Simple Encryption Algorithm with Improved Performance in Wireless Communications

Mustafa M. Matalgah [1], Amer M. Magableh [2]

[1] Radio and Wireless Department of Electrical Engineering,
The University of Mississippi University, MS 38677, USA
Email: mustafa@ieee.org

[2] Department of Electrical Engineering, Jordan University of Science and Technology, Irbid, Jordan
Email: magableh@ieee.org

Abstract—**In this paper, inspired by network coding theory we propose an efficient hybrid encryption-coding algorithm that requires using traditional encryption only for the first small amount of data. This amount of data, which we refer to as the first block, is determined by the traditional encryption algorithm to be applied on this first block. In our proposed algorithm, all the rest of the information will then be transmitted securely over the wireless channel, using network coding, without a need for using traditional encryption. Unlike the traditional and opportunistic encryption algorithms, the proposed algorithm achieves higher data rates and less avalanche error effect and at the same time it is as secure as traditional encryption algorithms. Assuming the additive white Gaussian noise (AWGN) channel model employing our proposed algorithm we analyze its performance in terms of throughput and security level. Numerical results of different case studies are provided.**

I. Introduction

Relay-based cooperative wireless networks have been extensively studied in the literature in the past decade. One deficiency in transmitting the information signal over the wireless channels, in general, and through the relay nodes in cooperative networks, in particular, is the lack of information security while the signal traversing the wireless channel or at the relay nodes. An intruder, anywhere in the transmission path or at the relay, can easily extract the signal and recover the data with no privacy considerations. One way to overcome this deficiency is to encrypt the data before the transmission process. However, employing encryption in relay-based cooperative wireless communication results in multiple drawbacks. First: encryption requires an extra large amount of bandwidth because of the added overhead packets. Second: the performance deteriorates extensively due to the avalanche effect (defined in [1] and [2]) in wireless fading channels, which tremendously reduces the effective bandwidth utilization. This is in addition to the delay caused by the processing time required by the encryption and decryption algorithms at the source and destination sides, respectively. All these drawbacks result in a large reduction in the achievable throughput. Moreover, performance deterioration due to fades in wireless multipath fading channels may in some extreme conditions make it almost impossible to decrypt the data at the destination side due to avalanche effect inherited in traditional encryption algorithms. For example, and without loss of generality, to achieve privacy and secure communication the regenerative cooperative communication type (decode and forward), the transmitted data should be encrypted before transmission. The encrypted data (cipher data) can then be decoded at the relay side without extracting the original information (plaintext) and forwarded to the destination side. Although, cryptography of the plaintext achieves security and privacy, it reduces the total throughput [2] and increases the amount of overhead bits [3]. These drawbacks motivate researchers to investigate other methods to develop effective algorithms to securely transmit information over the cooperative nodes in wireless communication. In [2], 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. It is well known that the advanced encryption standard (AES) requires a large number of logical operations that results in processing delay. In [3], a detailed quantitative study was performed to evaluate the overhead processing cycles for the logical operations required in both the encryption and decryption of an AES frame.

In this paper we propose an encryption algorithm, that is efficient for wireless communication systems, which requires encrypting (using traditional encryption algorithms) only the first block of each frame (or superframe) of the data stream and transmits the remaining of the blocks based on network coding theory. This amount of data (the first block length) as well as the encryption frequency (encryption rate or the ratio of the first encrypted block-length to the length of the whole frame or superframe) are determined by the adopted traditional encryption algorithm. The size of the first encrypted block, which may vary based on the adopted encryption algorithm, is chosen according to the encryption algorithm and the key size. For example, the key size in the advance encryption standards (AES) algorithm may vary from 128, 192, and 256 bits, while the key size for the standard data encryption standard (DES) is 64 bits. Our proposed hybrid encryption-coding algorithm is simple and achieves a predefined security level for the whole data frame with improved throughput and reduced overhead processing cycles. We assume a wireless channel model employing this algorithm and analyze its performance in terms of overhead, security level, and system throughput.

The remainder of this paper is organized as follows. Section

978-1-4244-7685-5/11/$26.00 ©2011 IEEE

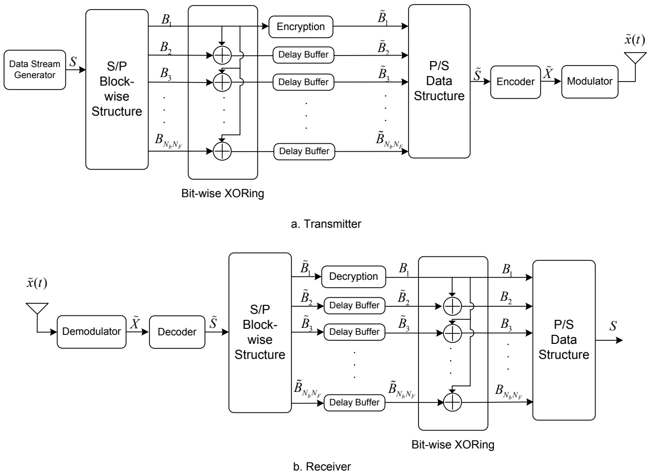
II introduces the structure and algorithm of the proposed encryption model. Performance analysis of the proposed encryption mechanism, in terms of overhead requirements and throughput, are provided in Section II. Numerical results with different case studies are presented in Section IV. Finally, some conclusions are drawn in Section V.

II. Proposed Encryption Model: Structure and Algorithm

We first describe the system and information signal model of our proposed hybrid encryption-coding algorithm as follows. Within this model, we propose a new hybrid encryption-coding algorithm that achieves same security level (among the whole encrypted-coded data) as the known traditional encryption algorithms and reduces the overhead processing cycles (PC), hence increasing the achievable system throughput. The traditional algorithm for message encryption to be used in encrypting the first block in our model is the AES cipher algorithm (also known as the Rijndael algorithm), which is a known standard algorithm that is very immune to adversary attack by intruders such as a brute force attacker. The encryption key is assumed to be known only to the destination node where the cipher message of the first block is received and decrypted to convey the plaintext. The AES cipher requires a 128 block size and a $128/192/256$ key size that satisfies the entropy condition for the key size. It is worth mentioning here that Rijndael supports many block sizes. However, the AES adopted the block size of 128 with different key lengths. The general design of the AES encryption algorithm has pre-round transformation (initial stage), $R-$rounds, key expansion, and a final stage. The number of rounds is determined by the key size. Particularly, the AES uses $10, 12$, and 14 rounds for key sizes of $128, 192$, and 256, respectively. The number of processing cycles for each operation (AND, OR, Exclusive OR (XOR), and SHIFT) varies based on the number of rounds included in the encryption algorithm as a result of different keys adopted. It is also worth pointing out here that the number of PC in the decryption is different than the number of PC used in encryption. In general, the number of PC is much larger in decryption compared to encryption.

A. Transmitter and Receiver Structures

A conceptual structure for the transceiver of the proposed hybrid encryption-coding mechanism is shown in Fig. 1. The transmitter structure for the proposed 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 (β_l)[1]. The first block undergoes a proper encryption algorithm satisfying a certain security level. All the remaining blocks are arranged systematically and enter a bit-wise XOR operation with the first block (before encryption, i.e., plaintext), as can be seen from the figure. Next, the data is mapped back into a serial format to be encoded before transmission (both source and channel encoding) to enhance transmission reliability. The data stream is then modulated using any digital modulation technique in order to be suitable for transmission. Without loss of generality, we consider the BPSK modulation technique to be studied in this paper and the analysis can be generalized to any other modulation type or higher-order modulation. The receiver structure, as can be seen in Fig. 1.b, completely reverses all the operations performed at the transmitter. Also, at the receiver side, only the first block is 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, all the data frame is transmitted securely by performing traditional encryption only on the first small amount of data (B_1 in Fig. 1) within a frame or superframe.



$$S = [B_1, B_2, ..., B_{N_b N_F}]$$

$$B_k = [m_1^k, m_2^k, \dots, m_{Bl}^k], \quad k = 1, 2, 3, ..., N_b N_F$$

$$\tilde{B}_1 = E_k[B_1]$$

$$\tilde{B}_k = B_1 \oplus B_k, \quad k = 2, 3, ..., N_b N_F$$

$$\tilde{S} = [\tilde{B}_1, \tilde{B}_2, ..., \tilde{B}_{N_b N_F}]$$

Fig. 1. Transmitter and receiver structure for the proposed encrypted-coded mechanism in wireless communication system.

B. Algorithm

We assume that we have a data sequence composed of N superframes. Each superframe contains N_F frames, and each frame consists of N_b blocks, each of $K = \beta_l$ bits sizeThe proposed encryption algorithm, for the transceiver in Fig. 1, is detailed in the text structure in Algorithm $algorithm1$. The notations used throughout Algorithm 1 are summarized right after it. As it is clear from the steps in Algorithm 1, we first encrypt the first block, B_1, with a highly immune standard traditional encryption algorithm (such as the AES). Following this step, the rest of the $N_b - 1$ blocks will be used as plaintexts (i.e., will not undergo traditional encryption). In these steps that follow, a bit-wise XOR operation is performed between the plaintext of the first block with each of the remaining $N_b - 1$ blocks and then transmitted to the destination. Consequently, the first block will not be recovered without performing the decryption process, which

[1] Our algorithm requires that the block size β_l be determined by the encryption algorithm that will be applied only on the first block.

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 performed only after decrypting the first block (B_1) at the receiver (see Fig. 1.b). By performing the proposed encryption algorithm, following the steps provided in Algorithm 1, where the first block is first traditionally encrypted and then the XOR operation is performed for the remaining blocks with the plaintext of the first block, the whole resultant data stream will then be secure with security level 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 the data will not be recovered by any intruder without breaking the first cipher. Without loss of generality, we consider a block size of 128 bits. However, any block size can be considered in this proposed encryption algorithm. The proposed encryption algorithm is repeated every one superframe or multiple of superframes with a new encryption key. The main reason for having this algorithm repeated every superframe (N_F frames) is to use a new key for each superframe to enhance security and reliability of the transmission.

```
Input: Data stream as plaintext
Output: Data stream as ciphertext
Divide the data sequence into $N$ superframes;
foreach $N_i$ superframe ($SF_i$), $i = 1, \cdots, N$, to be sent do
    Divide each superframe into $N_F$ frames;
    Divide the frame ($F_k$), $k = 1, \cdots, N_F$, into $N_b$
    blocks with block size of $K = \beta_l$;
    Encrypt the first block $B_1$ with an appropriate
    encryption algorithm, i.e., $\tilde{B}_1 = E_k[B_1]$
    foreach of the remaining blocks $B_j$, $j \in \{2, N_b\}$ do
        $\tilde{b}_{i,j} = b_{i,j} \oplus b_{i,1}$, $i \in \{0, K-1\}$;
        Generate the coded blocks as
        $\tilde{B}_j = [\tilde{b}_{0,j}, \cdots, \tilde{b}_{K-1,j}]$ ;
    end
    Generate the encrypted-coded frame.
end
Generate the encrypted-coded superframe. Repeat for
other superframes;
```

Algorithm 1: Generating secure encrypted-coded data using the proposed encryption algorithm

Algorithm Notations

B_j : The j^{th} block of data (plaintext).
$\tilde{B}_j$: The j^{th} block of the encrypted-coded data (ciphertext).
β_l : block length.
N_F : Number of frames within a superframe.
N_b : Number of block within a frame.
$b_{i,j}$: The i^{th} bit of the j^{th} block of the data (plaintext).
$\tilde{b}_{i,j}$: The i^{th} bit of the j^{th} block of the encrypted-coded data (ciphertext).

C. Encryption Ratio

We introduce a new figure of merit here, the encryption ratio (β_c), defined as the ratio of the overall ciphertext using the XOR operation to the encrypted text using traditional algorithms, which can be expressed mathematically as

$$\beta_c \quad = \quad (N_F N_b - 1) \, , \tag{1}$$

where N_F, N_b, and B_l are as defined earlier. This metric will be used in the performance analysis in the forthcoming section.

III. Performance Analysis

In this section, we provide some performance metrics for the proposed encryption algorithm, namely the amount of overhead reduction in terms of processing cycles (PC) and the normalized throughput assuming AWGN channel model. Performance analysis under small-scale fading channel models will be considered in in a future extension to this paper. In the rest of this paper, for performance evaluation purposes, we will assume the standard AES encryption algorithm in encrypting and decrypting the first block, B_1.

A. Throughput and Security Level

As we indicated earlier, in any encryption algorithm the security level is obtained at the cost of reduced achievable throughput and hence this tradeoff should be considered in evaluating any security algorithm. It is well known that the security level is directly proportional to the block length of the encrypted message, whereas the throughput is inversely proportional to the block length because of the associated overhead data and the fact that the block might be completely dropped due to avalanche effect in wireless channels.

In general, the security level can be defined as the amount of computational analysis required by a cryptanalysis to break down the algorithm and decrypt the cipher. The Brute force method (trying all the possible combinations for the key) to decrypt the cipher is usually used when describing the security level of any encryption algorithm. There are $2^{\text{key length}}$ combinations considering the Brute force attack to break the cipher, and therefore, the security level (S_N) for a block text with a block length (B_l) can be mathematically formulated as [2]

$$S_N = \log_2 [B_l] \cdot \tag{2}$$

Assuming the bit error probability is p_e, the probability of receiving a block of length B_l-bits correctly is $(1 - p_e)^{B_l}$. Consequently, the throughput ($\mathcal{T}$) can be defined as the number of correctly received bits (carrying information) per second, which can be written mathematically in terms of the bit rate ($\mathcal{R}$) as

$$\mathcal{T} = \mathcal{R} \, (1 - p_e)^{B_l} \cdot \tag{3}$$

As can be noted, the whole superframe consists of N_F frames, and each frame consists of N_b blocks. This superframe is encrypted in two steps, first encrypting the first block using an AES with one key, and all the remaining blocks are encoded via a bit-wise XOR operation with the first block (plaintext) yielding a full encrypted-coded superframe with the same security level as the first block. Then, the overall achievable security level can be given as

$$\overline{S} \;=\; \log_2[B_l], \tag{4}$$

where $S_i = S_{\text{first block}} = S$.

The average throughput can be obtained by averaging the throughput amounts of all the blocks within one superframe (since one encryption algorithm is used for the whole superframe) as follows:

$$\mathcal{T} \;=\; \frac{1}{(\beta_c+1)}\left[\mathcal{R}_1\left(1-p_1\right)^{B_l} + \sum_{i=2}^{(\beta_c+1)} \mathcal{R}_i\left(1-p_i\right)^{B_l}\right] \tag{5}$$

The results in (4) and (5) will be used to obtain the performance behavior curves for the security level and the normalized throughput at a certain error rate probability. Assuming a BPSK modulation technique with coherent detection to be used during the transmission over the AWGN channel, it is well-known that $p_i = \mathcal{Q}\left(\sqrt{2\gamma}\right)$ where γ is the average signal-to-noise-ratio (SNR) per bit (see, e.g., [5]). We also assume that same data rate is shared among all blocks excluding the first block, i.e., $\mathcal{R}_i = \mathcal{R}$, $i \geq 2$, which is a valid assumption. However, the effective data rate for the first block is assumed to be $\mathcal{R}_1 = \eta\mathcal{R}$, where $\eta < 1$ because of the overhead associated with the AES encryption used for the first block. Then, it is straightforward to show that the throughput expression in (5) reduces to

$$\mathcal{T} \;=\; \mathcal{R}\left(\frac{\beta_c+\eta}{\beta_c+1}\right)\left[1-\mathcal{Q}\left(\sqrt{2\gamma}\right)\right]^{B_l}. \tag{6}$$

The expression in (6) will be used in the numerical section to obtain the throughout performance curves considering the proposed encryption-coding algorithm in the AWGN wireless channel.

IV. Numerical Results

In this section, we provide the numerical results for all obtained expressions for the performance metrics of the proposed encryption-coding model. Fig. 2 provides a comparison between the proposed algorithm, traditional AES algorithm with fixed length [4], and the opportunistic encryption algorithm [2]. The security level was maintained at $\log_2(128) = 7$ for all encryption algorithms, and the required security level was set to 0.9832. The block length for the opportunistic algorithm was chosen from the set $[64, 80, 96, 112, 128]$. As can be seen from the figure, the throughput of the proposed algorithm outperforms the other two algorithms in the entire range of the SNR due to the fact that other algorithms require more overhead bits as the length of the superframe increases, unlike the proposed algorithm. In this figure, we assume no service when the $\overline{\gamma} < 4$ dB corresponding to a $P_e > 10^{-2}$ for the BPSK modulation technique.

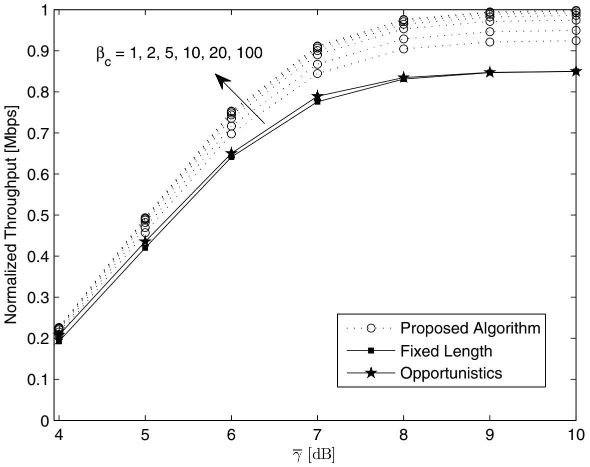


Fig. 2. Comparison between the normalized throughput of BPSK using the proposed encryption-coding algorithm, traditional AES algorithm with fixed block length, and the opportunistic encryption algorithm for $\eta = 0.80$ and different values of encryption ratio, β_c, in AWGN channel.

V. Conclusions

In this paper, we proposed a new simple encryption algorithm that achieves a predefined security level based on AES standard for the whole data frames. The overhead processing cycles required by the proposed algorithm are very small compared to the overhead processing cycles required by the fixed block length traditional AES encryption algorithm or the opportunistic encryption with variable block length. As a case study, we considered encrypted data with the BPSK modulation technique and we derive a complete analysis for the throughput assuming the wireless AWGN channel model. A complete analysis of the throughput, bit error rate, and outage probability for different multipath fading channel models will be reported in a future work.

Acknowledgment

This work was supported in part by NASA/MS Space Grant Consortium Research Infrastructure Project under Grant NNG05GJ72H.

References

[1] J. Reason, *End-to-End Confidentiality for Continuous-Media Applications in Wireless Systems,* Ph.D. dissertation, UC Berkeley, December 2000.

[2] 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, October-December 2007.

[3] Y. Xiao, B. Sun, H. Chen, S. Guizani, and R. Wang, “Performance Analysis of Advanced Encryption Standard,” *IEEE GLOBECOM 2006, Proceedings of the IEEE Global Telecommunication Conference.* Digital Object Identifier 10.1109/GLOCOM.2006.285, pp. 1-5, November 27 - December 1, 2006.

[4] Behrouz A. Forouzan, *Introduction to Cryptography and Network Security*, McGraw-Hill, 2007.

[5] B. P. Lathi and Zhi Ding, *Modern Digital and Analog Communication Systems*, 4th ed. Oxford University Press: New York 2009.