T.C

ALTINBAS UNIVERSITY
Electrical and Computer Engineering

AES-TURBO OVER RICIAN AND RAYLEIGH FADING CHANNELS

MUSTAFA RIYADH AHMED ALBANNA

Master Thesis

Supervisor
Prof. Dr. Osman N. UCAN

Istanbul 2019

AES-TURBO OVER RICIAN AND RAYLEIGH FADING CHANNELS

By

MUSTAFA RIYADH AHMED ALBANNA

Electrical and Computer Engineering

Submitted to the Graduate School of Science and Engineering

In partial fulfillment of the requirements for the degree of

Master of Science

ALTINBAS UNIVERSITY

2019

This is to certify that I have read this thesis and that in my opinion it is fully adequate, in scope and quality, as a thesis for the degree of Master of Science.

Prof. Dr. Osman Nuri UÇAN

Supervisor

Examining Committee Members (first name belongs to the chairperson of the jury and the second name belongs to supervisor)

Prof. Dr. Osman Nuri UÇAN	School of Engineering and Natural Sciences , Altinbaş University	_____
Prof. Dr. Hasan Hüseyin BALIK	Air Force Academy, National Defence University	_____
Asst. Prof. Dr. Muhammad ILYAS	School of Engineering and Natural Sciences , Altinbaş University	_____

I certify that this thesis satisfies all the requirements as a thesis for the degree of Master of Science.

Asst. Prof. Dr. Çağatay AYDIN

Head of Department

Prof. Dr. Oğuz BAYAT

Director

Approval Date of Graduate School of

Science and Engineering: ____/____/____

I hereby declare that all information in this document has been obtained and presented in accordance with academic rules and ethical conduct. I also declare that, as required by these rules and conduct, I have fully cited and referenced all material and results that are not original to this work.

MUSTAFA RIYADH AHMED ALBANNA

DEDICATION

I would like to dedicate this work to my very first teacher, my mother, my first supporter and role model, my father and my companion throughout the journey. Without you, this dream would never come true and my brothers and my friends .

ACKNOWLEDGEMENTS

I might want to offer my thanks to every one of the individuals who have upheld me all through the regularly extended periods of this voyage. I want to thank my advisor, Prof. Dr. Osman N. UCAN for being my compass notwithstanding when I believed I was lost and being in extraordinary part in charge of the zenith of this work. I might likewise want to thank my supervisors for their supportive exhortation, which incredibly enhanced the nature of this work. Finally, I thank this institution for hosting me during these years, securely earning its place as my home. I am very thankful to my mom and dad, whose values and education motivate me to keep asking questions; to my siblings and family for their infinitely appreciated love and to my country which, although inanimate, keeps me anchored and offers me an example of resiliency.

ABSTRACT

AES-TURBO OVER RICIAN AND RAYLEIGH FADING CHANNELS

MUSTAFA RIYADH AHMED ALBANNA

M.S., Electrical and Computer Engineering, Altınbaş University

Supervisor: Prof. Dr. Osman N. UCAN

Date: July /2019

Pages: 46

Web correspondence has turned out to be increasingly basic in this advanced world as of late, and one of the significant calculations utilized is AES calculation. In any case, the vast majority of the clients have insufficient perception and information regarding such calculation execution in correspondence field, exactness and security degree are going to be indicated through clients taking into account it is of high importance to keep moving certain information's privacy. The major goal of the presented study is building encryption and error detection algorithm, to develop and implement combined Encryption and Turbo Coding Scheme : AES-TURBO , also for testing the created prototype with regard to accuracy. Initially, the AES's concept has been examined, involving definition, historical background, as well as short comparison has been carried out between AES and other algorithms. After that, channel coding has been examined, involving convolutional codes and turbo codes, third AES-TURBO was implemented over fading channels Here, the reason of choosing AES-TURBO is because it is a combination of Encryption and Turbo coding together into one single step as the examined has been clarified. Then, prototype has been created through referring to various sources, also creating MATLAB communication Simulink toolbox. Random data was provided for studying the level of security and accuracy with regard to certain developed prototype. The results indicated that the created prototype Bit Error Rate for each one of the wireless fading channels has the ability for encrypting and decrypting data adequately with no errors. Based on the results obtained from this study, it might be indicated that the provided prototype showed improved security and accuracy in the case when transferring data between the sender and

the receiver. The results of comparison showed direct impact of applying AES-TURBO upon Rician and Rayleigh channels. The presented study has the aim of providing understanding to readers regarding AES-TURBO algorithm. More researches regarding such topic is suggested for increasing the effectiveness regarding Bit Error Rate at wireless channels implemented in communication field.

Key-words: Advanced Encryption Standard(AES), Turbo Coding, Encryption and Error Correction.

TABLE OF CONTENT

Pages

LIST OF TABLES ..... **xi**

LIST OF FIGURES ..... **xii**

LIST OF ABBREVIATION ..... **xiii**

1. INTRODUCTION **1**

1.1 OVERVIEW 2

1.2 RESEARCH PROBLEM STATEMENT 2

1.3 MOTIVATION 4

1.4 FADING 4

1.5 CRYPTOGRAPHY 4

1.6 RESEARCH OBJECTIVES 5

1.7 LITERATURE REVIEW 5

1.8 THESIS STRUCTURE 5

2. RELATED WORKS **7**

2.1 ADVANCE ENCRYPTION STANDARD (AES) 7

2.2 AES-TURBO 13

2.3 BIT ERROR RATE (BER) 16

2.4 AVERAGE SIGNAL-TO-NOISE RATIO (SNR) 16

2.5 Eb/No 16

2.6 QPSK MODULATION AND DEMODULATION 16

2.6.1 QPSK Modulation 17

2.6.2 QPSK Demodulation 17

2.7 CHANNEL CODING 18

2.7.1 Block Codes 19

2.7.2 Convolutional Codes 19

2.7.3 Turbo Codes 20

2.8 FADING CHANNELS 22

3. METHODOLOGY **23**

3.1 MATLAB 23

3.2 AES-TURBO IMPLEMENTATION 23

3.3 SYSTEM OBJECTS OF THE COMMUNICATIONS SYSTEM TOOLBOX 23

3.3.1 Generating Random Data 25

3.3.2 QPSK Modulation /Demodulation 25
3.3.3 Additiive White Gaussian Noise AWGN 26
3.3.4 Fading Channels 26
3.3.4.1 Rician fading 26
3.3.4.2 Rayleigh fading 26
4. DISCUSSION THE RESULTS 27
4.1 INTRODUCTION 27
4.2 BER RESULTS 27
4.2.1 BER Results Over AWGN Channel 27
4.2.2 BER Results Over Rician Channel 29
4.2.3 BER Results Over Rayleigh Channel 36
5. CONCLUSIONS AND RECOMMENDATIONS 40
5.1 CONCLUSIONS 40
5.2 RECOMMENDATION FOR FUTURE WORK 41
REFERENCES 42

LIST OF TABLES

Pages

Table 4.1: (BER) values over (AWGN)…….……..28

Table 4.2: (BER) values over Rician channel at K=10……...…….30

Table 4.3: (BER) values over Rician channel at K=20……...…….32

Table 4.4: (BER) values over Rician channel at K=30……...…….34

Table 4.4: (BER) values over Rician channel at K=100…….…….36

Table 4.6: (BER) values over Rayleigh channel…….38

LIST OF FIGURES

Pages

Figure 1.1: the four major aspects ……..…….1

Figure 2.1: Add Round Key…….…….8

Figure 2.2: SubBytes……..…….9

Figure 2.3: ShiftRows……..…..……10

Figure 2.4: MixColumns……..……..……10

Figure 2.5: AES Encryption process……..…….……..11

Figure 2.6: AES Decryption process……..……..…….12

Figure 2.7: AES-TURBO Encryption…….…….14

Figure 2.8: AES-TURBO Decryption…….……..……15

Figure 2.9: Turbo coder with two branches…….……21

Figure 2.10: Turbo Decoder with two branches…….……..……21

Figure 3.1: system objects toolbox……..……26

Figure 4.1: (BER) performance over (AWGN)…….…….…….28

Figure 4.2: (BER) performance over Rician channel at K=10…..…….…….29

Figure 4.3: (BER) performance over Rician channel at K=20…..…….…….31

Figure 4.4: (BER) performance over Rician channel at K=30…..…….…….33

Figure 4.5: (BER) performance over Rician channel at K=100…….…….35

Figure 4.6: (BER) performance over Rayleigh channel…….….37

LIST OF ABBREVIATION

AES	: Advance Encryption Standard
BER	: Bit Error Rate
EbNo	: Energy per Bit
SNR	: Signal to Noise Ratio
AWGN	: Additive White Gaussian Noise
QPSK	: Quadrature Phase Shift Keying
FEC	: Forward error correction
BEC	: Backward error correction
SISO	: Single Input Single Output
MIMO	: Multiple Input Multiple Output
AES-TURBO	: A Combined Encryption and Error Correction Scheme
LOS	: Line of Sight
RSC	: Recursive Systematic Convolutional

1. INTRODUCTION

Networking has been developed very rapidly and the world becomes interconnected with the internet more and more. All everyday issues require to convey data frameworks on the web. These data frameworks may utilize various innovations, for example, dispersed information stockpiling frameworks, encryption and validation procedures, remote access and web administrations , As the volume and advancement of PC system assaults increases [4]. This is proved by wide arrangements of numerous remote and wired systems of different sizes and topologies, such as (PANs), (LANs), (MANs), and (WANs), these networks can be of different topologies and formations [6], Keeping data correct and safe are the most challenging research domains of our time. Four major aspects are required to ensure security for the communications and networks. First of all, confidentiality of data that helps information to be private and confidential information isn't approachable or discovered for un-authorized entities. Secondly, integrity of data which helps that programs and information to be modified only via using authorized approach. Third data authentication which assures that system works promptly and each input enter to the system came from commit source. Finally, freshness that is preventing receiver or sender from rejecting transferred message [5], to do so data encryption and error correction techniques are required. Figure 1.1 shows the major aspects which is required to ensure security for networks .

Figure 1.1: the four major aspects.

1.1 OVERVIEW

Error can be defined as condition when send and received information aren't same as each other. During transmission, signals suffer from distortion and also suffering from noise which might make the binary errors in data bits that are moving between systems. This drives at one bit might be exchanging to zero bit might be exchanging to one. When moving data, it could be subjected to mixing through commotion or might be tainted. For the purpose of preventing this, the study will apply error-detecting codes, they are specified as additional bits which are added to certain digital message which is helping in catching when error happens throughout data transmission [6]. Error detection and correction has big technical impact for enhancing data integrity across noisy communication channels by adding extra information so fault data bits can be detected and gives the ability to restore the original data easily, there are too many channel coding algorithms according to my thesis I used turbo codes which will be explained in details at the next chapters .

Security is now a sensitive and serious issue, whether in cyber or real world. The security of the network is a complicated issue, the systems of security are majorly dependent on certain cryptographic algorithms like asymmetric-RSA, AES, and symmetric-DES. The perfect assumption is using more than one algorithm and its combination to get an optimal level of security, the world is becoming more related to the internet and the security of networks is of high importance to governments, military, organizations, as well as for personal computer users. Network security is the protection of hacking in any possible way, abuse or hacking of directories or data base in computer network system. Through improving the security of networks, the possibility of privacy spoofing will be decreased, also decreasing the identify or information theft, to secure networks, cryptography is of high importance [7]. Utilizing cryptography might be providing security to all documents, directories or files. Cryptography can be specified as the science which handle complex logics and mathematics for implementing solid encryption technique. Cryptography was classified into 2 major types: Symmetric (Secret Key) and Asymmetric (Public Key). The major approach to protect resources of network is providing it with distinctive identity associated to passwords. The developers were forced via the internet to improve data security. Before the current period, cryptography has been only focused on classification and transformation of message from recognized structures to muddled ones and

vice versa, rendering it mixed up through spies or interceptors with no mystery information. Encryption attempted on ensuring the communication's secrecy in order that only the intended individuals might find it and process it. Cryptography conversion of information from clear and easy to read state to clear nonsense. The sender shared the Decoding technology that is needed to recreate the original data , thereby to prevent unwanted persons from doing the same.

1.2 RESEARCH PROBLEM STATEMENT

The field of portable and remote correspondences has a noteworthy history that degrees over a time of innovative changes. remote is one of the most boundless center innovation empowering influences for specific figuring and correspondences applications. It is essential to help the nature of administration just as decrease time ,mistakes and asset utilization in remote correspondence arranges by drop down the losing likelihood of information parcels. A channel arranged by Gaussian clamor characterizes a breaking point, it is about the most extreme channel limit and mistake free transmission rates for an offered sign to-commotion proportion (SNR) and the channel data transfer capacity, known as Shannon's Limit. For information transmission with high piece blunder rate, remote frameworks needs usage of coding methods. Channel coding is a procedure of encoding information at a correspondence channel that appends examples of repetition in the transmission way to diminish the mistake rate [8]. In a controlled way, the quantity of images in the source encoded message is stretched out in order to help two primary targets of mistake location and blunder redress at the recipient end. The total of blunder identification and remedy required and its proficiency wards on SNR. The outstanding edge of forward blunder remedy is that a back-channel isn't fundamental and can avoid retransmission of information more often than not however in the other hand the misfortunes of higher data transfer capacity prerequisites by and large. Repetition is added to transmitted information at forward blunder redress as equality check bits. By and large, more the age at equality bits per information bit, and more the potential mistakes can be distinguished additionally amended. Distinctive forward mistake redress advantage various techniques is to check and address blunders and endeavors to shut in the breaking point that is recommended by Shannon for information transmission. Here, convolution and turbo codes are assessed , and their dissimilarities are quickly examined, likewise the advantages and disadvantages of each methodology are clarified.

1.3 MOTIVATION

The BER(bit error rate) is the most important limit in wireless communications for the quality measurement of recovered data. During the transmission Data may get corrupts it is necessary for Some applications for detecting and correcting those errors. With developing communications, transmitted data size will be much bigger and bigger so that it is very important to develop new methods for error correction over fading channels .

1.4 FADING

fading is the time variety of gotten sign power because of changes in transmission medium or ways , most remote correspondence frameworks are utilized in and around focal point of populace. The transmitter is situated over a tall structure or tower and it emanates at the most extreme permitted control. In the other hand, the beneficiary is well underneath the encompassing buildings [9]. Thusly, the remote channel is impacted by the encompassing structures, for example, vehicles, structures, the remote channel can be portrayed as a component of reality and the got sign is the mix of numerous reproductions of the first sign impinging at recipient (RX) from a wide range of ways . The sign on these various ways can valuably or dangerously meddle with one another. This is alluded as multipath. On the off chance that either the transmitter or the collector is moving, at that point these spread wonders will be time fluctuating, and blurring happens. Notwithstanding spread weaknesses, different marvels that breaking point remote interchanges are commotion and impedance. It is intriguing to see that remote correspondence wonders are chiefly because of dissipating of electromagnetic waves from surfaces or diffraction. over and around structures. The plan objective is to make the gotten power satisfactory to beat foundation commotion over each connection, while limiting obstruction to other progressively inaccessible connections working at a similar recurrence. There are numerous sorts of blurring models, for example, Rayleigh, Rician and Nakagami dispersions. At our research we used Rayleigh and Rician channels simulation in this research.

1.5 CRYPTOGRAPHY

Cryptography is the practice for encoding transferred data so that it can be decoded only by specific people. so that only the intended individuals have the ability of reading and processing

it. Earlier, cryptography was adequately comparable with encryption, changing data from justifiable state to clear drivel [10] . cryptosystem is the system which is used for performing the whole procedure in both sides. These routinely contains a procedure steps for joining original sent ("plaintext") with at least one “keys” , the single key may be number or strings of characters and it should be recognized just via recipient and sender. The output is usually known as (“ciphertext”) . usually a good cryptosystem has a big range of keys so that it is difficult or impossible to try all the keys. A strong cryptosystem which creates encrypted text that appears to be random and arbitrary to all the tests also can resist all known techniques for breaking codes. Key permits the ciphertext to be decrypted and allows the plaintext to be encrypted. There are 2 major types regarding encryption: asymmetric (public key) and symmetric (secret key).
There are many algorithms for encrypting/decrypting data based on these sorts. Some of the most common and familiar are listed below:

• (DES)
• (AES)

1.6 RESEARCH OBJECTIVES

The major aim of the presented study is implementing Combined Encryption And Error Correction Scheme (AES-TURBO) [1] with the use of matlab communication tool box [3] , passing the encrypted signal through multiple wireless channels and comparing BER performance for all cahnnels and recogniing the impact of AES-TURBO on such channels .

1.7 LITERATURE REVIEW

AES-TURBO scheme [1], has been presented and carried out, such combined performance of the systems has been assesed in AWGN channel type. The results have been compaired with system implementing perfect decryption and encryption [1].

1.8 THESIS STRUCTURE

In this section, we divided thesis into five chapters, which are structured around the objectives of the research. Thesis was organized as follows:

CHAPTER ONE: this chapter (introduction) presents the overview about our topic for background related and description, this chapter process the problem statement that foundation of the aim and objective that can formulate by the research.

CHAPTER TWO: In this chapter, we discuss the information on the problem. Moreover, we describe all the related topics which is discussed in the research the advantage and disadvantage, present the type of fading distribution channels and approaches. In addition, channel coding , Advanced Encryption Standards we also explained AES-TURBO also presented in this chapter.

CHAPTER THREE: discusses the procedure of the simulation and implementation . The software that run the algorithms and simulate the results. We used matlab communication toolbox , The usage of this software and the steps taken to run the experiments and collect the results , the computing environment used. In addition, the command which is used to create the required matlab objects.

CHAPTER FOUR: discusses the results of the simulation. Bit Error Rate for each case including the affection of error correction scheme .

CHAPTER FIVE: presents the conclusions drawn from the simulation and comparing our study with previous studies . Finally, future work are also presented.

2. RELATED WORKS

2.1 ADVANCE ENCRYPTION STANDARD (AES)

With regard to the cryptography field, AES can be defined as encryption standard of symmetric key, there are 3 block ciphers related to such standard, which are AES-128, AES-192 in addition to AES-256 that is referred to as Riijndael. Each one of those ciphers have block size of 128-bit, while the key sizes are 128, 192 and 256 bits. The design principle of substitution permutation network is the base for AES. Furthermore, it is fast in hardware as well as in software [2]. AES is operating on (4 x 4) byte's matrix, indicated as state. In distinctive finite field, the majority of AES calculations are conducted. AES cipher can be defined as the number of repetitions that are related to the transformation rounds which are converting input plain-text to cypher-text's final output. Each one of the rounds includes many steps of processing, involving one which is based on encryption key. Set regarding reverse rounds have been utilized for transforming the ciphertext to the original plain-text with the use of the identical encryption key [5]. Key expansion is the initial stage, keys will be derived from cipher key with the use of Rijndael's key schedule, then the number of rounds will be achieved depending on key size 128-bit key it is 10 rounds. Cipher includes N rounds, in which number of rounds is based on length of key. First N - 1 rounds include 4 unique transformation functions: Sub-Bytes, Shift-Rows, Mix-Columns, in addition to the Add-Round-Key, that will be specified later. The last round includes just 3 transformations, also there is initial single transformation (Add-Round-Key) prior to the initial round, that might be specified as Round 0 at Initial Round.

Each state's byte will be combined with round key with the use of bitwise XOR, then the other steps of AES rounds will be carried out in the following way:

1.Sub-Bytes: nonlinear step of substitution in which each one of the bytes will be subjected to replacing with other depending on lookup table.

2.Shift-Rows: a step of transposition in which each one of the state rows will be subjected to shifting cyclically a specific number of steps.

3.Mix-Columns: an operation of mixing in which it is operating on state's columns, combining 4 bytes in each one of the columns.

4.Add Round-Key with the use of bitwise XOR.

All step excluding Mix-Columns will be performed in the last round.

1. Add Round-Key

With regard to this step, sub-key will be combined with state. Regarding each one of the rounds, sub-key will be derived from the major key with the use of the key schedule of Rijndael; each one of the sub-keys have the same size as state [5]. Subkey will be added through the combination of every one of the state bytes with matching byte regarding subkey with the use of bitwise XOR.

In Add Round-Key, each one of the state bytes will be combined with byte related to round sub-key with the use of XOR operation . Figure 2.1 describe the step of Add Round-Key.

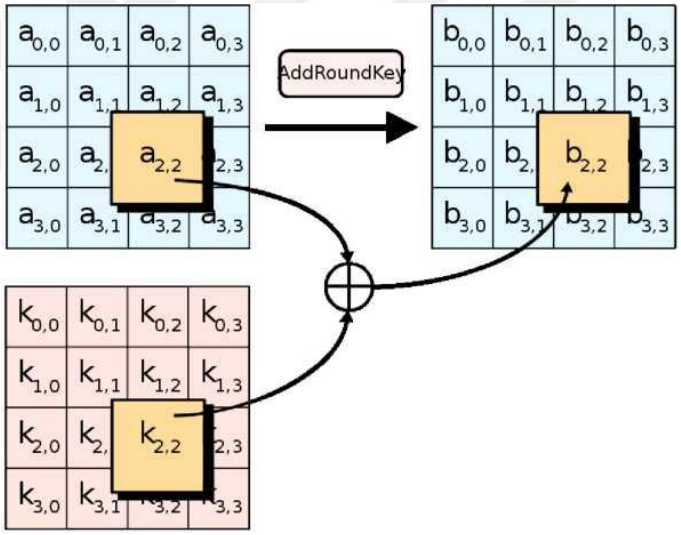

Figure 2.1: Add Round-Key [2]

2.Sub-Bytes

With regard to this step, each one of the matrix bytes will be subjected to updating with the use of substitution box of 8bits, Rijndael S-box. Such operation is providing the cipher with nonlinearity. The applied S-box has been derived from multiplicative inverse over, recognized for having excellent properties of nonlinearity. For avoiding certain attacks depending on straightforward algebraic properties, S-box will be created through combining inverse function with invertible affine transformation[5]. Furthermore, S-box will be chosen for avoiding all fixed points (so is derangement), also all opposite fixed points. With regard to this step, each one of

the state bytes will be replaced with its entry in fixed lookup table of 8bits. Figure2.2 describe the step of Sub-Bytes.

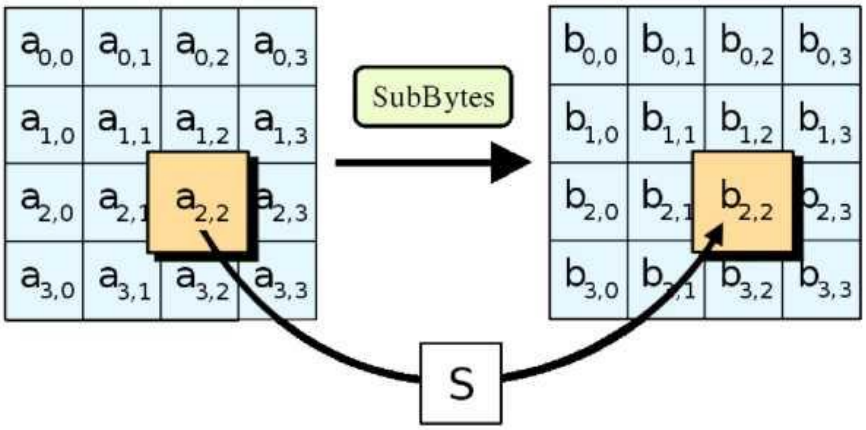

Figure 2.2: Sub-Bytes [2]

3.Shift-Rows

This step operates on the state's rows, it will be shifting bytes in a cyclic way in each one of the rows through specific offset. With regard to AES, first row will not be changed. Each one of the bytes in second row will be shifted one to left. Correspondingly, third and fourth rows will be shifted through offsets of 2 and 3.

The pattern of shifting is the same for block sizes of 128bits and 192bits. In such approach, each one of the columns regarding output state of Shift-Rows will be made up of bytes from every one of columns related to input state. (Rijndael variants with large block size have a little distinctive offsets). With regard to the condition of 256bit block, first row will not be changed and shifting for second, the third and the fourth rows will be one byte, three bytes and four bytes – such change will be ony applied in Rijndael cipher in the case when applied with 256bit block, since AES doesn't utilize 256bit blocks [5]. At this point, Aij is from the ciphertext, while Bij is from the key. Figure2.3 show the step of Shift-Rows.

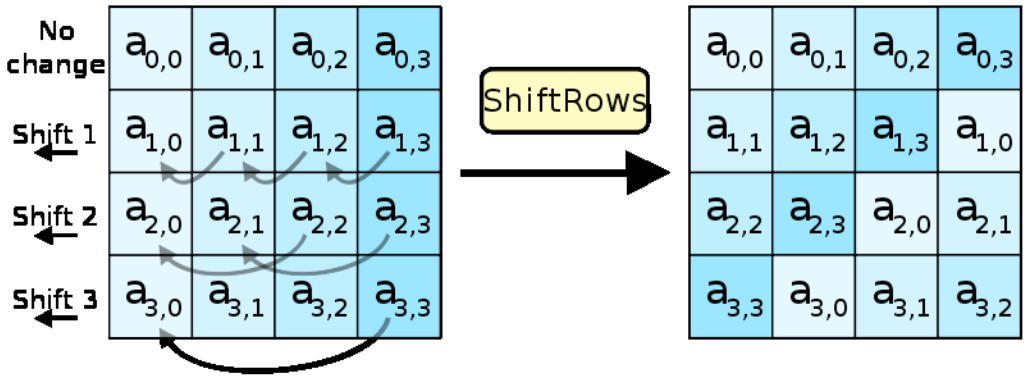

Figure 2.3: Shift-Rows [2]

4. Mix-Columns

With regard this step, the 4 bytes related to each one of the state's columns will be combined with using invertible linear transformation. The function of Mix-Columns takes 4 input bytes and 4 output bytes, in which each one of the input bytes impacting the 4 output bytes. In addition to the Shift-Rows, the step of Mix-Columns will offer diffusion in cipher. Throughout such operation, each one of the columns will be multiplied by recognized matrix for 128bit key is The multiplication operation will be specified as: multiplying by one meaning no change, multiplying by two indicating left shifting for the byte and multiplication by three indicates left shifting and after that conducting XOR with initial un-shifted value[5]. Following shifting, conditional XOR with 0x11B must be conducted in the case when shifted value larger in comparison to 0xFF. Figure 2.4 shows the step of Mix-Columns.

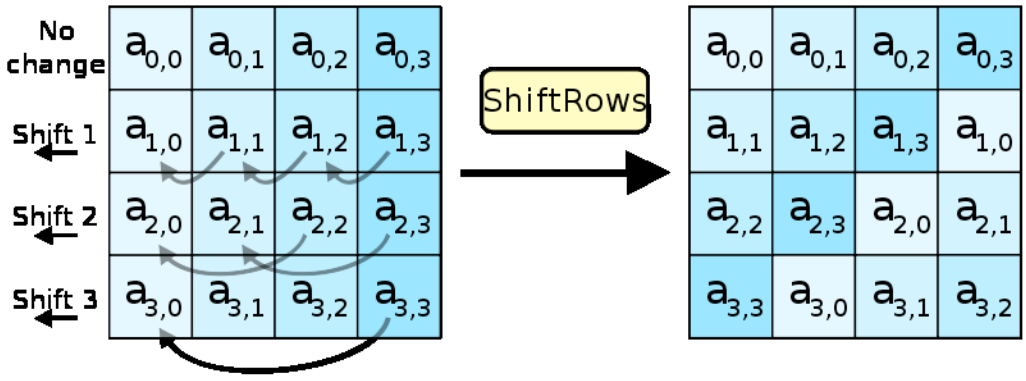

Figure 2.4: Mix-Columns [2]

All the indicates steps will be repeated at each one of the rounds in the process of encryption as can be seen in figure 2.5

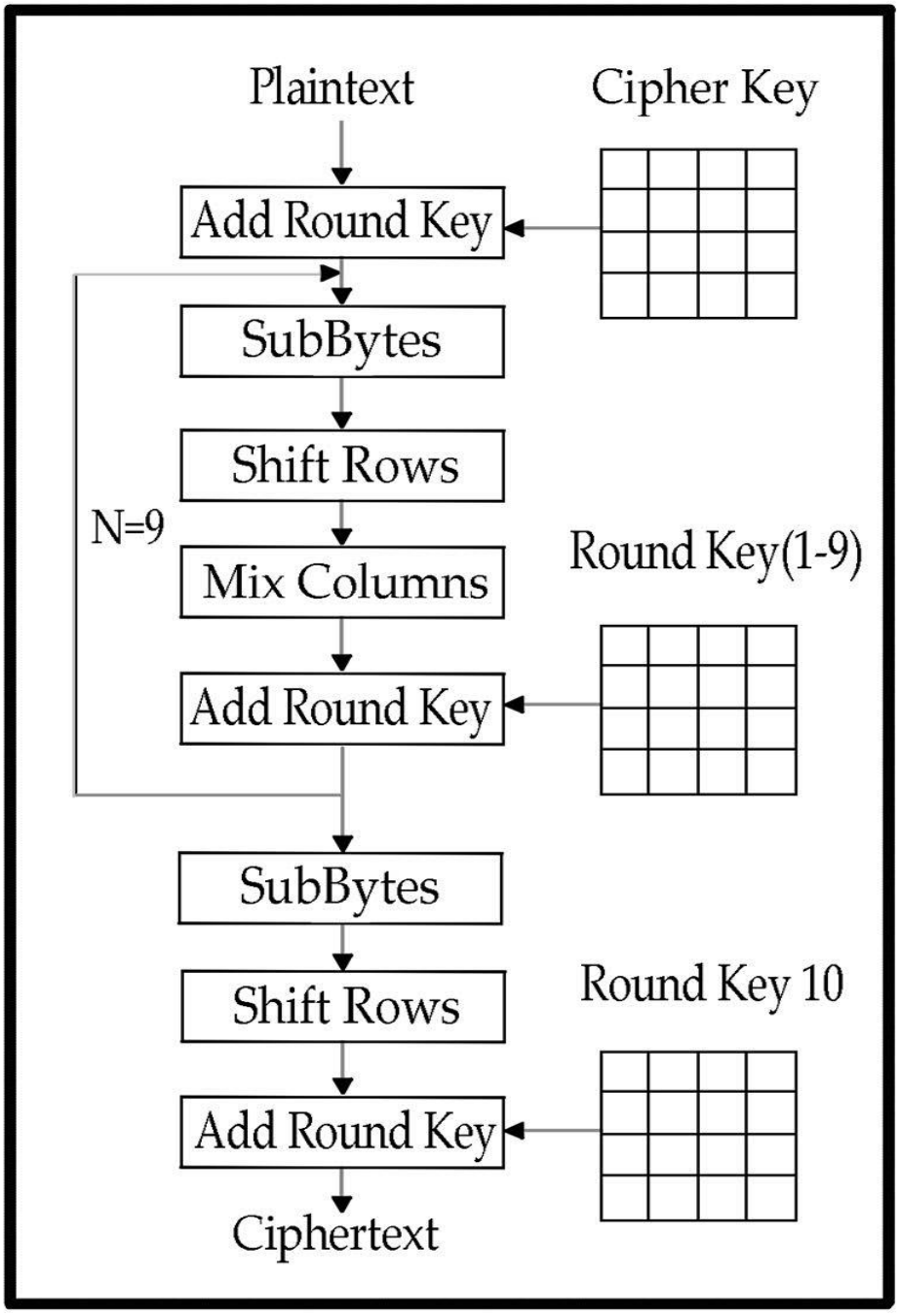

Figure 2.5: The process of AES Encryption [1]

With regard to the process of decryption, opposite operations inverse shift rows, inverse Mix columns and the opposite rounds will be achieved for reforming original plaintext as can be seen in figure 2.6

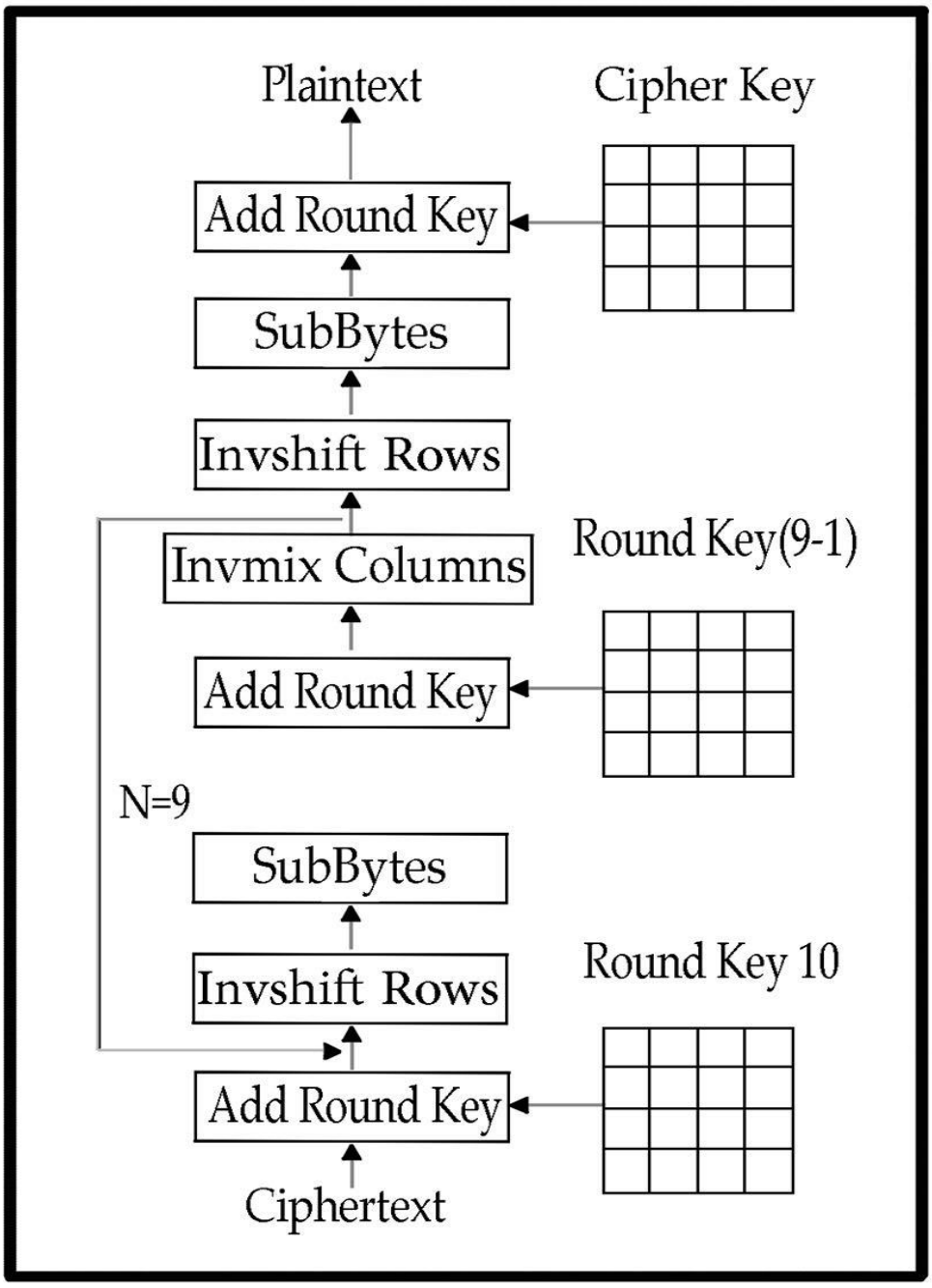

Figure 2.6: The process of AES Decryption [1]

2.2 AES-TURBO

Error correction and Encryption are applied to be separately handled; AES-TURBO can be specified as combination regarding encryption and error correction that is referred to as Combined Encryption and Turbo Coding Scheme: AES-TURBO" [1], AES is applied for encryption/decryption, the Turbo codes are utilized for Encoding/Decoding. The Turbo Encoder block will be embedded in the encryption block of AES in first round after sub-bytes block. Remaining steps related to the AES encryption will be normally followed. With regard to the phase of decryption, Turbo Decoder block will be embedded in the AES Decryption block in final round prior to the Sub-Bytes block. Remaining steps related to AES decryption will be normally followed.

Figure 2.7 indicates AES-TURBO at system's sender side.

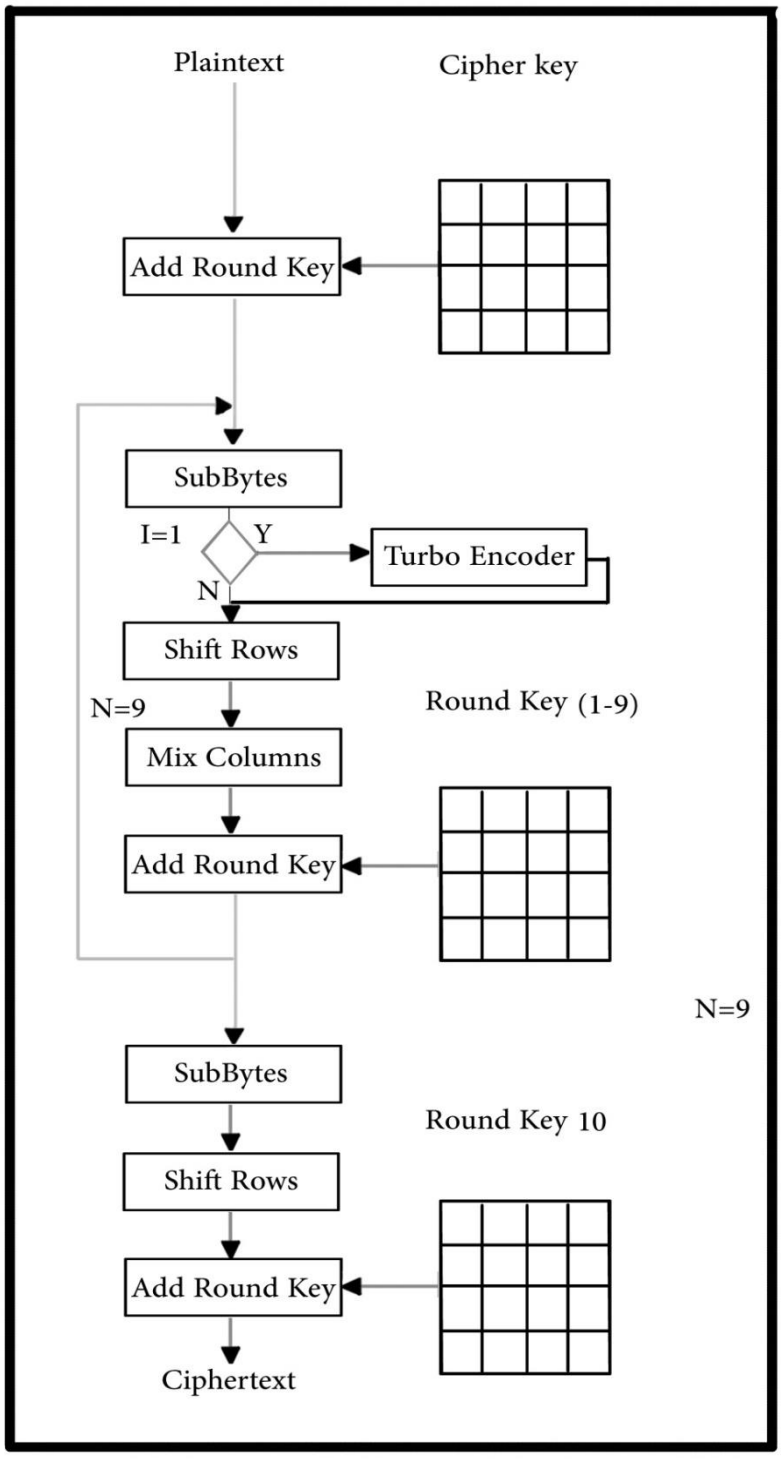

Figure 2.7: AES-TURBO Encryption [1]

Figure 2.8 indicates AES-TURBO at system's receiver side.

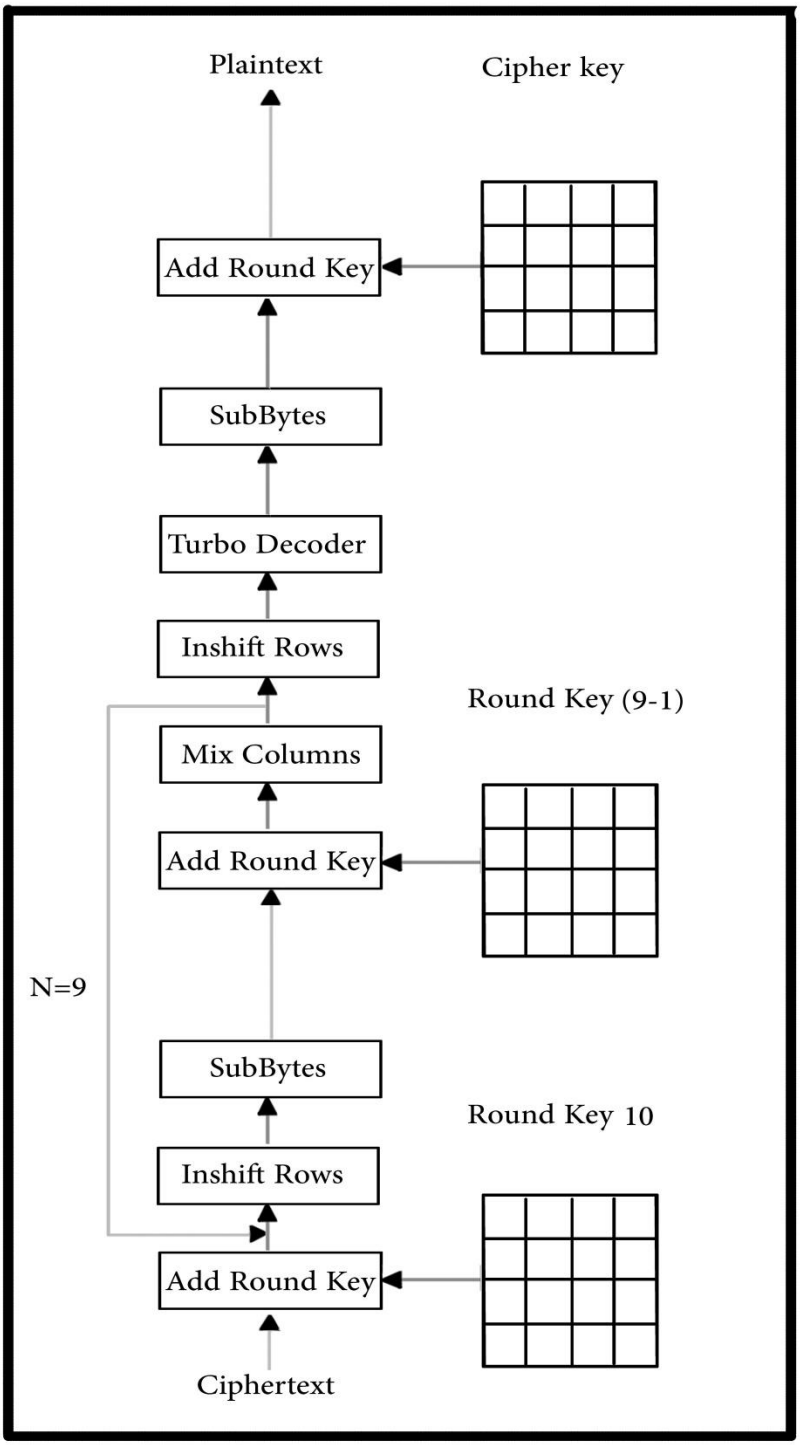

Figure 2.8: AES-TURBO Decryption [1]

2.3 BIT ERROR RATE (BER)

This is the major measurement regarding the performance of the system, since it's measuring the efficiency of transferring bits end-to-end. Whereas such performance is impacted through certain factors like distortion and signal-to-noise, eventually it might be defined as the capability of receiving error-free information which specify the quality regarding the link. BER is specified as the number of the bits which are received in error, divided by total number of received bits [11]. Furthermore, it is the percentage of bits which have errors relative to total number of received bits in transmission, typically specified as ten to a negative power. BER can be defined as indication regarding how frequently packets or other units of data must be retransmitted due to errors. In the case when BER is higher than what is normally anticipated for system, this might specify that slow data rate might enhance the total transmission time with regard to certain amount of the transmitted data due to the fact that BER could be decreased, reducing the number of packets which must be re-sent.

2.4 AVERAGE SIGNAL-TO-NOISE RATIO (SNR)

SNR is a major applied and recognized performance measure characteristic with regard to the digital communication systems. Frequently, this is measure of receiver's output and therefore associated to the process of data detection [12]. SNR specify the power ratio between signal (meaningful information) and background noise. Both signal and noise power (or amplitude) should be measured at equivalent or same system points, also in same system bandwidth. Due to the fact that a lot of signals have extremely wide dynamic range, SNR is typically defined with regard to logarithmic decibel scale. In decibels, SNR defined as ten times logarithm of power ratio.

2.5 Eb/No

Eb/No is typically specified as Energy ratio for each Bit (Eb) to Spectral Noise Density (No). Eb/No is measuring SNR with regard to digital communication systems [13]. It might be measured at input to receiver and applied as basic regarding the strength of signal. Various modulation forms have various curves regarding theoretical bit error rates versus Eb/No.

2.6 QPSK MODULATION AND DEMODULATION

2.6.1 QPSK Modulation

With regard to the methods of digital modulation, set of basis functions are selected for specific scheme of modulation. Typically, the basis functions are considered to be orthogonal to one another. The basis functions might be obtained with the use of 'Gram Schmidt orthogonalization' process. As soon as electing the basis function, all vectors in signal space could be specified as linear combination regarding basis functions. With regard to QPSK, there are 2 sinusoids (cos and sin) are provided as modulation's basis functions [14]. Modulation can be accomplished through different phase regarding basis functions based on symbols. With regard to QPSK, modulation is specified to be symbol based, in which single symbol includes two bits. QPSK modulator could be achieved in the following way. De-multiplexer (or serial to parallel converter) will be applied for separating even and odd bits from produced information bits. Every one of the even bits (in-phase arm) and odd bits (quadrature arm) will be converted to NRZ format in parallel approach. Signal on in-phase arm will be multiplied by the cosine component, while signal on quadrature arm will be multiplied by the sine component. QPSK modulated signal will be acquired through adding signal from quadrature arm and arm [17].

2.6.2 QPSK Demodulation

With regard to the QPSK demodulator, coherent demodulator will be provided as example. With regard to the technique of coherent detection, knowledge related to carrier frequency and phase should be recognized via receiver. Which might be carried out with the use of phase lock loop at receiver[14]. Essentially, the phase lock loop will be locking incoming carrier frequency as well as tracking variations in phase and frequency. With regard to the upcoming simulation, PLL won't be utilized, however the output regarding phase lock loop will be utilized. For the purpose of demonstrating, an assumption will be made that the carrier phase recovery is achieved and using generated reference frequencies at receiver (cos (ωt)) and (sin(ωt)). With regard to de-modulator, received signal will be multiplied by reference frequency generators (cos(ωt)) and (sin(ωt)) on separate arms (quadrature and in-phase arms). Multiplied output on all arms will be integrated over 1-bit period with the use of the integrator. Threshold detector will make decision on all integrated bits according to the threshold. Ultimately, bits on quadrature arm (odd bits) and in-phase arm (even bits) have been remapped for creating detected information stream. The

detector related to the in-phase arm will be specified below. With regard to the quadrature arm, below architecture is the same, yet sin(ωt) basis function should be applied [17].

2.7 CHANNEL CODING

Communication channels are presenting interference and noise for corrupting transmitted signals. With regard to receiver, channel corrupted transmitted signals will be mapped to binary bits. Received binary information can be considered as an estimation with regard to transmitted binary information. The bit errors might be caused because of transmission and number of bit errors is dependent on amount of interference and noise in communication channel. Frequently, the channel coding is utilized in the systems of digital communication for protecting digital information from interference and noise as well as reducing the number of bit errors. Majorly, the channel coding is achieved through the selective presenting of the redundant bits to transmitted information stream. Such additional bits are going to enable correction and detection of bit errors in received data stream as well as providing reliable information transmission. Costs related to utilizing channel coding for protecting information is decrease in the data rate or increase in the band-width, the major aim of channel coding is encoding information which is sent over communication channel in a way that the existence of channel noise, errors might be detected and/or corrected. The presented study will differentiate between 2 coding techniques, the first one is Backward error correction (BEC) which is requiring just error detection: in the case of detecting error, sender will be requested for message's re-transmission. Whereas such technique is straightforward and set low demands on code's error-correcting properties, it is requiring duplex communication and result in unwanted delay in transmission, the other technique is Forward error correction (FEC) which is requiring that the decoder must have the ability of correcting specific number of errors, i.e. it must have the ability to locate positions in which errors happened. Due to the fact that FEC codes needs just simplex communication, they are particularly used in systems of wireless communication for improving the system's energy efficiency [16].

There are three types of channel codes.

1) Block Codes

2) Convolutional codes

3) Turbo Codes

2.7.1 Block Codes

Block codes have been based rigorously on the abstract algebra and the arithmetic of the finite fields. They may be utilized for either the detection or the correction of the errors. Block codes get a block of k information bits and create a block of n coded bits. Via pre-determined rules, n-k redundant bits will be added to k information bits for the sake of forming n coded bits. Typically, those codes are known as (n,k) block codes. Some of the typically utilized block codes are the Hamming codes [23], There is a wide variety of ways for decoding the block codes and estimating k information bits.

2.7.2 Convolutional codes

Convolutional codes are a very commonly utilized channel codes in the systems of the practical communications. Convolutional codes are different from the block code via an operation approach. A convolutional encoder operates over the serial data, while the block codes operate over an input data block. In addition to that, memory elements' utilization is different in convolutional encoders. In block codes' case, there isn't any memory element which is involved in generating the encoded data. Those codes are advanced by a distinct strong mathematical structure and are mainly utilized for error corrections in real time. Convolutional codes are responsible for the conversion of the whole data stream to a single code-word. The encoded bits depend on the current input bits as well as previous bits of the input. The basic strategy of decoding for the convolutional codes has been based on the commonly utilized algorithm of the Viterbi. Convolutional codes can be represented as (n,k,L), n represents the number of the output bits from encoder, k represents the number of the input bits into the encoder and L represents the encoder's constraint length. Dissimilar expressions for the length of the constraint are typically found in various textbooks, however, the main concept is the same. The length of the constraint is utilized for the calculation of the number of the stages of memory or flip-flops which are utilized in the encoder. If L and the underlying formula are known, there is an ability for calculating how many memory stages (m) there are. Therefore, it isn't actually important the utilized expression for L [23].

The convolutional encoder may as well be characterized with the use of the finite state machine. The whole convolutional encoder's behavior is represented with a state diagram. The number of the states in the state diagram is dependent on the number of encoder's memory elements. In case where the memory elements' number = m, then the number of the states in the diagram of the state = 2×m.

2.7.3 Turbo Codes

In modern communication systems, forward error correction coding is a mandatory tool that is used broadly to improve the efficiency of the bit error rate of any of the communication systems usually at a cost in the reduction of transmission rate and increased computational complexity. Turbo code consists of two convolutional codes with interleaver. In a simplified turbo code, there are 2 recursive systematic convolution (RSC) encoders in a parallel manner with puncturing which is used to delete some parity bits. The information bits are damaged prior to the point where they enter the 2^{nd} encoder[16]. The code-word in the turbo code is made up of input bits that is to say, the code can be referred to as systematic – followed by bits of parity check from the 1^{st} encoder and after that, the bits of the parity from the 2^{nd} encoder.

The Random Interleaver re-arranges its input vector elements with the use of an arbitrary permutation. The received data undergoes re-arranging with the use of a set of produced indices of the permuter. Essentially, a permuter produces pseudorandom permutations of specific addresses of the memory. Data is arranged based on the pseudorandom memory address order. The deinterleaver has to be aware of permuter-indices precisely in the accurate order like the interleaver. The deinterleaver performs the arranging of interleaved data back to original state through the knowledge of permuter-indices.

The simplified turbo code block diagram in Figure 2.9 .

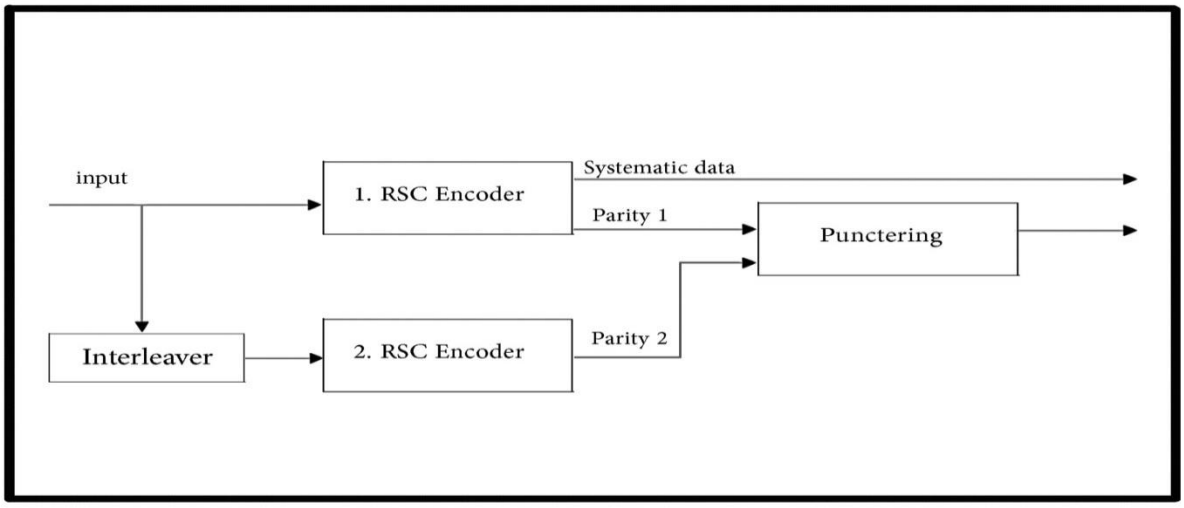

Figure 2.9: Turbo coder with two branches [1]

The simplified turbo decode block diagram in Figure 2.10 .

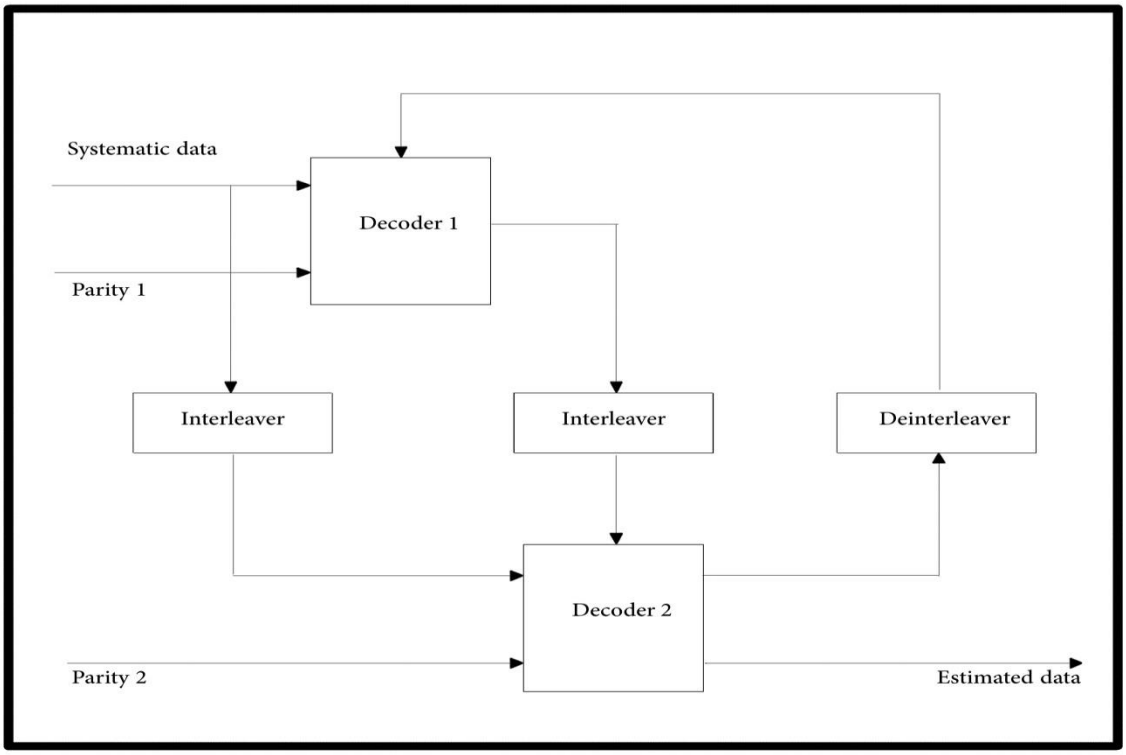

Figure 2.10: Turbo Decoder with two branches [1]

2.8 FADING CHANNELS

In the communication systems' study, the classic (optimal) additive-white-Gauss-noise (AWGN) channel, with samples of the statistically independent Gauss noise which corrupt the samples of the data free of the inter-symbol interference (ISI), is the typical start point for the understanding of the main relations of performance. The distorting which is experienced by the carrier signal throughout the transmitting can be referred to as fading and is a result of the multi-path propagation [17]. Fading may be defined as:

- Fast Fading: which takes place in the case where there's a high spread spectrum of Doppler in channel and the time of the coherence < symbol period.
- Slow Fading: which takes place in the case where there's a low spread spectrum of the Doppler in the channel and the time of the coherence > symbol period.
- Flat Fading: which takes place in case where the signal's band-width and delay spread is <channel band-width and symbol period respectively.
- Frequency Selective Fading: which takes place in case where the signal band-width and the delay spread is > channel band-width and symbol period respectively.

The coherence time term is that the time duration where the channel's impulse response is unchanged. The time which is required for completing one symbol is known as the symbol time.

At our thesis we focused on two fading channels which is considered as slow fading those two fading channels are Rician and Rayleigh

- Rayleigh Fading: in the case where there aren't any LOS paths between the transmitter and the receiver, however, only have indirect path than the resulting signal which is acquired at receiver is going to be the summation of all scattered and reflected waves [18].
- Rician Fading: which takes place in the case where there's an LOS in addition to the non-LOS path between transmitter and receiver, in other words, the acquired signal comprises on both direct and scattered multi-path waves [18].

3. METHODOLOGY

3.1 MATLAB

MATLAB is a commonly utilized programming language for developing algorithms, visualization, data analysis, as well as numerical computations and a development environment of high-level for the numerical calculations and mathematical modeling. Simulink has also been utilized, an environment for the graphic design for model-based design and system simulations, in addition to the variety of tool-boxes for MATLAB– application-specific components of libraries making modeling applications task in MATLAB simpler. For instance, for the sake of modeling the systems of communications, functionalities from Communication System Tool-box are used. The tool-box includes tools to design, prototype, simulate, and verify the communication systems, which include the wireless standards in each of Simulink and MATLAB. System objects can be defined as a group of algorithmic building blocks which are suited for the system design which is available in a variety of MATLAB tool-boxes. Those are self-documented algorithms, making the task of MATLAB test-benches' development for the easier performance of the system simulations. Through covering many different algorithms, they also remove the requirement for the recreation of fundamental communication systems' building blocks in C, MATLAB, or any other programming language [3]. System objects have been designed to model and simulate as well as provide implementation support. MATLAB has a long history in the design of the communication systems and is utilized by academics as well as the practitioners. It provides the designers with the opportunity of focusing on the algorithms instead of the low-level programming. A great deal of its characteristics and abilities are optimal to model the wireless systems it includes an interactive environment and program which match science's exploratory nature; it guarantees smooth access to the algorithms and data; and it has visualization tools, data analyses, and algorithm development.

3.2 AES-TURBO IMPLEMENTATION

A function is a group of statements that performs a task together according to specific entries , we created a Function for each step of AES-TURBO in order to call those functions as much as we need , at the encryption and decryption processes [1] .

The input of AES-TURBO is 128 bit of data , input binary data should be converted to 4*4 byte matrix to do so some steps need to be performed firstly reshaping one dimention binary data

vector to 16*8 matrix then convert binary to decimal by using (bi2de) in matlab and finally reshape the result 1*16 vector to 4*4 matrix , those processes are required because AES-TURBO deals with 4*4 byte matrix , at the end of

decryption process opposite operations are performed to return data to its origin state 128-bits .

In the first step Initialisation of AES components are done like S-box and InvS-box are created then poly matrices are produced and in the second step add round key. Then the shift rows, mix columns, cipher, encryption and decryption pseudocodes are written. a specific function are created for each step , and to be called in a sequence of the algorithm in both encryption and decryption.

These functions are carried out in MATLAB for AES encryption and decryption processes, this involves the S-box and Inv S-box creation, and four byte oriented operations. Plaintext is given as input by using symmetric key and using above byte oriented operations in the MATLAB, the AES algorithm is implemented. So that encryption and decryption is done separately.

At AES-TURBO Turbo codes are added to AES encryption and decryption processes, AES-TURBO encryption first round differs from the others and AES-TURBO decryption last round differs from other rounds , at the first round of encryption after Sub-Bytes we added turbo coder. Matlab communication toolbox includes Turbo Code function[3] , which is used here at AES-TURBO algorithm .this function creates a system object that encodes data into a turbo encoder this turbo coder is added after Sub Bytes at the first step at the sender side , other steps stay as it is, At the decryption of AES-TURBO last round differs from the others , we added Turbo decoder before Sub Bytes step, turbo decode function is used here at AES algorithm .that function creates a system object that decodes data and returns the original plaintext after decryption . off course turbo codes need interleaver to work properly for both turbo coding and turbo decoding processes , because our proposed system deals with 128 bit so interleaver should be 128 bit so we used a command for this which is exists also in Matlab communication toolbox.

3.3 SYSTEM OBJECTS OF THE COMMUNICATIONS SYSTEM TOOLBOX

Communications System Tool-box System objects, are part of the communication package and their names begin with common prefix “comm.” For the sake of accessing all Communication System Tool-box System objects [3], type “comm.” followed with the Tab key at MATLAB

command prompt, which produces an alphabetical list of all System objects which are available in tool-box. In concern to the newest MATLAB release, the Tool-box of the Communication System includes a total of 123 algorithms, which are provided as System objects. As shown in figure 3.1 .

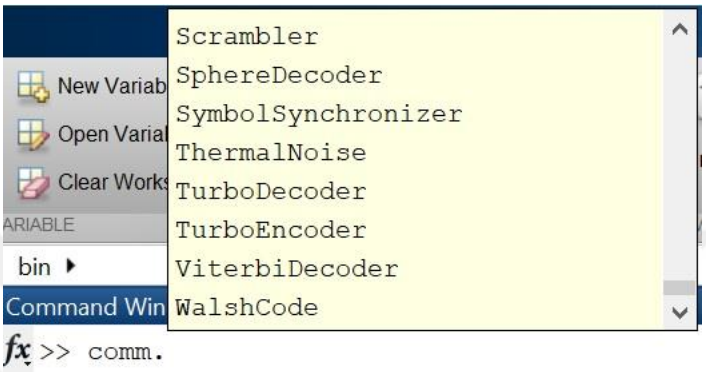

Figure 3.1: system objects toolbox

At this thesis we generated 128 bit of random data encrypted that data by using AES-Turbo ,then we used QPSK modulation to modulate that data , the modulated signal passed through wireless channels before applying demodulation and decryption processes to calculate bit error rate (BER) between the input and the output data .

Three types of wireless channels are used to compute the bit error rate for each channel and compare between those channels.

3.3.1 Generating Random Data

Best way to ensure that the input data is reliable and easy to generate in matlab is to use random data , there is familiar built in function in matlab is used for this purpose here we generated 128-bit of binary data.

3.3.2 QPSK Modulation /Demodulation

QPSK is one of the system objects which are available in Matlab communication system tool-box as a build in object, which creates an instance of this modulator type. same as for demodulation opposite function Those objects will produce modulated signal from digital data at matlab simulator , by using objects default properties appear when they are created.

3.3.3 Additiive White Gaussian Noise AWGN

We implemented AWGN channel simulation. The simulation was carried out AES-TURBO signal over AWGN channel this process uses default characteristics ,Which creates AWGN channel System object we used it for simulation and BER calculation.

3.3.4 Fading Channels

We simulated fading channels by using Matlab communications system toolbox, which includes objects for all fading channels to describe phenomena of the real world in the wireless communications, which include time dispersion, multi-path scattering effects, and Doppler shift, which result from relative motions between transmitters and receivers.

The main paths yield in arrival of the delayed signal at receiver versions. Moreover, the signal of the radio is scattered on a local scale for every one of the major paths. This type of the local scattering is usually defined by numerous reflections by the objects nearby the receiver. Those irresolvable elements are combined at receiver and result in a phenomenon which is referred to as the multi-path fading. As a result of this phenomenon, every one of the major paths acts as discrete fading path, the process of fading is defined by the Rayleigh's distribution for a Rician distribution and a non "line-of-sight" path for the "line-of-sight" path. We implemented AES-TURBO over fading channels by using matlab communication toolbox to recognize the different if we used AES-TURBO or we didn't use it , the difference appears upon the BER for each channel and the affection of AES-TURBO upon those fading channels .

3.3.4.1 Rician fading

We implemented rician fading channel simulation. The simulation was carried out AES-TURBO signal over rician channel this process uses default rician fading characteristics , by using matlab toolbox, Which creates a Rician fading channel System object we used it for rician simulation and BER calculation.

3.3.4.2 Rayleigh fading

We implemented rayleigh fading channel simulation. The simulation was carried out AES-TURBO signal over rayleigh channel this process uses default rayleigh fading characteristics , by usig matlab toolbox , Which creates a rayleigh fading channel System object we used it for simulation and BER calculation.

4. DISCUSSION THE RESULTS

4.1 INTRODUCTION

Today the prediction of errors upon wireless networks and correcting those errors are very necessary where it plays an important role of communications efficiency , security and accuracy, therefore we need to generate forecasting to have high transmission accuracy. In this chapter we preview the results that we obtained after applying AES-TURBO on different channels , comparing the Bit Error Rate obtained for each channel with using AES-TURBO and without using AES-TURBO.

4.2 BER RESULTS

At this section we presents and evaluates the results using matlab , the results are used the ratio of signal energy per bit to noise power density Eb/No and bit error rate BER to evaluate and analyze the performance of AES-TURBO over AWGN, Rician and Rayleigh fading channels we preview the Bit Error Rate results for each channel independently[44] , a special matlab function is used for this issue we called this function to obtain the BER at each Eb/No .it found in the matlab Communications System Toolbox and used for BER estimation for each channel with and without AES-TURBO we also compared and analyzed the importance of AES-TURBO at AWGN Rician and Rayleigh channels considering the effects of BER and SNR on their performance in fading as follow:

4.2.1 BER Results Over AWGN Channel

The modulated signal passed through AWGN channel and we calculated the BER obtained by the simulation with AES-TURBO to show the impact of error correction scheme upon BER figure 4.1 and table 4.1 explains the results as follows :

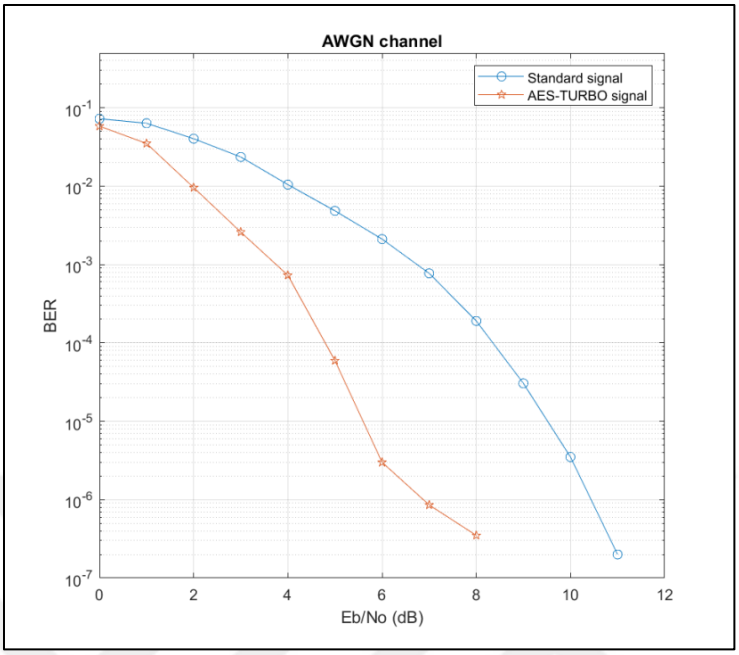

Figure 4.1: Bit Error Rate (BER) performance over Additive White Gaussian Noise (AWGN)

. **Table 4.1:** Bit Error Rate (BER) values over Additive White Gaussian Noise (AWGN).

Eb/No (dB)	BER of standard signal	BER of AES-TURBO signal
0	$7.26.10^{-2}$	$5.84.10^{-2}$
1	$6.35.10^{-2}$	$3.51.10^{-2}$
2	$4.04.10^{-2}$	$9.62.10^{-3}$
3	$2.36.10^{-2}$	$2.63.10^{-3}$
4	$1.04.10^{-2}$	$7.31.10^{-4}$
5	$4.85.10^{-3}$	$5.89.10^{-5}$
6	$2.11.10^{-3}$	3.10^{-6}
7	$7.72.10^{-4}$	$8.56.10^{-7}$
8	$1.91.10^{-4}$	$3.5.10^{-7}$
9	$3.05.10^{-5}$	0.0
10	$3.63.10^{-6}$	0.0
11	$2.12.10^{-7}$	0.0

Simulated results above shows the BER values for different SNR using AES-TURBO for AWGN channel we took Eb/No values from zero to eleven, the values of BER are decreasing in case of implementing AES-TURBO , at Eb/No equals to 0dB the value of BER is ($7.26.10^{-2}$) but with AES-TURBO it decreased to ($5.84.10^{-2}$) this difference explains the impact of this algorithm, the values of BER keep going with this decrement for each Eb/No. at Eb/No equals to 9dB BER is ($3.05.10^{-5}$) for standard signal on the other hand it decayed for AES-Turbo signal.

4.2.2 BER Results Over Rician Channel

The modulated signal passed through Rician channel at different values of K-factor, for K-factor 10,20,30 and 100 and we calculated the BER obtained by the simulation with AES-TURBO to show the impact of error correction scheme upon BER, figure 4.2 and table 4.2 explains the results at K=10 dB as follows :

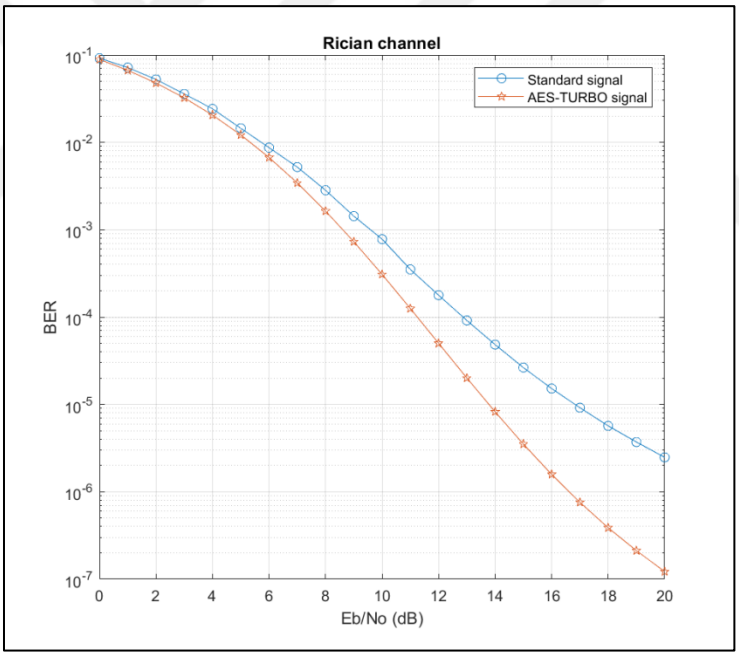

Figure 4.2: Bit Error Rate (BER) performance over Rician channel at K=10 dB.

Table 4.2: Bit Error Rate (BER) values over Rician channel at K=10 dB.

Eb/No (dB)	BER of standard signal	BER of AES-TURBO signal
0	$9.19.10^{-2}$	$8.92.10^{-2}$
1	$7.18.10^{-2}$	$6.71.10^{-2}$
2	$5.253.10^{-2}$	$4.67.10^{-2}$
3	$3.59.10^{-2}$	$3.24.10^{-2}$
4	$2.422.10^{-2}$	$2.04.10^{-2}$
5	$1.45.10^{-2}$	$1.28.10^{-2}$
6	$8.71.10^{-3}$	$6.71.10^{-3}$
7	$5.21.10^{-3}$	$3.51.10^{-3}$
8	$2.83.10^{-3}$	$1.64.10^{-3}$
9	$1.43.10^{-3}$	$7.31.10^{-4}$
10	$7.81.10^{-4}$	$3.11.10^{-4}$
11	$3.51.10^{-4}$	$1.26.10^{-4}$
12	$1.78.10^{-4}$	$5.02.10^{-5}$
13	$9.15.10^{-5}$	$2.01.10^{-5}$
14	$4.83.10^{-5}$	$8.23.10^{-6}$
15	$2.64.10^{-5}$	$3.48.10^{-6}$
16	$1.52.10^{-5}$	$1.61.10^{-6}$
17	$9.17.10^{-6}$	$7.59.10^{-7}$
18	$5.68.10^{-6}$	$3.89.10^{-7}$
19	$3.71.10^{-6}$	$2.21.10^{-7}$
20	$2.48.10^{-6}$	$1.24.10^{-7}$

Simulated results above shows the BER values for different SNR using AES-TURBO for Rician channel for K=10 dB we took Eb/No values from zero to twenty, the values of BER are decreasing in case of implementing AES-TURBO , at Eb/No equals to 0 dB the value of BER is ($9.19.10^{-2}$) but with AES-TURBO it decreased to ($8.92.10^{-2}$) this difference explains the impact

of this algorithm, the values of BER keep going with this decrement for each Eb/No. at Eb/No equals to 10 dB BER is ($7.81.10^{-4}$) for standard signal and ($3.11.10^{-4}$) for AES-TURBO signal and this difference grows up at each Eb/No at 20 dB BER is($2.48.10^{-6}$) for standard signal but it is ($1.24.10^{-7}$) for AES-TURBO signal .

figure 4.3 and table 4.3 explains the results at K=20 dB as follows :

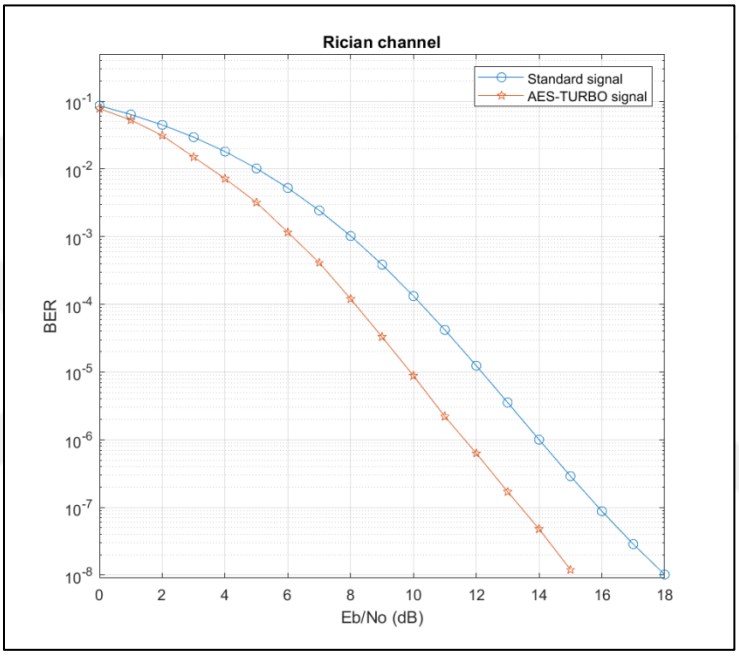

Figure 4.3: Bit Error Rate (BER) performance over Rician channel at K=20 dB.

Table 4.3: Bit Error Rate (BER) values over Rician channel at K=20 dB.

Eb/No (dB)	BER of standard signal	BER of AES-TURBO signal
0	$8.59.10^{-2}$	$7.81.10^{-2}$
1	$6.39.10^{-2}$	$5.27.10^{-2}$
2	$4.51.10^{-2}$	$3.13.10^{-2}$
3	$3.01.10^{-2}$	$1.52.10^{-2}$
4	$1.83.10^{-2}$	$7.21.10^{-3}$
5	$1.04.10^{-2}$	$3.22.10^{-3}$
6	$5.31.10^{-3}$	$1.16.10^{-3}$
7	$2.44.10^{-3}$	$4.13.10^{-4}$
8	$1.01.10^{-3}$	$1.25.10^{-4}$
9	$3.9.10^{-4}$	$3.31.10^{-5}$
10	$1.31.10^{-4}$	$8.79.10^{-6}$
11	$4.21.10^{-5}$	$2.21.10^{-6}$
12	$1.25.10^{-5}$	$6.33.10^{-7}$
13	$3.54.10^{-6}$	$1.74.10^{-7}$
14	$1.02.10^{-6}$	$4.85.10^{-8}$
15	$2.88.10^{-7}$	$1.23.10^{-8}$
16	$8.81.10^{-8}$	0.00
17	$2.86.10^{-8}$	0.00
18	$1.02.10^{-8}$	0.00

channel for K=20 dB we took Eb/No values from zero to eighteen, the values of BER are decreasing in case of implementing AES-TURBO , at Eb/No equals to 0 dB the value of BER is ($8.59.10^{-2}$) but with AES-TURBO it decreased to ($7.81.10^{-2}$) this difference explains the impact of this algorithm, the values of BER keep going with this decrement for each Eb/No. at Eb/No equals to 9 dB BER is ($3.9.10^{-4}$) for standard signal and ($3.31.10^{-5}$) for AES-TURBO signal and this difference grows up at each Eb/No at 16 dB BER is ($8.81.10^{-8}$) for standard signal but it decayed for AES-TURBO signal.

figure 4.4 and table 4.4 explains the results at K=30 dB as follows :

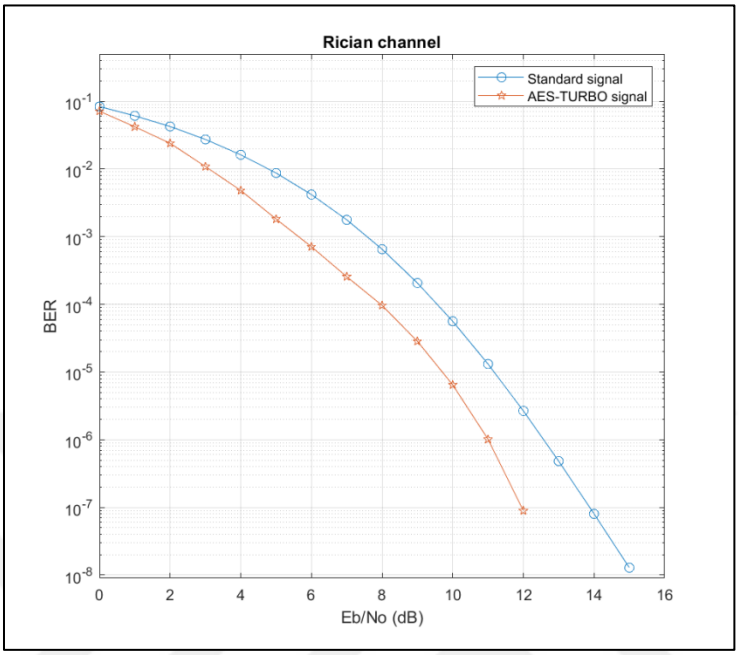

Figure 4.4: Bit Error Rate (BER) performance over Rician channel at K=30 dB.

Table 4.4: Bit Error Rate (BER) values over Rician channel at K=30 dB.

Eb/No (dB)	BER of standard signal	BER of AES-TURBO signal
0	$8.36.10^{-2}$	$7.14.10^{-2}$
1	$6.15.10^{-2}$	$4.22.10^{-2}$
2	$4.25.10^{-2}$	$2.46.10^{-2}$
3	$2.73.10^{-2}$	$1.09.10^{-2}$
4	$1.63.10^{-2}$	$4.82.10^{-3}$
5	$8.73.10^{-3}$	$1.88.10^{-3}$
6	$4.19.10^{-3}$	$7.1.10^{-4}$
7	$1.77.10^{-3}$	$2.56.10^{-4}$
8	$6.53.10^{-4}$	$9.65.10^{-5}$
9	$2.07.10^{-4}$	$2.84.10^{-5}$
10	$5.6.10^{-5}$	$6.45.10^{-6}$
11	$1.32.10^{-5}$	$1.02.10^{-6}$
12	$2.67.10^{-6}$	$8.96.10^{-8}$
13	$4.86.10^{-7}$	0.00
14	$8.03.10^{-8}$	0.00
15	$1.28.10^{-8}$	0.00

Simulated results above shows the BER values for different SNR using AES-TURBO for Rician channel for K=30 dB we took Eb/No values from zero to fifteen, the values of BER are decreasing in case of implementing AES-TURBO , at Eb/No equals to 0 dB the value of BER is ($8.36.10^{-2}$) but with AES-TURBO it decreased to ($7.14.10^{-2}$) this difference explains the impact of this algorithm, the values of BER keep going with this decrement for each Eb/No. at Eb/No equals to 7 dB BER is ($1.77.10^{-3}$) for standard signal and ($2.56.10^{-4}$) for AES-TURBO signal and this difference grows up at each Eb/No at 13 dB BER is($4.86.10^{-7}$) for standard signal but it is decayed for AES-TURBO signal.

figure 4.5 and table 4.5 explains the results at K=100 dB as follows :

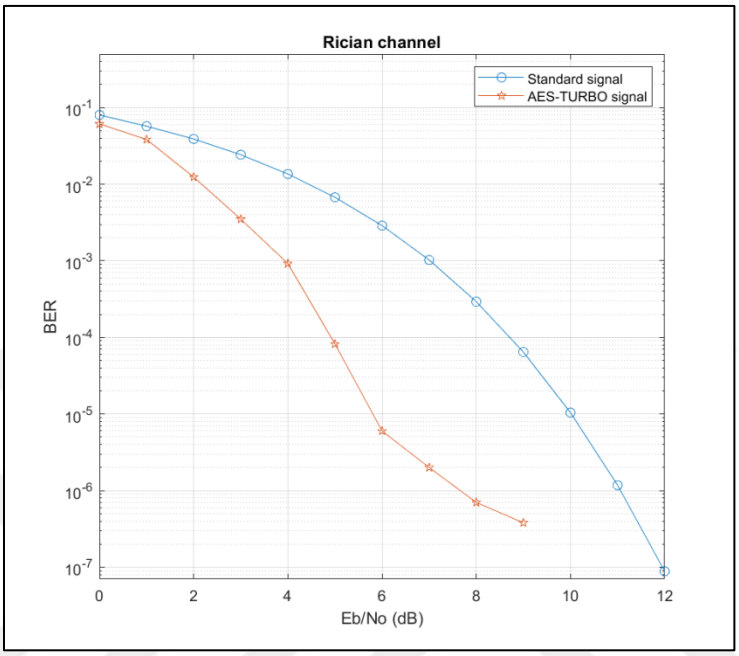

Figure 4.5: Bit Error Rate (BER) performance over Rician channel at K=100 dB.

Table 4.5: Bit Error Rate (BER) values over Rician channel at K=100 dB.

Eb/No (dB)	BER of standard signal	BER of AES-TURBO signal
0	$8.02.10^{-2}$	$6.21.10^{-2}$
1	$5.81.10^{-2}$	$3.84.10^{-2}$
2	$3.9.10^{-2}$	$1.24.10^{-2}$
3	$2.43.10^{-2}$	$3.51.10^{-3}$
4	$1.36.10^{-2}$	$9.22.10^{-4}$
5	$6.74.10^{-3}$	$8.23.10^{-5}$
6	$2.89.10^{-3}$	$6.13.10^{-6}$
7	$1.01.10^{-3}$	$2.5.10^{-6}$
8	$3.01.10^{-4}$	$7.63.10^{-7}$
9	$6.44.10^{-5}$	$3.81.10^{-7}$
10	$1.04.10^{-5}$	0.00
11	$1.17.10^{-6}$	0.00
12	$8.84.10^{-8}$	0.00

Simulated results above shows the BER values for different SNR using AES-TURBO of Rician channel for K=100 dB we took Eb/No values from zero to twelve, the values of BER are decreasing in case of implementing AES-TURBO , at Eb/No equals to 0 dB the value of BER is ($8.02.10^{-2}$) but with AES-TURBO it decreased to ($6.21.10^{-2}$) this difference explains the impact of this algorithm, the values of BER keep going with this decrement for each Eb/No. at Eb/No equals to 6 dB BER is ($2.89.10^{-3}$) for standard signal and ($6.13.10^{-6}$) for AES-TURBO signal and this difference grows up at each Eb/No at 10 dB BER is ($1.04.10^{-5}$) for standard signal but it decayed for AES-TURBO signal.

4.2.3 BER Results Over Rayleigh Channel

The modulated signal passed through Rayleigh channel and we calculated the BER obtained by the simulation with AES-TURBO to show the impact of error correction scheme upon BER figure 4.6 and table 4.6 explains the results as follows :

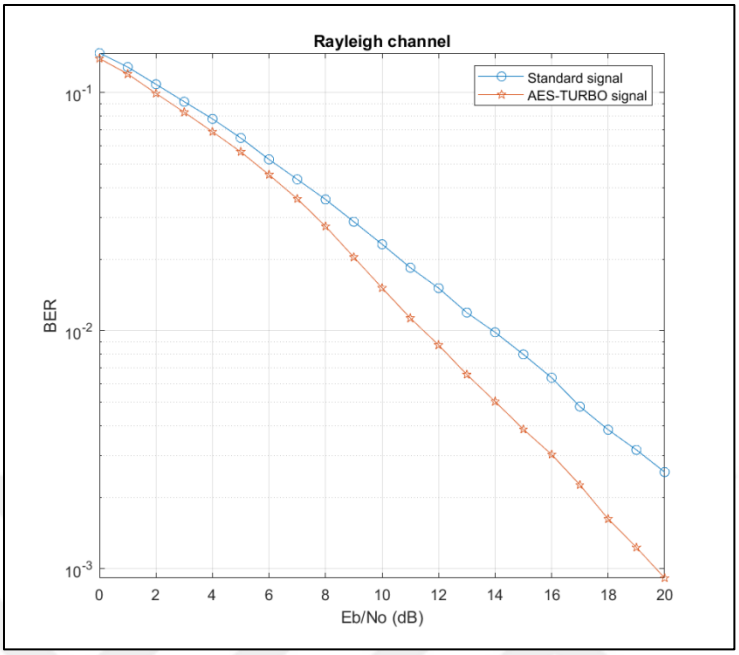

Figure 4.6: Bit Error Rate (BER) performance over Rayleigh channel.

Table 4.6: Bit Error Rate (BER) values over Rayleigh channel.

Eb/No (dB)	BER of standard signal	BER of AES-TURBO signal
0	$1.46.10^{-1}$	$1.39.10^{-1}$
1	$1.28.10^{-1}$	$1.19.10^{-1}$
2	$1.08.10^{-1}$	$9.93.10^{-2}$
3	$9.16.10^{-2}$	$8.27.10^{-2}$
4	$7.76.10^{-2}$	$6.85.10^{-2}$
5	$6.45.10^{-2}$	$5.64.10^{-2}$
6	$5.24.10^{-2}$	$4.52.10^{-2}$
7	$4.32.10^{-2}$	$3.58.10^{-2}$
8	$3.56.10^{-2}$	$2.75.10^{-2}$
9	$2.87.10^{-2}$	$2.03.10^{-2}$
10	$2.31.10^{-2}$	$1.51.10^{-2}$
11	$1.84.10^{-2}$	$1.13.10^{-2}$
12	$1.51.10^{-2}$	$8.71.10^{-3}$
13	$1.19.10^{-2}$	$6.54.10^{-3}$
14	$9.85.10^{-3}$	$5.04.10^{-3}$
15	$7.95.10^{-3}$	$3.86.10^{-3}$
16	$6.35.10^{-3}$	$3.02.10^{-3}$
17	$4.8.10^{-3}$	$2.25.10^{-3}$
18	$3.84.10^{-3}$	$1.62.10^{-3}$
19	$3.16.10^{-3}$	$1.23.10^{-3}$
20	$2.55.10^{-3}$	$9.15.10^{-4}$

Simulated results above shows the BER values for different SNR using AES-TURBO for Rayleigh channel we took Eb/No values from zero to twenty as such Rician channel, the values of BER are decreasing in case of implementing AES-TURBO , at Eb/No equals to 0 dB the value of BER is ($1.46.10^{-1}$) but with AES-TURBO it decreased to ($1.39.10^{-1}$) this difference explains the impact of this algorithm, the values of BER keep going with this decrement for each Eb/No.

at Eb/No equals to 10 dB BER is ($2.31.10^{-2}$) for standard signal and ($1.51.10^{-2}$) for AES-TURBO signal and this difference grows up at each Eb/No at 20 dB BER is ($2.55.10^{-3}$) for standard signal but it is ($9.15.10^{-4}$) for AES-TURBO signal .

5. CONCLUSIONS AND RECOMMENDATIONS

5.1 CONCLUSIONS

The link between signal to noise ratio and Bit error rate has been widely discussed in Literature. Turbo codes is one of the important error correction technique that contribute to reduce errors. Currently, emerging research have combined turbo codes with Advance Encryption Standard, named AES-TURBO, through (AWGN) channel. This thesis provides an in depth performance analysis of AES-TURBO which represents powerful encryption and error correcting schemes. This is obtained by combining error correction and encryption functionality into one single step by embedding Turbo Encoder block in AES encryption block at the first round after Sub-Bytes in the receiver side Turbo Decoder is added in the last round of AES before Sub-Bytes. In the current study the detailed analysis over Rayleigh and Rician fading channel models was covered. The work herein provides a detailed analysis by simulation approach over Rayleigh and Rician fading channel models. The detailed introduction of the performance of AES-TURBO is relatively new and is a step forward in the area of encryption and error correction. In this study the impact of AES-TURBO upon fading channels was demonstrated. This study, concludes that the results of simulation depicts clearly that AES-TURBO have the capability of approaching very low bit error rates. Furthermore, it has shown that AES-TURBO is capable of providing excellent performance for all fading channels. To conclude , the findings of this study can be summarized as follows:

- For Additive white Gaussian Noise (AWGN) channel, the impact of A Combined Encryption and Error Correction Scheme was obvious and strongly decayed the Bit Error Rate on this channel at Eb/No equals to nine while it's value is ($3.05.10^{-5}$) for standard signal .
- For Rician channel the Combined Encryption and Error Correction Scheme also affected and reduced the results of Bit Error Rate(BER) upon this channel and excellent performance was obtained for the higher values of signal to noise ratio as compared with other signal in which this algorithm was not used.
- For Rayleigh channel the Combined Encryption and Error Correction Scheme affected and enhanced the results of Bit Error Rate(BER) by comparing the results for AES-TURBO signal and standard signal. . Interestingly, the results of AES-TURBO signal

and standard signal is convergent to the signal to noise ratio only when the lower signal to noise ratio is low. Therefore, the increased the signal to noise ratio results in higher performance of AES-TURBO.

In conclusion, the findings of this study confirmed that AES-TURBO is effective with both Rician and Rayleigh channels.

5.2 RECOMMENDATION FOR FUTURE WORK

In this section we suggest some other possible cases to use AES-TURBO , in this thesis we simulated AES-TURBO in SISO Rician and Rayleigh fading channels. In future we will simulate AES-TURBO in MIMO fading channels , or in another case more than one turbo coder will be added to the encryption system to get better performance .

REFERENCES

[1] Hakan, C. A. M., Osman N.UCAN , & Ozduran, V. (2009). A combined encryption and error correction scheme: AES-Turbo. ISTANBUL University-Journal of Electrical & Electronics Engineering, 9(1), 891-896.

[2] Stallings, W. (2017). Cryptography and network security: principles and practice (pp. 92-95). Upper Saddle River: Pearson.

[3] Zarrinkoub, H. (2014). Understanding LTE with MATLAB: from mathematical modeling to simulation and prototyping. John Wiley & Sons.

[4] Bandyopadhyay, D., & Sen, J. (2011). Internet of things: Applications and challenges in technology and standardization. Wireless personal communications, 58(1), 49-69.

[5] Gerber, M., von Solms, R., & Overbeek, P. (2001). Formalizing information security requirements. Information Management & Computer Security, 9(1), 32-37.

[6] Stallings, W. (2007). Data and computer communications. Pearson Education India.

[7] Luntovskyy, A., & Spillner, J. (2017). Security in Distributed Systems. In Architectural Transformations in Network Services and Distributed Systems (pp. 247-308). Springer Vieweg, Wiesbaden.

[8] Johnson, G. W., Dowla, F. U., & Ruggiero, A. J. (2007). U.S. Patent No. 7,277,644. Washington, DC: U.S. Patent and Trademark Office.

[9] Haykin, S. S., & Moher, M. (2011). Modern wireless communications. Pearson Education India.

[10] Ryan, W. E. (2003). Concatenated convolutional codes and iterative decoding. Wiley Encyclopedia of Telecommunications.

[11] Schodorf, J. B. (2003). Land-Mobile Satellite Communications. Wiley Encyclopedia of Telecommunications.

[12] Simon, M. K., & Alouini, M. S. (2005). Digital communication over fading channels (Vol. 95). John Wiley & Sons.

[13] Stüber, G. L., & Stèuber, G. L. (1996). Principles of mobile communication (Vol. 2). Norwell, Mass, USA: Kluwer Academic.

[14] Proakis, J. G., & Salehi, M. (2001). Digital communications (Vol. 4, pp. 593-620). New York: McGraw-hill.

[15] Proakis, J. G., Salehi, M., Zhou, N., & Li, X. (1994). Communication systems engineering (Vol. 2). New Jersey: Prentice Hall.

[16] Wang, Y., & Zhu, Q. F. (1998). Error control and concealment for video communication: A review. Proceedings of the IEEE, 86(5), 974-997.

[17] Kumar, P., Sumithra, M., & Sarumathi, M. (2013). Performance evaluation of Rician fading channels using QPSK, DQPSK and OQPSK modulation schemes in Simulink environment. International Journal of Engineering Science Invention, 2(5), 07-16.

[18] Konstantinou, K. (2008). Low-height channel modelling with application to multihop UMTs. University of Surrey (United Kingdom).

[19] He, S. (2015). Advanced Analysis Algorithms for Microscopy Images (Doctoral dissertation, Columbia University).

[20] Paulraj, A., Rohit, A. P., Nabar, R., & Gore, D. (2003). Introduction to space-time wireless communications. Cambridge university press.

[21] Forney, G. (1970). Convolutional codes I: Algebraic structure. IEEE Transactions on Information Theory, 16(6), 720-738.

[22] Richardson, T. J., Shokrollahi, M. A., & Urbanke, R. L. (2001). Design of capacity-approaching irregular low-density parity-check codes. IEEE transactions on information theory, 47(2), 619-637.

[23] Costello Jr, D. J., Pusane, A. E., Bates, S., & Zigangirov, K. S. (2006, February). A comparison between LDPC block and convolutional codes. In Proc. Information Theory and Applications Workshop (pp. 6-10).

[24] Chen, J., Dholakia, A., Eleftheriou, E., Fossorier, M. P., & Hu, X. Y. (2005). Reduced-complexity decoding of LDPC codes. IEEE transactions on communications, 53(8), 1288-1299.

[25] Goldsmith, A. J., & Wicker, S. B. (2002). Design challenges for energy-constrained ad hoc wireless networks. IEEE wireless communications, 9(4), 8-27.

[26] Molisch, A. F., Balakrishnan, K., Chong, C. C., Emami, S., Fort, A., Karedal, J., ... & Siwiak, K. (2004). IEEE 802.15. 4a channel model-final report. IEEE P802, 15(04), 0662.

[27] Pu, Q., Gupta, S., Gollakota, S., & Patel, S. (2013, September). Whole-home gesture recognition using wireless signals. In Proceedings of the 19th annual international conference on Mobile computing & networking (pp. 27-38). ACM.

[28] Team, C. A. I. (2017). Europe and the future for WPT: European contributions to wireless power transfer technology. IEEE Microwave Magazine, 18(4), 56-87.

[29] Parasuraman, R., Kershaw, K., & Ferre, M. (2013). Experimental investigation of radio signal propagation in scientific facilities for telerobotic applications. International Journal of Advanced Robotic Systems, 10(10), 364.

[30] Bianchi, G. (2000). Performance analysis of the IEEE 802.11 distributed coordination function. IEEE Journal on selected areas in communications, 18(3), 535-547.

[31] Delorme, A., & Makeig, S. (2004). EEGLAB: an open source toolbox for analysis of single-trial EEG dynamics including independent component analysis. Journal of neuroscience methods, 134(1), 9-21.

[32] Atzori, L., Iera, A., & Morabito, G. (2010). The internet of things: A survey. Computer networks, 54(15), 2787-2805.

[33] Tsow, A., Jakobsson, M., Yang, L., & Wetzel, S. (2006). Warkitting: the drive-by subversion of wireless home routers. Journal of Digital Forensic Practice, 1(3), 179-192.

[34] Smit, L. T., Smit, G. J., & Hurink, J. L. (2003). Energy efficient wireless communication for mobile multimedia terminals. na.

[35] Dagres, I., Zalonis, A., Dimitriou, N., Nikitopoulos, K., & Polydoros, A. (2005). Flexible radio: A framework for optimized multimodal operation via dynamic signal design. EURASIP Journal on Wireless Communications and Networking, 2005(3), 284-297.

[36] Feng, P. (2012, June). Wireless LAN security issues and solutions. In 2012 IEEE symposium on robotics and applications (ISRA) (pp. 921-924). IEEE.

[37] Piscitello, D. M., & Phifer, L. (2002). Best practices for securing enterprise networks. Business Communications Review, 32(12), 32-37.

[38] Dimitriadis, C. K. (2007). Improving mobile core network security with honeynets. IEEE Security & Privacy, 5(4), 40-47.

[39] Turab, N., & Moldoveanu, F. (2009). A comparison between wireless LAN security protocols. Universitatea Politehnica Bucuresti Scientific Bulletin, 61-80.

[40] Proakis, J. G., & Salehi, M. (2001). Digital communications (Vol. 4, pp. 593-620). New York: McGraw-hill.

[41] Bayat, O., Shafai, B., & Ucan, O. N. (2004, June). An Efficient Channel Equalization on the Transmission of Turbo Coded Signals. In Communications in Computing (pp. 73-78).

[42] Panayirci, E., Aygolu, U., & Ucan, O. N. (1995). Error performance analysis of quadrature partial response trellis coded modulation (QPR-TCM) in fading mobile satellite channels. IEEE transactions on communications, 43(2/3/4), 1653-1662.

[43] Cam, H., Ucan, O. N., & Ozduran, V. (2011). Multilevel/AES-LDPCC-CPFSK with channel equalization over WSSUS multipath environment. AEU-International Journal of Electronics and Communications, 65(12), 1015-1022.

[44] Osman N. Ucan & Mustafa R. Albanna. (2019). AES-TURBO over Rician and Rayleigh fading channels . Aurum Journal of Engineering and Systems Architecture .

[45] Osman N. Ucan, Buyukatak, K., Gose, E, & Odabasioglu, N. (2006). Performance of multilevel-turbo codes with blind/non-blind equalization over WSSUS multipath channels. International Journal of Communication Systems, 19(3), 281-297.