VNU Journal of Science:
Computer Science and Communication Engineering

Journal homepage: http://www.jcsce.vnu.edu.vn/index.php/jcsce

Original Article

# Performance of Orthogonal Frequency Division Multiplexing Based Advanced Encryption Standard

Duc-Tai Truong, Quoc-Tuan Nguyen, Thai-Mai Thi Dinh*

*VNU University of Engineering and Technology, Vietnam National University, Hanoi,*
*144 Xuan Thuy, Cau Giay, Hanoi, Vietnam*

Received 06 December 2019
Revised 07 March 2020; Accepted 12 May 2020

**Abstract:** Currently, there are a lot of secure communication schemes have been proposed to hide secret contents. In this work, one of the methods deploying encryption to cipher data is represented. The primary object of this project is applying Advanced Encryption Standard (AES) in communications based Orthogonal Frequency Division Multiplexing (OFDM). This article discusses the security of the method encrypting directly QAM symbols instead of input bit-stream. This leads to improving the security of transmitting data by utilization of authentication key between the mobile and base station. The archived results demonstrate that the performance of the AES-OFDM system is completely acceptable to compare with the criteria for 4G.

*Keywords:* Orthogonal Frequency Division Multiplexing (OFDM), Advanced Encryption Standard (AES), Quadrature Amplitude Modulation (QAM), Authentication Key, Cellular Network, Encryption, Physical Layer, 4G, LTE.

## 1. Introduction

In recent years, the issue of information security has been more and more urgent. In wireless communications, the security requirement is strongly essential broadcast over the wireless environment which is less secure than over wire one. Due to the characteristics of wireless communications, attackers can eavesdrop on a system to steal transmitted information as well as impersonate mitigate users. When adversaries can access to an underlying secret of the system, the information security shall be threatened.

Though security is commonly integrated at the higher layer of the protocol stack, it can get passed by adversaries. Generally, higher layers' security is based on authentication. That means users have their own authorized key or password. Attackers can use the exhaustive algorithm to overcome this type of security. Meanwhile, physical layer security obtains advantages, which are not archived by higher layers. Physical layer security exploits the randomness of noise and communication channel, therefore intruders are limited to extract data. Moreover, there is no

* Corresponding author.
*E-mail address:* dttmai@vnu.edu.vn

https://doi.org/10.25073/2588-1086/vnucsce.240

assumption of limitation for eavesdroppers in terms of network parameters or computation resources. Hence, if physical layer security is applied to the system, transmitted data is surely more secured.

The work of Jessen [1] mentioned two different areas of the secure wireless system at the physical layer. The first area is the authentication. Authentication focuses on preventing attackers from impersonating the user. Some applicable methods of identification can be listed such as unique transceiver print and one-time password [2]. The second area is the cryptosystem using a shared secret key. Data Encryption Standard (DES) and Advanced Encryption Standard (AES), for example, convert plaintext to ciphertext by symmetric ciphering algorithms [3]. The difficulty of eavesdroppers is that they have to discover the correct secret key to decrypt received cipher-text. Therefore the key's length requires a huge number of computations, generally. In contrast, if an eavesdropper reveals the secret key, the cryptosystem will be useless. Xiao et al. [4] proposed to apply a dynamic secret method to secure wireless communication cryptosystem. The dynamic secret method generates hash value to change system secret. Thus, eavesdroppers cannot steal any information when the secret is updated.

OFDM is a technique that is applied widely in wireless communication now [5]. OFDM has high spectral performance and can limit the ISI interference. However, it is needed to cooperate additional encryption methods with OFDM enhance the security. There are a number of methods assisting with OFDM such as cryptosystem, watermarking and so on [6]. In the work of A. Al-Dweik et al. [7], joint secured and robust transmission for OFDM system was represented. The proposed system using symmetric key cryptography to encrypt OFDM symbols. Due to unknowing key and permutation matrix, intruders will receive like-noise signals. The approach using overloading of subcarriers for OFDM system is proposed in the paper of Tsouri, and Wulich [8]. This method is relied on superposition modulation, reverse piloting and joint decoding. Channel reciprocity, decorrelation, and key distribution are also three of techniques to ensure the security for this OFDM system. Besides, other implementing methods including generation of robust joint constellations and mitigation of effects of power control errors, mobility, and synchronization errors are further mentioned in the work of Tsouri, and Wulich. In the paper of Rajaveerappa, and Almarimi [9], the authors proposed to combines symmetric key cryptography with public key cryptography to encrypt data before applying Walsh Hadamard spreading codes. Public key cryptography of this system bases on RSA (Rivest, Shamir, and Adleman) and symmetric key cryptography relies on shift cipher algorithm.

Various researches had exploited AES with OFDM system [10-12]. Their methods are to encrypt input images in advance, then transmitting by OFDM systems. In those cases, they deploy the encryption of AES at the application level. However, some works [13, 14] tried to use cryptography at the physical layer. In paper [13], the basic idea is to secure the communication link in the OFDM modulation scheme by using AES cipher. The reciprocal channel coefficient is mapped on the discrete number system to be the key in AES encryption. However, that work uses an asymmetric diagram between transmitter and receiver. That can lead to an increase in the error rate when using a symmetric algorithm like AES. Yuan Liang et. al. [14] proposed a secure pre-coded OFDM (SP-OFDM) to transmit reliably and efficiently under disguised jamming. The basic idea of that approach is to randomize the phase of sent symbols utilizing the secure Pseudo-Noise (PN) sequences generated from AES algorithm. The target is to change the phase shift randomly before mapping by m-PSK. The limitation of that approach is only available if the OFDM system using m-PSK modulation technique. In our work, we mapping symbols to hexadecimal number before encrypting them by AES. Due to encrypting the symbols, our method is available in both with m-PSK and m-QAM. Hence, it is not limited to phase shift keying like proposed method in paper [14].

Idea of our work is implementing AES at the physical layer by encrypting the modulated symbols. The encryption component can be designed as a plug-in module. Hence, this method will not change any parts of the current LTE systems. This article proposes a model, which combines AES with QAM modulation in communications based on OFDM. The article focuses on the area of cryptosystems of secure wireless communications at the physical layer. By transforming QAM symbols to AES-QAM symbols, received OFDM signals are definitely different from original QAM symbols and only decrypted by correct authentication key. The authors also show the performance of proposed AES-OFDM, which is acceptable for wireless communication.

The rest of this article is organized as follows. The second section will be the discussion of previous work, while the third section would like to explain how AES-OFDM system work and its diagram. The fourth section analyzes simulation results and assesses the security and performance of the AES-OFDM model. The conclusion will be given in the final section.

## 2. Proposed method

### *2.1. Advanced encryption standard algorithm*

AES is an algorithm adopted by the U.S government and widely used to protect data [15]. AES cipher block of 128-bit or 16-byte data symmetrically. The basic unit in AES is a byte. XOR operation effectuates the addition of two bytes. The multiplication of two bytes in AES is a multiplication in GF(28) which has an irreducible polynomial $m(x) = x^8 + x^4 + x^3 + x + 1$. The secret key of AES has three types of length which are 16, 24 and 32 bytes (128, 192 and 256 bits). AES-128, AES-192, AES-256 is three algorithms corresponding to the length of the cipher key.

The brief description of this algorithm can be listed in the following steps:

Step 1: 128-bit input is considered as a matrix $4 \times 4$ plain text which called state.

Step 2: Key expansion is a function in which the key is expanded into several 32-bit words, w[i]. Each round requires a round key contained four distinct words (128 bits) in serial. The number of rounds bases on the length of the key. Therefore, the number of words is also in change.

Table 1. The relation of key length and number of rounds and words

| Length of key | Number of rounds | Number of words |
|---|---|---|
| 128 | 10 | 44 |
| 192 | 12 | 52 |
| 256 | 14 | 60 |

In the whole of this work, AES-128 is chosen to implement.

Step 3: There are four functions implemented sequentially except for the last round. The general AES algorithm is determined as following pseudo-code:

Algorithm 1. Pseudo-algorithm at transmitter

```
Begin
  Add round key with current state
  Expand key;
  For i = 1 to 9 do
        Hexadecimal numbers.
        Substitution of state using S-box;
        Shift left each word in round
        Mix Columns state using arithmetic over GF($2^8$)
        Add round key [i] with current state by XOR.
  End
        Substitution of state by S-box
        Shift left each word in round
        Add round key [10] with current state by XOR
End
```

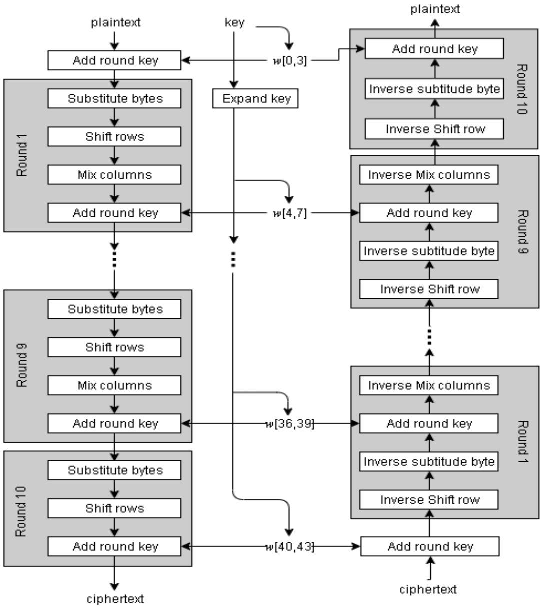

Figure 1. Shows the overall AES cryptosystem that illustrates the symmetric feature of the AES algorithm.

## 2.2. Sharing key process

There are three procedures to protect information transmitted on mobile systems. They are identification, authentication, and encryption. Center Equipment Identity Register takes Mobile Station International Subscriber Directory Number (MSISDN) and International Mobile Station Equipment (IMEI) from User Equipment (UE) to check for subscriber identification. If the subscriber identification is precise, an authentication protocol is applied to supply to UE some important parameters such as cipher key. Figure 3 demonstrates the LTE security protocol in mobile communication. The authentication between a mobile station (MS) and a network is two-way where the master secret key K is used. Posterior to that user UE sends International Mobile Subscriber Identity (IMSI) to Home Network (HN), HN sends back an authentication vector (AV) to Mobile Management Entity (MME). Each AV contains a group of expected response (XRES), a random number (RAND), an authentication token (AUTN), and a master secret key KASME which contains information of a ciphering key (CK) and an integrity key (IK). MME sends RAND and AUTN to UE to check authentication and calculate response (RES).

RES is sent back to MME to compare with XRES. If RES equals XRES, MME sends None Access Stratum (NAS) Security mode command (cipher algorithm, integrity algorithm, NAS key set ID and Capability - CAP) is sent to UE. After UE calculates CK from KASME and NAS encryption algorithm, the AES algorithm uses CK to encrypt at the transmitter and decrypt at the receiver. CK is secure because there is no threat to steal CK without knowledge about MSISDN, IMEI, and IMSI. Figure 2 illustrates the above process.

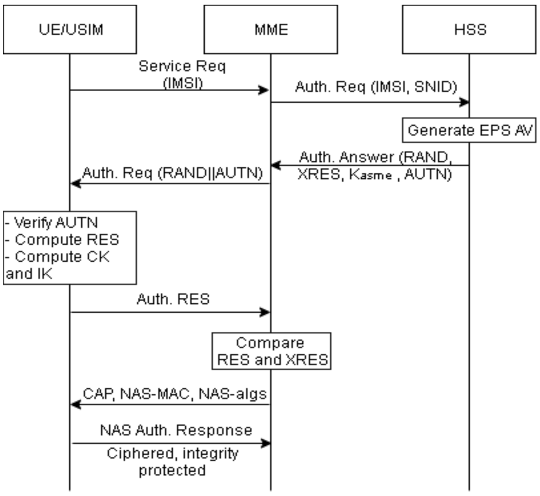

Figure 2. State diagram for authentication in mobile communication.

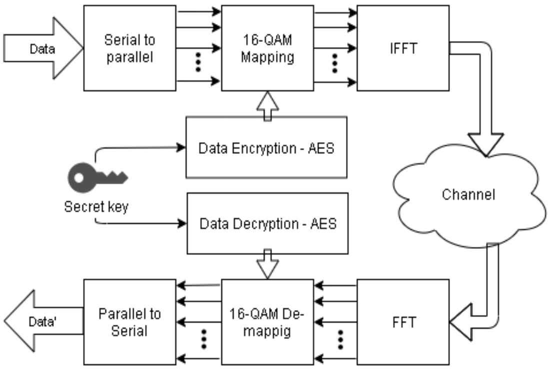

Figure 1. Proposal AES-OFDM model.

### *2.3. AES-OFDM model*

To secure transmit data at the physical layer, this article proposes a combination of AES and OFDM, so-called AES-OFDM. The main idea is encoding QAM symbols directly in the OFDM classical model. Figure 2 illustrates the proposed AES-OFDM model. The process of the proposed system is mostly the same as the original OFDM model except for the constellation mapping step where the AES algorithm is embedded. After converting from serial to parallel, each sub-channel contains 128 bits, thus 1000 sub-channels constitute 128000 bits. The data transmission rate is the same at all individual channels because of orthogonality and the same bandwidth. AES algorithm operates with a byte as the data unit which is represented as a couple of hexadecimal numbers. Consequently, 16-QAM modulation is appropriate to cooperate with the AES algorithm due to that a byte can convey two 16-QAM states also. This way not only improves the security of pure OFDM but also makes the attacker hard to decrypt the information. The reason is that the encryption is performed with 16-QAM symbols while the normal security methods apply AES on the bit-stream. Thus, the attempt of attacker to decrypt the bit-stream or to decrypt at the application layer will fail. In detail, the mapping of 16-QAM states and hexadecimal numbers are shown in Table 2.

After the encryption process, the ciphertext will be remapping to QAM again and perform similar steps as the traditional OFDM model. Whole system operation can be represented by mathematical as follow:

Firstly, the original data is paralleled by N substreams which contain 128 bits each as shown: $\begin{bmatrix} b_{11} & b_{12} & \cdots & b_{1128} \\ b_{21} & b_{22} & \cdots & b_{2128} \\ \vdots & \vdots & \ddots & \vdots \\ b_{N1} & b_{N2} & \cdots & b_{N128} \end{bmatrix}_{N\times128}$

For instance, a sub-stream $b_l = \begin{bmatrix} b_{l1} & b_{l2} & \cdots & b_{lM} \end{bmatrix}$ has M bits. Those bits are constellation mapped. If 16-QAM is applied, the number of elements each substream having now is 32:

$$s_l(t) = \begin{bmatrix} s_{l1} & s_{l2} & \cdots & s_{l32} \end{bmatrix}$$

The elements are encrypted by AES to become completely new symbols.

$$s'_l(t) = \begin{bmatrix} s'_{l1} & s'_{l2} & \cdots & s'_{l32} \end{bmatrix}$$

Table 2. QAM states and corresponding hexadecimal number

| **Input** | **Carrier phase** | **Carrier amplitude** | **Hexadecimal mapping** |
|---|---|---|---|
| 0000 | 225° | 0.33 | 0 |
| 0001 | 255° | 0.75 | 1 |
| 0010 | 195° | 0.75 | 3 |
| 0011 | 225° | 1.0 | 2 |
| 0100 | 135° | 0.33 | 4 |
| 0101 | 105° | 0.75 | 5 |
| 0110 | 165° | 0.75 | 7 |
| 0111 | 135° | 1.0 | 6 |
| 1000 | 315° | 0.33 | C |
| 1001 | 285° | 0.75 | D |
| 1010 | 345° | 0.75 | F |
| 1011 | 315° | 1.0 | E |
| 1100 | 45° | 0.33 | 8 |
| 1101 | 75° | 0.75 | 9 |
| 1110 | 15° | 0.75 | B |
| 1111 | 45° | 1.0 | A |

Therefore, the transmitted data will be totally different from the original data. This step ensures the transmission security.

After that, IFFT is used to divide signals into several frequency stacks. The final transmitted AES-OFDM is given as below:

$$m(t) = \sum_{l=0}^{N} s'(t)\cos(2\pi f_l t)$$

Pseudo-algorithm at the transmitter is considered as follow:

Algorithm 2. Pseudo-algorithm at transmitter

```
Begin
  For each *frame* do
        Modulated Data = 16-QAM modulation of original data;
        Plain text = mapping 16-QAM modulated symbols to hexadecimal numbers.
        Ciphered text = implement AES with plaintext and key;
        Ciphered symbols = Remapping ciphertext to 16-QAM symbols;
        IFFT ciphered symbols;
        Add cyclic prefix;
  End
End
```

At the receiver, symmetric blocks are used to demodulate sent signals. Due to the effect of the channel, the received message differs from the transmitted signal. Thus, received symbols is fluctuated with fixed values in table 1, so it requires a balancing method in blocks of AES decryption. By applying boundaries, every symbol is assigned to a fixed value in Table 2. This approach improves the symbol error rate which is mentioned in the next section. The pseudo algorithm at the receiver is shown as below:

Algorithm 3. Pseudo-algorithm at receiver

```
Begin
  For each frame do
        Remove cyclic prefix;
        FFT received symbols;
        Estimate received symbols to 16 values of 16-QAM;
        Ciphertext = Mapping received symbols to hexadecimal numbers
        Plaintext = AES decryption of ciphertext and key
        Modulated Symbols = Remapping plaintext to 16-QAM symbols
        Output data = demodulate modulated symbols
  End
End
```

Execute time is an important parameter to consider a system being available or not with a temporary technology. The required transmission time interval in a 4G system must below 1 millisecond. In the journal of Schneier et al. [16], AES - Rijndael encryption and decryption setup take respectively 300 and 1370 clock cycles on 32-bit CPUs. On the other hand, each OFDM symbol needs 7142 clocks cycles to be processed entirely [17]. Definitely, total required clocks for AES-OFDM processing is maximum at around 23600 cycles that takes 9.83 microseconds on 2.4 GHz CPUs. That executive time is much less than the required transmission time interval in 4G. Thus, the proposed AES-OFDM system can be possible to deal with 4G technology.

## 3. Simulation result

In this section, simulation results focus on two criteria, security, and error rate of AES-OFDM. The scenario is there will be 32000 16-QAM symbols randomly created to transmit by AES-OFDM. The simulation results are investigated on the AWGN channel.

To determine the security of AES-OFDM, the 16-QAM symbols before and after AES are observed. It is notable that there is no clue to detect the key when the attackers have both original and encrypted symbols without knowledge of the cipher algorithm. In a random test case as an instance, there are three symbols represented as 3.0000 + 1.0000i in thirty-two original symbols. However, the three corresponding symbols after applying AES are totally nonrelative, -1.0000 - 1.0000i -3.0000 + 3.0000i -1.0000 + 3.0000i. Therefore the security of the OFDM signal is ensured. However, the security in this work relies on the secret key mostly. If the key is not reveal, the attacker cannot decrypt the encrypted signals. Since the secret key is generated randomly, the protection of the AES-OFDM is certain.

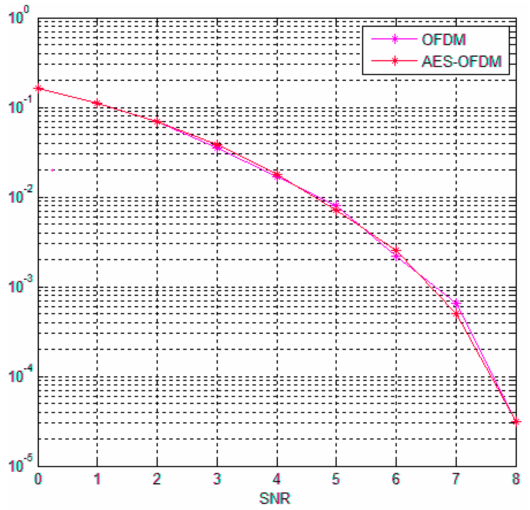

Figure 2. The performance of AES-OFDM comparing with OFDM on AWGN channel.

The second criterion to evaluate the AES-OFDM system is the error rate. The simulation result of the AES-OFDM model is compared with a conventional OFDM. Figure 4 shows the comparison of performance between OFDM and AES - OFDM on the AWGN channel. AES-OFDM has nearly the same performance comparing with general OFDM. With an SNR value of 8 dB, both OFDM and AES-OFDM symbol error rates fall to 3×10-5. When SNR grows to 10 dB, SER values of both OFDM and AES-OFDM bottom to asymptotic of zero. The SER of AES-OFDM, consequently, is acceptable when compared with conventional OFDM.

## 4. Conclusion

In this article, the authors presented the combination of AES and QAM in OFDM communications. AES encrypts the QAM signal to create AES-QAM symbols. That step improves the information security on a transmission channel due to completely transform the QAM signal form. The simulation result using MATLAB shows that: SER of AES-OFDM is acceptable when compared with the conventional OFDM model. The time to execute the AES-OFDM algorithm is a little bit longer than the time of OFDM. So, the execution time of AES-OFDM is still less than 1 millisecond which is appropriate for applying in 4G communications. For further work, AES-OFDM needs to improve the data rate by increasing the level of modulation, which is 16-QAM in the current model.

## References

[1] M.A. Jessen, “Wireless communication security: Physical-Layer techniques exploiting radio and propagation characteristics”, Wireless Information Technology and Systems (ICWITS), IEEE International Conference, 2012.

[2] M. Kim, M. Lee, S. Kim, D. Won, “Weakness and Improvements of a One-time Password Authentication Scheme”, International Journal of Future Generation Communication and Networking, 2009.

[3] Alabaichi, Ashwaq, Salih, Adnan, “Enhance security of advance encryption standard algorithm based on key-dependent S-box”, 2015, pp. 44-53.

[4] S. Xiao, W. Gong, D. Towsley, “Secure Wireless Communication with Dynamic secrets”, IEEE INFOCOM, 2010.

[5] N.U. Rehman, L. Zhang, M.Z. Hammad, “ICI cancellation in OFDM system by frequency offset reduction”, Journal of Information Engineering and Applications, 2014.

[6] Nikita Agrawal, Neelesh Gupta, “Security of OFDM through Steganography”, International Journal of Computer Applications 121(20) (2015) 41-43.

[7] A. Al-Dweik, M. Mirahmadi, A. Sharmi, Z. Ding, R. Hamila, “Joint Secured and Robust technique for OFDM systems”, Western University, Canada, IEEE ICC 2013.

[8] G.R. Tsouri, D. Wulich, “Securing OFDM over Wireless Time-varying channel using subcarrier overloading with Joint signal constellations”, Hindawi Publishing Corporation, EURASIP Journal on Wireless Communication and Networking, 2009.

[9] Rajaveerappa, D. & Almarimi, A., “RSA/Shift secured IFFT/FFT based OFDM wireless system,” Fifth International Conference on Information Assurance and Security, 2009.

[10] M. Hilmey, S. Elhalafwy, M. Zein Eldin, “Efficient transmission of chaotic and AES encrypted images with OFDM over an AWGN channel”, 2009 International Conference on

Computer Engineering & Systems, Cairo, 2009, pp. 353-358.

[11] B.V. Naik, N.L.K. Sai, C.M. Kumar, "Efficient transmission of encrypted images with OFDM system", 2017 IEEE International Conference on Power, Control, Signals and Instrumentation Engineering (ICPCSI), Chennai, 2017, pp. 2383-2388.

[12] S.M.S. Eldin, "Optimized OFDM Transmission of Encrypted Image Over Fading Channel", An International Journal on Sensing and Imaging 15(1) (2014), pp. 1-14.

[13] C. Akbar, H. Mahmood, Q. Minhas, I. Mustafa, "Secure AES OFDM with channel reciprocity exploitation through relative calibration", 2016 International Conference on Open Source Systems & Technologies (ICOSST), Lahore, 2016, pp. 54-61.

[14] Y. Liang, J. Ren, T. Li, "Secure OFDM System Design and Capacity Analysis Under Disguised Jamming", in IEEE Transactions on Information Forensics and Security 15 (2020) 738-752.

[15] Westlund, B. Harold, "NIST reports measurable success of Advanced Encryption Standard", Journal of Research of the National Institute of Standards and Technology, 2002.

[16] B. Schneier, J. Kelsey, D. Whiting, D. Wagner, C. Hall, N. Ferguson, Performance Comparison of the AES Submissions, Proceedings of the Second AES Candidate Conference, 1999.

[17] S. He, A. Tang, H. Zhang, "A high-performance Implementation of OFDM-MIMO base-band in wireless video system", Information Technology Journal 13 (2014), pp. 1678-1685.