An Integrated Signaling-Encryption Mechanism to Reduce Error Propagation in Wireless Communications: Performance Analyses

Mohammed M. Olama[1], Mustafa M. Matalgah[2] and Miljko Bobrek[3]

[1]Computational Sciences and Engineering Division
[3]Electrical and Electronics Systems Research Division
Oak Ridge National Laboratory
Oak Ridge, TN 37831
Email: {olamahussemm, bobrekm}@ornl.gov

[2]Department of Electrical Engineering
The University of Mississippi
University, MS 38677
Email: mustafa@olemiss.edu

***Abstract*— Traditional encryption techniques require packet overhead, produce processing time delay, and suffer from severe quality of service deterioration due to fades and interference in wireless channels. These issues reduce the effective transmission data rate (throughput) considerably in wireless communications, where data rate with limited bandwidth is the main constraint. In this paper, performance evaluation analyses are conducted for an integrated signaling-encryption mechanism that is secure and enables improved throughput and probability of bit-error in wireless channels. This mechanism eliminates the drawbacks stated herein by encrypting only a small portion of an entire transmitted frame, while the rest is not subject to traditional encryption but goes through a signaling process (designed transformation) with the plaintext of the portion selected for encryption. We also propose to incorporate error correction coding solely on the small encrypted portion of the data to drastically improve the overall bit-error rate performance while not noticeably increasing the required bit-rate. We focus on validating the signaling-encryption mechanism utilizing Hamming and convolutional error correction coding by conducting an end-to-end system-level simulation-based study. The average probability of bit-error and throughput of the encryption mechanism are evaluated over standard Gaussian and Rayleigh fading-type channels and compared to the ones of the conventional advanced encryption standard (AES).**

Keywords—cryptography; quality of service (QoS); throughput; bit-error rate; error correction coding; Rayleigh fading; advanced encryption standard (AES); Monte Carlo simulations

I. INTRODUCTION

Transmitting information over a wireless link poses a threat to information security due to inherent interception-type vulnerability of the wireless channel [1]. Thus, intercepting signals from wireless media is the reality that makes wireless communication accessible to intruders. Consequently, it is harder to maintain the confidentiality, integrity, and authenticity (CIA) of the information traversing through wireless media. Currently, every facet of services such as vast commercial communications, national security and battle field communications, electric power delivery, and industrial and scientific research has been increasingly using wireless communications. Given the insecure nature of wireless links, CIA based on encryption is relied upon to satisfy users demand for end-to-end trustworthy communications.

Encryption, which is a technique of transforming information text to ciphertext, is the dominant protection against interception by intruders. Traditional Encryption algorithms have been designed to provide security against an attack as the main criterion, where the avalanche effect is a desirable property [2]. The avalanche effect requires that a single bit change to the ciphertext or user key must result in significant and random-looking changes to the decrypted plaintext. In general, an alteration of one ciphertext bit to the decryption device will result in an average 50% change of decrypted information bits. This fact guarantees a highly secured data transmission assuming that the channel causes no error of the information packet, and an ideal channel can offer that. However, wireless channels suffer from multipath fading and interference, which cause random errors to the ciphertext. Due to these random bit errors in the ciphertext, the avalanche effect that makes a block cipher secure also makes it prone to fading and interference of the wireless channel. Thus, ciphertext is more vulnerable to channel-induced errors than the non-encrypted text. It is shown in [1] and [3] that secret-key encryption systems multiply bit errors by more than an order of magnitude. As a result, systems that use traditional encryption algorithms degrade quality-of-service (QoS) in exchange for end-to-end data confidentiality.

Employing traditional encryption in wireless communication results in multiple drawbacks: (1) the probability of bit-error performance degrades due to fades and interference in wireless channels (avalanche effect), (2) traditional encryption requires extra bandwidth because of the

added packet overhead, and (3) the processing time required by the encryption and the decryption algorithms at the source and destination, respectively, results in communication delay. Thus, even though encryption of the plaintext achieves data security, these drawbacks add to large reduction in the effective transmission data rate (throughput). Moreover, performance deterioration due to fades in wireless channels may in some extreme conditions make it almost impossible to decrypt the data at the destination. These drawbacks motivate investigating more effective techniques to securely transmit information over wireless communication systems.

Most of the proposed solutions in the literature [3], [4] are based on developing joint encryption and error correction coding schemes that improve the QoS but require enormous overhead. In [5], the authors provide an opportunistic encryption with variable block lengths to tackle the trade-off between the security level and the throughput reduction that results from the avalanche effect. However, it requires a large number of logical operations that results in large processing delay. In [6], a quantitative study is performed to evaluate the overhead processing cycles for the logical operations required in both the encryption and decryption of an advanced encryption standard (AES) frame.

In [7], the authors propose an integrated signaling-encryption mechanism, where a small portion of an entire transmitted frame is selected for encryption and the rest is not subject to traditional encryption but goes through a designed transformation (signaling) with the plaintext of the portion selected for encryption. This mechanism eliminates the drawbacks stated herein and, therefore, it does not suffer from performance degradation in wireless channels as compared to traditional encryption techniques. In this paper, we investigate the QoS of the integrated signaling-encryption mechanism in terms of average throughput and bit-error rate (BER). We also propose to incorporate error correction coding solely on the small encrypted (not transformed) portion of the data to drastically improve the overall BER performance while not noticeably increasing the required bit-rate. We focus on validating the encryption mechanism utilizing Hamming and convolutional error correction encoding by conducting an end-to-end system-level simulation-based study. The average probability of bit-error and throughput of the encryption mechanism are evaluated over standard Gaussian and Rayleigh fading-type channels and compared to the ones of the conventional AES. The security aspect of the integrated signaling-encryption mechanism will be addressed in future works.

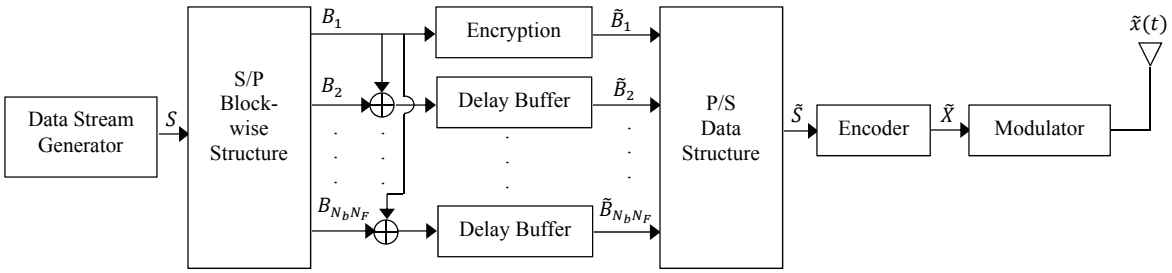
The remainder of this paper is organized as follows. Section II provides a summary of the integrated signaling-encryption mechanism proposed in [7]. In Section III, a figure of merit called the encryption ration is illustrated. Performance analyses of the integrated signaling-encryption mechanism with and without error correction encoding, in terms of overhead requirements and throughput, are provided in Section IV. Section V presents numerical results that demonstrate the performance of the encryption mechanism in terms of average probability of bit-error and throughput over standard Gaussian and Rayleigh fading-type channels. Finally, Section VI provides concluding remarks.

II. Summary of the Integrated Signalling-Encryption Mechanism

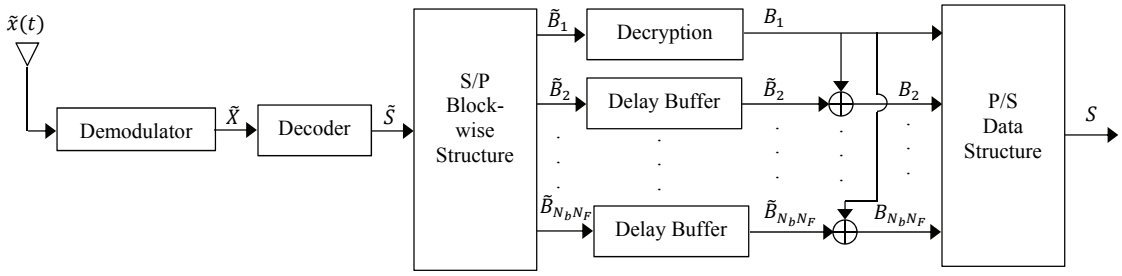
A conceptual structure for the integrated signaling-encryption transceiver is shown in Fig. 1. The transmitter structure for the system is depicted in Fig. 1(a), where the incoming serial data stream (S in bits) is mapped into parallel data blocks, each with a common pre-specified block length. The first block undergoes a highly immune standard encryption algorithm satisfying a certain security level (such as the AES). All the remaining blocks are arranged systematically and enter a bit-wise XOR (exclusive-or or exclusive-disjunction) operation with the *plaintext* of first block (before encryption). Next, the data is mapped back into a serial format to be encoded before transmission (channel encoding) to enhance transmission reliability. The data stream is then modulated using any digital modulation technique in order to be suitable for transmission. The receiver structure, as can be seen in Fig. 1(b), completely reverses all the operations performed at the transmitter in order. Also, at the receiver side, only the first block is needed to be decrypted using the appropriate traditional decryption algorithm and the decryption key, whereas all the other blocks are also bit-wise XORed with the first decrypted block (plaintext). As a result, the entire data frame is transmitted securely by only performing encryption of the first amount of data (B_1 in Fig. 1) within a frame/superframe. We would like to note here that the operations performed by the bank of XOR gates along with the serial-to-parallel (S/P) and parallel-to-serial (P/S) processes, illustrated in Fig. 1, can be simply implemented in practice by a shift-register, one XOR gate, and a switch.

For defining the data structure to be used in the algorithm, let us assume that the data sequence composed of N superframes. Each superframe contains N_F frames, and each frame consists of N_b blocks, each of size β_l bits. In the proposed encryption algorithm, the first block B_1 will be encrypted with a highly immune standard encryption algorithm such as the AES. The rest of the $N_F N_b - 1$ blocks will be used as plaintexts (i.e., will not undergo traditional encryption), but will undergo a bit-wise XOR operation with the *plaintext* of the first block. Consequently, the first block will not be recovered without performing the decryption process, which is assumed to be very immune for cryptanalysis, and therefore the other blocks will not be detected by the intruders since the *plaintext of the first block is required* to undo the XOR operation. This latter operation can be obtained *only after* decrypting the first block (B_1) at the receiver (Fig. 1(b)). The notations used throughout the algorithm are summarized in Fig. 1(c).

The size of the encrypted block (we refer to as the first block in the first transmitted frame) is determined by the traditional encryption algorithm used. More specifically, the block size for the conventional AES scheme is 128 bits, while the block size for the conventional data encryption standard (DES) is 64 bits. By performing the signaling-encryption algorithm by first traditionally encrypting the first block and then performing the XOR operation for the remaining blocks, the whole resultant data stream will then be secure with security level provably as high as the security level of the first block. The whole data stream will share the same security level since the XOR operation is a one-to-one mapping function and



(a) Transmitter



(b) Receiver

$$
\begin{aligned}
S &= [B_1, B_2, \dots, B_{N_bN_F}] \\
B_k &= [b_{1,k}, b_{2,k}, \dots, b_{\beta_l,k}], \qquad k = 1,2, \dots, N_bN_F \\
\tilde{B}_1 &= E_k[B_1] \\
\tilde{B}_k &= B_1 \oplus B_k, \qquad k = 2, \dots, N_bN_F \\
\tilde{S} &= [\tilde{B}_1, \tilde{B}_2, \dots, \tilde{B}_{N_bN_F}]
\end{aligned}
$$

(c) Notations of digital signal vectors

Fig. 1. Transmitter and receiver structure of the integrated signaling-encryption mechanism in a wireless communication system.

the data will not be recovered by any intruder without breaking the first cipher. The encryption algorithm is repeated every superframe (N_F frames) or multiple of superframes with a new key for the first block of each superframe to enhance security and reliability of the transmission. A detailed description of the integrated signaling-encryption mechanism can be found in [7].

III. Encryption Ratio

We review the figure of merit here, the encryption ratio, denoted by β_c that was introduced in [7]. It is defined as the ratio of the overall transformed text using the XOR operation to the encrypted text using traditional encryption algorithms, which can be expressed mathematically as

$$\beta_c = \frac{\text{Transformed text using the XOR}}{\text{Encrypted text using traditional algorithms}}$$

$$\beta_c = \frac{(N_F N_b - 1)\beta_l}{\beta_l} = (N_F N_b - 1) \tag{1}$$

where N_F, N_b, and β_l are as defined earlier. The encryption ratio reveals the amount of overhead processing cycles reduction obtained when using the integrated encryption algorithm. It is clear that as the value of β_c increases for a given superframe of data, the encryption overhead as well as the avalanche effect decreases and hence the effective system throughput increases. This metric will be used in the performance analysis section presented next.

IV. Performance Analysis

In this section, we provide the throughput analysis of the integrated signaling-encryption mechanism and compare it with the conventional encryption algorithm. For the rest of this paper, for performance evaluation purposes, we will consider the standard AES-128 encryption technique [8] in encrypting and decrypting the first block, B_1. We consider two cases, namely, without error correction encoding and with error correction encoding only the first encrypted block.

In general, the throughput (T) can be defined as the number of correctly received bits (carrying information) per second, which can be described in terms of the bit rate (R) as

$$T = R(1 - P_e)^{\beta_l} \tag{2}$$

where P_e is the block bit-error rate (BER) and $(1 - P_e)^{\beta_l}$ is the probability of receiving a block of length β_l-bits correctly. Within one superframe, with $N_F N_b$ blocks, the average throughput can be obtained by averaging the throughput amounts of all the blocks within the superframe as

$$T = \frac{1}{N_F N_b} \sum_{i=1}^{N_F N_b} R_i \left(1 - P_{e_i}\right)^{\beta_l} \tag{3}$$

which is equivalent to

$$T = \frac{1}{\beta_c + 1} \left[R_1 \left(1 - P_{e_1}\right)^{\beta_l} + \sum_{i=2}^{\beta_c + 1} R_i \left(1 - P_{e_i}\right)^{\beta_l} \right] \tag{4}$$

We assume that the same data rate is shared among all blocks excluding the first block, i.e., $R_i = R$, $i \geq 2$, which is a valid assumption. Because here we evaluate the throughput for the data carrying the actual information, the effective transmission data rate for the first (encrypted) block is assumed to be $R_1 = \eta R$, where $\eta < 1$ because of the overhead associated with the conventional encryption used in the first block. In addition, if we consider error correction encoding applied to the first encrypted block (here we only consider error correction encoding the first block in a superframe while the remaining blocks are uncoded), then the effective transmission data rate for the error correction encoded and encrypted block is going to be $R_1 = \eta R_c R$, where R_c is the coding rate. By employing these definitions in (4) and conducting simple algebra, we can respectively write the superframe average throughput for no encryption, conventional encryption, and the integrated signaling-encryption mechanisms considering the two cases (without error correction encoding and with error correction encoding only the first block) as follows:

$$T_{No\_Enc} = R\left(1 - P_e^{No\_Enc}\right)^{\beta_l} \tag{5}$$

$$T_{Conv} = \eta R (1 - P_e^{Conv})^{\beta_l} \tag{6}$$

$$T_{Prop} = R \left(\frac{\beta_c + \eta}{\beta_c + 1}\right) \left(1 - P_e^{Prop}\right)^{\beta_l} \tag{7}$$

$$T_{Prop}^{Encoding} = R \left(\frac{\beta_c + \eta R_c}{\beta_c + 1}\right) \left(1 - P_e^{Prop\_Encoding}\right)^{\beta_l} \tag{8}$$

Expressions (5)-(8) will be used in the next section to numerically obtain the throughout performance graphs in standard Gaussian and Rayleigh fading-type wireless channels.

V. Numerical and Simulation Results

In this section, we provide numerical results to compare between the performance of the integrated signaling-encryption mechanism and the conventional one in terms of the superframe average BER and normalized throughput.

An end-to-end system-level simulation-based study is conducted for computing the average BER of the integrated signaling-encryption technique with and without error correction encoding in addition to the conventional AES-128 encryption technique. Two wireless channel models are considered: an additive white Gaussian noise (AWGN) channel and a Rayleigh flat fading channel whose maximum Doppler shift is 100 Hz. BPSK modulation with coherent detection is used for the transmission over the AWGN channel, while differential BPSK modulation is used for the transmission over the Rayleigh channel. In case of data transmission with error correction encoding, the first block of each superframe is only encoded by a Hamming code or a convolutional code. We assume the AES-128 is used to encrypt the first block of each superframe with block size (β_l) of 128 bits, superframe size ($N_F N_b$) of 1000 blocks, and Monte Carlo simulations over 1280000 bits are used for the computation of the BER for each scenario.

Figures 2 and 3 demonstrate the average bit-error probability of the integrated signaling-encryption mechanism over AWGN channel using Hamming and convolutional encoding, respectively, and compared with the conventional AES. It can be observed that there is a minor improvement in BER performance using the presented encryption mechanism compared with the conventional AES when the data is not encoded by any error correction code. However, the performance of the presented mechanism improves dramatically by incorporating error correction coding solely on the first (encrypted) block of each superframe.

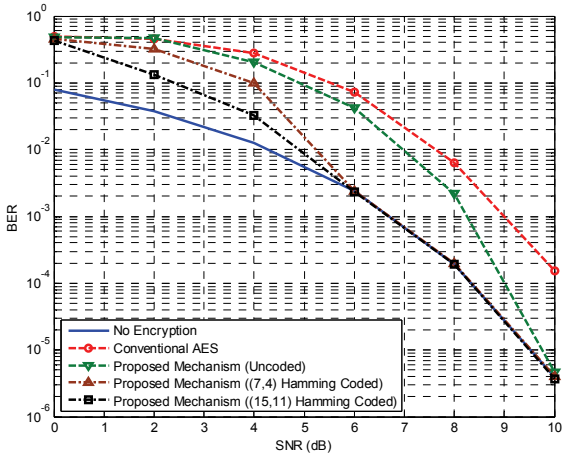


Fig. 2. The average bit-error probability of the integrated signaling-encryption mechanism over AWGN channel and using the Hamming code. Performance comparison.

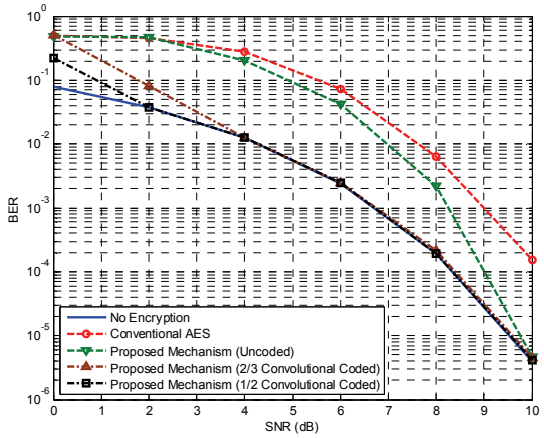


Fig. 3. The average bit-error probability of the integrated signaling-encryption mechanism over AWGN channel and using the convolutional code. Performance comparison.

This massive improvement in BER performance by using error correction coding only to first block of each superframe (only 0.1% of the total transmitted data is error correction encoded in this numerical example) is due to the fact that if the first block is in error and cannot be recovered, then all the remaining blocks in a superframe become unrecoverable. Therefore, by protecting the first block of each superframe from random errors using error correction coding, the overall average BER reduces dramatically. It is worth mentioning that by applying error correction coding only to a small portion of the total transmitted data (0.1% in this example), it won't add much overhead and, therefore, it won't noticeably increase the required bit rate.

Figures 4 and 5 demonstrate the average bit-error probability of the integrated signaling-encryption mechanism over Rayleigh channel using Hamming and convolutional encoding, respectively, and compared with the conventional AES. It can be observed that the convolutional code improves the BER performance much greater as compared with the Hamming code in Rayleigh fading channels, while it does not when the channel is AWGN as demonstrated in Fig. 2 and Fig. 3. We can also observe from Fig. 4 that the BER performance of the presented encryption mechanism is in some cases (e.g. at SNR = 15 dB) worse than that of the conventional one. However, this is not because of the proposed mechanism design but because of the weak performance of the Hamming code in Rayleigh fading channels. Figure 5 supports our last statement where it is clear that applying the convolutional code shows the superiority of the mechanism over the conventional one in terms of the BER performance. From Fig. 5, notice that about 15 dB gain is achieved using the proposed mechanism over the conventional one in Rayleigh fading environments.

Figures 6 and 7 demonstrate the average normalized throughput of the integrated signaling-encryption mechanism over AWGN channel using Hamming and convolutional encoding, respectively, and compared with the conventional AES. It is obvious that the integrated mechanism provides higher throughput over the conventional one without and with encoding. However, encoding the first block further improves the integrated mechanism throughput. Because the convolutional code provides better BER performance as compared with the Hamming code, it further improves the integrated mechanism throughput which is clearly obvious in the low SNR range. Figures 8 and 9 repeat the same comparisons as in Fig. 6 and Fig. 7 but considering the Rayleigh fading channel and we can witness the same observations. From Fig. 9, notice that more than 150% improvement in throughput is achieved using the integrated mechanism over the conventional one in Rayleigh fading environments.

VI. CONCLUSIONS

Performance evaluation analyses have been conducted for the integrated signaling-encryption mechanism in terms of BER and throughput in wireless channels. We considered error correction encoding only the first encrypted block in order to achieve higher data throughput. Numerical results show that the BER performance and throughput of the integrated mechanism are superior to those of the conventional AES over standard Gaussian and Rayleigh fading-type channels.

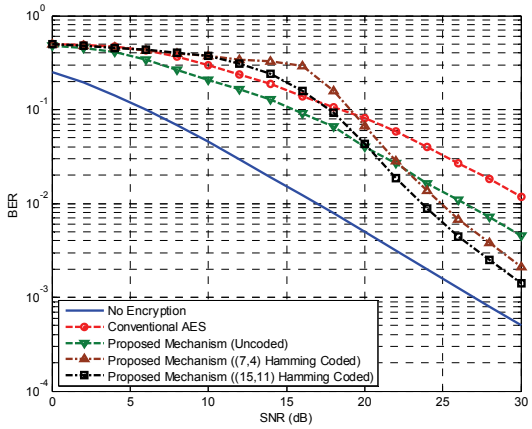


Fig. 4. The average bit-error probability of the integrated signaling-encryption mechanism over Rayleigh fading channel and using the Hamming code. Performance comparison.

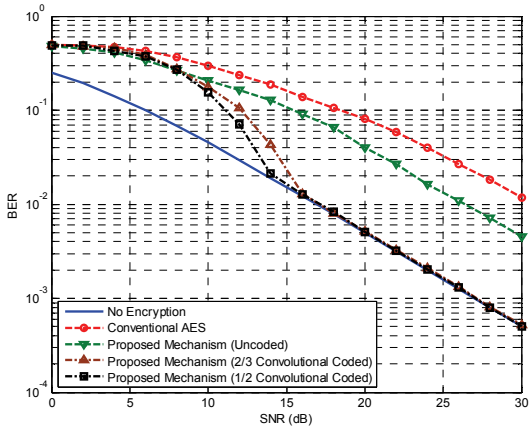


Fig. 5. The average bit-error probability of the integrated signaling-encryption mechanism over Rayleigh fading channel and using the convolutional code. Performance comparison.

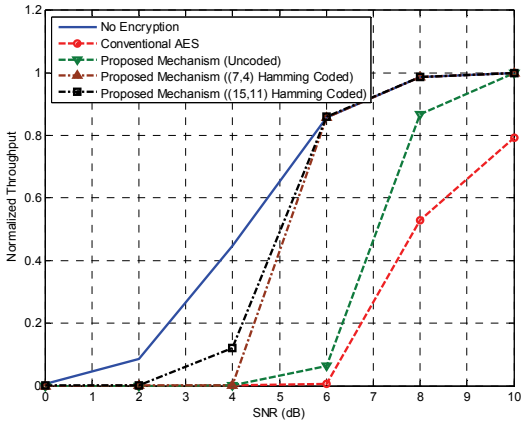


Fig. 6. The average normalized throughput of the integrated signaling-encryption mechanism over AWGN channel and using the Hamming code. Performance comparison.

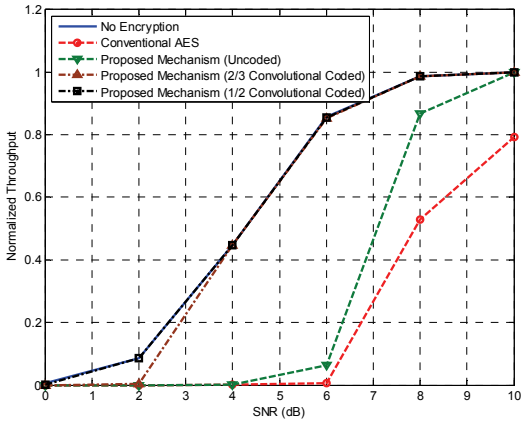


Fig. 7. The average normalized throughput of the integrated signaling-encryption mechanism over AWGN channel and using the convolutional code. Performance comparison.

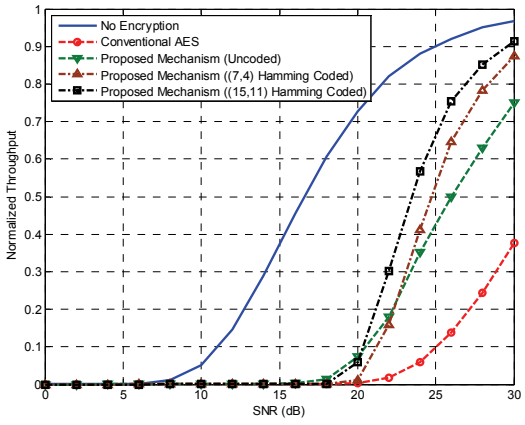


Fig. 8. The average normalized throughput of the integrated signaling-encryption mechanism over Rayleigh fading channel and using the Hamming code. Performance comparison.

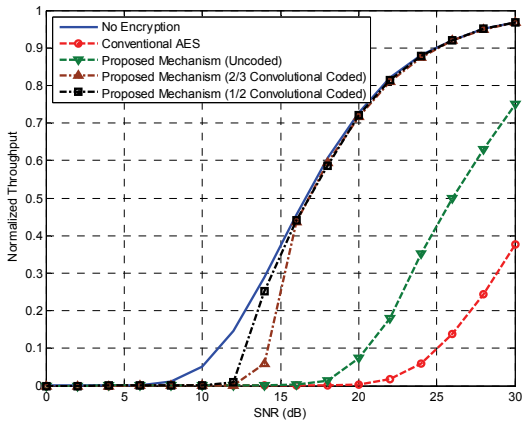


Fig. 9. The average normalized throughput of the integrated signaling-encryption mechanism over Rayleigh fading channel and using the convolutional code. Performance comparison.

The security aspect of the integrated signaling-encryption mechanism can be enhanced by adding a security process box to the current design after and before the XORing processes at the transmitter and the receiver, respectively. The new security box performs key-based multiplexed permutation operations to significantly improve the security of the transmission mechanism. Performance analysis in terms of security and QoS of the integrated mechanism with the new security process box will be investigated in a future paper.

REFERENCES

[1] J. M. Reason, "End-to-end confidentiality for continuous-media applications in wireless systems," Ph.D. Dissertation, UC Berkeley, 2000.

[2] R. Forre, "The strict Avalanche criterion: Spectral properties of Boolean functions and an extended definition," *Proc. of the 8th Annual International Cryptology Conference - Advance in Cryptology (CRYPTO'88)*, pp. 450-468, 1988.

[3] O. Adamo and M. R. Varanasi, "Joint scheme for physical layer error correction and security," *ISRN Journal of Communications and Networking*, 2011.

[4] D. A. Moghadam, V. T. Vakili, and A. Falahati, "Combination of turbo coding and cryptography in NONGEO satellite communication systems," *International Symposium on Telecommunications*, pp. 666-670, 2008.

[5] M. A. Haleem, C. N. Mathur, R. Chandramouli, and K.P. Subbalakshmi, "Opportunistic encryption: A trade-off between security and throughput in wireless networks," *IEEE Transactions on Dependable and Secure Computing*, vol. 4, no. 4, pp. 313-324, 2007.

[6] Y. Xiao, B. Sun, H. Chen, S. Guizani, and R. Wang, "Performance analysis of advanced encryption standard," *Proc. of the IEEE GLOBECOM*, pp. 1-5, 2006,

[7] M. M. Matalgah and A. M. Magableh, "Simple encryption algorithm with improved performance in wireless communications," *Proc. of the IEEE Radio and Wireless Symposium (RWS)*, pp. 215-218, 2009.

[8] "Announcing the Advanced Encryption Standard (AES)," US NIST, Nov. 2001. Retrieved from http://csrc.nist.gov/publications/fips/fips197/fips-197.pdf.