IOSR Journal of Computer Engineering (IOSR-JCE)
e-ISSN: 2278-0661,p-ISSN: 2278-8727, Volume 18, Issue 4, Ver. IV (Jul.-Aug. 2016), PP 78-84
www.iosrjournals.org

Investigating the Impact of Secure Image Transmission over MIMO-OFDM System

Omar H. Abdulaziz[1], Fawzi M. Al-Naima[2,3]
[1]Department of Computer Engineering/ University of Mosul, Iraq
[2] Al-Mamoon University College, [3] Department of Computer Engineering/ Al-Nahrain University, Iraq

Abstract: *The paper implements secure MIMO-OFDM systems to achieve the data confidentiality using the following three different cryptographic techniques, namely, AES block cipher, RC4 stream cipher and the proposed Partial Selective Encryption (PSE). These implemented systems have been investigated using PC with processor corei7, 6G RAM and running on Windows 10 as operating system. The investigation involves the measure of the impact of security and quality on the transmission of encrypted images between parties in the MIMO-OFDM wireless domain. The simulation results show the system performs well, the security of the system has been enhanced, and the good point is the enhancement of the Bit Error Rate (BER) by (1.5-1.9) dB. The results also show the secrecy of the transmitted image is achieved from the randomness and cross-correlation results between the original and the transmitted images. Furthermore, the results show that the AES and PSE perform better in terms of BER and privacy whereas the RC4 gives better results in terms of delay and Peak Signal to Noise Ratio (PSNR) compared to AES whereas the PSE gives a compromise results*

Keyword : *MIMO-OFDM, AES, RC4, Image Transmission, PSNR, BER, Partial and Selective Image*

I. Introduction

Multiple Input Multiple Output Orthogonal-Frequency Division Multiplexing (MIMO-OFDM) has been adopted in 4G LTE system and 5G wireless and used in most modern applications. Such technology is highly recommended air-interface solution for next-generation wireless local area networks (WLANs), wireless metropolitan area networks (WMANs), and fourth-generation mobile cellular wireless systems [1], [2], [3]. This is because spatial multiplexing can increase the spectral efficiency and higher throughputs can be reached by increasing the number of antennas of cellular systems [4], [5]. However, wireless transmission is not always safe because of the interception. Thus, information security is one of the major issues that needs to be considered to protect the information passing through the system.

The major studies that have been published on the security of MIMO-OFDM technology concentrated on several compromising aspects such as complexity of the algorithms, good performance and reasonable security. Others show the performance when different types of block cipher in correlated channels environment are applied. In this aspect, Advanced Encryption Standard (AES) is one of well-known block cipher that has been recommended for many applications including wireless communication systems and wireless networks that adopt MIMO–OFDM system [6]. However, the inclusion of AES to encrypt any form of data in the MIMO-OFDM system needs to be investigated from different security points of view such as, delay, complexity, throughput, quality and BER performance. Furthermore, the investigation should decide whether the AES is the best choice to be considered among other forms of ciphering. By this problem specification we will set out research investigation on the impact of inclusion a security system on the MIMO-OFDM in order to enhance its security and measure the most important concepts and factors that are related to MIMO-OFDM system performance [6], [7].

The aim of this research paper is to implement a MIMO-OFDM system using MATLAB program, which attempts to carry secure image between the two ends of communication. The research will also investigate the effect of inclusion of different forms of security on the BER performance of the MIMO-OFDM system, image PSNR and delay. Further investigation will also check the correlation between the input and encrypted images.

II. MIMO-OFDM System

MIMO has become the main focusing technique in the development of 5G wireless communication systems. On the one hand, OFDM is being tested with MIMO for the design and implementation of 5G simulations due to the reduced Intersymbol Interference and increased channel capacity, and on the other hand this system has more complicated components than a normal wireless system as shown in Fig. 1.

During transmission, data are collected from the data source and then passed to the channel encoder. This channel encoder is used to process the data from the data source to a form which can be transmitted over the communication channel. This is done by using additional information in the form of more bits, but this

DOI: 10.9790/0661-1804047884

tradeoff between the number of bits used and the flexibility to choose the desired channel is worth tolerating. Many channel coding schemes have been introduced which are being explored for use in MIMO-OFDM systems such as, Reed Solomon coding, Turbo codes, etc. [8], [9]. Once the channel coding is done, the data will be forwarded to the MIMO encoder from the digital modulation block. MIMO encoder takes the data symbols and converts them into symbols to be transmitted from multiple antennas [10], [11]. The encoded signal is then sent to the serial to parallel converter block so that it is grouped into data for multiple subcarriers. These subcarriers are then passed to the Inverse Fast Fourier Transform (IFFT) block which produces a time domain representation of the frequency domain signals. Finally, the data will pass through the parallel to serial converter where the guard interval is also added to prevent the symbols from interfering into each other. The guard interval is a cyclic prefix which avoids inter-symbol interference. The serial data are then passed through the front end circuitry including the digital-to-analog converter and antenna for transmission through the analog channel [12]. Signal is affected differently while propagating through the multiple path fading wireless medium. This fading is associated with contribution of some channel parameters that have a major impact on signal quality and channel capacity [13].

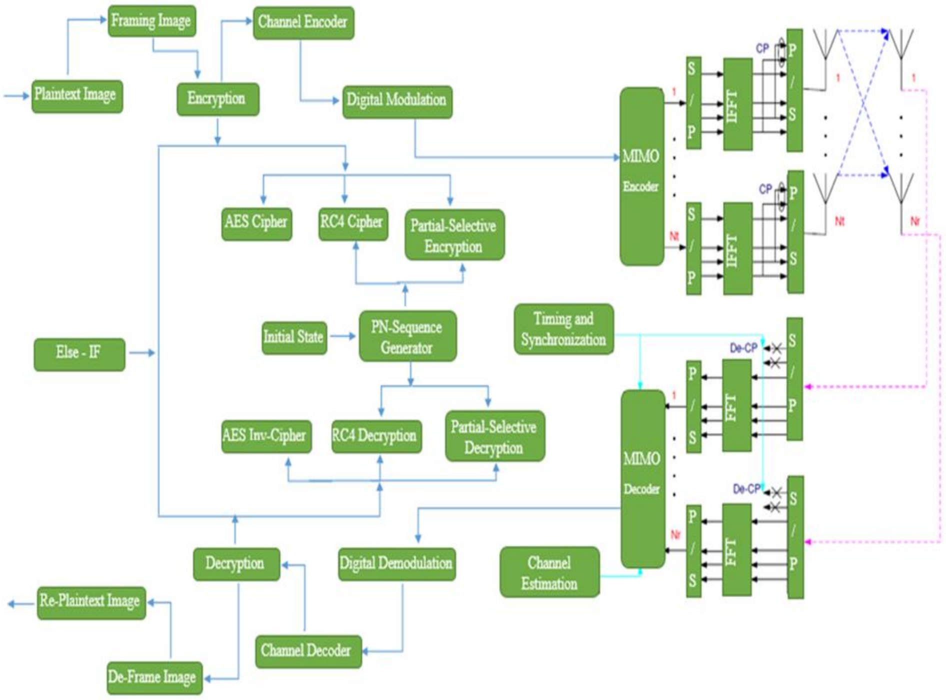

Fig. 1. MIMO-OFDM system under investigation

III. Secure MIMO-OFDM Systems

Encryption is applied to the messages before they are transmitted over the wireless medium as shown in Fig. 1. Stream ciphers provide much better security in wireless structures since such medium is more prone to errors and attacks in comparison to their wired counterparts [14]. Stream ciphers prevent the probability of error propagation in the decoding process. In block ciphers, a single bit error will cause error in the whole block of symbol and thus more data are corrupted or wrongly detected at the receiver end. Hence, the stream ciphers are much better in ensuring security and protection of data against attacks and errors in contrast to the block ciphers [14].

3.1 AES Encryption

The AES cipher is an iterative cipher which handles the data in blocks of 128 bits in the process of encryption and decryption. Depending on the round operation to complete the process, three types of round have been used, 10, 12 and 14 rounds, which are related to the lengths of the used key 128, 192 or 256 bits respectively. Its operation relies on substitution permutation network concepts. AES deals with the computations depending on bytes not bits. It handles the 16 bytes (128 bits) of data input as 4x4 plaintext matrix. Details about the encryption operation, the round structure process and decryption process can be found elsewhere [6].

3.2 RC4 Stream Cipher

RC4 is considered as one of the stream ciphers having symmetric key algorithms that depend on a key of variable size. Random permutation has been applied to be used in this algorithm. RC4 has been used and tested in various wireless communication systems and protocols. It is considered as byte oriented cipher having the same bulk of data (8 bits) of input plaintext data encrypted by using XOR operation with the same bulk of key length (8 bits) to produce (8 bits) of data as cipher text. The byte (8 bits) of the key could be any byte from the range of 1 to 256 bytes, as the maximum length of the key. The pseudo random sequence generator is used to produce a random sequence of state of active 256 bytes to prepare the encryption key [15], [16]. Generally, the cipher depends on the length of the key to measure the degree of security. RC4 is considered secure enough when the size of the key is not less than 16 bytes (128 bits). Further details about the keystream generation using RC4 is found elsewhere [17].

3.3 Secure PSE

One of the proposed enhancements for the AES block cipher and the stream cipher is a form of combination between stream cipher and AES. Further enhancement on the complexity can be gained by partial image encryption as shown in Fig. 2. This enhancement is achieved through the selective image encryption technique (Partial Encryption). The implementation procedure of the PSE can be divided into the following steps:

Partial Image Selection.

The selected parts of the image will be chosen to be part of the plaintext. Here each image is re-arranged to consist of equal matrices that are not be overlapped. The chosen plaintext depends on the Entropy values of the neighbor blocks. This is very essential to allocate the Region of Interest (ROI) by calculating the best Entropy values. This selective area will represent 25-35% of the full image size for better encryption performance and can enhance the speed and throughput.

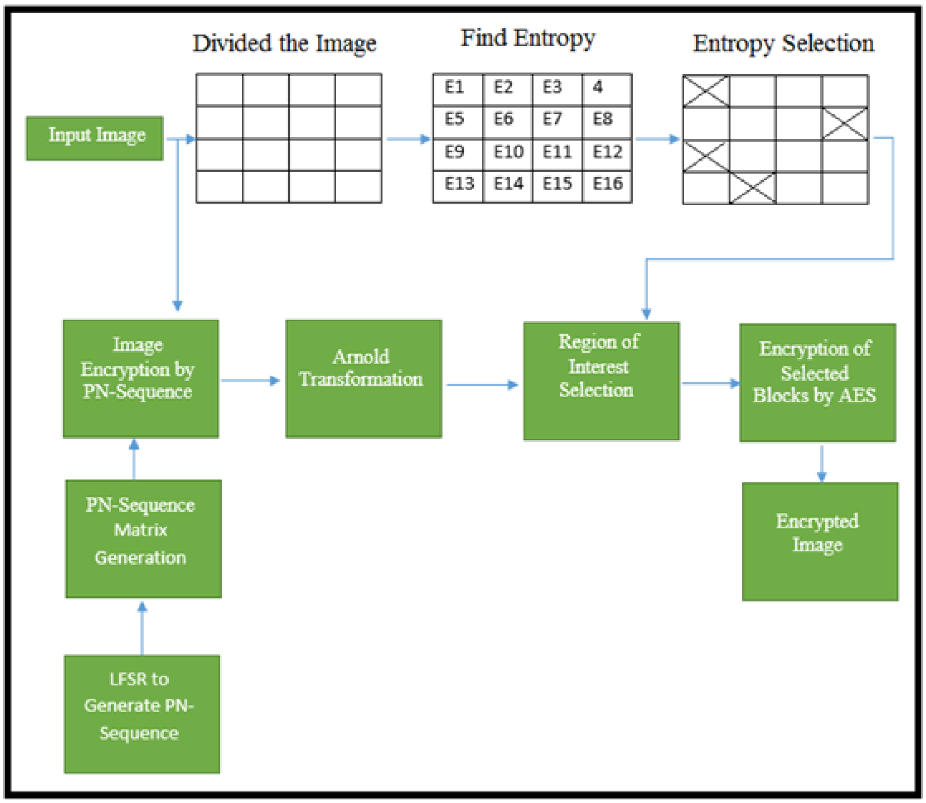
Divided the Image
Find Entropy
Entropy Selection
Input Image
E1
E2
E3
4
E5
E6
E7
E8
E9
E10
E11
E12
E13
E14
E15
E16
Image Encryption by PN-Sequence
Arnold Transformation
Region of Interest Selection
Encryption of Selected Blocks by AES
PN-Sequence Matrix Generation
Encrypted Image
LFSR to Generate PN-Sequence

Fig. 2. Block diagram and Partial-Selective Image Encryption

PN-Sequence Generation.

One of the main aspects of the PSE is the use of scrambling in PN-sequence and XOR operation. The used pseudorandom sequence generator is the linear feedback shift register (LFSR). The initial state of the cipher is important to set up the encryption process, it should also depend on the generator polynomial. The length of its vector must be the same as that of the generator polynomial whereas the coefficients that decide the operation of the PN-Sequence of nonzero terms of the polynomial contain the exponents of z and the last term should be equal to one. To improve the encryption performance of this simple cipher, a shifted version has been adopted which decreases the autocorrelation value between the original input image and the ciphered image.

Image Transformation.

The image is randomized to be more secure using Image Arnold Transformation. This transformation can be represented as scrambling technique to enhance the encrypting process that is already done by LFSR. However, the main drawbacks are because of the pixels and bits of the image do not change their values but just move to other locations, so the image histogram will be the same for both input image and the encrypted image. Furthermore, if the process is performed many times and many rounds, it may produce the original image again, for these two reasons the PN-Sequence has been used in the previous operation to solve these problems.

AES Block Cipher.

The final step of the PSE is to use the AES cipher. The AES is used to encrypt part of the image, about 25% of the full image. The adoption of AES because of its strength, it needs 2128 attempts for Distributed Denial of Service (DDOS) attack. With this suggestion the complexity of the image encryption will drop almost to half that of AES. The inverse cipher function is applied to the selected area that represents the 25% of the full image. The image recovery requires the allocation of each image pixel to its position. This is accomplished via the same Arnold Transformation process which has been applied in the encryption process. The final step is to use the same key of the LFSR and XOR with the encrypted image, the result will be the decrypted image, i.e, the original input image. Security parameters need to be identified as mentioned in AES initialization even before reading the input image. AES cipher parameters are polynomial matrix, s-box and expanded key, and these parameters are used to generate the encrypted data on the transmitter side for both AES encryption and PSE process.

IV. Secure MIMO-OFDM Systems Assessments

The input image is transferred into frames pattern to be ready for the encryption process. This process needs to fill the last empty part of the frame with zeros (zero padding) to avoid errors at the receiver side. The code has been divided into two parts transmitter and receiver side. The transmitter side will contain all functions that will simulate and process the transmitted data. Next, a convolutional bit coding is performed to generate bits that will be inserted into the matrix for error correcting process. In this case, it is important to fill the empty parts with zero padding bits. The MIMO-OFDM system uses different paths to transfer the signal, and it uses multiple channels to transmit and receive the signals. The number of receiver antennas multiplied by the number of transmitter antennas gives the total number of channels that are used in the loop.

The images under investigation are shown in Fig. 3. This figure shows the original, transmitted, received and the recovered images. The original image consists of 730880 bits and applied to the MIMO-OFDM system. The specifications adopted in the MIMO-OFDM system are 16-QAM digital modulation, Rayleigh fading channel and 2X2 Tx - Rx antennas. With the test shown in Fig. 3, it is assumed that the SNR used is 29 dB. This is because the quality of the recovered image is mainly depending on the range of the SNR used. The original image was encrypted using the AES security system adopted in this investigation and then transmitted over the MIMO-OFDM system.

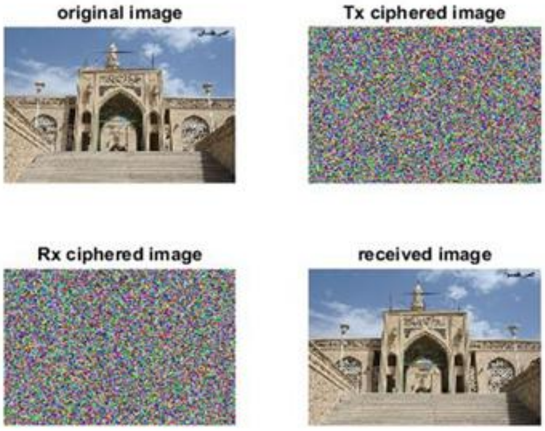

Fig. 3. Original, transmitted encrypted, received encrypted and recovered images by the AES cipher

It is clear from Fig. 3 that the original image is exactly as that recovered image at the receiver, whereas the transmitted encrypted image is almost the same as the received image and all the information has been concealed. The same tests at SNR 29 dB have been carried out with the RC4 stream cipher and PSE. The results with all adopted security systems are all the same. Therefore, extra forms of tests have been carried out to distinguish between the secured systems. These involve BER performance, PSNR, delay, cross correlation, etc.

4.1 BER Performance

The performance of these secure MIMO-OFDM systems were compared with the conventional MIMO-OFDM system to show the impact of security on the BER performance as shown in Table 1. It is clear from the results that the advantages gained by the AES over other secure and unsecure MIMO-OFDM systems. At a bit error rate equals to the (1*10-4) as a reference of comparison, the secure system with RC4 stream cipher will need 1.5 more dB to achieve the performance as that achieved by the AES cipher, whereas the advantages gained increased to about 1.9 dB compared with the unsecure MIMO-OFDM system. However, the PSE gain is better than that of RC4, but less than that of AES by 0.7 dB.

Table 1. SNR in dB required to achieve BER of investigated systems

BER	Unsecure	AES	PSE	RC4
$1*10^{-4}$	25.4	23.5	24.2	25
$8*10^{-5}$	26.2	24	24.7	25.5
$6*10^{-5}$	26.8	24.5	25.2	26.1
$4*10^{-5}$	27.8	25.5	26.1	27
$2*10^{-5}$	28.8	26.7	27.6	28.7

4.2 Image PSNR

The value of the PSNR is calculated by:

$$\text{PSNR} = -10log10(MSE/s^2) \qquad (1)$$

where s2 is the mean square value of the input image pixels and MSE is the mean square error between the input original image pixels and recovered received image pixels. Within secure MIMO-OFDM systems investigation, it has been used to measure the difference between two images, the original and the recovered images to determine the impact of adding the AES block cipher, the RC4 stream cipher and the PSE to the MIMO-OFDM system. The higher the value of the PSNR the better the quality of the recovered image at the receiver side. The variation of PSNR as function of SNR for all secure MIMO-OFDM systems are as shown in Fig. 4.

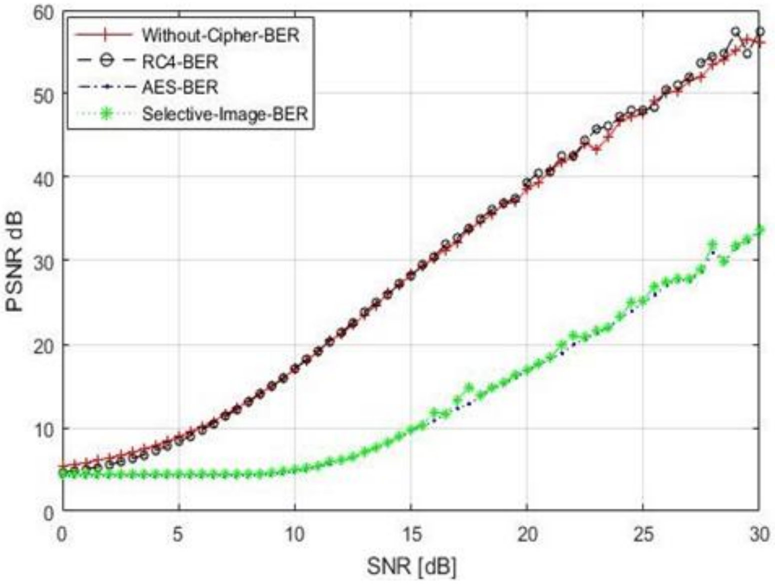

Fig. 4. PSNR of Secure and Unsecure MIMO-OFDM Systems

It is clear that the inclusion of the AES in the secure MIMO-OFDM system has a negative impact on the PSNR whereas the inclusion of the RC4 has no effect. However, the value of PSNR of 32 dB obtained at SNR of 30 dB is quite satisfactory. But in the attention that at a SNR 20 dB the PSNR is less than 20 dB whereas with RC4 is almost 40 dB. This suggests that as the SNR increases the results show more improvement with AES inclusion than that with the RC4.

4.3 Cross Correlation

The main objective of the proposed secure MIMO-OFDM systems is the level of security provided to the transmitted image. Thus the test here involves measurement of the correlation between the original image and the encrypted image. Uncorrelated images (cross correlation between the original input image and the encrypted images) mean no information can be gained from the transmitted encrypted images. The target of uncorrelated means that the value of the cross correlation should be zero. This test involves the measurement of how random are the encrypted image. The results of these tests for all secure MIMO-OFDM systems are as shown in Table 2. It is clear that the PSE gives the best results with lower cross correlation, 0.0050, between the input original and the encrypted images.

Table 2. Cross-Correlation comparison of different MIMO-OFDM Systems

Unsecure	AES	Partial-Selective	RC4
1	0.0055	0.0050	0.0089

4.4 Systems Delay

The same conditions are applied as before, 16-QAM modulation and Rayleigh Fading channel, with two antennas at the transmitter and two antennas at the receiver. In such circumstances, the transmission time delay was found to be 0.030580 seconds. However, after applying the AES cipher the delay increased to 0.030583 seconds. The difference will reflect on the time required by the AES on the secure MIMO-OFDM system. While the MATLAB running encryption time delay for AES was 25.91 seconds. On the other hand, test with RC4 stream cipher gives better time delay than that of the AES, the time required by the RC4 is reduced to 10.17893 seconds. Finally, tests with the PSE technique gives even better time delay than that of the RC4, the time delay is reduced to only 7.063066 seconds. This can be of significant importance to show that better security can be achieved together with better BER performance enhancement with less encryption delay.

From the obtained results, it can conclude that the encryption technique has a very small impact on transmission time delay of a MIMO-OFDM system, with about 0.000003 second, but the extra time was due to the time needed for encryption and decryption of the transmitted image. Table 3. shows the comparison in time delay for the three cases.

Table 3. Time delay comparison for different secure MIMO-OFDM Systems

Process	Unsecure	AES	Partial-Selective	RC4
Encryption Time	0	25.91	7.063066	10.17893
Transmission Time	0.030580	0.030583	0.030583	0.030583
Total Delay	0.030580	25.9406	7.093649	10.20951

4.5 Key Size Impact on BER Performance

AES block cipher works with blocks of 128 bits of data, but it has three levels of security depending on the key length size. The secret key might be 128 bits, 192 bits or 256 bits which corresponds to 10, 12 and 14 rounds respectively. The most preferred key in most applications is the 128 bits, as it provides unbroken cipher and has the fastest algorithm. However, it is worth to investigate the impact of security key size on the BER performance, PSNR, time delay and cross-correlation of the secure MIMO-OFDM system. Test of secure MIMO-OFDM system that adopts AES shows that there is a slight difference between the BER performances of the system with different key sizes. However, there is a significant effect on PSNR and time delay as the key size is increased.

V. Conclusion

The paper shows the impact of adding secure system on the performance of MIMO-OFDM system when an image is transmitted through such system over Rayleigh fading channel. The implemented MIMO-OFDM system has two antennas at the transmitter and two antennas at the receiver side with 64-QAM digital modulation. The results achieved from such investigation reached the following conclusions:

1. Enhancing the security level of the MIMO-OFDM system leads to BER performance improvement with about (1.5 – 1.9) dB when adding AES cipher. However, with PSE the enhancement is less and with RC4 the enhancement still there but the least.
2. PSE returns the lowest value of Cross-Correlation among the other ciphers. Thus, it can be considered as the best secure system.
3. All ciphers have an acceptable PSNR values at SNR equal 30 dB. However, RC4 give the best PSNR compared to block cipher AES and PSE.
4. The time delay is an important value to measure the superior encryption system. All three ciphers have a very short setup time delay, but the comparison done on the encryption-decryption time delay, AES cipher increased the security level to maximum but it has a higher time delay. The RC4 secure system time saved

about 60.6% when compared with AES, and PSE time saving about 72.7% when compared with AES. Thus, the PSE is the most preferred encryption system from the time delay point of view.

5. Increasing the size of the key enhances the PSNR and randomness values, but it increases the time delay as well.

References

[1] S. K. Mohammed, A. Zaki, A. Chockalingam, and B. S. Rajan, High-Rate Space–Time Coded Large-MIMO Systems: Low-Complexity Detection and Channel Estimation, *IEEE J. Sel. Topics Signal Process,3(6)*, 2009, 958-974.

[2] T. Marzetta, Noncooperative Cellular Wireless with Unlimited Numbers of Base Station Antennas, *IEEE Trans. Wireless Commun., 9(11)*, 3590-3600, 2010.

[3] R. Kudo, S. M. D. Armour, J. P. McGeehan, and M. Mizoguchi, A Channel State Information Feedback Method for Massive MIMO-OFDM, *IEEE Journal of Communications and Networks, 15(4*), 352-361, 2013.

[4] F. Rusek, D. Persson, B. K. Lau, E. G. Larsson, O. Edfors, F. Tufvesson, and T. L. Marzetta, Scaling Up MIMO: Opportunities and Challenges with Very Large Arrays, *IEEE Signal Process. Mag., 30*, 40-60, 2013.

[5] M. Matthaiou, N. Chatzidiamantis, and G. Karagiannidis, A New Lower Bound on the Ergodic Capacity of Distributed MIMO Systems, *IEEE Signal Process. Letter, 18(4)*, 227-230, 2011.

[6] National Institute of Standards and Technology, Specification for the Advanced Encryption Standard (AES), http://csrc.nist.gov/ publications/fips/fips197/fips-197.pdf, 2001.

[7] S. Fluhrer, I. Mantin, and A. Shamir, Weaknesses in the Key Scheduling Algorithm of RC4, *Proceedings of the 4th Annual Workshop on Selected Areas of Cryptography, 2259*, 1-24, 2001.

[8] M. Sabbaghian, Y. Kwak, B. Smida and V. Tarokh, Near Shannon Limit and Low Peak to Average Power Ratio Turbo Block Coded OFDM, *IEEE trans. Commun., 59(8)*, 2042-2045, 2011.

[9] Z. Iqbal, S. Nooshabadi and H. Lee, Analysis and Design of Coding and Interleaving in a MIMO-OFDM Communication System, *IEEE Trans. Consumer Electronics, 58(3)*, 758-766, 2012.

[10] Z. Iqbal and S. Nooshadi, Effects of Channel Coding and Interleaving in MIMO-OFDM systems, *IEEE 54th International Midwest Symposium on Circuits and Systems (MWSCAS)*, 1-4, 2011.

[11] R. F.H. Fischer and C. Siegl, Reed-Solomon and Simplex Codes for Peak-to-Average Power Ratio Reduction in OFDM, *IEEE Trans. Information Theory, 55(4)*, 1519-1528, 2009.

[12] G. V. Meerbergen, M. Moonen and H. de Man, Reed –Solomon Codes Implementing a Coded Single-Carrier with Cyclic Prefix Scheme, *IEEE Trans. Commun., 57(4)*, 1031-1038, 2009.

[13] D. Tse, and P. Viswanath, Fundamentals of Wireless Communication, *University Press. Print, 2005.*

[14] L. Chen and G. Gong, Communication System Security, *Boca Raton, USA: CRC Press, 2012*.

[15] Forouzan, B. A., *Cryptography & Network Security*, 2/E (English) 2nd Edition. India: Mcgraw Hill Education, 2011.

[16] Stallings, W., *Cryptography & Network Security*: Principles & Practice, Pearson; 7 edition, 2016.

[17] P. Jindal and B. Singh, A Survey on RC4 Stream Cipher, *International Journal of Computer Network and Information Security (IJCNIS), 7(7)*, 37-45, 2015.