo code at the same coding rate. However, since the secret key is fixed, the unauthenticated users may deduce the secret key or even the original information.

Sahnoune *et al* developed the chaotic interleaver for Turbo code to obtain a lower latency and complexity of the implementation [8]. This method also increases the reliability and confidentiality of the communication system. In 2019, the authors in [11] proved that the processing time decreases more 10% than the conventional block interleaver at the same time while maintaining the bit error rate (BER) in an acceptable range by implementing sub interleavers. In other methods proposed in [7], [12], the BER performances are slightly reduced when the Turbo code's interleaver is adjusted. In all the studies we considered above, the simulations were only performed in the Additive White Gaussian Noise (AWGN) channel.

Some researchers combined the Turbo code in the AES cryptography techniques to keep data confidentiality and increase data reliability and accuracy [13]–[15]. However, the complexity of these algorithms are issues that need to be addressed.

This paper proposes an encryption and coding scheme based on a dynamic puncturing mechanism. It combines encryption and Turbo coding in a single step. To do this, the puncturing mechanism is controlled by a pseudo-random bit sequence that is based on a dynamic secret key. The secret key can be changed by deploying the

Manuscript received April 15, 2022; revised October 27, 2022.
Corresponding author email: yem.vuvan@hust.edu.vn
doi:10.12720/jcm.17.11.948-955

measurement of the propagation channel instead of depending upon the previous keys. This key generation technique results in a better security mechanism because of the difficulties for brute force attackers to attempt all possible keys in a short time. The dynamic secret key is used as a seed to generate a pseudo-random bit sequence that controls the Turbo convolutional code's puncturing mechanism. The pseudo-random bit sequence is generated by using DES and AES 128/192/256-bit generators. Consequently, the hardware structure of the transceiver devices remains the same, allowing secured transmissions in terms of error and secrecy without additional cost.

The paper is organized as follows, Section II presents the proposed Turbo-based encryption and coding scheme. Simulation results are shown in Section III and finally, Section IV concludes this paper.

II. The Proposed Turbo-Based Encryption and Coding Scheme

A. Channel Model

Firstly, we consider the communication scheme (Fig. 1). Two legitimate users, Alice and Bob, communicate with each other in the presence of an eavesdropper – Eve.

In this scenario, $\mathbf{h}_{ab}$ is the transmission channel vector from Alice to Bob while $\mathbf{h}_{ba}$ is the channel vector from Bob to Alice. Eve observes Bob and Alice via the propagation channels $\mathbf{h}_{eb}$ and $\mathbf{h}_{ea}$. We assume that Alice, Eve, and Bob use compatible equipment based on the same transmission norm. Therefore, they use the same source coding, the same channel coding, and the same modulation. Eventually, they also share the same pilot bits for Channel State Information identification and encryption protocol if they exist.

Due to the reciprocal properties of the channel, we may assume that Alice and Bob in Fig. 1 have $\mathbf{h}_{ab} = \mathbf{h}_{ba}$ which are forward and reverse channels for legitimate users [16]. On the other hand, the propagation channels by the mean by whom Eve observes Alice and Bob, $\mathbf{h}_{eb}$ and $\mathbf{h}_{ea}$, are assumed to be orthogonal to both $\mathbf{h}_{ab}$ and $\mathbf{h}_{ba}$, as is the case for the wireless propagation channel when the distance between Eve and Bob (or Eve and Alice) exceeds some hundreds of wavelength. Alice and Bob estimate their channels $\hat{\mathbf{h}}_{ab}$ and $\hat{\mathbf{h}}_{ba}$ correspondingly in the following forms (1).

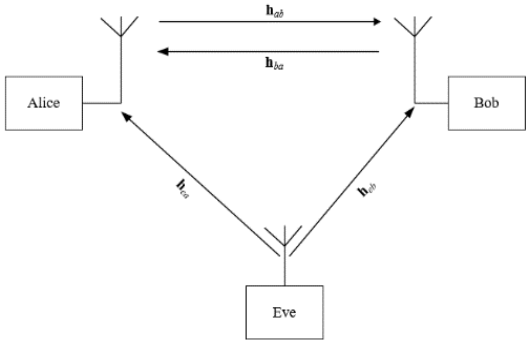

Fig. 1. Channel model with reciprocal properties

$$\begin{cases} \mathbf{h}_{ab} = \mathbf{h}_{ab} + \mathbf{n}_{ab} \\ \mathbf{h}_{ba} = \mathbf{h}_{ba} + \mathbf{n}_{ba} \end{cases} \quad (1)$$

Eve eavesdrops on Alice and Bob by the mean of the wiretap-channels $\hat{\mathbf{h}}_{ea}$ and $\hat{\mathbf{h}}_{eb}$.

$$\begin{cases} \mathbf{h}_{ea} = \mathbf{h}_{ea} + \mathbf{n}_{ea} \\ \mathbf{h}_{eb} = \mathbf{h}_{eb} + \mathbf{n}_{eb} \end{cases} \quad (2)$$

In (1) and (2), $\mathbf{n}_{ab}$, $\mathbf{n}_{ba}$, $\mathbf{n}_{ea}$, and $\mathbf{n}_{eb}$ are estimation errors that Alice, Bob, and Eve have during imperfect estimation. Alice and Bob extract their channel parameters to get the secret key [17], [18].

We assume that from this channel model, Alice and Bob apply a common quantization function $f(.)$ to generate their own secret keys K_{ab} and K_{ba} from the estimated Complex Impulse Response $\hat{\mathbf{h}}_{ab}$ and $\hat{\mathbf{h}}_{ba}$.

$$\begin{cases} K_{ab} = f(\mathbf{h}_{ab}) \\ K_{ba} = f(\mathbf{h}_{ba}) \end{cases} \quad (3)$$

Due to the reciprocal properties of the channel, the final secret key is $K=K_{ab}=K_{ba}$ (Fig. 2). The distillation key algorithm is assumed to be robust to $\mathbf{n}_{ab}$, $\mathbf{n}_{ba}$.

In the same way, the quantization function $f(.)$ is used by Eve to calculate her secrete keys from $\hat{\mathbf{h}}_{ea}$ and $\hat{\mathbf{h}}_{eb}$.

$$\begin{cases} Kea = f(\mathbf{h}_{ea}) \\ Keb = f(\mathbf{h}eb) \end{cases} \quad (4)$$

This secret key is modified according to the change of the channel measurement and a common agreement between legitimate users. Meanwhile, Eve experiences independent statistics of the channel between Alice and Bob. It can be considered that these transmission links only differ in their propagation. Thus, Eve can't distill the right secret key [16]. This secret key is used to encrypt dynamically the information transmissions between Bob and Alice.

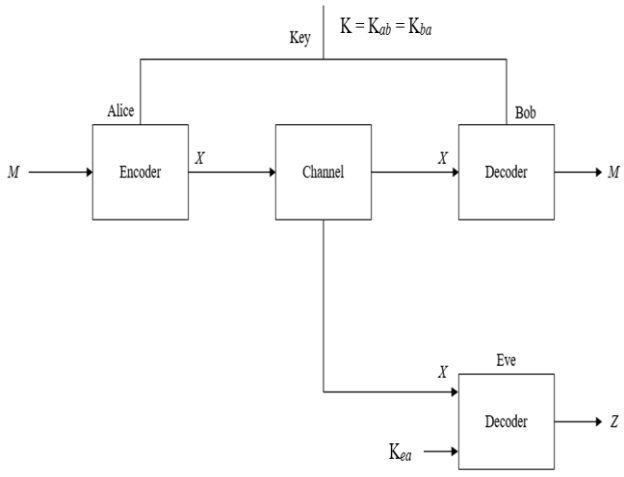

Fig. 2. Secured transmissions between Alice and Bob

B. Proposed Encryption and Coding Scheme

In the Turbo coding scheme, the puncturing mechanism of the encoder and the decoder must be identical. Now we use a pseudo-random bit stream to control the puncturing mechanism, only the legal receiver with the same pseudorandom bit stream can classify X_i, Y_{1i}, Y_{2i} correctly with the same puncturing mechanism, and then decode successfully. By this means, the information will be encrypted.

On the other hand, an inappropriate puncturing mechanism will reduce the error correction capability of the Turbo code. In order to ensure a good BER performance, the reserved parity bits should be irrelevant as much as possible.

We propose an encryption and coding scheme based on the dynamic puncturing mechanism of the Turbo code. In one coding step, this scheme provides good security and high error correction capability. The encryption and decryption processes are described as follows.

- Encryption process

In Fig. 3, we propose a scheme that jointly uses the Turbo code for error control and dynamic encryption. A pseudo-random number generator (PRNG) uses the deterministic algorithms DES and AES to generate a pseudo-random bit sequence from the secret key. The DES and AES are considered to ensure the confusion and diffusion between the input and output of the algorithm [19]. These pseudo-random bit sequences will control the puncturing mechanism in the Turbo code.

Assuming the length of the RSC encoder is K, the memory is $M = K$-1, and the generators of the two RSC encoders are $G_1 = [g_{10}, g_{11}, ..., g_{1,K-1}]$ and $G_2 = [g_{20}, g_{21}, ..., g_{2,K-1}]$, respectively. Then the outputs of the k^{th} input bit d_k are:

$$X_k = d_k \tag{5}$$

$$Y_{1k} = \sum_{i=0}^{K-1} g_{1i} d_{k-i} \quad \text{mod} 2, \tag{6}$$

$$Y_{2k} = \sum_{i=0}^{K-1} g_{2i} d_{k-i} \quad \text{mod} 2. \tag{7}$$

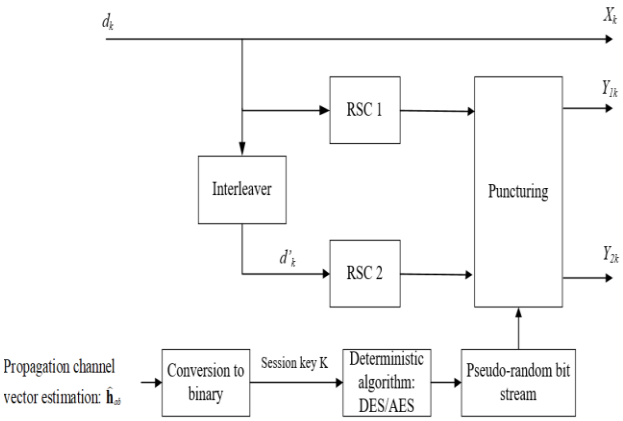

Fig. 3. Flowchart of the encryption and coding process

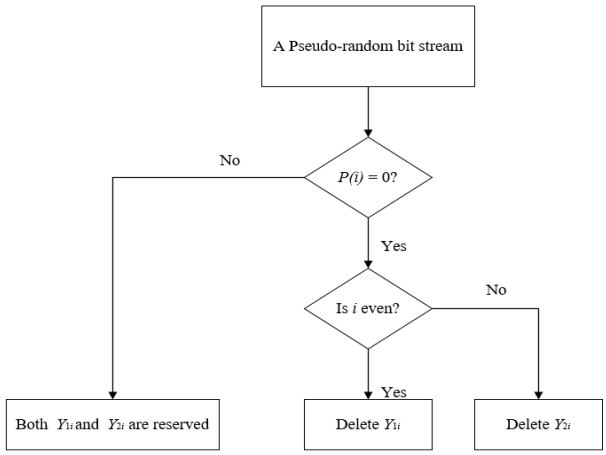

Fig. 4. Flowchart of the dynamic puncturing mechanism

In the proposed encryption and coding scheme, the following steps are implemented:

Step 1: After having the secret key K from channel parameters, the transmitter uses the secret key K as a seed input to the DES-PRNG and AES-PRNG 128/192/256-bit to generate a pseudo-random bit stream P. This stream of bits then controls the puncturing mechanism.

Step 2: If $P(i) = 0$ and i is even, the parity bit in the first RSC convolutional component Y_{1i} would be deleted. On the other hand, if $P(i) = 0$ and i is old, the parity bit in the second RSC convolutional component Y_{2i} would be eliminated. Meanwhile, if $P(i) = 1$, both Y_{1i} and Y_{2i} are reserved. Fig. 4 shows the flowchart of this process.

- Decryption process

The receiver also has the secret key K from channel parameters. During the decryption, the pseudo-random bit stream P is generated from DES-PRNG and AES-PRNG 128/192/256-bit by using the secret key K. X_i, Y_{1i}, and Y_{2i} are classified in the received sequence according to P. Then the receiver sends them to a Turbo decoder. Among the three kinds of the received bits, X_i and Y_{1i} are input to the first decoder, and X_i and Y_{2i} are input to the second decoder. After that, the Turbo decoder will start the iterative decoding process.

In the Turbo decoding process, the Log-MAP algorithm is implemented. Let us give some definitions firstly below.

d_k: the k^{th} original information bit

S_k: the state of the k^{th} note of the decoder

R: the vector of all the received bits in a frame

d_k : the k^{th} output of the decoder after judgment

In a Log-MAP decoding algorithm, the decoder decides $d_k = 1$ if $P(d_k = 1|r) > P(d_k = 0|r)$, and decides $d_k = 0$ otherwise. Therefore we compute the Logarithm of Likelihood Ratio $L(d_k)$ of the k^{th} input bit d_k and judge d_k by it.

$$L(d_k) = \log\left[\frac{P(d_k = 1|observation)}{P(d_k = 0|observation)}\right] \tag{8}$$

where $P(d_k = i|observation)$, i = 0 or 1, is the *a posteriori probability* (APP) of the input bit d_k.

In addition, a conditional probability can be used to represent the APP, therefore (8) becomes:

$$L(d_k)=\log\left[\frac{\sum_m P(d_k=1,S_k=m|R)}{\sum_m P(d_k=0,S_k=m|R)}\right] \quad (9)$$

In (9), $P(d_k=i,S_k=m|R)$ is the joint probability of d_k and state S_k under the condition of the received sequence R. This soft output from each constituent decoder is separated into three sections: the extrinsic output L_{e_k} which is new information derived by the current stage of decoding, a weighted version of the systematic input L_{s_k}, and a copy of the input *a priori* information L_{a_k}.

$$L(u_k)=L_{e_k}+L_{s_k}+L_{a_k} \quad (10)$$

The Turbo decoder judges the result d_k according to $L(d_k)$ after several iterations.

In the decoding process, if the receiver uses the wrong secret key to build sequence P, the eavesdropper will confuse X_i, Y_{1i}, and Y_{2i}, and the decoding will fail. Only a legal receiver can generate the right P, which is equal to that of the transmitter. Then he will extract X_i, Y_{1i}, and Y_{2i} accurately and decode them successfully. By this means, successful information decryption can be achieved.

III. Simulation Results

In order to examine the impact of the proposed encryption and coding scheme on the BER of the single input single output (SISO) system, we consider the union bound to the bit error probability [20]. The puncturing mechanism is controlled by the pseudo-random bit sequences generated from the DES and AES 128/192/256-bit generators (see subsection II-B). All simulations are performed in both AWGN and Rayleigh channels by using MATLAB software, while the parameters of the conventional Turbo code are defined in Table I.

When the secret key is used as the seed of the DES/AES generators, to stay compatible with DES/AES standards, the Turbo code has the following parameters (Table II and Table III).

TABLE I: Parameters of the Conventional Turbo Code

Item	Parameter
Generate Matrix	g = [1 1 1;1 0 1]
Frame length	400 bits
Iteration Number	5
Decoding algorithm	MAP

TABLE II: Parameters of des Pseudo-Random Generator Controlling the Puncturing Mechanism

Item	Parameter
Generate Matrix	g = [1 1 1;1 0 1]
Frame Size	64 bits
Key length	56 bits
Iteration Number	5
Decoding algorithm	MAP

TABLE III: Parameters of aes Pseudo-Random Generator Controlling the puncturing Mechanism in SISO System

Item	Parameter
Generate Matrix	g = [1 1 1;1 0 1]
Frame Size	128/192/256 bits
Key length	128/192/256 bits
Iteration Number	5
Decoding algorithm	MAP

Firstly, we consider the channel is affected by AWGN. In the simulations, only 5 iterations of the iterative-decoding processes are represented at Eb/N0 ranging from 0 to 4 dB. It can be concluded from figures 5, 6, 7, 8, and 9 that a fast convergence after 3 iterations of the Turbo decoding. Consequently, in order to have a reasonable processing time, only 5 iterations will be performed in all the simulations involving a Turbo code.

Fig. 5 shows the BER performance of the conventional Turbo code for different values of Eb/N0 between 0 to 4 dB and 5 iterations of the Turbo decoder. After 5 iterations, the BER decreases from $3.4\text{x}10^{-4}$ to $2.4\text{x}10^{-6}$ at Eb/N0 = 4 dB. Fig. 6 displays the BER performance of the Turbo code when the puncturing mechanism is controlled by a pseudo-random bit sequence generated from the DES generator. The system reaches 10^{-3} to $4.3\text{x}10^{-5}$ at Eb/N0 = 4 dB for BER. Compared to Fig. 5, significant degradation of the performance can be observed, due to the variation of the code rate induced by the puncturing.

Fig. 7 depicts the BER performance in the case of a puncturing mechanism controlled by a pseudo-random bit sequence generated from the AES 128-bit generator. It can see that the BER performances are better than the case of the DES generator. Compared to the curves presented in Fig. 5, it is seen that no significant decrease could be noticed.

Fig. 8 illustrates the BER performance of the system when using the AES 192-bit generator. It can be observed that the performances are slightly improved when compared to the case of the AES 128 bit. Within 5 iterations, the BER performance declines from $2.5\text{x}10^{-4}$ to $2.2\text{x}10^{-6}$ at Eb/N0 = 4 dB.

Fig. 9 shows the performances of the AES 256-bit generator. It is clear that the AES 256-bit generator provides better performance than the AES 192-bit generator. At Eb/N0 = 4 dB and 5^{th} iteration, the system reaches the BER = 10^{-6}. Thus, the BER performance of the AES-256 bit generator improves twice as much as that of the conventional Turbo code.

Compared to the previous work reported in [7] for the AWGN channel, we can see that the DES generator of our proposed method also provides a considerable degradation of the BER performance. In [7], the authors used the key length of 400 bits to control directly the puncturing mechanism of the Turbo code, but a small degradation of the performance is observed when compared to the conventional Turbo code. Therefore, the AES 192/256-bit generators of our Turbo-based encryption and coding scheme are greater than that reported in [7].

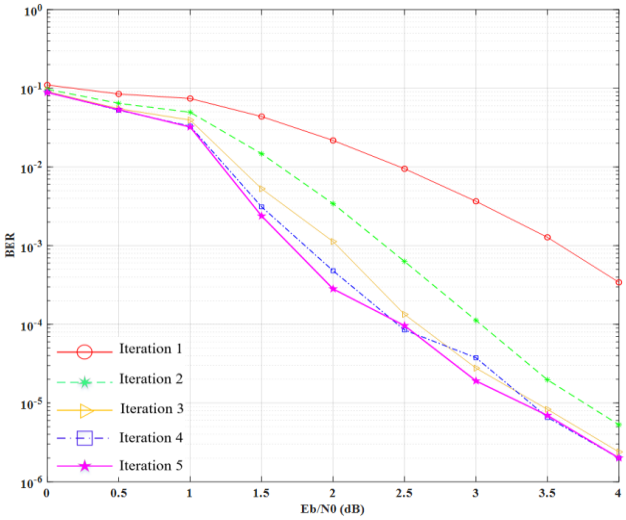

Fig. 5. BER performance for the conventional Turbo code in AWGN channel

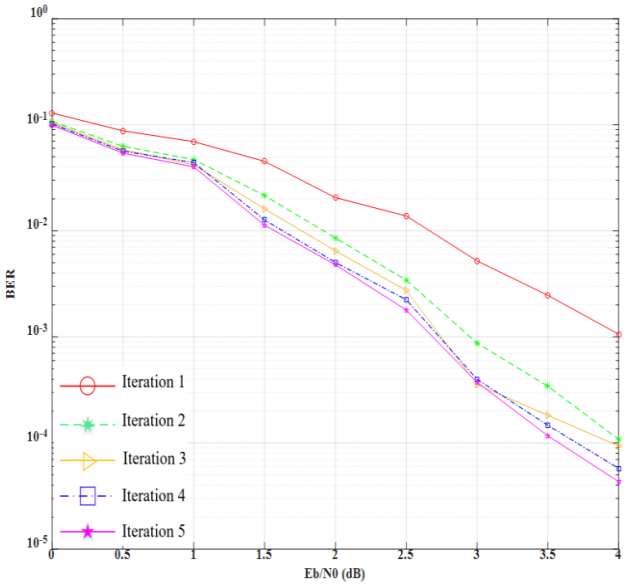

Fig. 6. BER performance for DES generator in AWGN channel

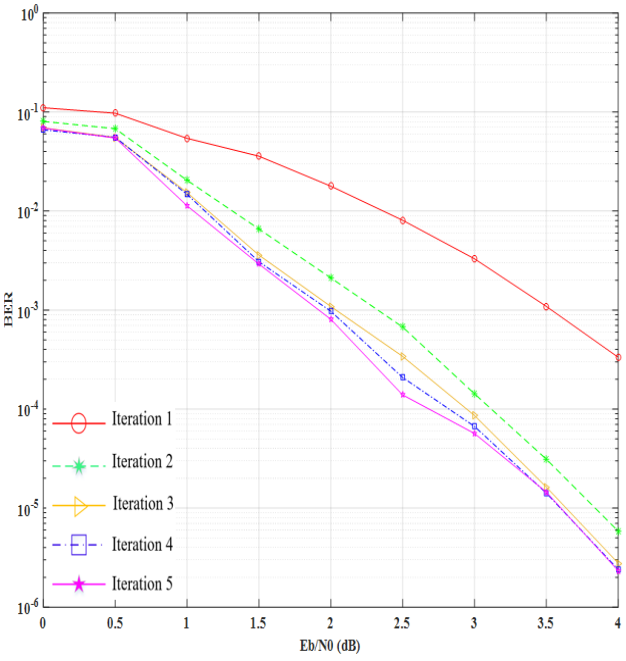

Fig. 7. BER performance for AES 128-bit generator in AWGN channel

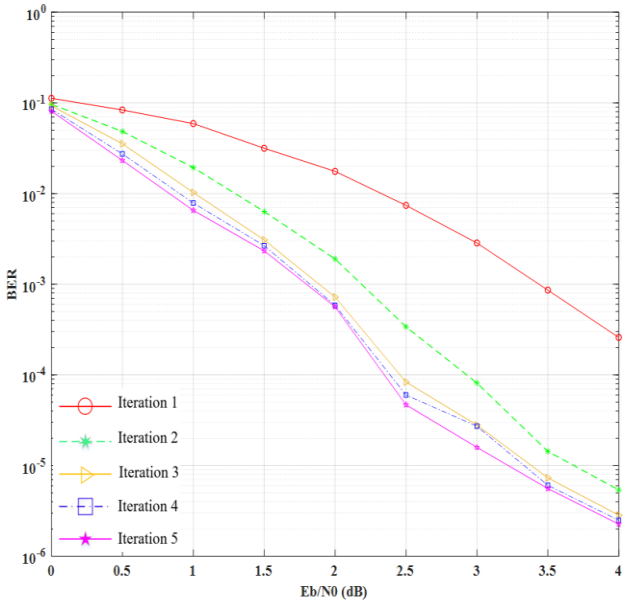

Fig. 8. BER performance for AES 192-bit generator in AWGN channel

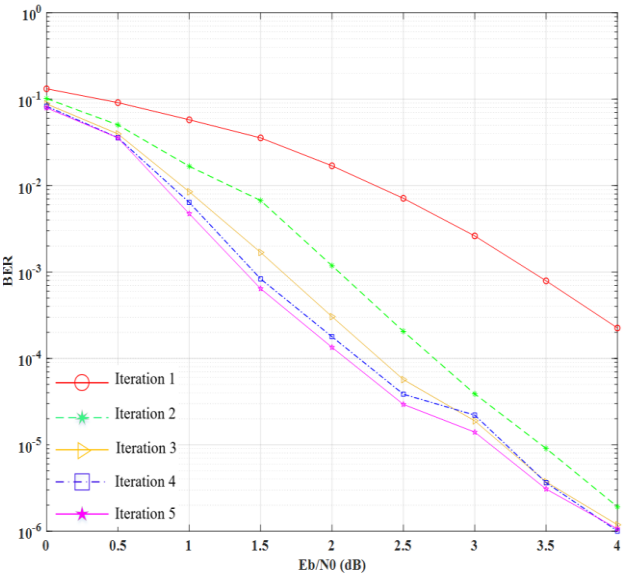

Fig. 9. BER performance for AES 256-bit generator in AWGN channel

Next, we perform in the Rayleigh channel with five simulations such as the conventional Turbo code, the puncturing mechanism of the Turbo code controlled by the DES generator, and the AES 128/192/256-bit generators, respectively. Figures 10, 11, 12, 13, and 14 display the BER performances for different values of Eb/N0 between 0 to 6 dB and five iterations of the Turbo–decoder. It is shown that the BER performances of five iterations are the same from 0 to 1 dB, after that the BER decreases rapidly as Eb/N0 increases. The system affected by the Rayleigh channel also converges after 3 iterations of the Turbo-decoder. Comparing the results obtained in the AWGN channel can see that the Rayleigh channel offers a remarkable decrease in the BER performance. After 5 iterations, the BER performances only reach from $5x10^{-3}$ to 10^{-2} for all the cases at Eb/N0 = 4 dB. It is similar to the AWGN channel, the comparison with the conventional Turbo code (Fig. 10) shows a considerable reduction in the BER performance of the

DES generator (Fig. 11) and no change in the BER performance of the AES 128-bit generator (Fig. 12). For the same Eb/N0 of 6 dB at the 5th iteration, the BER obtains 8.1×10^{-4} for the DES generator, and about 2.5×10^{-5} for both the conventional Turbo code and AES 128-bit generator, respectively.

In Fig. 13, and Fig. 14, it is observed that the AES 192/256-bit generators give better performance than the conventional Turbo code. It can be concluded that the system's performance increases as the key length of the AES generator rises. After 5 iterations and Eb/N0 is equal to 6 dB, the system can achieve BER = 1.8×10^{-5} for AES 192-bit generator and 6.2×10^{-6} for AES 256-bit generator, respectively. Therefore, the BER of the AES 256-bit generator can reduce four times compared to the conventional Turbo code. Consequently, the Turbo code with the puncturing mechanism controlled by the AES 256-bit generator could be a good candidate for joint encryption and channel coding.

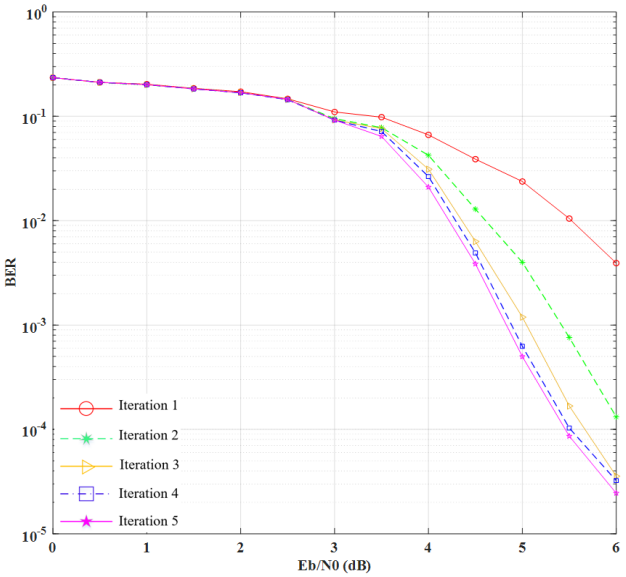

Fig. 10. BER performance for the conventional Turbo code in Rayleigh channel

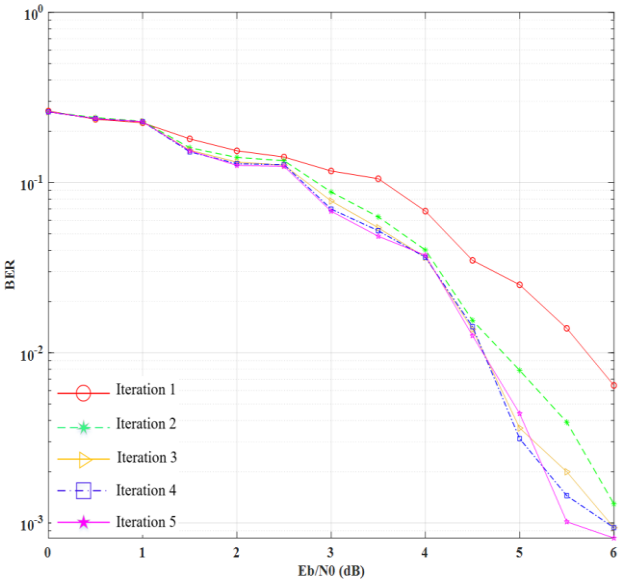

Fig. 11. BER performance for DES generator in Rayleigh channel

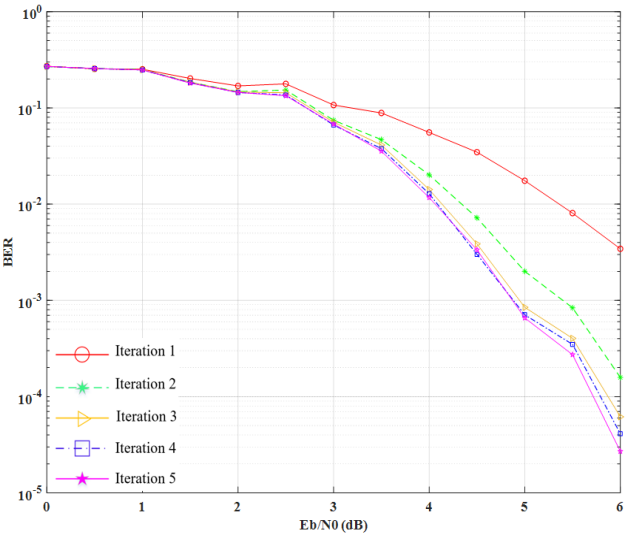

Fig. 12. BER performance for AES 128-bit generator in Rayleigh channel

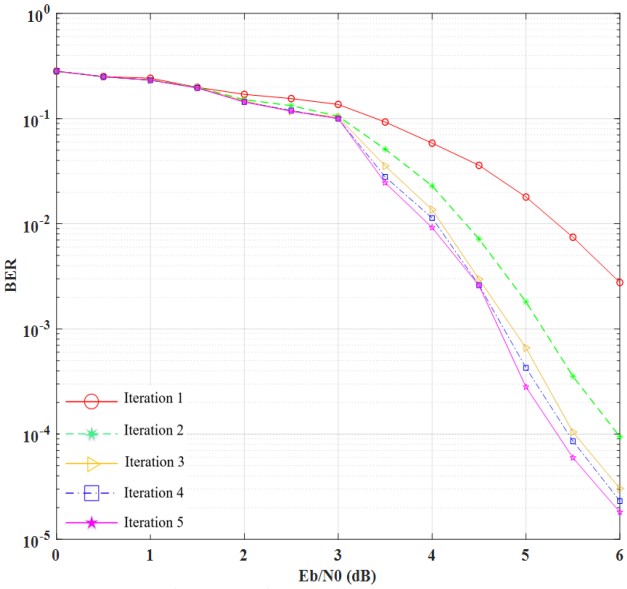

Fig. 13. BER performance for AES-192 bit generator in Rayleigh channel

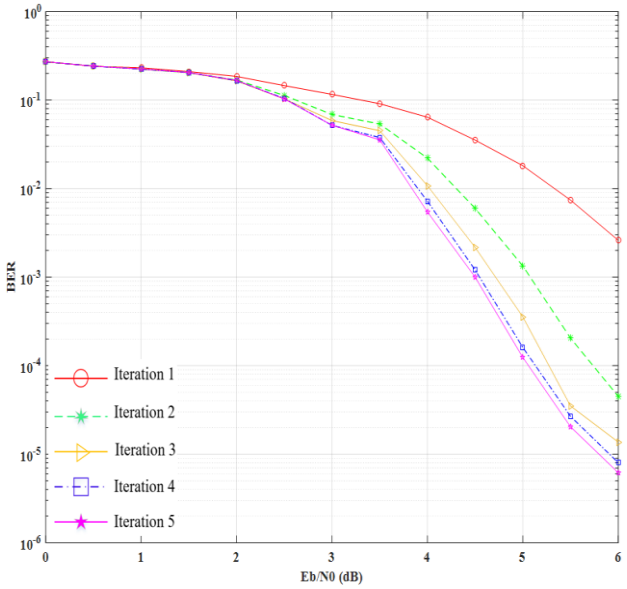

Fig. 14. BER performance for AES 256-bit generator in Rayleigh channel

IV. Conclusion

In this paper, we propose an encryption and coding scheme based on Turbo code. The puncturing mechanism of the Turbo code is controlled by a pseudo-random bit sequence generated by using the DES or the AES generators with dynamic secret keys. The secret key is the distillation of the reciprocal channel state information of the two legitimate users. A great advantage of this encryption and coding scheme is that the hardware structure of the transceiver devices remains the same.

The simulations are carried out to show the error correction capability of the proposed encryption and coding method over AWGN and Rayleigh channels. We can conclude from the results that the system converges quickly after 3 iterations. The performance of this encryption and coding scheme based on the AES generators is more efficient than that of the DES generator. Moreover, compared to the conventional Turbo code, the AES 128-bit generator provides the same BER, while using the AES 192/256-bit generators can reduce the BER performance four times. The proposed encryption and coding scheme would achieve the best BER performance when using the AES 256-bit generator. The proposed method not only improves the error correction performance of the communication system but also increases the confidentiality performance of the wireless communication system. It has a wide range of potential applications in advanced secure wireless communication systems. Especially, our proposed method is suitable for military wireless communication systems.

Conflict of Interest

The authors declare no conflict of interest.

Author Contributions

Dinh Van Linh did the simulation, and analyzed the data. Vu Van Yem organized the content of the paper and checked the simulation and theoretical results. Dinh Van Linh and Vu Van Yem wrote the paper and approved the final version.

Acknowledgment

Dinh Van Linh is funded by Vingroup JSC and supported by the Master, Ph.D. Scholarship Programme of Vingroup Innovation Foundation (VINIF), Institute of Big Data, code VINIF.2021.TS.144.

This work is carried out in the framework of the project "Nghiên cứu thiết kế chế tạo hệ thống IoT tự động quan trắc và cảnh báo các thông số môi trường nước ứng dụng trong nuôi trồng thủy sản tại tỉnh Kiên Giang". The authors would like to thank the Department of Science and Technology of Kien Giang, Vietnam for supporting this research.

References

[1] J. C. Gonzalez-Arango, D. C. Ocampo-Munera, L. F. Castano-Londono, G. D. Goez-Sanchez, and R. A. Velasquez-Velez, "Performance evaluation of symmetric cryptographic algorithms in resource constrained hardware for wireless sensor networks," *IEEE Lat. Am. Trans.*, vol. 19, no. 10, pp. 1632–1639, 2021.

[2] K. Bagheri, T. Eghlidos, M. R. Sadeghi, D. Panario, and H. Khodaiemehr, "A joint encryption, channel coding and modulation scheme using QC-LDPC lattice-codes," *IEEE Trans. Commun.*, vol. 68, no. 8, pp. 4673–4693, 2020.

[3] C. Berrou, A. Glavieux, and P. Thitimajshima, "Near SHANNON limit error-correcting coding and encoding: Turbo-codes," in *Proc. IEEE Int. Conf. Commun.*, no. 1, 1993, pp. 1064–1070.

[4] D. Gligoroski, S. J. Knapskog, and S. Andova, "Cryptcoding - Encryption and error-correction coding in a single step," in *Proc. Int. Conf. Secur. Manag. SAM'06*, 2006.

[5] A. Payandeh, M. Ahmadian, and M. R. Aref, "Adaptive secure channel coding based on punctured turbo codes," *IEE Proc. Commun.*, vol. 153, no. 2, pp. 313–316, 2006.

[6] Q. Mao and C. Qin, "A novel turbo-based encryption scheme using dynamic puncture mechanism," *J. Networks*, vol. 7, no. 2, pp. 236–242, 2012.

[7] T. H. T. Nguyen and J. P. Barbot, "Joint error control and dynamic security coding," in *Proc. Int. Conf. Adv. Technol. Commun.*, 2013, pp. 285–290.

[8] A. Sahnoune and D. Berkani, "On the performance of chaotic interleaver for turbo codes," *SN Appl. Sci.*, vol. 3, no. 1, pp. 1–9, 2021.

[9] T. H. M. Soliman, F. Yang, and S. Ejaz, "A proposed chaotic-switched turbo coding design and its application for half-duplex relay channel," *Discret. Dyn. Nat. Soc.*, vol. 2015, 2015.

[10] F. J. Escribano, S. Kozic, L. López, M. A. F. Sanjuán, and M. Hasler, "Turbo-like structures for chaos encoding and decoding," *IEEE Trans. Commun.*, vol. 57, no. 3, pp. 597–601, 2009.

[11] M. R. Devi, K. Ramanjaneyulu, and B. T. Krishna, "Performance analysis of sub-interleaver based turbo codes," *Cluster Comput.*, vol. 22, pp. 14091–14097, 2019.

[12] K. S. Arkoudogiannis and C. E. Dimakis, "Performance analysis of the odd-even uniform interleaver for turbo codes," *IET Commun.*, vol. 13, no. 16, pp. 2469–2477, 2019.

[13] D. Kuswanto and A. Rachmad, "Combination scheme of AES encryption and error correction turbo code for cryptography of cloud storage," in *Proc. Internaltional Conference on Science and Technology*, no. 1, 2018.

[14] D. Kuswanto, "Performances Combination Schemes AES-Turbo Code Based-on Keys Length," in *Proc. IOP Conf. Ser. Mater. Sci. Eng.*, 2021, vol. 1125, no. 1, p. 012047.

[15] T. J. Jeyaprabha and G. Sumathi, "A pragmatic study on hybrid-crypto-coding schemes for secure data access," *J. Internet Technol.*, vol. 22, no. 2, pp. 371–384, 2021.

[16] X. Lu, J. Lei, W. Li, K. Lai, and Z. Pan, "Physical layer encryption algorithm based on polar codes and chaotic sequences," *IEEE Access*, vol. 7, pp. 4380–4390, 2019.
[17] N. Aldaghri and H. Mahdavifar, "Physical layer secret key generation in static environments," *IEEE Trans. Inf. Forensics Secur.*, vol. 15, pp. 2692–2705, 2020.
[18] J. Zhang, T. Q. Duong, A. Marshall, and R. Woods, "Key generation from wireless channels: A review," *IEEE Access*, vol. 4, pp. 614–626, 2016.
[19] B. Schneier, *Applied Cryptography (2nd ed.): Protocols, Algorithms, and Source Code in C*, vol. 1, no. 69. 1995.
[20] J. Liu, M. Zhang, C. Wang, R. Chen, X. An, and Y. Wang, "Upper bound on the bit error probability of systematic binary linear codes via their weight spectra," *Discret. Dyn. Nat. Soc.*, vol. 2020, 2020.

Dinh Van Linh was born in Vietnam, in 1991. He received the Bachelor's degree from Politehnica University of Bucharest, Romania, in 2015 and the Master's degree from Hanoi University of Science and Technology, in 2020. He is currently pursuing a Ph.D. degree at the Hanoi University of Science and Technology. His research interests include physical layer security, channel coding, and wireless communication technology.

Vu Van Yem was born in Vietnam in 1975. He received the Bachelor's and Master's Degree from the Hanoi University of Science and Technology, Vietnam. He was awarded Doctor of Philosophy in Electronics and Telecommunication Engineering from Télécom ParisTech in 2005. He is currently working as a professor in the School of Electrical and Electronic Engineering, Hanoi University of Science and Technology. His main research interests are wireless communication systems, antennas, ultra-high frequency techniques.