Simulation Based Bit Error Rate Measurement of Uncoded, Coded and Encrypted Wireless Communication Channel

Thesis submitted in partial fulfillment of the requirements for the degree

of

Master of Engineering
in
Electronics and Tele-Communication Engineering

by

Suman Dey

Class Roll No.: 002010702027
Registration No.: 154096 of 2020-21
Examination Roll No.: M4ETC22027

Under the guidance of

Dr. Jaydeb Bhaumik

Professor
Department of Electronics and Tele-Communication Engineering
Jadavpur University
Kolkata - 700032
West Bengal, India

FACULTY OF ENGINEERING AND TECHNOLOGY
JADAVPUR UNIVERSITY

CERTIFICATE OF RECOMMENDATION

This is to certify that the thesis entitled **"Simulation Based Bit Error Rate Measurement of Uncoded, Coded and Encrypted Wireless Communication Channel"** submitted by **Suman Dey** (Class Roll No.: **002010702027**, Examination Roll No.: **M4ETC22027** and Registration No.: **154096 of 2020-21**) of Jadavpur University, Kolkata is a record of bonafide research work carried out by him under my guidance and supervision and can be accepted in partial fulfillment of the requirement for the degree of **Master of Engineering in Electronics and Tele-Communication Engineering**, with specialization in **Communication Engineering**, of the University. The results presented in this thesis have been verified and are found to be satisfactory. The results presented in this thesis are not included in any other paper submitted for the award of degree to any other University or Institute.

Jaydeb Bhaumik 23/08/22

Prof. Jaydeb Bhaumik
Supervisor
Department of Electronics and
Tele-Communication Engineering
Jadavpur University
Kolkata - 700032

Professor
Electronics & Tele-communication
Engg Dept.
Jadavpur University

Manotosh Biswas 23/08/22

Prof. Manotosh Biswas
Head of the Department
Department of Electronics and
Tele-Communication Engineering
Jadavpur University
Kolkata - 700032

MANOTOSH BISWAS
Professor and Head
Electronics and Telecommunication Engineering
Jadavpur University, Kolkata - 32

Chandan Mazumdar 23/8/22

Prof. Chandan Mazumdar
Dean
Faculty Council of Engineering &
Technology
Jadavpur University
Kolkata - 700032

DEAN
Faculty of Engineering & Technology
JADAVPUR UNIVERSITY
KOLKATA-700 032

FACULTY OF ENGINEERING AND TECHNOLOGY
JADAVPUR UNIVERSITY

CERTIFICATE OF APPROVAL*

The foregoing thesis entitled **"Simulation Based Bit Error Rate Measurement of Uncoded, Coded and Encrypted Wireless Communication Channel"** is hereby approved as a creditable study of an engineering subject carried out and presented in a manner satisfactory to warrant its acceptance as a prerequisite to the degree for which it has been submitted. It is understood that by this approval, the undersigned do not necessarily endorse or approve any statement made, opinion expressed or conclusion drawn therein but approve the thesis only for the purpose for which it has been submitted.

Committee on Final Examination
for Evaluation of the Thesis

Signature of External Examiner

Signature of Supervisor
Prof. Jaydeb Bhaumik
Supervisor
Department of Electronics and
Tele-Communication Engineering
Jadavpur University
Kolkata - 700032

*Only in the case the thesis is approved.

FACULTY OF ENGINEERING AND TECHNOLOGY
JADAVPUR UNIVERSITY

DECLARATION

I hereby declare that this thesis entitled **"Simulation Based Bit Error Rate Measurement of Uncoded, Coded and Encrypted Wireless Communication Channel"** contains a literature survey and original research work by the undersigned, as part of my degree of **Master of Engineering in Electronics and Tele-Communication Engineering**, with specialization in **Communication Engineering**.
All information 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 materials and results that are not original to this work.

Name: **Suman Dey**
Class Roll No.: **002010702027**
Registration No.: **154096 of 2020-21**
Examination Roll No.: **M4ETC22027**
Thesis Title: **Simulation Based Bit Error Rate Measurement of Uncoded, Coded and Encrypted Wireless Communication Channel**

Suman Dey 23/08/2022

Signature of Candidate

Dedicated to
my mother
Mrs. Bandana Dey

and
my father
Mr. Bikash Dey

and
my sister
Mrs. Suravi Dey Ghosh

ACKNOWLEDGEMENTS

This is a great opportunity to express my gratitude and respect to all the persons who have supported me in their own way, during my thesis work.

First and foremost, I would like to express my sincere gratitude to my thesis supervisor, Dr. Jaydeb Bhaumik, Professor of Department of Electronics and Tele-Communication Engineering, Jadavpur University, for guiding and motivating me throughout my thesis work. I am most grateful to him for giving me so much time in spite of his busy schedule and the meeting with him helped me a lot to understand the concepts and solving many things. I am also grateful to him for guiding me in writing of this thesis.

I would like to express my thanks to Prof. Manotosh Biswas, Head of the Department, Department of Electronics and Tele-Communication Engineering, Jadavpur University. I would also like to express my thanks to Prof. Ananda Shankar Chowdhury and all other faculty members of Department of Electronics and Tele-Communication Engineering, Jadavpur University.

I am also thankful to my senior researchers, friends, technical and non-technical staff of Jadavpur University.

I want to express my gratitude to my parents Mrs. Bandana Dey & Mr. Bikash Dey and my sister Mrs. Suravi Dey Ghosh, my brother-in-law Mr. Saikat Ghosh and other family members also. Whatever I am today, it is because of their sacrifice, invaluable love, support, encouragement and faith in me.

Suman Dey
Jadavpur University
Kolkata - 700032
West Bengal
India

ABSTRACT

In wireless communication, the transfer of data between two or more points occurs wirelessly. Bit error rate(BER) is one of the important performance measures of any communication system. In this thesis, performance of wireless communication channel is evaluated by measuring BER. BER performance of uncoded communication channel is evaluated. Here, first AWGN channel is considered with M-ary PSK and M-ary QAM modulation. Then Rayleigh fading channel is considered with AWGN noise and M-ary PSK & M-ary QAM modulation. Next, BER performance of coded communication channel is evaluated. RS(255,239) code, (7,1/2) convolutional code and DVB-S.2 rate 1/2 LDPC code are the error correcting codes considered in the experiments. AWGN channel is considered with M-ary PSK and M-ary QAM modulation. Then Rayleigh fading channel is also considered with AWGN noise and M-ary PSK & M-ary QAM modulation. Also, BER performance of communication channel with encryption and coding is evaluated. CCSDS standard LDPC(k=1024, rate=1/2) code is considered. Here channel noise is AWGN and modulation scheme is BPSK. BER performance of communication channel with LDPC coding is evaluated. Then BER performance of communication channel with AES in three different modes of operation(ECB,CTR and CBC) and LDPC coding are measured. Then BER performance of communication channel with another block cipher HDNM8 in CTR mode operation and LDPC coding is measured. From simulation study, it is found that BER performance of coded communication channel is better than uncoded communication channel. BER performance of AWGN channel is better than Rayleigh fading channel with AWGN. BER performance of the communication channel with LDPC coding is better than BER performance of the communication channel with encryption and LDPC coding. BER performance of the communication channel in CTR mode is better than the other two cases with ECB and CBC mode.

Keywords: Bit Error Rate, Error Control Coding, Encryption, Block Cipher, Modulation, Additive White Gaussian Noise, Rayleigh Fading.

Contents

List of Figures

List of Tables

Chapter 1

Introduction

Wireless communication can be described as the transfer of information between two or more points wirelessly. There are various advantages of wireless communication. Some of the advantages are as follows:

- There is no cable needed in wireless network.
- Installation of wireless network is very easy and it can be done faster also.
- Wireless network is also very cost effective.

However, there are some impairments present in wireless channel. Those channel impairments are noise, fading and interference. The channel impairments affect the transmitted signal. As a result, the same signal, that was transmitted, is not received at the receiver side. So, BER performance is degraded. Now, to improve reliability of the wireless communication channel, error control coding or channel coding is used. Channel coding adds redundancy to the transmitted message signal. This additional redundant bits help in detection and correction of errors at the receiver. So, channel coding gives a protection against channel errors and provide more reliability in information transmission. However, there is a cost of using channel coding; that is either expansion in bandwidth or reduction in data rate.

Now, to understand the effect of channel coding and encryption, first it is necessary to study the uncoded communication channel in all cases. So, BER performance has been evaluated for uncoded communication channel where AWGN has been considered as the channel noise. Then Rayleigh fading channel has been considered with AWGN noise to understand the fading effect and BER performance has been evaluated. After that, error correcting codes have been considered. Here RS(255,239), (7,1/2) convolutional code, DVB-S.2 standard rate 1/2 LDPC code have been considered. BER performance of the coded communication channel has been evaluated.

Here also, first AWGN channel has been considered for the experiment. Then Rayleigh fading channel has been considered with AWGN noise to understand the fading effect.

Encryption is a process of converting information into secret code and the secret code hides the true meaning of information. Encryption basically converts plaintext into ciphertext. Decryption converts ciphertext into plaintext. There are two types of encryption algorithms based on input type. Those are block cipher and Stream cipher. Block ciphers are considered in this thesis.

Now, BER performance has been evaluated for CCSDS standard LDPC(k=1024, rate=1/2) coded AWGN channel for BPSK modulation. Then AES encryption scheme in three different modes namely electronic codebook(ECB) mode, counter(CTR) mode and cipher block chaining(CBC) mode have been considered. BER performance of the AWGN channel with AES based three different modes of operations and LDPC(k=1024, rate=1/2) coding have been measured. Also, another block cipher HDNM8 has been considered. BER performance of the AWGN channel with HDNM8 in counter(CTR) mode of operation and LDPC(k=1024, rate=1/2) coding has been evaluated. All the experiments have been simulated in MATLAB.

1.1 Aim of Thesis

Bit error rate(BER) measurement of communication channel under different situations.

1.2 Thesis Layout

The rest of the thesis is organized as follows.

Chapter 2: In this chapter, theoretical backgrounds and concepts are described. After that, literature survey is provided in this chapter.

Chapter 3: BER performance of uncoded communication channel is described in this chapter. All the results and graphs obtained from experiments are shown in this chapter.

Chapter 4: In this chapter, BER performance of coded communication channel is described. Also simulation results and corresponding plots of BER vs E_b/N_0 are provided.

Chapter 5: BER performance of communication channel with encryption and channel coding is described in this chapter. The results and graphs which are obtained from the experiments are shown and described here.

Chapter 6: Finally, the thesis is concluded with summary and future scopes.

Chapter 2

Background and Literature Survey

All the basics of related topics have been discussed in this chapter. Three different error correcting codes namely Reed Solomon code, convolutional code and LDPC codes which have been used in the experiments. Two types of modulation techniques: MPSK and MQAM have been considered in this thesis. AWGN noise has been considered as channel noise. Rayleigh fading has been considered in this work. AES block cipher and HDNM8 block cipher are also considered in this thesis. Block cipher based ECB, CTR and CBC modes of operations have been also considered in some experiments. Therefore, basics of error correcting codes, encoding and decoding processes, modulation techniques, AWGN noise, Rayleigh fading, AES encryption and decryption process, HDNM8 encryption process, various block cipher modes of operations are discussed in brief. After that, literature survey is presented in this chapter.

2.1 Modulation Schemes

In modulation technique, one or more properties of carrier wave like amplitude, phase or frequency can be varied by modulating signal.
In this thesis, M-ary phase shift keying(MPSK) and M-ary quadrature amplitude modulation(MQAM) modulation schemes have been used.

2.1.1 M-ary Phase Shift Keying(MPSK)

Phase shift keying is a modulation technique in which phase of the carrier wave is varied according to digital modulating signal.

In M-ary phase shift keying(MPSK) [32], two or more bits are grouped together to form symbol. During each symbol period of duration τ_s one of M possible signals, $s_1(t), s_2(t), s_3(t), ..., s_M(t)$ is sent. Where M is the number of possible signals and $M = 2^n$ where n is an integer.
The modulated waveform is defined as

$$s_i(t) = \sqrt{\frac{2\xi_s}{\tau_s}} \cos\left(2\pi f_c t + \frac{2\pi(i-1)}{M}\right), \quad 0 \le t \le \tau_s \quad \text{where} \quad i = 1, 2, ..., M \quad (2.1)$$

Energy per symbol is $\xi_s = (\log_2 M) E_b$, where E_b is the bit energy and symbol period is $\tau_s = (\log_2 M) T_b$, where T_b is the bit duration.

We can write the above equation in quadrature form as follows:

$$s_i(t) = \sqrt{\frac{2\xi_s}{\tau_s}} \cos\left[(i-1)\frac{2\pi}{M}\right] \cos(2\pi f_c(t)) - \sqrt{\frac{2\xi_s}{\tau_s}} \sin\left[(i-1)\frac{2\pi}{M}\right] \cos(2\pi f_c(t)) \quad (2.2)$$

Where $i = 1, 2, ..., M$
In the above equation,orthogonal basis signals, defined over interval $0 \le t \le \tau_s$, are

$$\phi_1(t) = \sqrt{\frac{2}{\tau_s}} \cos(2\pi f_c t) \quad \text{and} \quad \phi_2(t) = \sqrt{\frac{2}{\tau_s}} \sin(2\pi f_c t) \quad (2.3)$$

So we can express MPSK signal set as

$$s_{MPSK}(t) = \{\left(\sqrt{\xi_s} \cos\left[(i-1)\frac{\pi}{2}\right] \phi_1(t)\right), \left(-\sqrt{\xi_s} \sin\left[(i-1)\frac{\pi}{2}\right] \phi_2(t)\right)\} \quad (2.4)$$

where $i = 1, 2, ..., M$

In M-ary phase shift keying M is the modulation order. In the experiments, various orders of MPSK modulation have been considered. The considered schemes under MPSK modulation are BPSK, QPSK, 8PSK,16PSK and 32PSK modulation.

2.1.2 M-ary Quadrature Amplitude Modulation(MQAM)

Quadrature amplitude modulation(QAM) [32] can be described as the modulation technique which is a combination of amplitude and phase modulation of carrier wave into a single channel. Information is transmitted by changing both the amplitude and phase of a carrier wave. Each combination of amplitude and phase is called symbol.

In M-ary quadrature amplitude modulation(MQAM), modulation order M can be defined as

$$M = 2^N \quad (2.5)$$

Where N is number of bits per symbol.

It can be known from MQAM that carrier signal can be modulated into any of the M different amplitude and phase states.

To describe the amplitude and phase values, different points can be used. The set of possible message points is called constellation diagram. The constellation points in constellation diagram of MQAM are situated in a square grid with equal distance in vertical and horizontal. So, the constellation diagram of MQAM is square lattice of signal points. Euclidean distance is the minimum distance between constellation points. The energy per symbol is not constant for MQAM. The distance between possible symbol states are not constant also. Constellation points are spaced closely for higher order modulation in MQAM and it is more susceptible to noise.

General form of MQAM signal can be defined as

$$S_i(t) = \sqrt{\frac{2\xi_{min}}{\tau_s}} a_i \cos(2\pi f_c t) + \sqrt{\frac{2\xi_{min}}{\tau_s}} b_i \sin(2\pi f_c t) \tag{2.6}$$

Where $0 \leq t \leq T$ and $i = 1, 2, 3, ..., M$

Here a_i and b_i are independent integers. a_i and b_i are chosen according to the signal point's location.

ξ_{min} indicates energy of the signal with lowest amplitude.

The basis function can be defined as

$$\Psi_1(t) = \sqrt{\frac{2}{\tau_s}} \cos(2\pi f_c t) \quad \text{where} \quad 0 \leq t \leq \tau_s \tag{2.7}$$

$$\Psi_2(t) = \sqrt{\frac{2}{\tau_s}} \sin(2\pi f_c t) \quad \text{where} \quad 0 \leq t \leq \tau_s \tag{2.8}$$

4QAM, 8QAM, 16QAM, 32QAM and 64QAM are the modulation techniques which have been considered under MQAM modulation in the experiments.

2.2 Noise in Communication Channel

Some undesired signal gets introduced in the communication channel during signal transmission and corrupts the original signal. The undesired signal is act as noise of the communication channel. In the experiments, additive white gaussian noise(AWGN) is considered as the channel noise.

2.2.1 Additive White Gaussian Noise(AWGN)

Additive white gaussian noise(AWGN) [23] is one of the simple noise models.
AWGN noise is added to the signal in the communication channel. The received signal can be defined as

$$r(t) = s_{tx}(t) + \eta(t) \tag{2.9}$$

Where $s_{tx}(t)$ is transmitted signal and $\eta(t)$ is AWGN noise.
The power spectral density of AWGN noise is constant for all frequencies. AWGN noise follows the Gaussian distribution or normal distribution. The probability density function(pdf) of AWGN noise also folows the gaussian pdf as shown below:

$$f_n(\chi) = \frac{1}{\sqrt{2\pi\sigma^2}} e^{-\frac{(\chi-\mu)^2}{2\sigma^2}} \tag{2.10}$$

Where μ is the mean value and σ is the standard deviation of the gaussian process.

The autocorrelation function of AWGN is defined as

$$R_n(\tau) = \frac{N_0}{2}\delta(\tau) \tag{2.11}$$

The power spectral density of AWGN is constant and the PSD is defined as

$$S_n(f) = \frac{N_0}{2} \tag{2.12}$$

2.3 Fading in Communication Channel

Fading can be defined as the time variation of signal power which is received at the receiver due to changes in paths or transmission medium. Rayleigh fading has been considered as the channel fading. A general concept of Rayleigh fading has been provided here.

2.3.1 Rayleigh Fading

Rayleigh fading [32] is considered when there is no line of sight path exists between the transmitter and receiver. So, there exists only indirect path between transmitter and receiver. Then the reflected and scattered signals are summed up to find the resultant signal at the receiver. The statistical time varying nature of received envelop can be described by Rayleigh distribution. The probability density function(pdf) of Rayleigh distribution can be defined as [32]

$$\begin{aligned} f(r) &= \frac{r}{\sigma^2} exp(\frac{-r^2}{2\sigma^2}) \quad \text{where} \quad 0 \leq r \leq \infty \\ &= 0 \quad \text{where} \quad r < 0 \end{aligned} \tag{2.13}$$

There are some important terms that influence Rayleigh fading channel.

2.3.1.1 Multipath Fading

Signal amplitude fluctuation is happened as a result of multipath fading. The signals are arriving at the receiver with different phases. The phase difference occurs because the signals have traveled different distances in different paths.

2.3.1.2 Flat Fading

Flat fading channel is also called amplitude varying channel. Signal goes through flat fading when

- Bandwidth of signal is less than bandwidth of channel.
- Delay spread is less than symbol period.

2.3.1.3 Frequency Selective Fading

Signal goes through frequency selective fading when
• Bandwidth of signal is greater than bandwidth of channel.
• Delay spread is greater than symbol period.

2.3.1.4 Doppler Shift

Doppler shift is caused by relative motion between transmitter and receiver. Assume, receiver receives signal with many incoming waves which comes from multipath channel. Let ith reflected wave with amplitude c_i and phase ϕ_i which is arrived from an angle β relative to the direction of motion of antenna.
The doppler shift can be defined as follows:

$$\begin{aligned} f_{doppler} &= \frac{v}{\lambda}\cos(\beta) \\ &= \frac{1}{2\pi}\frac{\Delta\Psi}{\Delta t} \end{aligned} \tag{2.14}$$

Where $\Delta\Psi$ can be defined as

$$\begin{aligned} \Delta\Psi &= \frac{2\pi\Delta L}{\lambda} \\ &= \frac{2\pi u\Delta t}{\lambda}\cos(\beta) \end{aligned} \tag{2.15}$$

2.4 Error Control Coding

Error control coding adds redundancy to the transmitted message signal and helps to detect and correct errors at the receiver. Reed Solomon code, convolutional code and LDPC code have been considered in the experiments. A brief description of the error correcting codes has been provided.

2.4.1 Reed Solomon(RS) Code

Reed Solomon(RS) codes [4] are non-binary codes. For RS(n,k) code, where message size is k symbols and codeword length is $n \leq 2^m - 1$ symbols. So there are $(n-k)$ redundant symbols. This RS(n,k) code can correct upto $t = \frac{(n-k)}{2}$ symbols error and the minimum distance between two codewords is $d_{min} = n - k + 1$.

Let code vector of Reed Solomon code is defined as C and C can be written as

$$C = (c_0, c_1, c_2, ...c_{n-1})$$

Where $c_0, c_1, c_2, ...c_{n-1}$ are non binary coefficients. Where each coefficient is sequence of 0s and 1s. The coefficients lie in GF(q), where the size of alphabet is $q = 2^m$ and m is number of bits in each alphabet. So each symbol can also be represented by m bits. Here GF stands for Galois Field.

2.4.1.1 Encoding of Reed-Solomon Code

A hardware implementation of RS(n,k) encoder[4] is shown in Fig. 2.1. During the first k clock cycles switch 'b' is connected to the lower position and as a result the k message symbols are directly transferred to the output register as shown in Fig. 2.1. In this first k clock cycles, the switch 'a' is also closed at the same time. So the message symbols are also shifted into the (n-k) stage shift register.
After the first k clock cycles, the switch 'a' will be opened and switch 'b' will be moved towards the upper position.
Then the parity symbols contained in the shift register will be moved to the output register in the remaining (n-k) clock cycles and appended to the message symbols.
So the n symbols of the codeword are now available in the output register.

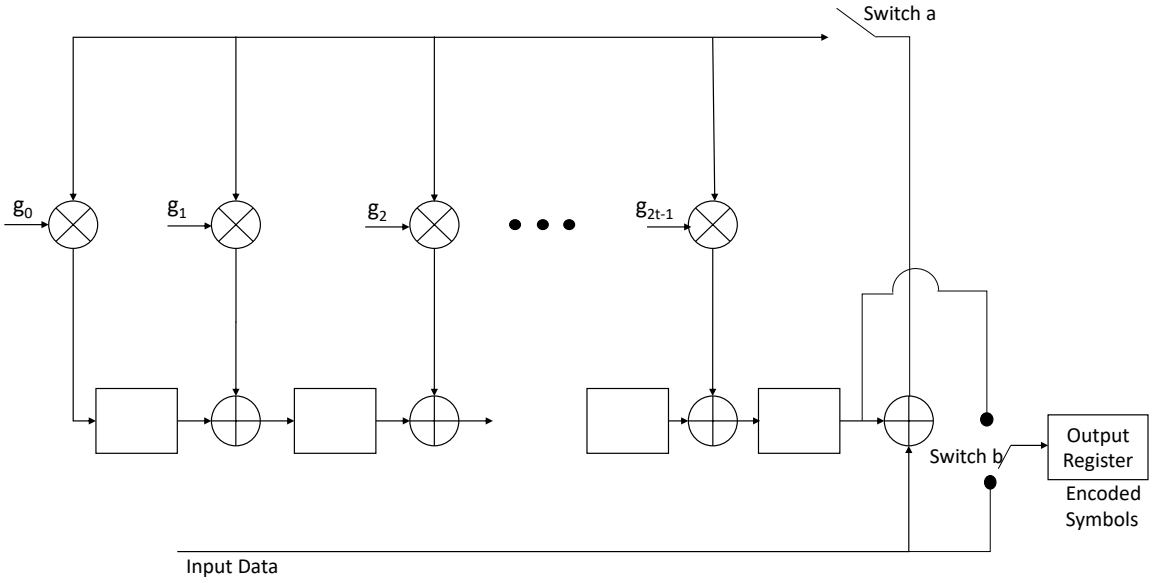

Figure 2.1: Hardware implementation of Reed Solomon encoder

2.4.1.2 Decoding of Reed-Solomon Code

Decoding process [6] of Reed Solomon code is discussed here. The transmitted message can be represented as a polynomial $\tau(x)$ and the introduced error can be considered as a polynomial $\xi(x)$. So the message which is incoming to the Reed-Solomon(RS) decoder can be expressed as shown below

$$R(x) = \tau(x) + \xi(x)$$

Now $\xi(x)$ should be identified at decoder and $\tau(x)$ can also be written as

$$\tau(x) = R(x) + \xi(x)$$

Now the received codeword is divided by generator polynomial g(x) and if there exists any remainder, the remainder can be called the syndrome(S_i).

Syndrome(S_i) can be described in polynomial as shown below.

$$\begin{aligned} Syndrome(S_i) &= R(\alpha^i) \\ &= R_{n-1}(\alpha^i)^{n-1} + R_{n-2}(\alpha^i)^{n-2} + R_{n-3}(\alpha^i)^{n-3} + ... + R_1(\alpha^i) + R_0 \end{aligned}$$

Now,

$$\begin{aligned} Syndrome(S_i) &= R(\alpha^i) \\ &= \tau(\alpha^i) + \xi(\alpha^i) \\ &= \xi(\alpha^i) \\ &= y_1\alpha^{ie_1} + y_2\alpha^{ie_2} + y_3\alpha^{ie_3} + ... + y_v\alpha^{ie_v} \\ &= y_1\chi_1^i + y_2\chi_2^i + y_3\chi_3^i + ... + y_v\chi_v^i \end{aligned}$$

Where $\chi_j = \alpha^{e_j}$
Here location of errors are $e_1, e_2, e_3, ..., e_v$ and the corresponding error magnitudes are $y_1, y_2, y_3, ...y_v$ respectively. Here v is the degree of error polynomial.

Error locator polynomial can be written as

$$\begin{aligned} \Lambda(x) &= (1 + \chi_1 x)(1 + \chi_2 x)...(1 + \chi_v x) \\ &= 1 + \lambda_1 x^1 + \lambda_2 x^2 + ... + \lambda_v x^v \end{aligned}$$

Here $\chi_1, \chi_2, \chi_3, ..., \chi_v$ are called error locators.
$\chi_1^{-1}, \chi_2^{-1}, ..., \chi_v^{-1}$ are roots of the error locator polynomial $\Lambda(x)$
So it can be written as

$$1 + \lambda_1\chi_j^1 + \lambda_2\chi_j^2 + ... + \lambda_v\chi_j^v = 0$$

Now multiplying both sides by $y_j\chi_j^{i+v}$ and then taking summation in the range $j = 1$ to v, the equation can be written as

$$S_{i+v} + \lambda_1 S_{i+v-1} + ... + \lambda_v S_i = 0$$

Now $(2t - v)$ simultaneous equations can be derived by substituting i with values in the range $[0, 2t - v - 1]$.
Now, Berlekamp's algorithm has been used in the experiments to compute the coefficients of error locator polynomial $\Lambda(x)$.

So, $\chi_1, \chi_2, \chi_3, ...\chi_v$ can be found easily because $\chi_1^{-1}, \chi_2^{-1}, ..., \chi_v^{-1}$ are roots of the Error Locator Polynomial $\Lambda(x)$ and the coefficients of error locator polynomial has already been computed using Berlekamp's algorithm.

To find Error Polynomial Coefficients y_j Forney's algorithm has been used.

Generator polynomial $g(x)$ can be written as shown below:

$$g(x) = (x + \alpha^b)(x + \alpha^{b+1})(x + \alpha^{b+2})...(x + \alpha^{b+2t-1})$$

The syndrome polynomial can be defined as shown below:

$$S(x) = S_{b+2t-1}x^{2t-1} + ... + S_{b+2}x^2 + S_{b+1}x + S_b$$

Where $S_{b+2t-1}, ..., S_{b+1}, S_b$ are $2t$ syndrome values which are calculated from received codeword.
The error magnitude polynomial can be defined as

$$\Omega(x) = \Omega_{v-1}x^{v-1} + \Omega_{v-2}x^{v-2} + ... + \Omega_2x^2 + \Omega_1x + \Omega_0$$

Error evaluator polynomial $\Omega(x)$ can be calculated using the following equation

$$\Omega(x) = (S(x)\Lambda(x))mod x^{2t}$$

and here all terms above degree (2t-1) in $S(x)\Lambda(x)$ are neglected.
Now Error Polynomial Coefficients y_j can be derived as shown below:

$$y_j = \frac{\Omega(\chi_j^{-1})}{\Lambda'(\chi_j^{-1})}$$

Where $\Omega(x)$ is Error Magnitude Polynomial or Error Evaluator polynomial and $\Lambda'(\chi_j^{-1})$ is the derivative of $\Lambda(\chi_j^{-1})$.

2.4.2 Convolutional Code

Convolutional Codes are widely used in error control coding. It is not based on blocks of bits. Here codeword frames depend on present information frame and some previous information frames.

Block codes depends on message blocks where k bits message block is encoded in encoder and n bits codeword is generated. And $(n-k)$ parity check bits are contained in n-bits codeword. The decoding process of linear block code starts after receiver receives the entire block of encoded data. So delay will be high when the message block length is very large. Besides buffer is needed in the process of encoding of linear block codes.

Now if message bits are coming serially instead of large message block, buffer is not desirable. Convolutional code is preferable in this case.

Now, It is possible to represent codewords of convolutional code by using code tree. So, sometimes convolutional code can be called tree code. A shift register encoder of tree codes is shown below.

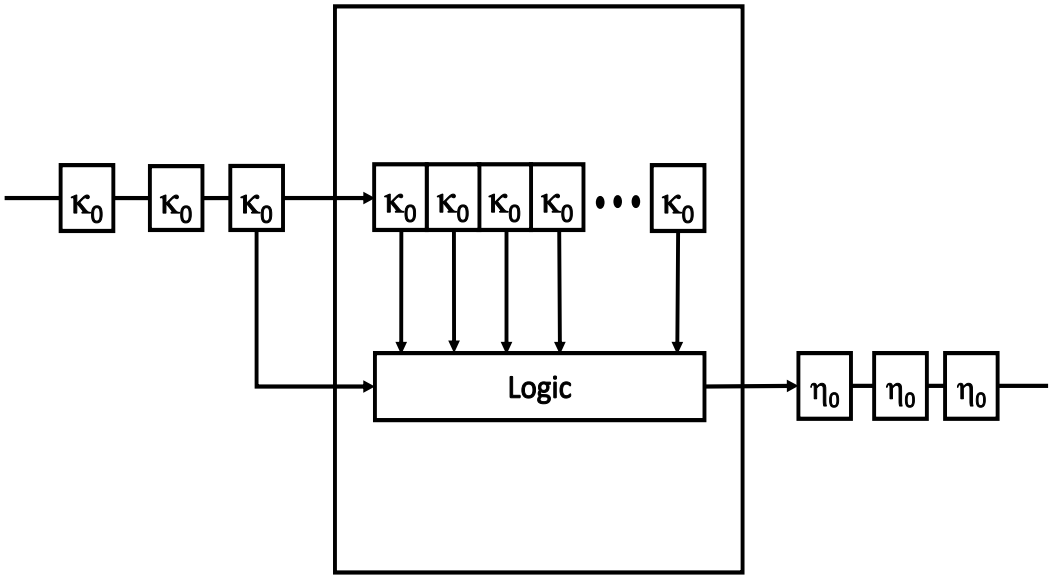

Figure 2.2: A general shift register encoder for generating tree codes

An infinite length bitstream is coming and this incoming bitstream are broken into κ_0-bits segments. Here each segment of κ_0 uncoded data is called **information frame**.
Each information frame of length κ_0 bits is encoded into length of η_0 bits which is called **codeword frame**.

2.4.2.1 Encoder of Convolutional Code

Convolutional encoder (constraint Length(K)=3, rate(R)=1/2) has been considered as an example here to understand the encoding process [37] of convolutional code.

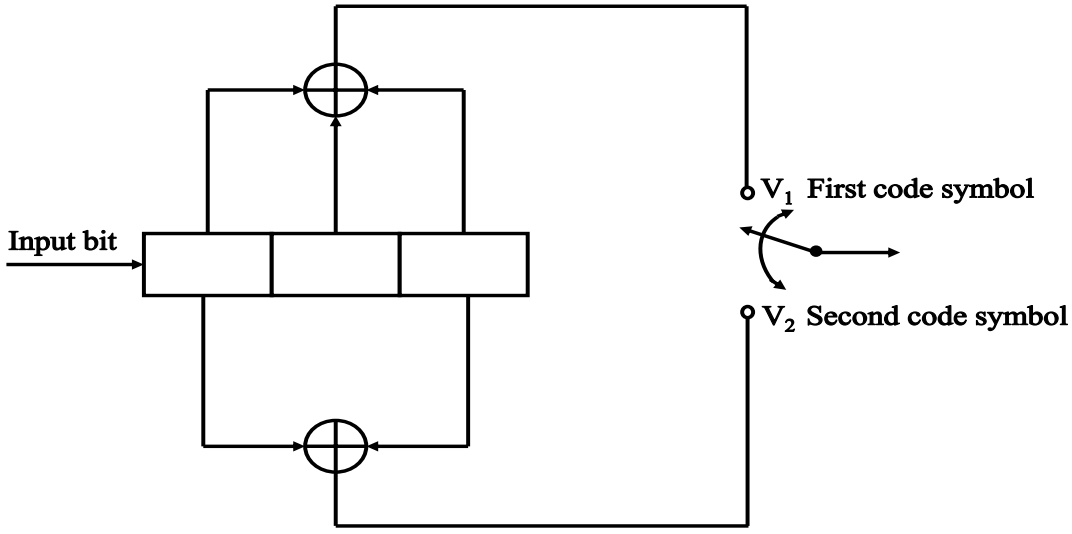

Figure 2.3: Convolutional encoder (Constraint length(K)=3, Rate(R)=1/2)

Figure 2.3 shows a convolutional encoder which has information frame length $\kappa_0 = 1$ and codeword frame length $\eta_0 = 2$. It has constraint length $K = 3$.
There are three shift-registers and two modulo-2 adders in the convolutional encoder. The first shift-register takes the current input data bit and rest shift-registers acts as memory of the encoder. So the output of convolutional encoder depends on current input data bit and $(K-1)$ preceding bits.

The first code symbol V_1 can be found by modulo-2 addition of the current input data bit which is incoming in the first shift-register and the two preceding data bits which are stored in next two shift-registers. The second code symbol V_2 can be found

by modulo-2 addition of the incoming data bit and the stored bit in the rightmost shift register. The incoming data bit's corresponding output of the convolutional encoder will be $\{V_1, V_2\}$.

The convolutional encoder has two paths for code symbol generation. The generator polynomial of the upper path or path 1 is
$\Psi^1(D) = 1 + D + D^2$
The generator polynomial of lower path or path 2 is
$\Psi^2(D) = 1 + D^2$
The incoming message sequence is represented by polynomial m(D). Convolution in time domain is converted into multiplication in D-domain using Fourier transform. So the output polynomial of upper path or path 1 is defined as
$C^1(D) = \Psi^1(D)m(D)$
The output polynomial of lower path or path 2 is defined as
$C^2(D) = \Psi^2(D)m(D)$

Table 2.1 represents the state table of the convolutional encoder shown in Fig. 2.3. The first shift register is for incoming data bit and the next two shift-registers are memory of the convolutional encoder. Now the state of the convolutional encoder depends on the second and third shift register. The state table of the convolutional encoder(constraint Length(K)=3, Rate(R)=1/2) is shown below.

Incoming Bit	Current State of Encoder		Next State of Encoder		Output Bits	
0	0	0	0	0	0	0
1	0	0	1	0	1	1
0	0	1	0	0	1	1
1	0	1	1	0	0	0
0	1	0	0	1	1	0
1	1	0	1	1	0	1
0	1	1	0	1	0	1
1	1	1	1	1	1	0

Table 2.1: State table of convolutional encoder

Now, the state diagram of convolutional encoder is shown in Fig. 2.4.

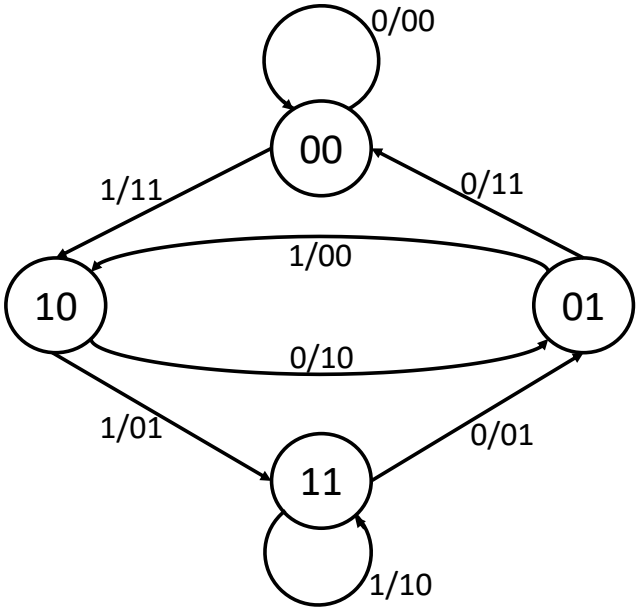

Figure 2.4: State diagram of convolutional encoder

Now, Trellis diagram of the convolutional encoder is shown in Fig. 2.5.

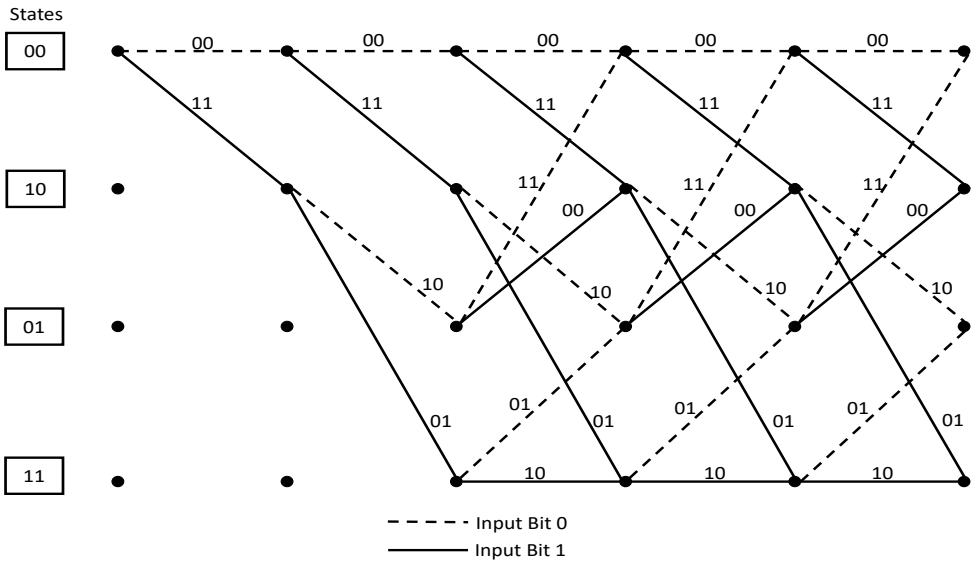

Figure 2.5: Trellis diagram of the convolutional encoder

2.4.2.2 Decoder of Convolutional Code

There are two main techniques of decoding of convolutional codes. Those are
• Maximum likelihood decoding(Viterbi algorithm)
• Sequential decoding
However, in the experiments, maximum likelihood decoding (Viterbi algorithm) has been used. Now, decoding based on Viterbi algorithm [17] is described below.

Decoding Based on Viterbi Algorithm

Viterbi algorithm is a maximum likelihood decoder. There are some steps in this decoding as shown below:

Initialization step

Firstly, Initialization is done by setting the all zero state of the trellis to zero.

First computational step

At time unit i, the computation is started and determining the metric for the path that enters each state of the trellis is done. Then identifying survivor is done and storing the metric for each one of the states is done.

Second computational step

The metrics for all 2^{K-1} paths that enter a state for the next time unit $(i+1)$ are determined. Here K is the constraint length of the convolutional encoder. Hence following steps are done:

• Add the metrics which are entering the state to the metric of the survivor at the preceding time unit i.
•Comparison is done among the metrics of all 2^K paths entering the state.
• Selection of the survivor with the largest metric is done. Then storing it with its metric is done and discarding all other paths in the trellis is done.

Third computational step

Continue the search to convergence. Second computational step is repeated here for time unit $i < L + L_1$. Where L is message sequence length and L_1 is termination sequence length.
Stop the computation when the time unit is reached to $i = L + L_1$.

2.4.3 Low Density Parity Check(LDPC) Code

Low Density Parity Check(LDPC) codes [17] can be described by parity check matrix H. The parity check matrix contains mostly 0s and a small number of 1s. So here parity check matrix H is sparse parity check matrix.

LDPC code can be defined by parameters (n, W_c, W_r) Where n is block length, W_c is weight of the column of parity check matrix(i.e a column contains W_c number of 1s) and W_r is weight of the row in parity check matrix(i.e a row contains W_r number of 1s).

2.4.3.1 Regular LDPC Code

A regular (n, W_c, W_r)LDPC code has a parity check matrix of dimension $m \times n$ where each column contains a small fixed number(W_c) of 1s, where $W_c \geq 3$ and each row contains a small fixed number(W_r) of 1s, where $W_r \geq W_c$.

Here low density means $W_c \ll m$ and $W_r \ll n$

The total number of 1s in parity check matrix(H) is=$W_c \cdot n = W_r \cdot m$

Here also $m \geq n - k$ and k is the message length.

$\Rightarrow R = \frac{k}{n} \geq 1 - \frac{W_c}{W_r}$ and thus $W_c < W_r$

2.4.3.2 Irregular LDPC Code

In irregular LDPC, column weight may be different if we look column to column and row weight may be different if we look row to row in the sparse parity check matrix.

For irregular LDPC code, the variable nodes have multiple degrees in the tanner graph and the check nodes also have multiple degrees in the tanner graph.

We can define the degree distribution of the variable nodes or column distribution of an irregular LDPC in the Tanner graph as shown below

$$\lambda(X) = \sum_{d=1}^{d_N} \lambda_d X^{d-1} \tag{2.16}$$

Where X is a node variable in the Tanner graph, λ_d is the fraction of variable nodes with degree d in the graph, d_N is the maximum degree of the variable node in the Tanner graph.

We can define the degree distribution of the check nodes or row distribution of an irregular LDPC in the Tanner graph as shown below

$$\rho(X) = \sum_{d=1}^{d_c} \rho_d X^{d-1} \tag{2.17}$$

Where X is a check node in the Tanner graph, ρ_d is the fraction of check nodes with degree d in the graph, d_c is the maximum degree of the check node in the Tanner graph.

2.4.3.3 Encoding of LDPC Codes

LDPC code is linear error control code. LDPC code uses sparse parity check matrix H. The LDPC encoder uses generator matrix G to encode message bits. The generator matrix can be defined as shown below

$$G = [I_k | P^T] \tag{2.18}$$

m is $k \times 1$ message vector. Then codeword is generated by the following equation

$$c = mG \tag{2.19}$$

Codeword is valid if the codeword satisfies the following equation

$$Hc^T = 0 \tag{2.20}$$

2.4.3.4 Decoding of LDPC Code

Decoding of LDPC code based on belief propagation algorithm and Min-Sum algorithm are discussed [19, 35].

Belief Propagation Decoding

A basic block diagram of belief propagation decoding as follows:

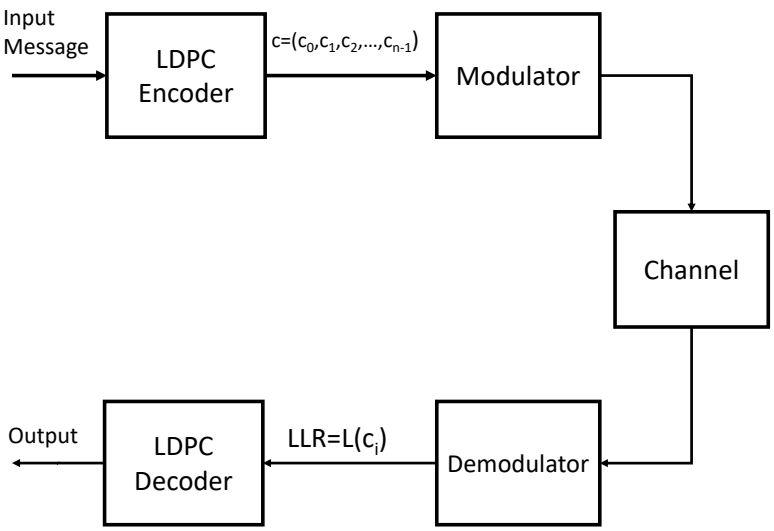

Figure 2.6: Block diagram for belief propagation decoding

Belief propagation algorithm which is based on the decoding algorithm presented by Gallager has been used in LDPC decoding. The belief propagation algorithm is also known as a message passing algorithm. The algorithm has been described below. LDPC encoder encodes message into codeword which is represented by

$$c = c_0, c_1, c_2, c_3, ..., c_{n-1} \tag{2.21}$$

Now, the input of the LDPC decoder for the transmitted LDPC encoded codeword is considered as log likelihood ratio(LLR) value which is defined below.

$$L(c_i) = \log \frac{Pr(c_i = 0/Channeloutputforc_i)}{Pr(c_i = 1/Channeloutputforc_i)} \tag{2.22}$$

Initialization is done before the first iteration

$$L(q_{ij}) = L(c_i) \tag{2.23}$$

The main components of the algorithm are updated in each iteration based on the following equations:

$$Ł(\Gamma_{ji}) = 2atanh(\prod_{i' \in V_j \backslash i} \tanh(\frac{1}{2} L(q_{i'j}))) \tag{2.24}$$

$$L(q_{ij}) = L(c_i) + \sum_{j' \in C_i \backslash j} L(\Gamma_{j'i})) \tag{2.25}$$

and

$$L(Q_i) = L(c_i) + \sum_{j' \in C_i} L(\Gamma_{j'i}) \tag{2.26}$$

$L(Q_i)$ gets the updated estimation of the LLR value for transmitted bit c_i after each iteration. Now, the soft decision output value is $L(Q_i)$ for c_i.
For c_i, hard decision output is 1 if $L(Q_i) < 0$. Otherwise, hard decision output for c_i is 0.
The algorithm checks the parity check equation at the end of each iteration.

$$HC^T = 0 \tag{2.27}$$

The decoding process stops when all the parity checks are satisfied or the number of iteration reaches its' maximum value.

V_{j1} and $C_{i\text{j}}$ are the index sets based on parity check matrix. V_j represents all non zero elements in row j and C_i represents all non zero elements in column i.

Min-Sum Decoding

To understand min-sum algorithm we can discuss sum product algorithm in log domain firstly in another way. Let the LDPC encoder encodes the message into codeword $c = c_0, c_1, c_2, c_3, ..., c_{n-1}$. Let the received codeword is $v = v_0, v_1, v_2, v_3, ..., v_{n-1}$. Now log likelihood ratio(LLR) of v is shown below.

$$L(v_i) = log(\frac{Pr(v_i = 0/y_i)}{Pr(v_i = 1/y_i)}) \tag{2.28}$$

Here the channel is additive white gaussian noise(AWGN) channel. The received symbol is y_i and the noise power is σ^2. So LLR of the received symbol is described below.

$$L(v_i) = \frac{2y_i}{\sigma^2} \tag{2.29}$$

The messages are passed variable node i to check node j can be computed in LLR as $L(q_{ij})$. α_{ij} and β_{ij} are the sign and magnitude of $L(q_{ij})$ respectively.
The messages are passed from check node to variable node can be described in LLR as shown below.

$$L(\Gamma_{ji}) = [\prod_{i' \in V_j \backslash i} \alpha_{i'j}].\psi(\sum_{i' \in V_j \backslash i} \psi(\beta_{i'j})) \tag{2.30}$$

Here

$$\psi(x) = \log(\frac{e^x + 1}{e^x - 1}) \tag{2.31}$$

The messages are passed from variable node to check node can be computed in LLR as

$$L(q_{ij}) = L(V_i) + \sum_{j' \in C_i \backslash j} L(\Gamma_{j'i}) \tag{2.32}$$

Symbols are decoded by comparing $L(Qi)$ with threshold. $L(Q_i)$ can be described as shown below

$$L(Q_i) = L(v_i) + \sum_{j \in C_i} L(\Gamma_{ji}) \tag{2.33}$$

The algorithm checks parity check equation at the end of each iteration. The decoded symbol can be computed as shown below
Decoded output is 1 if $L(Q_i) < 0$. Otherwise, output is 0.

The Min-Sum algorithm(MSA) is actually modified version of the Sum-Product algorithm(SPA). The check node operation is simplified. So the complexity of the algorithm is reduced. In Min-Sum algorithm the equation of $L(\Gamma_{ji})$ becomes

$$L(\Gamma_{ji}) = [\prod_{i' \in V_j \backslash i} \alpha_{i'j}]. \min_{i' \in V_j \backslash i} \beta_{i'j} \tag{2.34}$$

Another form of the above equation of MSA is shown below.

$$L(\Gamma_{ji}) = [\prod_{i' \in V_j \backslash i} sign(L(q_{i'j}))]. \min_{i' \in V_j \backslash i} (|L(q_{i'j})|) \tag{2.35}$$

2.5 Encryption Algorithms

Encryption is the process of converting information into secret code. The secret code hides the true meaning of information. Advanced encryption standard(AES) algorithm and high diffusion nonlinear key mixing with 8 rounds(HDNM8) algorithm have been considered.

2.5.1 Advanced Encryption Standard(AES) Algorithm

Block diagram of AES algorithm is shown as follows:

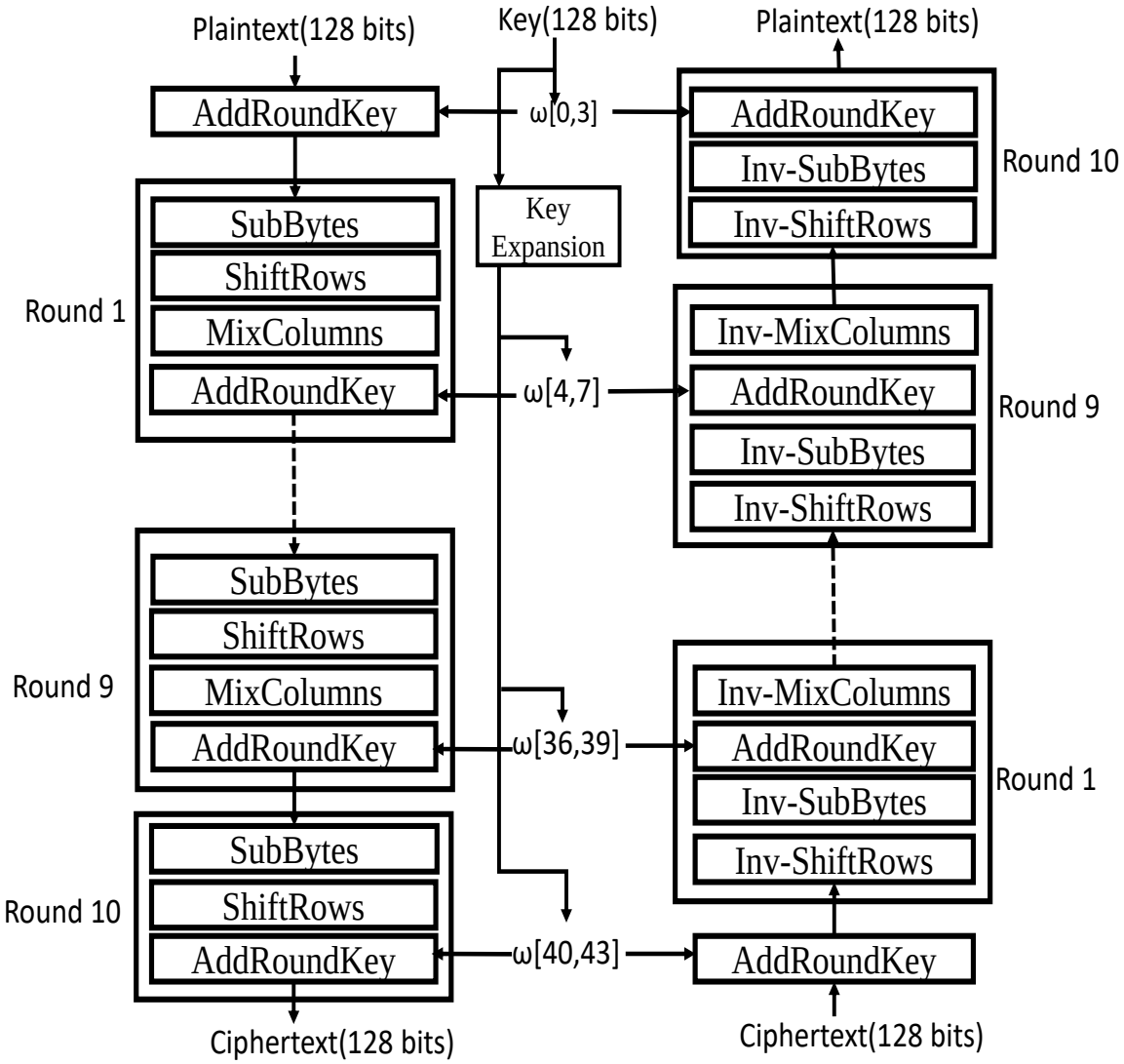

Figure 2.7: Basic encryption and decryption structure of AES

Advanced encryption standard(AES) [9] is block cipher encryption algorithm. There are three different key size available in AES. Three different key lengths are 128 bits, 192 bits and 256 bits. But here 128 bits length key has been considered.

2.5.1.1 Creation of Round Keys or Key Expansion in AES

There is a initial key of 128 bits(16 bytes) which can be represented in a 4×4 array. Each cell of the array is 1 byte. Here 4 cells together form a word. Word represents one column in the array here. So there are 4 words in the initial key. The AES key expansion algorithm takes the 4 words initial key as input and gives total 44 words. The first four-word round key is used in first AddRoundKey and the other ten keys are used in subsequent ten rounds.

2.5.1.2 Encryption Part of AES Algorithm

AES encryption takes blocks of length 128 bits as input which is called plaintext.The output of AES encryption gives block length of 128 bits which is called cipher text.

There are total ten rounds in encryption part in AES algorithm. Firstly the 128 bits input plaintext is passed through AddRoundKey process. Then there are subsequent ten rounds are present. First nine rounds each consists of four subprocesses: SubBytes, ShiftRows, MixColumns and AddRoundKey.
Now in the last tenth round of AES encryption MixColumns is not present. Tenth round consists of the subprocesses: SubBytes, ShiftRows and AddRoundKey
The AES encryption gives 128 bits cipher text after the tenth round.

2.5.1.3 Decryption Part of AES Algorithm

The decryption process of AES takes blocks of length 128 bits ciphertext as input. The output of AES decryption gives block length of 128 bits plaintext back.

There are total ten rounds in decryption part in AES algorithm. Firstly the 128 bits input ciphertext is passed through AddRoundKey process. Then there are subsequent ten rounds are present. First nine rounds each consists of the four subprocesses: Inv-ShiftRows, Inv-SubBytes, AddRoundKey and Inv-MixColumns.
However, Inv-MixColumns is not present in the tenth round of AES decryption. Tenth round consists of the subprocesses: Inv-ShiftRows, Inv-SubBytes and AddRoundKey
The AES decryption gives 128 bits plaintext back after the tenth round.

2.5.2 HDNM8 Block Cipher

HDNM8 [3] stands for High Diffusion Nonlinear Key Mixing with 8 rounds. HDNM8 is 128 bits substitution permutation networks(SPN) type block cipher. The input plaintext is 128 bits and the output is 128 bits ciphertext.

2.5.2.1 Encryption Part of HDNM8 Algorithm

There are total eight rounds in encryption part in HDNM8. In one to eight rounds, there are three layers present in each round as shown below:

- Nonlinear round key mixing layer
- Substitution layer which have 16 AES S-boxes
- Single 128 bit diffusion layer

After that, one nonlinear round key mixing layer is present.

Block diagram of HDNM8 is shown in figure 2.8. Now, by using the HDNM8 encryption module, counter(CTR) mode of operation is performed.

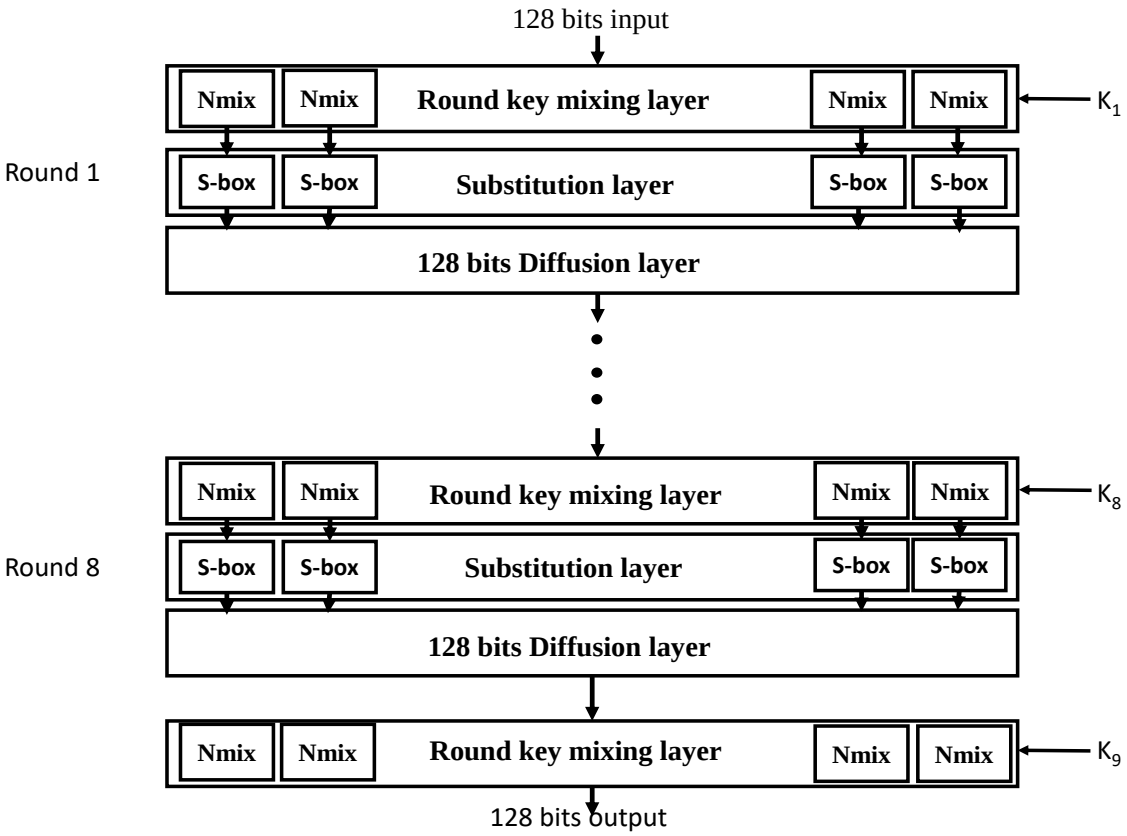

Figure 2.8: Block diagram of HDNM8

2.6 Block Cipher Modes of Operation

Block cipher is one types of encryption algorithm which takes fixed size of input data or plaintext and produces same fixed size of ciphertext. If the input length is larger than the fixed input length, the input is divided into blocks of the fixed size.

There are various modes of operations [11] for a block cipher. The modes of operations are

- Electronic codebook(ECB) mode
- Counter(CTR) mode
- Cipher block chaining(CBC) mode
- Cipher feedback(CFB) mode
- Output feedback(OFB) mode

ECB, CTR and CBC mode of operations have been considered in this thesis.

2.6.1 Electronic Codebook(ECB) Mode

Electronic codebook(ECB) mode is one of the simplest block cipher mode of operation. The plaintext is divided into blocks. Each block is of same fixed size. In this ECB mode operation each block of the input plaintext is directly encrypted into block of cipher text using a key. The first block of plaintext is encrypted into first block of cipher text using a key. The second block of plaintext is encrypted using the same key and this process will continue. So, it is possible to create a codebook of ciphertexts for all possible blocks of plaintexts. The forward cipher function in ECB mode encryption operation is used direcltly and independently to each plaintext block. Parallel encryption of blocks is possible in ECB mode of operation. So it is one of the faster ways of encryption.

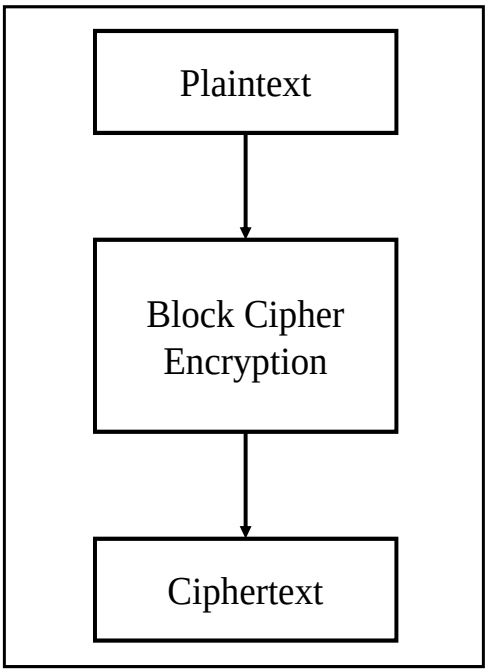

Figure 2.9: Block diagram of block cipher based ECB mode encryption

In ECB mode decrypton, similarly the inverse cipher function is also directly and independently used to obtain plaintext from ciphertext.

2.6.2 Counter(CTR) Mode

In counter(CTR) mode operation, the counter initiates value every time of operation. The counter value is encrypted first using key. Then the encrypted block is XORed with plaintext block and ciphertext is produced. Let the length of the last block of plaintext is less than the length of previous blocks. Let the length of each previous block of plaintext is l and the length of the last block of plaintext is v. v is less than l. In this case, most significant v bits of the encrypted value is used to XORed with the v length plaintext and the remaining $(l - v)$ bits from the encrypted block are discarded. In CTR mode the counter value is different for each block.

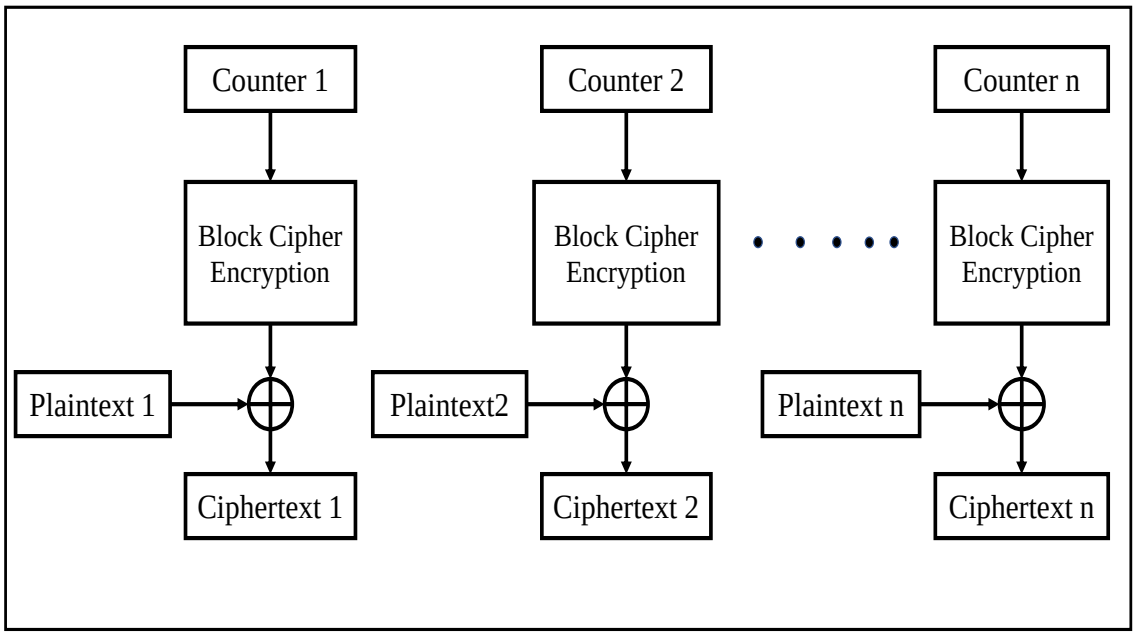

Figure 2.10: Block diagram of block cipher based CTR mode encryption

In counter(CTR) mode decryption, counter initiates value every time of operation. The counter values are same as counter(CTR) mode encryption process. In CTR mode decryption, the same encryption block is used which is used in CTR mode encryption. The counter value is encrypted using a key. The encrypted block is XORed with the ciphertext block. Let the length of each previous block of ciphertext is l and the length of the last block of ciphertext is v. Then most significant v bits of

the encrypted value is used to XORed with the v length ciphertext and the remaining $(l-v)$ bits from the encrypted block are discarded. The CTR mode can be performed in parallel because this mode is independent of feedback use.

2.6.3 Cipher Block Chaining(CBC) Mode

In cipher block chaining(CBC) mode encryption an Initial vector(IV) is needed. The first input block is obtained by XOR operation between the first plaintext block and the initial vector(IV). The input block is passed through the encryption process. The output of the encryption process is the first cipher block. The output block is then XORed with the second plaintext block and the result is passed through the encryption process to get the second output block. Each plaintext is XORed with the previous output or ciphertext block to get the new input block and the input block is passed through the encryption process to get the ciphertext block.

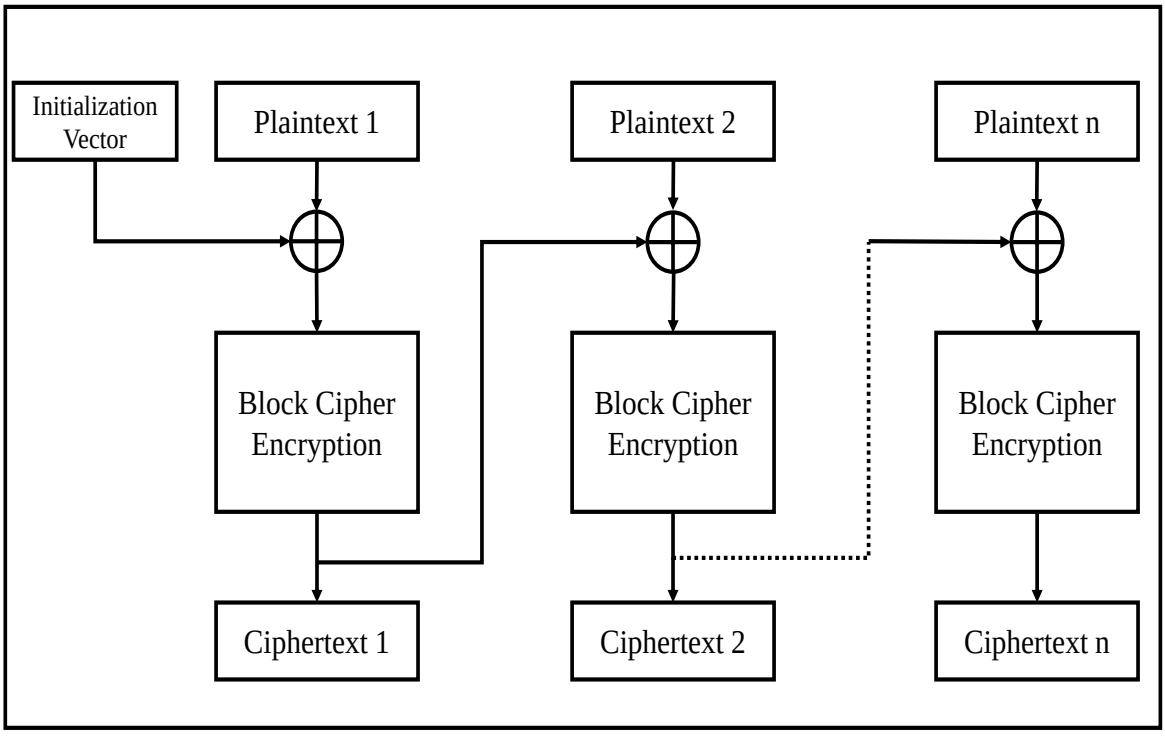

Figure 2.11: Block diagram of block cipher based CBC mode encryption

Similarly, in cipher block chaining(CBC) mode decryption, the first ciphertext block is passed through decryption process and the decrypted block is XORed with the initial vector(IV) to get the first block of plaintext. The second ciphertext block is passed through decryption process and the decrypted block is XORed with the first ciphertext to get the second plaintext block. To get plaintext block of any round, first the ciphertext is passed through decryption process and the decrypted block is XORed with the previous ciphertext.

2.7 Literature Survey

Reed Solomon(RS) codes are an important group of error correcting codes. Reed Solomon(RS) codes were introduced by Irving Stoy Reed and Gustave Solomon in 1960 [33]. The algebraic structure of RS codes are easily understandable and as a result it is possible to implement efficient decoder [12]. RS codes are non binary codes and they are able to correct burst errors.

Convolutional codes were introduced by Peter Elias in 1955. Andrew Viterbi determined an important thing in 1967 that convolutional codes could be decoded using maximum likelihood decoding and the decoding could be done using Viterbi decoder with reasonable complexity.

Robert Gray Gallager developed the LDPC concept in 1960. LDPC codes are also called Gallager codes. This codes were impractical to implement when it was first developed by Gallager [15] in 1963. Gallager's work was rediscovered by Mackay and Neal in 1996. LDPC codes are capacity approaching codes.

Turbo codes were discovered in 1993. Turbo codes are another class of capacity approaching codes. The advances of LDPC codes surpassed turbo codes in terms of error floor and performance in high code rate.

BER is very important in performance analysis. Performance of communication channel, the effect of error correcting codes, effect of modulation techniques, effect of AWGN channel, effect of fading channel and various things can be described by BER performance of communication channel. The communication channel is also wireless. Various experiments have been already done.

Sharma et al. [36] considered various error correcting codes like Reed Solomon codes, convolutional codes for their different code rates and various modulation techniques like BPSK, QPSK, 16QAM and 64QAM. They considered Viterbi decoder for convolutional codes. They considered AWGN channel and evaluated BER performance. They showed concatenated RS-CC code had better performance than individual RS code or CC code over AWGN channel.

Usha et al. [38] performed BER analysis using different modulation order of QAM such as 16QAM, 64QAM, 128QAM and 256QAM with using same satellite link. They concluded that bit error rate(BER) was high for higher order modulation of MQAM.

Mahapatra et al. [25] did performance analysis of modulation schemes(PSK, QAM, OQPSK) for wireless sensor networks. They found that energy consumption was one

of the major issues for increased lifetime of wireless sensor network. They considered AWGN noise and Rayleigh fading, Rician fading for different modulation schemes PSK, FSK, QAM, PAM and OQPSK. They showed that OQPSK was a good choice as modulation schemes in wireless sensor network.

Panwar et al. [29] considered AWGN channel and Rayleigh fading channel. They took BPSK as modulation scheme. They compared BER performance of AWGN channel and BER performance of Rayleigh fading channel. They showed that BER performance was degraded for Rayleigh fading channel due to rapid amplitude fluctuation in the received signal due to Rayleigh fading.

Kobayashi et al. [22] provided description and analyzed NASA's high data rate downlink system considering Ka-band. This system was proposed for NASA's NISAR mission. They considered (8160, 7136) CCSDS LDPC channel coding and OQPSK modulation scheme. The system was able to deliver 35 Tbits per day data from the considered two onboard SAR systems.

Kang [21] considered Reed Solomon(RS) code and Reed Solomon Product Code(RSPC) and determined whether the forward error correction algorithms translated directly to their effectiveness. If bit flips happens and it is beyond RS code's correction limit, RSPC can be used.

Coulibaly et al. [7] proposed their own joint AES-LDPC system. They considered joint encryption and channel coding. LDPC coding and AES algorithm based on 128 bits key was considered. They showed that their proposed method was able to achieve data security and error correction. The proposed method also reduced complexity of computation.

Ning et al. [27] provided their own joint encryption and error control method by using LDPC coding and AES encryption algorithm. They designed their own structure in satellite communication. They showed BER performance for their method is better than some other method.

Pal et al. [28] proposed an algorithm and also architecture for error detection and error correction which was based on LDPC coding. They gave importance on maintaining data integrity in a noisy channel and retrieving original data. They showed that their simulation for their own algorithm worked successfully.

The Consultative Committee for Space Data Systems recommended a standard in a blue book [1] to develop the system in telemetry synchronization and channel coding . They considered some particular Reed Solomon code, convolutional codes, LDPC

codes and other error correcting codes in channel coding. The Consultative Committee for Space Data Systems also presented a informational report [34] where they explained the background to support the CCSDS recommended standard in channel coding and telemetry synchronization.

Fang et al. [14] considered a simple practical channel model called block fading channel and root-protograph LDPC codes. Their simulation result showed that root protograph related codes are capable to achieve outage limit approaching word error rate performance.

Yu et al. [40] proposed a wireless error model based on two state Markov error model. They considered QPSK, 16QAM and 64QAM as modulation techniques. They considered turbo coding and LDPC coding as channel coding techniques. Their model helped in evaluation of the error control strategies with shorter simulation period and the computational complexity is also less.

Elagooz et al. [13] proposed a efficient decoding scheme for CCSDS Reed Solomon code. They also considered AWGN channel and Rayleigh fading channel. Their simulation result was able to achieve good coding gain compared with RS code's algebraic decoding.

Huang et al. [18] proposed a multilevel Reed Solomon codes. They also proposed iterative multistage soft decoding in visible light communication. Their proposed decoding algorithm was able to achieve good performance gain compare to existing algorithm for decoding.

Jeon et al. [20] proposed joint encryption and channel coding method, namely cipher feedback-advanced encryption standard-Turbo. Their proposed scheme improved security performance in satellite data transmission.

Li et al. [24] proposed two new decoding algorithms for Reed Solomon codes. They considered burst Rayleigh fading channel with AWGN noise. They showed that the performance of their proposed algorithms are better than classic Berlekamp-Messay algorithm. The computational complexity is also less for proposed algorithms.

Garzon et al. [16] proposed an opportunistic transmission system where they considered AWGN noise, flat and slow Rayleigh fading, co-channel interference. They performed mean bit error rate performance analysis in their experiment for different modulation schemes.

Rajagopalan et al. [31] considered LDPC code and CCSDS defined encoding scheme

for telecommand operation. They also considered soft decision and hard decision decoding algorithm. They performed performance analysis of the decoding algorithms for LDPC code and got 6 dB coding gain for soft decision algorithm and 4 dB coding gain for hard decision algorithm. Where they considered 4-bit quantized inputs.
Almaktof et al. [2] compared BER performance of M-ary PAM over AWGN channel and fading channels. They considered Rayleigh fading channel and Rician fading channel. They also considered 16PAM, 32PAM, 64PAM, 128PAM and 256PAM under M-PAM. BER performance was degraded when M was increased. They also showed that BER performance of M-PAM over Rician channel is better than the cases of M-PAM over AWGN and Rayleigh channels.

There are some advantages of LDPC codes. LDPC codes fulfill the satellite requirements due to parallel decoding and low decoding complexity [10]. LDPC codes also has ability of self error detection using syndrome. LDPC codes have great performance with iterative decoding and it is able to achieve very close to Shannon limit [8]. LDPC decoding algorithm has low implementation complexity and more parallelization compared to decoding algorithm of convolutional code [8] Now if burst error correction capability is considered then the capability of RS codes are excellent. The length of burst error correction can reach half of the parity bits for RS codes[39]. The performance of convolutional codes are worst. For turbo codes, the burst error correction length cannot reach up to half of the parity bits. LDPC codes' burst error correction capability are acceptable. NASA, ESA and various standard organizations have used error correcting codes in their several missions. Convolutional codes were used in NASA's Pioneer missions. They also used convolutional convolutional codes in their various missions like Voyager, Galileo, Mars Pathfinder, Juno etc. They also used Reed Solomon code in various missions like Voyager 2, Galileo, Mars Pathfinder etc. They also used LDPC codes in mission Curiosity [5]. European Space Agency used covolutional code in various missions like Giotto, Cassini, Rosetta etc. They also used Reed Solomon codes in missions like Giotto, Cassini, Rosetta, Gaia [5]. So they used various error correcting codes like Reed Solomon codes, convolutional codes, Low density parity check codes in their various missions. They sometimes used single error correcting codes and sometimes used concatenated between two error correcting codes. Therefore, the objective of this thesis is to find bit error rate(BER) performance of wireless communication channel considering AWGN noise and Rayleigh fading when error correcting codes like Reed Solomon codes, convolutional codes, LDPC codes

are used as error correcting codes and various M-ary phase shift keying(MPSK) and M-ary quadrature amplitude modulation(MQAM) modulation techniques are used. Also BER performance of a wireless channel has been studied where both encryption and channel coding have been implemented at physical layer.

2.8 Conclusion

Theoretical background of all the required concepts have been discussed and literature survey has been done in this chapter. Error correcting codes and their encoding and decoding processes, modulation schemes, AWGN noise, Rayleigh fading, AES encryption and decryption process, HDNM8 encryption process, block cipher modes of operations etc have been discussed. In the next three chapters, BER performance of wireless communication channel under different channel impairments are presented.

Chapter 3

BER Performance of Uncoded Communication Channel

Uncoded communication channel has been considered in this chapter. The channel is uncoded communication channel because no channel coding technique has been used. AWGN has been considered as channel noise. In this chapter, BER performance analysis of the uncoded communication channel with AWGN noise has been done for MPSK and MQAM modulation techniques. Then Rayleigh fading has been considered to understand the fading effect and BER performance analysis of Rayleigh fading communication channel with AWGN for MPSK and MQAM has been performed. All the experiments have been simulated in MATLAB.

3.1 AWGN Channel with M-ary PSK and M-ary QAM Modulation

In this section, BER performance of uncoded communication channel with AWGN noise for M-ary phase shift keying(MPSK) modulation scheme and M-ary quadrature amplitude modulation(MQAM) modulation scheme has been discussed.

3.1.1 AWGN Channel with M-ary PSK Modulation

BER performance of uncoded communication channel with AWGN noise for M-ary phase shift keying modulation scheme has been discussed here.

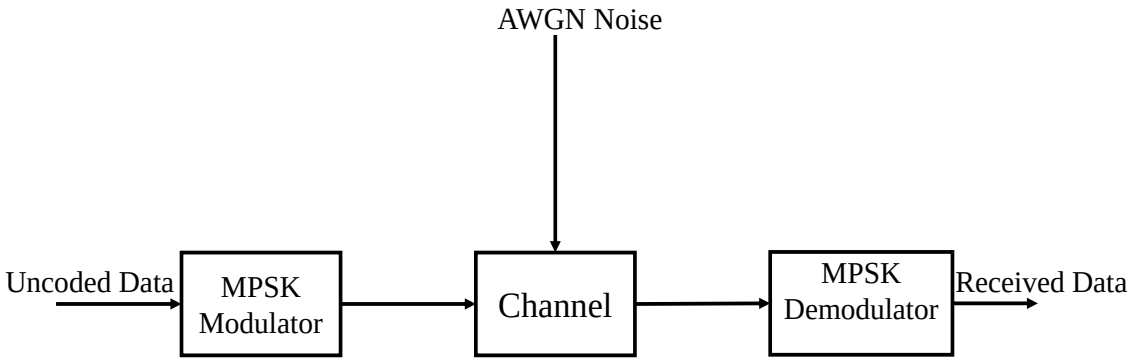

Figure 3.1: Block diagram of uncoded AWGN channel with MPSK modulation

In this experiment, message signals have been considered which are random in nature. The uncoded message signal has been passed through MPSK modulator. After that the modulated signal has been sent through communication channel. The communication channel which has been considered is wireless. The communication channel has been affected by additive white gaussian noise(AWGN). The noise corrupted signal has been demodulated by MPSK demodulator at the receiver side. Then the demodulated signal has been compared with the original message signal and bit

error rate(BER) has been calculated. The measured BER values in this experiment have been shown in Table 3.1. This experiment has been simulated in MATLAB.

E_b/N_0(dB)	BER(BPSK)	BER(QPSK)	BER(8PSK)	BER(16PSK)	BER(32PSK)
0	0.0787368	0.07872	0.122584	0.174376	0.22485
1	0.0562657	0.0563754	0.100861	0.153571	0.206807
2	0.0374323	0.0375126	0.0806892	0.133793	0.18914
3	0.0229193	0.0228508	0.0622563	0.115609	0.17124
4	0.0125501	0.0125322	0.0459319	0.0985762	0.153893
5	0.00596839	0.00593733	0.0318309	0.0829587	0.136729
6	0.00237061	0.00239628	0.0204644	0.0681619	0.120827
7	0.000776444	0.000775944	0.0119491	0.0542615	0.105532
8	0.000190222	0.000193667	0.00618561	0.0414496	0.0914452
9	3.38889e-05	3.31111e-05	0.00277333	0.0300009	0.0784573
10	4.36111e-06	3.72222e-06	0.00100289	0.0202152	0.0661217
11	2.68519e-07	2.59259e-07	0.000286556	0.0125929	0.0545408
12	9.25926e-09	0	6.08333e-05	0.00702872	0.0434778
13	0	0	8.38889e-06	0.00343428	0.0332728
14	0	0	7.96296e-07	0.00142967	0.0239896
15	0	0	6.48148e-08	0.0004745	0.0162672
16	0	0	9.25926e-09	0.000119167	0.0100852
17	0	0	0	2.33333e-05	0.00565989
18	0	0	0	2.94444e-06	0.00279111
19	0	0	0	1.85185e-07	0.00116489
20	0	0	0	9.25926e-09	0.000386889
21	0	0	0	0	0.000101944
22	0	0	0	0	1.8e-05
23	0	0	0	0	2.11111e-06
24	0	0	0	0	1.2037e-07
25	0	0	0	0	9.25926e-09
26	0	0	0	0	0

Table 3.1: BER measurement of uncoded AWGN channel for MPSK

Based on simulation result a graphical representation of BER vs E_b/N_0 has been presented in Fig. 3.2.

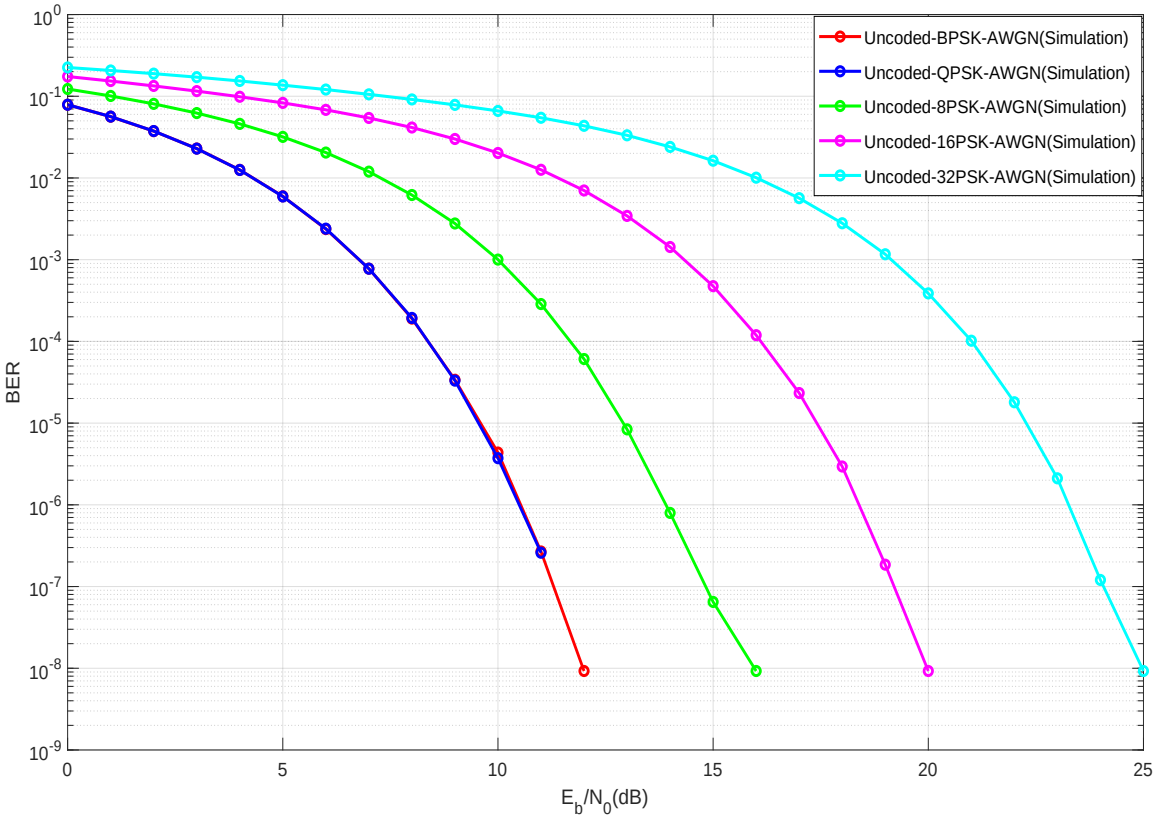

Figure 3.2: BER vs E_b/N_0 graph of uncoded AWGN channel for MPSK

The graph(Fig. 3.2) shows how BER is changed with E_b/N_0 for various MPSK when communication channel is affected by AWGN noise. Here BPSK, QPSK, 8PSK, 16PSK and 32PSK modulation schemes have been considered under MPSK. It can be seen from the graph(Fig. 3.2) that BER performance of BPSK and QPSK are similar and BER performance is degraded when modulation order of MPSK is increased further.

There are two basis functions in QPSK. In-phase component of the carrier signal is modulated by using even bits (or odd bits) and quadrature-phase component of carrier signal is modulated by using odd bits(or even bits). If basis functions of BPSK and QPSK are compared it can be seen that QPSK can be considered as two

independent BPSK signals. They can be demodulated independently also. So BER performance of the uncoded communication channel for BPSK and QPSK are same.

Now, QPSK uses half of the channel bandwidth of the bandwidth used by BPSK. So bit rate of QPSK will be twice of the bit rate of BPSK for same channel bandwidth. Bandwidth efficiency(BWE) can be defined as shown below.

$$BWE = \frac{BitRate}{ChannelBandwidth} \tag{3.1}$$

The required bandwidth(BW) is reduced when modulation order M is increased in MPSK modulation. So bandwidth efficiency(BWE) is increased when modulation order M is increased. However, as modulation order M is increased in MPSK the number of symbols is increased. The constellation points of MPSK modulation scheme are situated in a circle. The distance between adjacent symbols is

$$d_{adjacent} = 2\sqrt{\varepsilon_s}\sin(\frac{\pi}{M}) \tag{3.2}$$

Where ε_s is energy per symbol and M is modulation order of MPSK.
When modulation order M is increased the symbols comes closer to each other. As a result the distance between the constellation points are reduced, so effect of noise will be more. As a result BER performance is degraded when modulation order M of MPSK is increased.

It can be also seen from the graph(Fig. 3.2) that BER performance is improved when E_b/N_0 is increased for any particular modulation order of MPSK.
When energy per bit of transmitted signal(E_b) is increased for a specified noise spectral density $N_0/2$, the message points corresponding to symbols are moved further apart. So the distance between constellation points are increased when E_b/N_0 is increased. So, if E_b/N_0 is increased for a particular modulation order M , BER is improved.

3.1.2 AWGN Channel with M-ary QAM Modulation

BER performance of uncoded communication channel with AWGN noise for M-ary quadrature amplitude modulation scheme has been discussed here.

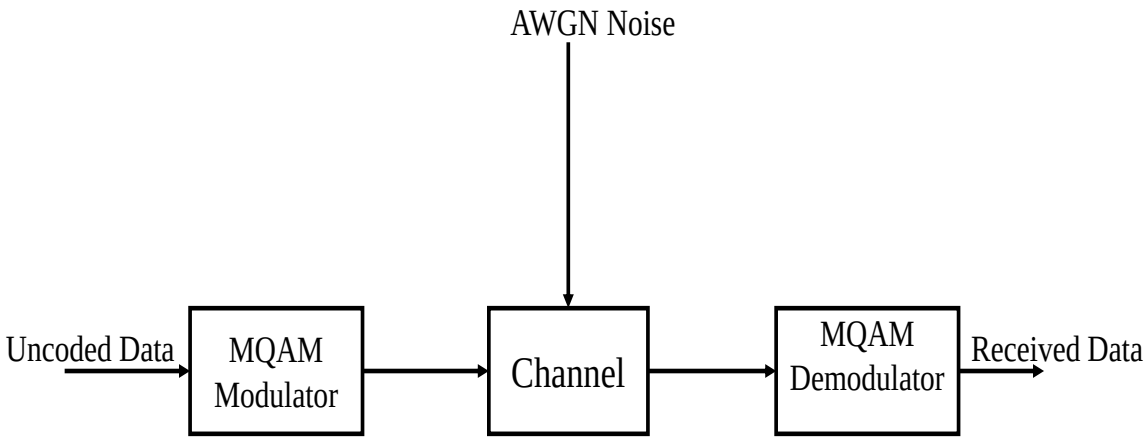

Figure 3.3: Block diagram of uncoded AWGN channel for MQAM

The message signals are random in nature which have been considered in this experiment. Uncoded message signal has been passed through MQAM modulator. QAM, 8QAM, 16QAM,32QAM and 64QAM modulation schemes have been considered under MQAM modulation. The modulated signal has been sent through the communication channel. The considered channel is wireless. AWGN noise has been added with the signal in the communication channel. So the modulated signal has been noise corrupted in the channel. Then the noise corrupted signal has been received by MQAM demodulator at the receiver side. The MQAM demodulator has demodulated the received signal. BER has been calculated by comparing demodulated signal with the original message signal. The measured BER values in this

experiment have been shown in Table 3.2. The experiment has been simulated in MATLAB.

E_b/N_0(dB)	BER(QAM)	BER(8QAM)	BER(16QAM)	BER(32QAM)	BER(64QAM)
0	0.0786044	0.132612	0.141	0.179971	0.19983
1	0.0562326	0.109298	0.119006	0.158711	0.177827
2	0.0374644	0.0866907	0.0977004	0.137533	0.156949
3	0.0228583	0.0658193	0.0773916	0.116983	0.13706
4	0.0124463	0.04713	0.0586618	0.0967552	0.118519
5	0.00596178	0.0313729	0.0418816	0.0772018	0.100791
6	0.00238667	0.0192084	0.0278519	0.0587402	0.0838371
7	0.000771833	0.0104398	0.0169802	0.0422636	0.0675582
8	0.000198167	0.00500117	0.00925906	0.0282511	0.0523473
9	3.42222e-05	0.00201622	0.00439061	0.0173168	0.0385371
10	3.97222e-06	0.000650389	0.001752	0.00951172	0.0265566
11	2.03704e-07	0.000162389	0.000567111	0.00456061	0.0168872
12	1.85185e-08	2.95e-05	0.000138778	0.00185022	0.00972428
13	0	3.02778e-06	2.51667e-05	0.000595111	0.00493472
14	0	2.31481e-07	2.94444e-06	0.0001515	0.0021185
15	0	0	1.57407e-07	2.64444e-05	0.000782611
16	0	0	9.25926e-09	2.91667e-06	0.000215833
17	0	0	0	1.75926e-07	4.48333e-05
18	0	0	0	4.62963e-08	7.5e-06
19	0	0	0	0	4.25926e-07
20	0	0	0	0	1.85185e-08
21	0	0	0	0	0

Table 3.2: BER measurement of uncoded AWGN channel for MQAM

A graphical representation of BER vs E_b/N_0 based on simulation result has been shown in Fig. 3.4 .

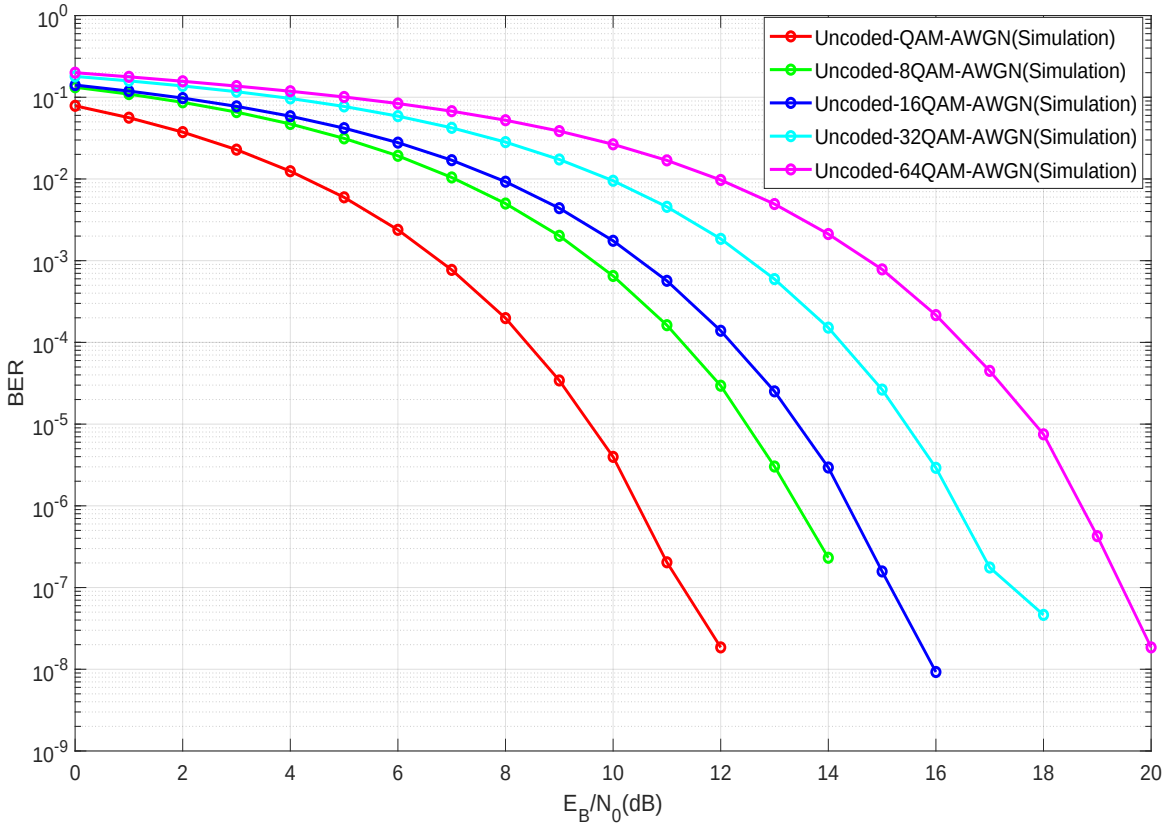

Figure 3.4: BER vs E_b/N_0 graph of uncoded AWGN channel for MQAM

The graph(Fig. 3.4) shows how BER is changed with E_b/N_0 for various MQAM when communication channel is affected by AWGN noise. The graph (Fig. 3.4) also shows that BER performance is degraded with increasing the modulation order of MQAM.

The amplitude and phase of carrier signal are varying nature in MQAM. So the carrier experiences phase as well as amplitude modulation. The constellation diagram consists of a square lattice of symbol points for MQAM. The energy per symbol of MQAM is not constant. The amplitudes and phases may be different for the constellation points in MQAM. The amplitude variation will be more for higher modulation order of MQAM because number of symbols are increased with higher modulation

order. The number of symbols will also be increased in the constellation diagram when modulation order M is increased. As a result the distance between constellation points are decreased. So effect of noise is more and there is a higher possibility of data errors. So BER performance is best for 4QAM and BER performance is degraded with increasing the modulation order(M) of MQAM further. However, data rates will be higher when modulation order M is increased.

It can be seen from the graph(Fig. 3.4) that BER performance is improved when E_b/N_0 is increased for any particular modulation order of MQAM.

BER can be calculated analytically from following equation [26]

$$P_{error} = (1 - \frac{1}{\sqrt{M}})\frac{1}{\log_2(\sqrt{M})} erfc(\sqrt{\frac{3\log_2(M)E_b}{2(M-1)N_0}}) \tag{3.3}$$

If E_b/N_0 is increased for any particular modulation order of MQAM , the symbols are moved further apart. So the euclidean distance between two symbol points is increased. As a result effect of noise is less. So, BER performance is improved when E_b/N_0 is increased for any particular modulation order(M) of MQAM modulation.

3.2 Rayleigh Fading Channel with AWGN and M-ary PSK & M-ary QAM Modulation

BER performance of uncoded Rayleigh fading communication channel with AWGN noise for M-ary phase shift keying modulation scheme and M-ary quadrature amplitude modulation scheme has been discussed in this section.

3.2.1 Rayleigh Fading Channel with AWGN and M-ary PSK Modulation

BER Performance analysis of uncoded Rayleigh fading communication channel with AWGN for various modulation order(M) of MPSK has been conducted in this experiment. BPSK, QPSK, 8PSK, 16PSK and 32PSK have been considered as the modulation schemes under MPSK. MATLAB has been used for this experiment.

Uncoded message signals have been considered in this experiment which are random in nature. The uncoded message signal has been passed through MPSK modulator. After that the modulated signal has been sent through Rayleigh fading communication channel. Then additive white gaussian noise(AWGN) has been added. So, the Rayleigh faded signal has been corrupted by AWGN noise. Then it has been demodulated by MPSK demodulator at the receiver side and the demodulated signal has been compared with the original message signal to calculate bit error rate(BER). The measured BER values has been shown in Table 3.3.

E_b/N_0(dB)	BER(BPSK)	BER(QPSK)	BER(8PSK)	BER(16PSK)	BER(32PSK)
0	0.365747	0.366759	0.39063	0.407995	0.418285
1	0.349689	0.35149	0.377639	0.397076	0.409058
2	0.332522	0.334898	0.362876	0.385174	0.398904
3	0.313754	0.316907	0.346784	0.37244	0.388264
4	0.292944	0.297086	0.32961	0.358819	0.376704
5	0.270627	0.276269	0.311244	0.344129	0.364994
6	0.246461	0.253788	0.291641	0.329865	0.353675
7	0.220685	0.231014	0.271344	0.314999	0.342552
8	0.194124	0.207407	0.251495	0.300625	0.331984
9	0.166452	0.183324	0.232079	0.287254	0.322977
10	0.138501	0.159676	0.213749	0.275128	0.31549
11	0.111257	0.136714	0.197767	0.264708	0.309911
12	0.0855966	0.115041	0.184094	0.256078	0.307019
13	0.0623198	0.0952191	0.173319	0.249169	0.306198
14	0.0424921	0.0774398	0.165625	0.244108	0.307896
15	0.0266438	0.0612796	0.160075	0.240731	0.31189
16	0.0150192	0.0470282	0.156636	0.238791	0.317542
17	0.007526	0.034393	0.154158	0.237631	0.323867
18	0.00315108	0.0239521	0.152404	0.237321	0.331019
19	0.00110908	0.0153531	0.150373	0.237806	0.338025
20	0.00030275	0.00892983	0.148501	0.238988	0.344602
21	5.85e-05	0.00463158	0.146341	0.240443	0.350959
22	7.83333e-06	0.00205083	0.14383	0.242324	0.356805
23	6.66667e-07	0.000759167	0.141153	0.244295	0.362674
24	0	0.00022075	0.137821	0.246198	0.368402
25	0	4.49167e-05	0.134433	0.247751	0.373977
26	0	7.16667e-06	0.13063	0.248892	0.379265
27	0	5e-07	0.126403	0.249544	0.384294
28	0	0	0.121551	0.249848	0.388742
29	0	0	0.11642	0.249964	0.392475
30	0	0	0.110616	0.249994	0.395412

Table 3.3: BER measurement of uncoded Rayleigh fading channel with AWGN for MPSK

E_b/N_0(dB)	BER(BPSK)	BER(QPSK)	BER(8PSK)	BER(16PSK)	BER(32PSK)
31	0	0	0.104279	0.25	0.397524
32	0	0	0.0975253	0.25	0.398808
33	0	0	0.0900349	0.25	0.399514
34	0	0	0.0819885	0.25	0.399847
35	0	0	0.0733489	0.25	0.39996
36	0	0	0.0644805	0.25	0.399993
37	0	0	0.0551874	0.25	0.399999
38	0	0	0.0458781	0.25	0.4
39	0	0	0.0368565	0.25	0.4
40	0	0	0.0283424	0.25	0.4
41	0	0	0.0206236	0.25	0.4
42	0	0	0.0140318	0.25	0.4
43	0	0	0.008755	0.25	0.4
44	0	0	0.00497367	0.25	0.4
45	0	0	0.00244217	0.25	0.4
46	0	0	0.00101983	0.25	0.4
47	0	0	0.00035025	0.25	0.4
48	0	0	9.41667e-05	0.25	0.4
49	0	0	1.65833e-05	0.25	0.4
50	0	0	1.91667e-06	0.25	0.4

Table 3.3: BER measurement of uncoded Rayleigh fading channel with AWGN for MPSK

Based on simulation result a graphical representation of BER vs E_b/N_0 has been presented in Fig. 3.5.

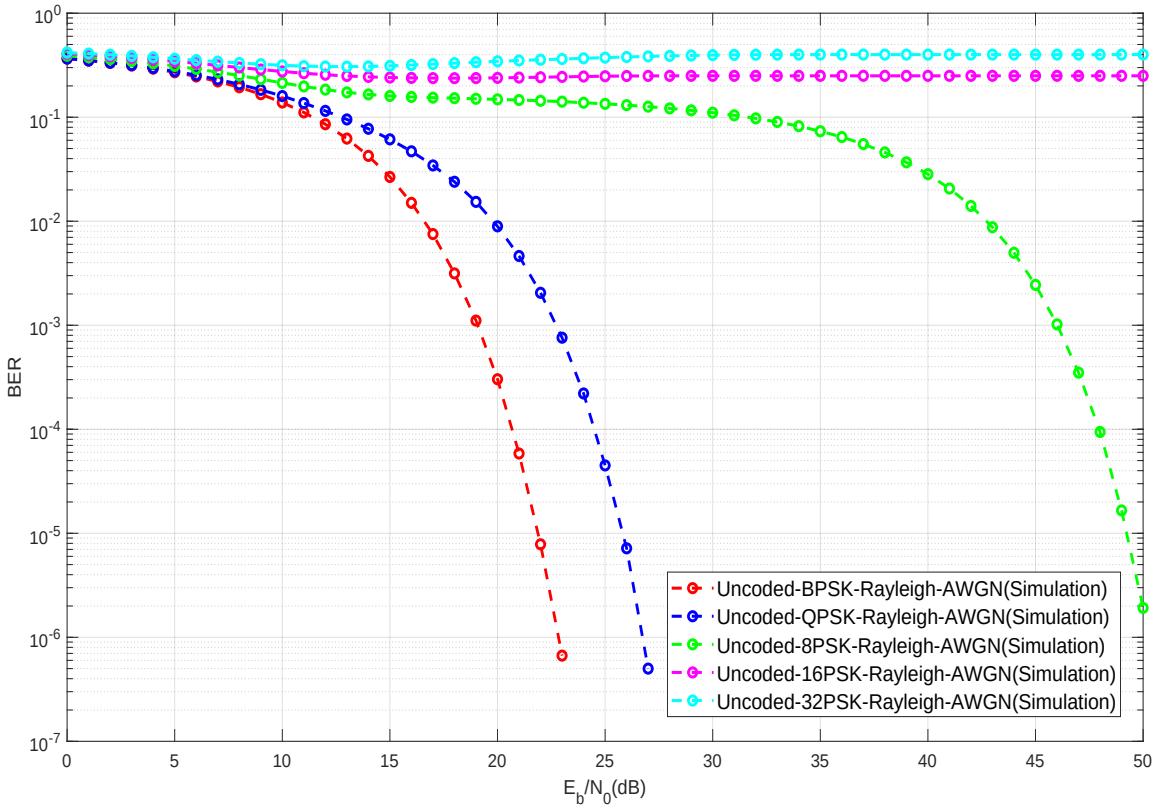

Figure 3.5: BER vs E_b/N_0 graph of uncoded Rayleigh fading channel with AWGN for MPSK

The graph(Fig. 3.5) shows how BER is changed with E_b/N_0 for various MPSK modulation schemes when uncoded Rayleigh fading communication channel is affected by AWGN noise. It can be seen in graph(Fig. 3.5) that BER performance is degraded with increasing the modulation order(M) of MPSK.

If modulation order M is increased, the number of symbols is increased. So, the symbols come closer to each other. As a result the distance between the constellation points are reduced. As a result, effect of noise will be more. So, BER performance is degraded when modulation order of MPSK modulation is increased.

It can be seen from the graphs(Fig. 3.2 and Fig. 3.5) that BER performance

of uncoded communication channel with AWGN noise is better than BER performance of uncoded Rayleigh fading communication channel with AWGN noise for any particular modulation order of MPSK.

The channel has been considered Rayleigh fading channel. There is no line-of-sight path existed between the transmitter and receiver. The path between transmitter and receiver is called non-line-of-sight path. The path between transmitter and receiver has been blocked by various obstacles like tall buildings, mountains etc. So, those obstacles reflect, refract, diffract and attenuate the signal. The signal has undergone flat fading. As a result, all frequency components of the signal experience same or equal magnitude of fading. Now, the magnitude of the signal that has passed through the Rayleigh fading communication channel is varied randomly according to the Rayleigh distribution. The probability density function(pdf) of Rayleigh distribution is shown in equation 2.13. Now, rapid amplitude fluctuation is induced in the received signal by Rayleigh fading channel and this lead to performance degradation seriously. The Rayleigh faded signal has been also corrupted by the AWGN noise in channel. As a result BER performance is degraded. So, for any particular modulation order of MPSK, BER performance of uncoded communication channel with AWGN noise is better than BER performance of uncoded Rayleigh fading communication channel with AWGN noise.

3.2.2 Rayleigh Fading Channel with AWGN and M-ary QAM Modulation

BER performance analysis of uncoded Rayleigh fading communication channel with AWGN for various orders of MQAM modulation scheme has been conducted in this experiment. The experiment has been simulated in MATLAB.

The message signals are random in nature which have been considered in this experiment. Uncoded message signal has been passed through MQAM modulator. QAM, 8QAM, 16QAM,32QAM and 64QAM have been considered as the modulation schemes under MQAM in this experiment. The MQAM modulated signal has been sent through the Rayleigh fading communication channel. AWGN noise has been considered as channel noise. So the Rayleigh faded signal has been noise corrupted in the channel. Then the noise corrupted signal has been received by MQAM demodulator at the receiver side. The MQAM demodulator has demodulated the received signal. BER has been computed by comparing original message signal with the demodulated signal. The measured BER values have been shown in Table 3.4.

E_b/N_0(dB)	BER(QAM)	BER(8QAM)	BER(16QAM)	BER(32QAM)	BER(64QAM)
0	0.366414	0.399693	0.405419	0.418598	0.432653
1	0.351511	0.39054	0.397315	0.411217	0.428605
2	0.335028	0.381839	0.389641	0.403658	0.424455
3	0.316842	0.372144	0.382155	0.396543	0.420757
4	0.297119	0.362218	0.374967	0.389961	0.417068
5	0.27645	0.351809	0.367578	0.383655	0.412962
6	0.254182	0.340372	0.359998	0.378249	0.40919
7	0.230884	0.329273	0.352301	0.373298	0.405603
8	0.207101	0.317768	0.34423	0.368579	0.402218
9	0.183184	0.306484	0.336578	0.364709	0.399303
10	0.159486	0.295952	0.329525	0.361012	0.396764
11	0.136781	0.286038	0.32287	0.357766	0.394678
12	0.115216	0.276987	0.316914	0.355003	0.392876
13	0.0953491	0.268474	0.312086	0.35247	0.391607
14	0.0773749	0.261169	0.30789	0.350514	0.390509
15	0.0612717	0.254522	0.304535	0.34886	0.389917
16	0.0469955	0.24876	0.301686	0.347438	0.389304
17	0.0344604	0.24384	0.29989	0.346153	0.388993
18	0.0239222	0.239346	0.298002	0.345123	0.388722
19	0.0153872	0.235747	0.29684	0.34444	0.388657
20	0.00899011	0.233114	0.295884	0.343826	0.388492
21	0.00466122	0.231078	0.295589	0.343226	0.388342
22	0.00204872	0.229875	0.295272	0.343063	0.388566
23	0.000772111	0.229588	0.295348	0.342922	0.388333
24	0.000221167	0.23003	0.296086	0.342957	0.388428
25	4.61111e-05	0.23101	0.296839	0.34317	0.388307
26	7e-06	0.232934	0.298277	0.343379	0.388308
27	9.44444e-07	0.23506	0.299698	0.343705	0.388448
28	0	0.237459	0.301175	0.344201	0.388448
29	0	0.239401	0.303049	0.34472	0.388386
30	0	0.241681	0.304635	0.345338	0.38829

Table 3.4: BER measurement of uncoded Rayleigh fading channel with AWGN for MQAM

E_b/N_0(dB)	BER(QAM)	BER(8QAM)	BER(16QAM)	BER(32QAM)	BER(64QAM)
31	0	0.243987	0.306341	0.346147	0.38827
32	0	0.245735	0.30797	0.34693	0.38808
33	0	0.247207	0.309379	0.347462	0.388203
34	0	0.248267	0.310325	0.348127	0.387967
35	0	0.249182	0.311228	0.348578	0.387971
36	0	0.249614	0.311876	0.349116	0.38788
37	0	0.249854	0.312103	0.349551	0.387711
38	0	0.250058	0.312291	0.349491	0.387747
39	0	0.250266	0.312373	0.349832	0.38756
40	0	0.250123	0.312536	0.349932	0.387412
41	0	0.249846	0.312454	0.350029	0.387065
42	0	0.249865	0.312422	0.349973	0.387164
43	0	0.249979	0.31239	0.350145	0.386637
44	0	0.249935	0.31256	0.349893	0.38629
45	0	0.25004	0.312401	0.350007	0.386306
46	0	0.250135	0.312401	0.350184	0.385877
47	0	0.249971	0.312397	0.350115	0.385645
48	0	0.250167	0.312364	0.350074	0.385626
49	0	0.249979	0.31249	0.349812	0.385598
50	0	0.250145	0.312409	0.349915	0.385519

Table 3.4: BER measurement of uncoded Rayleigh fading channel with AWGN for MQAM

BER vs E_b/N_0 graph has been shown in Fig. 3.6 which is based on simulation result.

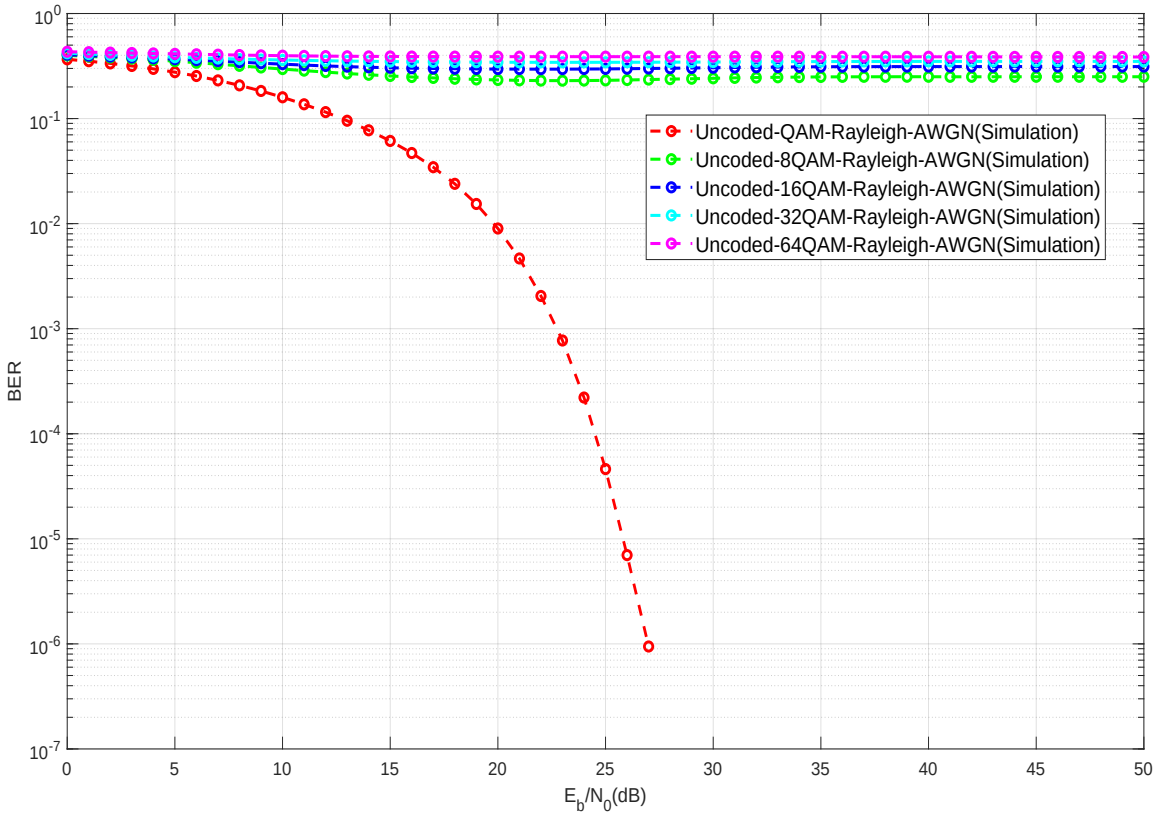

Figure 3.6: BER vs E_b/N_0 graph of uncoded Rayleigh fading channel with AWGN for MQAM

The graph(Fig. 3.6) shows how bit error rate(BER) is changed with E_b/N_0 for various orders of MQAM modulation scheme when uncoded Rayleigh fading communication channel is affected by AWGN noise. It can be seen in graph(Fig. 3.6) that BER performance is degraded with increasing the modulation order(M) of MQAM.

In MQAM modulation, the carrier experiences phase as well as amplitude modulation. The constellation diagram consists of a square lattice of symbol points for MQAM. The energy per symbol of MQAM is not constant. The number of symbols is increased when modulation order of MQAM is increased. So, the amplitude variation will be more for higher order modulation. Also, the distances between constellation points are decreased when modulation order of MQAM is increased. So

there is a higher possibility of data errors. As a result, if modulation order of MQAM is increased, BER performance is degraded.

It can also be seen from the graphs(Fig. 3.4 and Fig. 3.6) that BER performance of uncoded communication channel with AWGN noise is better than BER performance of uncoded Rayleigh fading communication channel with AWGN noise for any particular modulation order of MQAM.

Rayleigh fading channel has been considered. Here non-line-of-sight path has been considered in this experiment. The path between transmitter and receiver has been blocked by various obstacles and those obstacles reflect, refract, diffract and attenuate the signal. The signal has undergone flat fading. As a result, all frequency components of the signal experience same or equal magnitude of fading. Now, the magnitude of the signal that has passed through the Rayleigh fading communication channel is varied randomly according to the Rayleigh distribution. The probability density function(pdf) of Rayleigh distribution is shown in equation 2.13. Rapid amplitude fluctuation is induced in the received signal by the Rayleigh fading channel and as a result huge performance degradation occurs. The Rayleigh faded signal has been also corrupted by the AWGN noise in the channel. So, BER performance is degraded. As a result, BER performance of uncoded communication channel with AWGN noise is better than BER performance of uncoded Rayleigh fading communication channel with AWGN noise for any particular modulation order of MQAM modulation.

3.3 Conclusion

BER performance analysis of uncoded communication channel has been done in this chapter. The channel has been considered here is wireless. First AWGN noise has been considered as channel noise and BER performance analysis has been done for MPSK and MQAM. Then Rayleigh fading along with AWGN noise has been considered and BER performance analysis has been done for MPSK and MQAM modulation. Now, it can be seen from the experimental results that BER performance is degraded when modulation order(M) of MPSK or MQAM is increased. It can also be seen that BER performance is improved when E_b/N_0 is increased for any particular modulation order of MPSK or MQAM. Now, it can be seen from the experimental results that BER performance of uncoded communication channel with AWGN noise is better than BER performance of uncoded Rayleigh fading communication channel with AWGN noise for any particular modulation order of MPSK or MQAM. Now, error control coding can be considered and it will be interesting to see how the channel coding techniques will impact to the BER performance of communication channel.

Chapter 4

BER Performance of Coded Communication Channel

In this chapter, error correcting codes have been considered to improve the reliability of message signal. The error correcting codes which have been used in the experiments shown in this chapter are RS(255,239) code, (7,1/2) convolutional code and DVB-S.2 standard rate=1/2 LDPC code. The channel which has been considered is wireless. BER performance analysis of coded communication channel with AWGN noise for MPSK and MQAM has been done. Next Rayleigh fading has been considered and AWGN noise also added. Then considering both Rayleigh fading and AWGN noise, BER performance analysis of coded communication channel has been done for MPSK and MQAM modulation techniques.

4.1 AWGN Channel with Channel Coding and Modulation Schemes(M-ary PSK and M-ary QAM Modulation)

In this section, BER performance of coded communication channel with AWGN noise for M-ary phase shift keying(MPSK) and M-ary quadrature amplitude modulation(MQAM) has been discussed.

4.1.1 AWGN Channel with RS(255,239) Channel Coding and M-ary PSK Modulation

BER performance analysis of RS(255,239) coded communication channel with AWGN noise for M-ary phase shift keying(MPSK) modulation has been done. Here RS(255,239) code has been used as error correcting code in this experiment. RS(255,239) takes 239 symbols as input and gives codeword block length of 255 symbols. This RS(255,239) code can correct upto

$$t = \frac{(255 - 239)}{2} = 8 \quad \text{symbols error.}$$

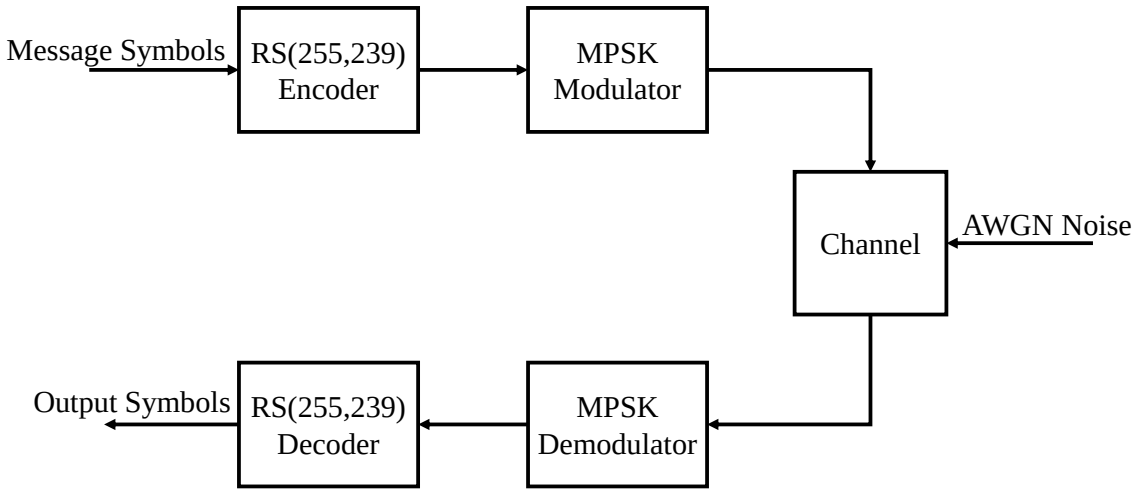

Figure 4.1: Block diagram of RS(255,239) coded AWGN channel for MPSK

Information symbols which have been considered as input message symbols in this experiment are random in nature. The channel encoder maps each 239 information symbols into 255 symbols length codeword. The codeword has been passed through MPSK modulator. Here BPSK, QPSK, 8PSK, 16PSK and 32PSK are the modulation schemes which have been considered under MPSK. The MPSK modulator maps the information sequence into signal waveform. Now the modulated signal has been sent through communication channel. The communication channel has been affected by additive white gaussian noise(AWGN). So the modulated signal has been affected by AWGN noise. After that the noise corrupted signal waveform has been demodulated by MPSK demodulator. Then the RS decoder has received the demodulated symbols and decoded it. The decoder has corrected some errors from the received symbols. Now comparison has been done between the original message bits and decoded information bits and BER has been computed. The measured BER values in this experiment have been shown in Table 4.1.

E_b/N_0(dB)	BER(BPSK)	BER(QPSK)	BER(8PSK)	BER(16PSK)	BER(32PSK)
0	0.0855748	0.0856548	0.129094	0.18043	0.229471
1	0.0622547	0.0621297	0.106566	0.15894	0.211827
2	0.0422286	0.0425628	0.0859895	0.139328	0.193532
3	0.0265528	0.026773	0.0673488	0.12076	0.176406
4	0.015147	0.0150267	0.050126	0.10356	0.158722
5	0.00729969	0.00729341	0.0356145	0.0871496	0.141401
6	0.000979079	0.000968619	0.023443	0.0725717	0.125338
7	2.16953e-06	2.41893e-06	0.0140471	0.0582918	0.109698
8	0	0	0.00743149	0.0448248	0.0953447
9	0	0	0.00121496	0.0329759	0.0817986
10	0	0	7.91056e-06	0.0227756	0.0694419
11	0	0	0	0.0144587	0.0575162
12	0	0	0	0.00823222	0.0464932
13	0	0	0	0.00272908	0.035954
14	0	0	0	9.67573e-05	0.0266287
15	0	0	0	0	0.0184372
16	0	0	0	0	0.0116841
17	0	0	0	0	0.00638128
18	0	0	0	0	0.00127772
19	0	0	0	0	1.84362e-05
20	0	0	0	0	0

Table 4.1: BER measurement of RS(255,239) coded communication channel with AWGN for MPSK

Based on simulation result, a graphical representation of BER vs E_b/N_0 has been presented in Fig. 4.2.

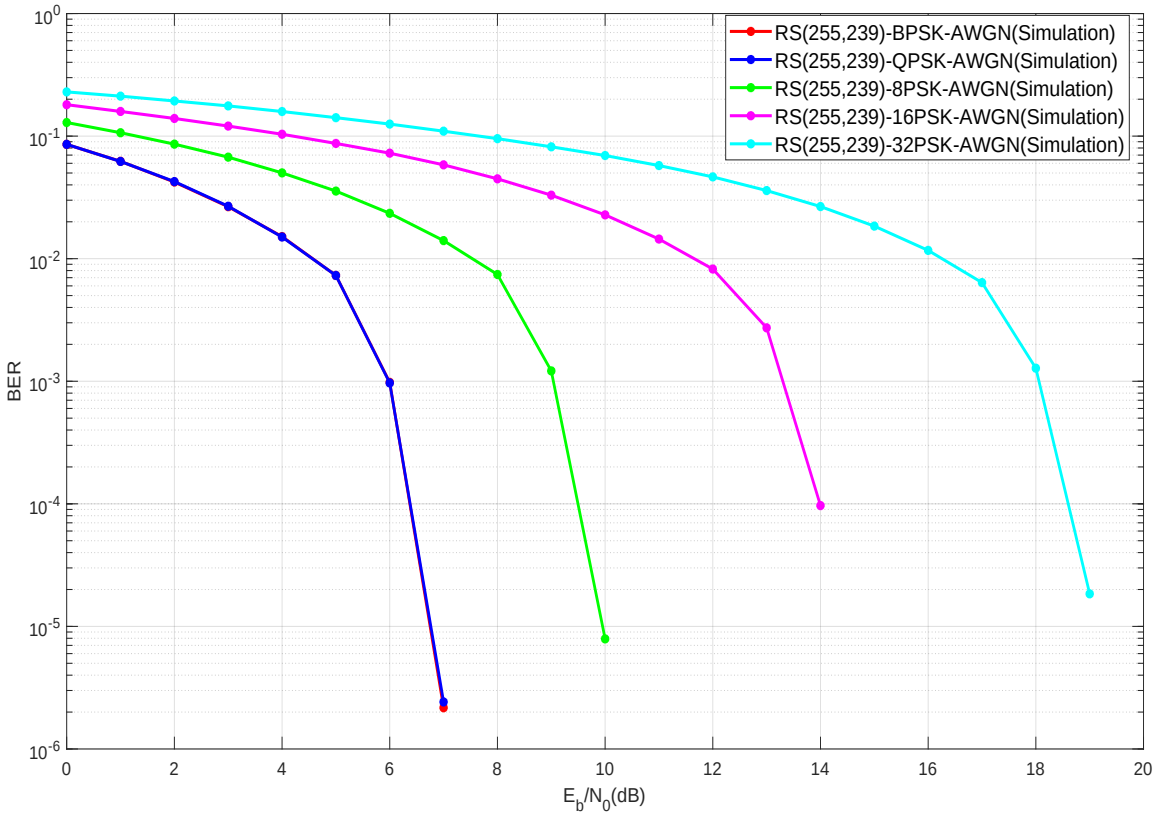

Figure 4.2: BER vs E_b/N_0 graph for RS(255,239) coded communication channel with AWGN for MPSK

The graph(Fig. 4.2) shows how bit error rate(BER) is changed with E_b/N_0 for various modulation order of MPSK when RS(255,239) channel coding technique is used. The graph(Fig. 4.2) shows that BER performance of RS(255,239) coded BPSK and QPSK modulated channels are similar and BER performance is degraded when modulation order of MPSK is increased further.

Now if basis functions of BPSK and QPSK are compared, it can be seen that QPSK can be considered as two independent BPSK signals. They can be demodulated independently also. So BER performance of the case BPSK and BER performance of the case QPSK are same here. Now, the number of symbols is increased when

modulation order is increased. So the distance between two adjacent symbols in the constellation diagram is reduced. As a result, the effect of noise is more. So, BER performance is degraded when modulation order is increased.

It can be seen from graph(Fig. 4.2) that BER performance at lower value of E_b/N_0 is not good and after a certain value of E_b/N_0 the BER performance of RS(255,239) coded channel is improved very much compare to uncoded BER performance.

BER performance at lower value of E_b/N_0 is not good because random errors have been introduced by AWGN. Now, each symbol is 8 bits for RS(255,239) code. RS(255,239) code can correct errors in any eight symbols in the block of 255 symbols. If there is a burst error which affects 62 bits then the burst error corrupts 8 symbols. Now RS(255,239) decoder replaces the incorrect symbols with correct symbols. RS(255,239) decoder replaces one incorrect symbol with correct symbol whether one bit or all eight bits in a symbol are corrupted. So, RS(255,239) code performs very well against burst noise. So BER performance is improved very much. Now, if E_b/N_0 is increased ,the message points corresponding to symbols are moved further apart and the distance between constellation points are increased. So for the described reasons, BER performance is improved when E_b/N_0 is increased for any particular modulation order of MPSK and BER performance of RS(255,239) coded channel is better than uncoded BER performance.

4.1.2 AWGN Channel with RS(255,239) Channel Coding and M-ary QAM Modulation

BER performance analysis of RS(255,239) coded communication channel has been conducted in this experiment. Where M-ary quadrature amplitude modulation(MQAM) has been considered as Modulation scheme and Additive white gaussian noise(AWGN) channel has been considered. MATLAB has been used for this experiment.

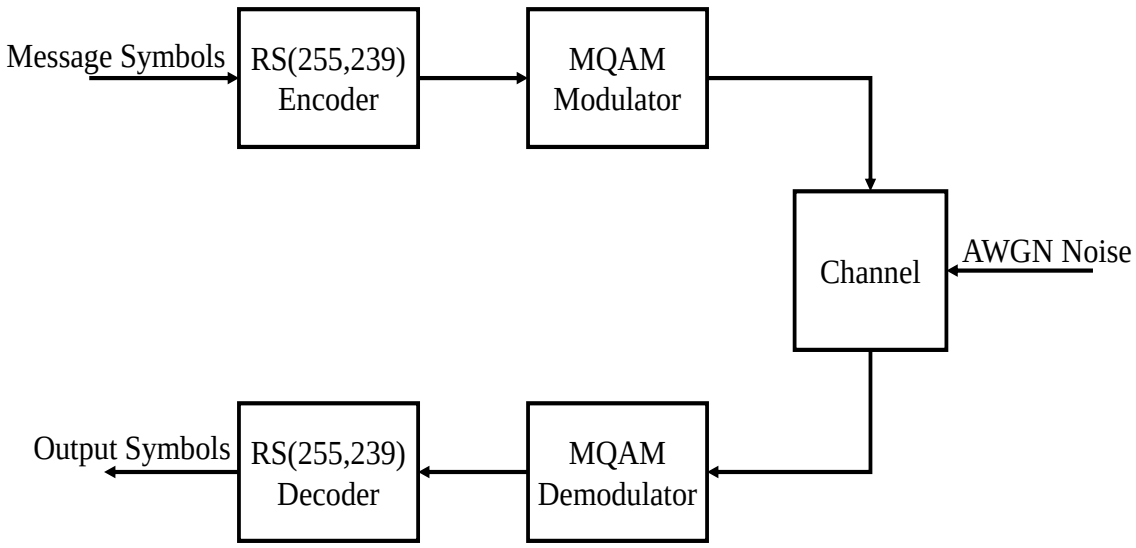

Figure 4.3: Block diagram of RS(255,239) coded AWGN channel for MQAM

The message symbols which have been considered in this experiment are random in nature. The channel encoder encodes 239 symbols length message into 255 symbols length codeword. The codeword has been passed through MQAM modulator. 4QAM, 8QAM, 16QAM, 32QAM and 64QAM have been considered as the modulation schemes under MQAM modulation. Then the modulated signal has been sent through AWGN channel. Here the AWGN noise affects the incoming signal. At the receiver side, the noise affected signal has been received MQAM demodulator. The demodulator has demodulated the received signal. The demodulated signal has been passed through RS(255,239) decoder. Some errors have been corrected by

RS(255,239) decoder. Then comparison has been done between original message bits and decoded bits. BER has been computed. The measured BER values have been shown in Table 4.2.

E_b/N_0(dB)	BER(QAM)	BER(8QAM)	BER(16QAM)	BER(32QAM)	BER(64QAM)
0	0.0857322	0.139937	0.147369	0.185926	0.207667
1	0.0614017	0.11534	0.125633	0.165	0.184069
2	0.0425994	0.0938075	0.10512	0.143007	0.163619
3	0.0261454	0.0716161	0.083886	0.122416	0.140853
4	0.0150785	0.0515952	0.0644665	0.102035	0.124059
5	0.00707113	0.0361454	0.0466527	0.0829969	0.104942
6	0.000925732	0.0217939	0.0320293	0.0641632	0.0883054
7	1.95411e-06	0.0125785	0.0194822	0.0458421	0.0718253
8	0	0.00605649	0.0114278	0.0316423	0.0565429
9	0	0.000381799	0.00514121	0.0199686	0.0428138
10	0	6.38794e-07	0.000195258	0.0116946	0.029749
11	0	0	6.18832e-07	0.00438808	0.0194404
12	0	0	0	0.000353033	0.0112448
13	0	0	0	2.69491e-07	0.00530335
14	0	0	0	0	0.000530858
15	0	0	0	0	3.24075e-06
16	0	0	0	0	0

Table 4.2: BER measurement of RS(255,239) coded AWGN channel for MQAM

In Fig. 4.4, BER vs E_b/N_0 graph has been shown based on simulation result.

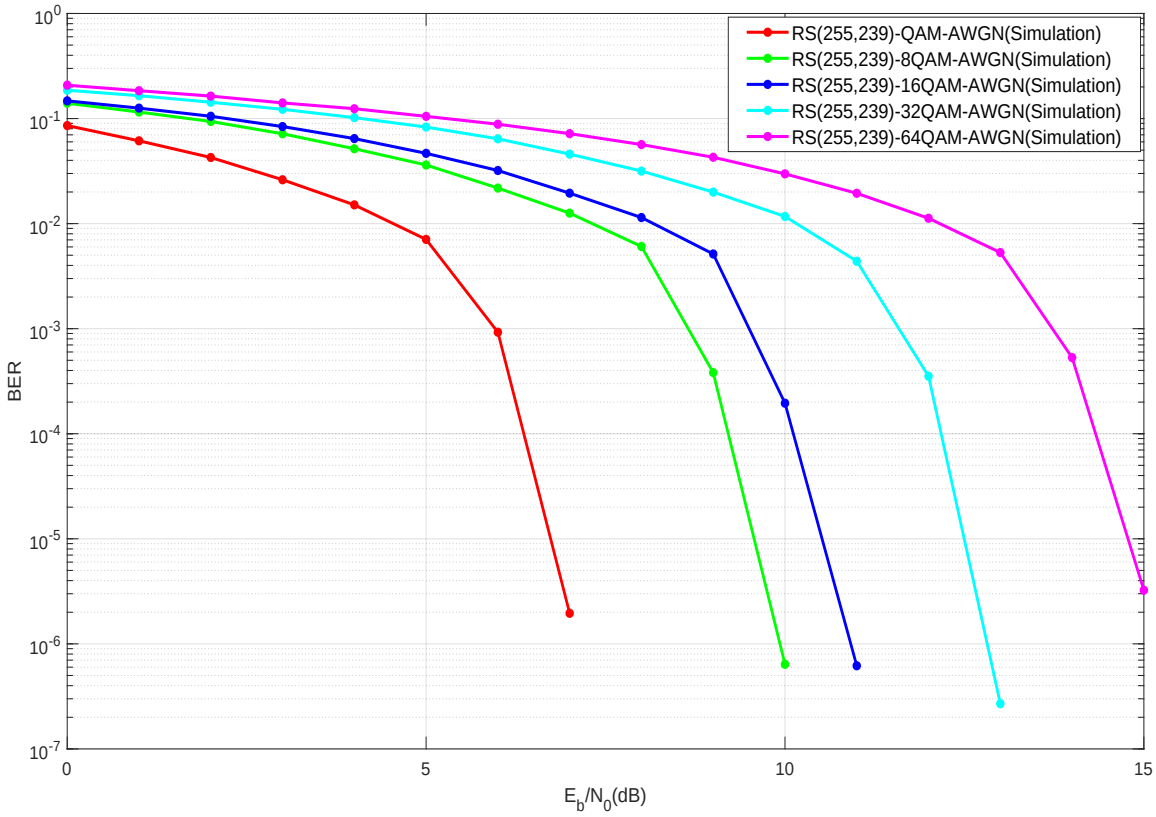

Figure 4.4: BER vs E_b/N_0 graph of RS(255,239) coded AWGN channel for MQAM

The graph(Fig 4.4) shows how BER is changed with E_b/N_0 for various MQAM when RS(255,239) channel coding is used and the communication channel is affected by AWGN noise. It can also be seen from the graph(Fig 4.4) that BER performance is degraded with increasing the modulation order of MQAM.

Both phase and amplitude of carrier signal are modulated in MQAM. So amplitude and phase both are varied for various constellation points in MQAM modulation. The constellation points are situated in a square lattice structure in constellation diagram. If modulation order M is increased, the number of symbols is increased in constellation diagram. As a result the distances between them are decreased and there is higher possibility of data errors. So, in RS(255,239) coded channel, BER performance is degraded when modulation order(M) of MQAM is increased.

It can be seen from the graph(Fig 4.4) that BER performance is improved when E_b/N_0 is increased for any particular modulation order of MQAM.

At lower value of E_b/N_0, BER performance is not improved because random errors are introduced by AWGN. Now, let E_b/N_0 is increased for any particular modulation order of MQAM. Then the symbols are moved further apart. So the distance between constellation points are increased. As a result BER is improved. So BER is improved when E_b/N_0 is increased for any particular modulation order.

It can be seen from the graphs(Fig. 4.4 and Fig. 3.4) that the BER performance of RS(255,239) coded channel is improved very much compare to uncoded one after a certain value of E_b/N_0 for any particular value of modulation order of MQAM.

There are 8 bits in each symbol for RS(255,239) code. RS(255,239) code can correct errors in any eight symbols in the block of 255 symbols. Assume there exists a burst of noise. The burst noise lasts for duration 60 bits. So, 8 symbols are affected by the burst noise. RS(255,239) code performs very well against burst noise. RS(255,239) decoder replaces one incorrect symbol with correct symbol whether one bit or all eight bits in a symbol are corrupted. RS(255,239) decoder replaces the incorrect symbols with correct symbols. So, BER performance is improved very much for the case of RS(255,239) code.

4.1.3 AWGN Channel with (7,1/2) Convolutional Channel Coding and M-ary PSK Modulation

BER performance of (7,1/2) convolutional coded communication channel with AWGN noise for M-ary phase shift keying(MPSK) has been discussed.

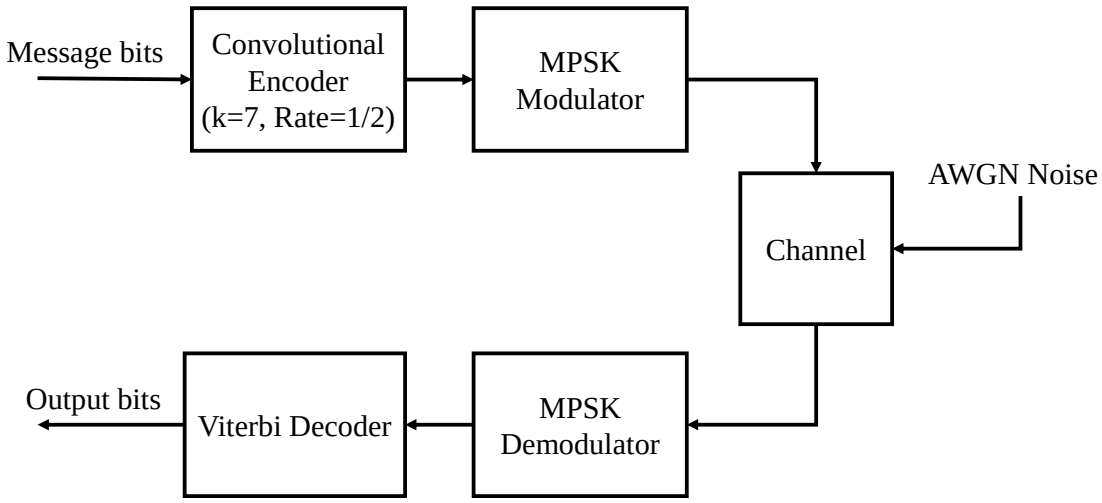

Figure 4.5: Block diagram of (7,1/2) convolutional coded AWGN channel for MPSK

$(7, 1/2)$ convolutional code has been used in this experiment. The constraint length of this code is K=7 and the rate of this code is $R = 1/2$. BER performance analysis of $(7, 1/2)$ convolutional coded communication channel has been conducted. M-ary phase shift keying(MPSK) is the modulation scheme that has been considered. Additive white gaussian noise(AWGN) has been considered as the channel noise. MATLAB has been used for this experiment.

Let an infinite bitstream has come to the encoder. The convolutional encoder has $rate = 1/2$ i.e for every one bit of input the encoder gives two bits output. The generator of the encoder can be represented by $g = [g_1, g_2] = [1111001, 1011011]$. The ones in g_1 basically represent the position of the shift registers which are connected to modulo-2 adder to produce first output bit. Similarly, The ones in g_2 basically represent the position of the shift registers which are connected to modulo-2 adder

to produce second output bit. Now encoded signal has been passed through MPSK modulator. Here modulation schemes which have been considered under MPSK are BPSK, QPSK, 8PSK, 16PSK and 32PSK. The MPSK modulator maps the information sequence into signal waveform. Now the modulated signal has been passed through communication channel. The channel which has been considered in the experiment is wireless. AWGN noise has been added to the signal in the channel. So the passed signal has been affected by noise. Then the MPSK demodulator has received the noise corrupted signal waveform and demodulated it. The demodulated data has been sent to hard decision based Viterbi decoder. The Viterbi decoder has corrected some errors from the received bits. Now the decoded information bits have been compared with the original message bits to find bit error rate(BER). The measured BER values have been shown in Table 4.3.

Eb/N0(dB)	BER(BPSK)	BER(QPSK)	BER(8PSK)	BER(16PSK)	BER(32PSK)
0	0.374671	0.372508	0.468384	0.494568	0.49892
1	0.257691	0.256463	0.425651	0.488321	0.49934
2	0.120909	0.120451	0.349999	0.475761	0.496384
3	0.0339128	0.0352162	0.230737	0.448219	0.492837
4	0.00590614	0.00586547	0.103176	0.392951	0.487133
5	0.000518679	0.000616681	0.0316734	0.305164	0.473965
6	2.80002e-05	3.43337e-05	0.00627615	0.187963	0.450967
7	2.19048e-06	2.76191e-06	0.000777351	0.0884707	0.405375
8	0	0	0.000118003	0.0297547	0.32982
9	0	0	8.85717e-06	0.00752151	0.229591
10	0	0	2.85715e-07	0.00138737	0.127778
11	0	0	0	0.000218005	0.0556173
12	0	0	0	3.35558e-05	0.0188031
13	0	0	0	6.57145e-06	0.00495878
14	0	0	0	5.7143e-07	0.0012367
15	0	0	0	0	0.000238672
16	0	0	0	0	3.70004e-05
17	0	0	0	0	1.18889e-05
18	0	0	0	0	1.33334e-06
19	0	0	0	0	0

Table 4.3: BER measurement of $(7, 1/2)$ convolutional coded AWGN channel for MPSK

A graphical representation of BER vs E_b/N_0 has been shown in Fig. 4.6 which is based on simulation result.

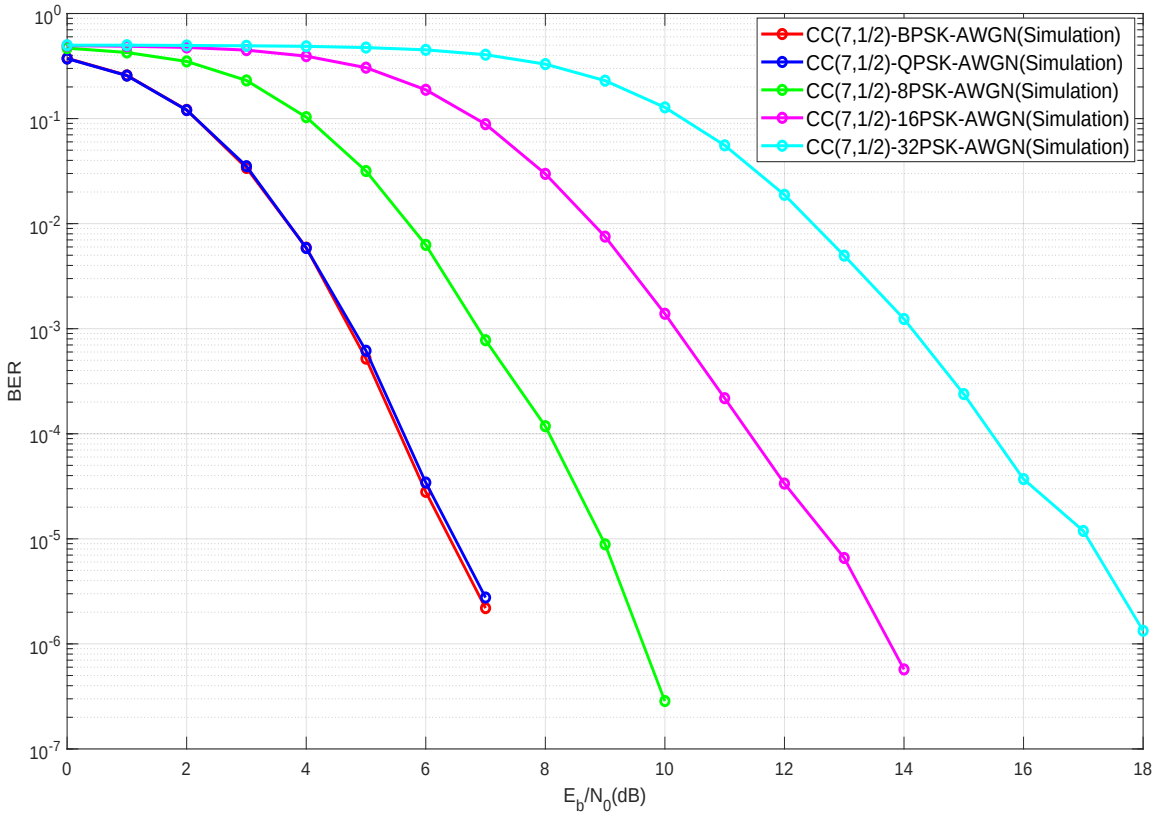

Figure 4.6: BER vs E_b/N_0 graph of $(7, 1/2)$ convolutional coded AWGN channel for MPSK

The graph (Fig. 4.6) shows how BER is changed with E_b/N_0 for various MPSK when $(7, 1/2)$ convolutional channel coding is used and the channel is affected by AWGN. It can be seen from graph (Fig. 4.6) that BER performance of $(7, 1/2)$ convolutional coded channel is similar for BPSK and QPSK modulation. The BER performance is degraded as modulation order M of MPSK modulation is increased further.

It is known that QPSK can considered as two independent BPSK signals. They can be demodulated independently also. As a result, BER performance is similar for BPSK and QPSK modulation. Now, the number of symbols are increased for higher order modulation. The symbols are situated in a circle for MPSK. So, if

modulation order M of MPSK is increased, the distances between constellation points are decreased. As a result, there is higher chance of data errors. So BER performance of $(7, 1/2)$ convolutional coded channel with AWGN is degraded if modulation order of MPSK is increased.

Now it can be seen from the graph (Fig. 4.6) that BER performance of $(7, 1/2)$ convolutional coded channel at low value of E_b/N_0 for any particular modulation order is worse than uncoded BER performance(uncoded BER performance has been shown in Fig. 3.2) and if E_b/N_0 is increased, the BER performance of $(7, 1/2)$ convolutional coded channel is far better than uncoded one after a certain E_b/N_0.

Bit error probability for the considered convolutional code is bounded as shown in following equation[30]

$$P_b \leq \frac{1}{b} \sum_{d=0}^{\infty} \omega_d P_e(d) \tag{4.1}$$

Where d is the number of bit positions differing in any two code sequences in the trellis. d is called the Hamming distance here.

$P_e(d)$ is the probability of confusing two code sequences which are differing in d positions.

ω_d is the weight spectrum of the code and it represents the average number of bit errors associated with the sequences which have weight d.

ω_d is zero when $d \leq d_{free}$

Now the minimal Hamming distance between different encoded sequences is called free distance which is represented by d_{free}. Now the union bounds become loose at low value of SNR E_b/N_0 and become tight when SNR E_b/N_0 is increased. For high value of SNR, the lowest order term is the dominating term in bit error probability. In the lowest order dominating term d is equal to d_{free} i.e $d = d_{free}$. The $(7, 1/2)$ convolutional code is able to achieve free distance $d_{free} = 10$. Maximization of free distance is an important thing to improve BER performance. The bit error rate falls of exponentially with d_{free} at low error rates when maximum likelihood(ML) decoding is used. Now, if E_b/N_0 is increased the symbol points are also moved further. So the distances between constellation points are also increased. So, here BER performance is improved when E_b/N_0 is increased for any particular modulation order and also better than uncoded channel.

4.1.4 AWGN Channel with (7,1/2) Convolutional Channel Coding and M-ary QAM Modulation

BER performance of (7,1/2) convolutional coded communication channel with AWGN noise for M-ary quadrature amplitude modulation has been discussed.

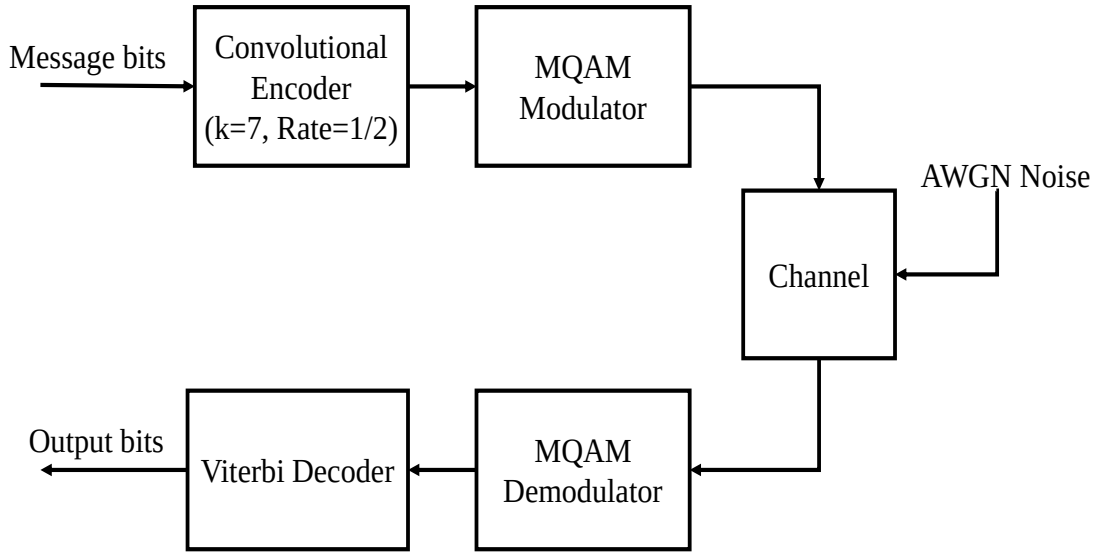

Figure 4.7: Block diagram of (7,1/2) convolutional coded AWGN channel for MQAM

In this experiment, $(7, 1/2)$ convolutional code has been used. The convolutional code has constraint length K=7 and the rate of this code is $R = 1/2$. BER performance analysis of $(7, 1/2)$ convolutional coded communication channel has been conducted. M-ary quadrature amplitude modulation(MQAM) schemes : 4QAM, 8QAM, 16QAM, 32QAM and 64QAM have been considered. Additive white gaussian noise(AWGN) has been considered as the channel noise. The experiment has been simulated in MATLAB.

Now consider an infinite bitstream comes to the encoder. The convolutional encoder has $rate = 1/2$. So, for every one bit of input the encoder gives two bits output. The generator of the (7,1/2) convolutional encoder is represented by $g = [g_1, g_2] = [1111001, 1011011]$. The ones in g_1 basically represent the positions

of the shift registers which are connected to modulo-2 adder to produce first output bit. Similarly, The ones in g_2 basically represent the positions of the shift registers which are connected to modulo-2 adder to produce second output bit. Now, convolutional encoder encoded signal has been passed through MQAM modulator. Then the modulated signal has been sent through communication channel. The channel has been affected by AWGN. The noise affected signal has been received by MQAM demodulator and demodulated by the demodulator. The demodulated data has been passed through hard decision based Viterbi decoder. Some errors have been corrected by the Viterbi decoder. Then the decoded bits have been compared with the original message bits and BER has been calculated. The measured BER values have been shown in Table 4.4.

E_b/N_0(dB)	BER(QAM)	BER(8QAM)	BER(16QAM)	BER(32QAM)	BER(64QAM)
0	0.375495	0.474956	0.481461	0.492763	0.496957
1	0.257459	0.443525	0.46016	0.486579	0.494816
2	0.121097	0.382943	0.415325	0.470128	0.487709
3	0.0338428	0.277546	0.3302	0.43942	0.477012
4	0.00588947	0.147733	0.210132	0.384379	0.452983
5	0.000514679	0.0530092	0.0957276	0.296667	0.407435
6	3.50004e-05	0.0113423	0.0285653	0.188943	0.323403
7	1.90477e-06	0.00177604	0.00582347	0.0938735	0.210508
8	0	0.000181338	0.000810019	0.0348041	0.103474
9	0	1.38889e-05	0.000110669	0.00978023	0.0370195
10	0	4.76192e-07	5.7143e-06	0.00221338	0.00958422
11	0	0	0	0.000444677	0.00179338
12	0	0	0	5.96674e-05	0.000266006
13	0	0	0	1.34667e-05	3.20002e-05
14	0	0	0	1.14286e-06	4.76192e-06
15	0	0	0	0	3.80954e-07
16	0	0	0	0	0

Table 4.4: BER measurement of $(7, 1/2)$ convolutional coded AWGN channel for MQAM

Based on simulation result, a graphical representation of BER vs E_b/N_0 has been shown in Fig. 4.8.

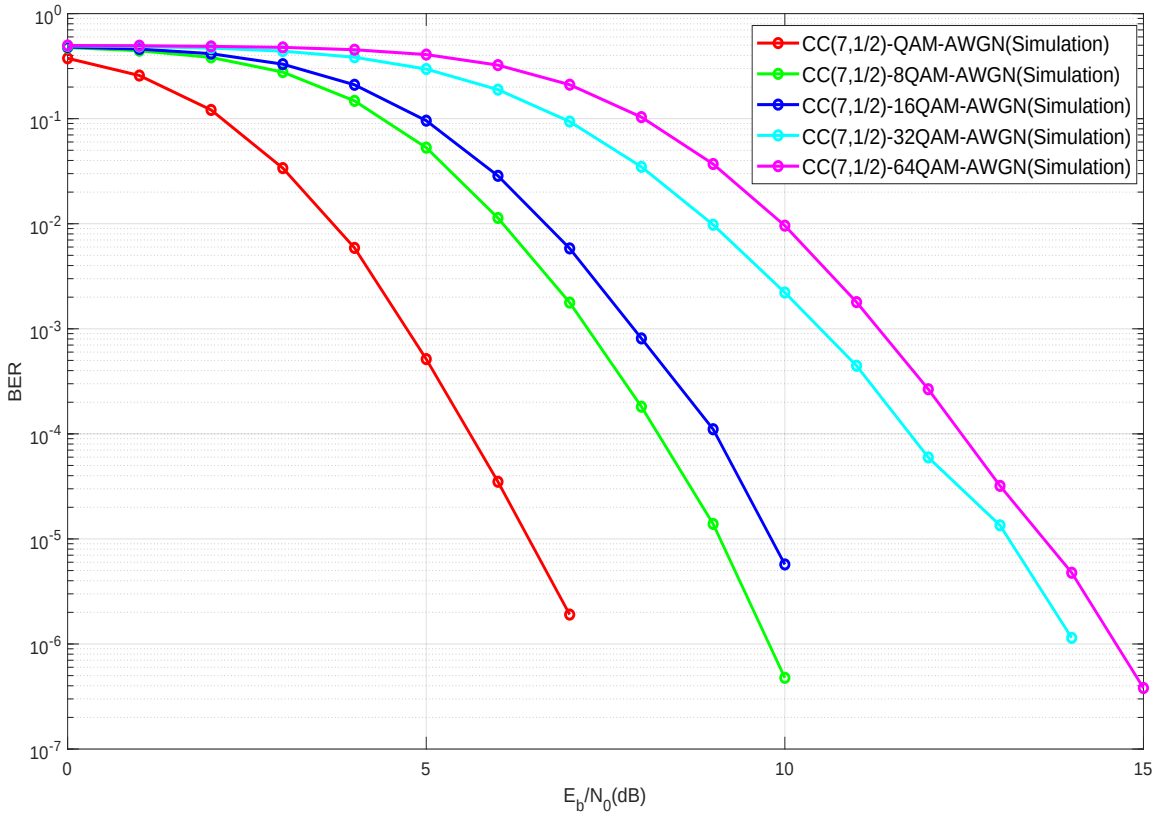

Figure 4.8: BER vs E_b/N_0 graph of $(7, 1/2)$ convolutional coded AWGN channel for MQAM

The graph (Fig. 4.8) shows how BER is changed with E_b/N_0 for various MQAM when $(7, 1/2)$ convolutional channel coding is used and the channel is affected by AWGN. It can be seen from the graph (Fig. 4.8) that BER performance is degraded when modulation order M of MQAM is increased.

The constellation points are situated in square grid in MQAM modulation. Now the number of symbols is increased in constellation diagram when modulation order of MQAM is increased. As a result, the distance between two constellation points is decreased. The amplitude variation will also be more for higher order modulation. So the possibility of data errors is more. So, BER performance is best for 4QAM and BER performance is degraded with increasing the modulation order further.

Now, it can be seen from the graphs (Fig. 4.8 and Fig. 3.4) that BER performance of $(7, 1/2)$ convolutional coded channel at low value of E_b/N_0 for any particular modulation order is worse than uncoded BER performance and if E_b/N_0 is increased the BER performance of $(7, 1/2)$ convolutional coded channel is far better than uncoded one after a certain E_b/N_0.

For the convolutional code, bit error probability can be bounded as shown in equation 4.1. Now the union bounds become loose at low value of SNR E_b/N_0 and become tight when SNR E_b/N_0 is increased. For high value of SNR, the the lowest order term is the dominating term in bit error probability. In the lowest order dominating term d can be described as $d = d_{free}$. The $(7, 1/2)$ convolutional code is able to achieve free distance $d_{free} = 10$. Maximization of free distance is an important thing to improve BER performance. The bit error rate falls of exponentially with d_{free} at low error rates when maximum likelihood(ML) decoding is used. The symbol points are also moved further when E_b/N_0 is increased. So the distance between constellation points is also increased. So, if E_b/N_0 is increased for any particular modulation order of MQAM, BER is improved here.

4.1.5 AWGN Channel with DVB-S.2 Standard Rate 1/2 LDPC Channel Coding and M-ary PSK Modulation

BER performance of DVB-S.2 standard Rate 1/2 LDPC Coded communication channel with AWGN noise for M-ary phase shift keying(MPSK) has been discussed.

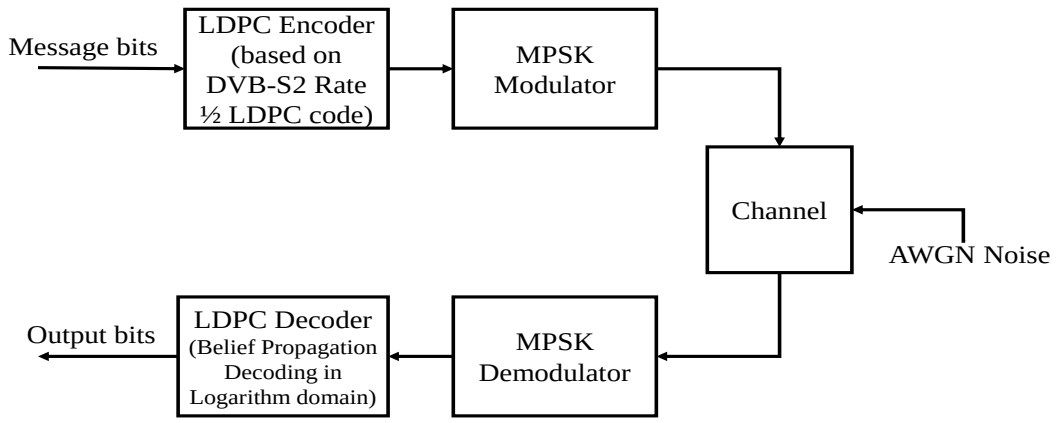

Figure 4.9: Block diagram of DVB-S.2 standard Rate=1/2 LDPC coded AWGN channel for MPSK

Here DVB-S.2 $rate = 1/2$ LDPC code has been used in this experiment. The information block length is 32400 bits and the codeword block length is 64800 bits. BER performance analysis of DVB-S.2 standard Rate 1/2 LDPC coded communication channel has been conducted. M-ary phase shift keying(MPSK) has been considered as Modulation scheme. Additive white gaussian noise(AWGN) has been considered as channel noise here. MATLAB has been used for this experiment.

The information block of length 32400 bits has been passed through LDPC encoder based on DVB-S.2 standard Rate 1/2 LDPC Code and the encoder has encoded the information block into 64800 bits block length codeword. Then the encoded signal has been passed through MPSK modulator. BPSK, QPSK, 8PSK, 16PSK and 32PSK are the modulation schemes which have been considered under MPSK modulation. The modulated signal has been sent through the communication channel. The channel has been affected by AWGN noise. Then noise corrupted signal has been received by MPSK demodulator and the demodulator has demodulated it. The demodulated

signal has been passed through LDPC decoder based on belief propagation algorithm in logarithm domain. The decoder has corrected some errors. Then BER is calculated by comparing decoded bits with the original message bits. The measured BER values have been shown in Table 4.5.

E_b/N_0(dB)	BER(BPSK)	BER(QPSK)	BER(8PSK)	BER(16PSK)	BER(32PSK)
0	0.132901	0.13392	0.191574	0.238642	0.276481
0.4	0.0930247	0.102315	0.17466	0.23179	0.270617
0.8	0.00167901	0.00186265	0.160463	0.216235	0.262037
1.2	0	0	0.141914	0.206111	0.254012
1.6	0	0	0.121944	0.193981	0.245895
2	0	0	0.10284	0.184475	0.237809
2.4	0	0	1.49972e-07	0.172562	0.233086
2.8	0	0	0	0.161142	0.217932
3.2	0	0	0	0.144167	0.213673
3.6	0	0	0	0.132284	0.20463
4	0	0	0	0.114198	0.190556
4.4	0	0	0	0.0173148	0.183981
4.8	0	0	0	0	0.170895
5.2	0	0	0	0	0.159568
5.6	0	0	0	0	0.150586
6	0	0	0	0	0.13216
6.4	0	0	0	0	0.119136
6.8	0	0	0	0	0.0977778
7.2	0	0	0	0	0.0036301
7.6	0	0	0	0	0
8	0	0	0	0	0

Table 4.5: BER measurement of DVB-S.2 standard Rate=1/2 LDPC coded AWGN channel for MPSK

A graphical representation of BER vs E_b/N_0 has been shown in Fig. 4.10 which is based on simulation result.

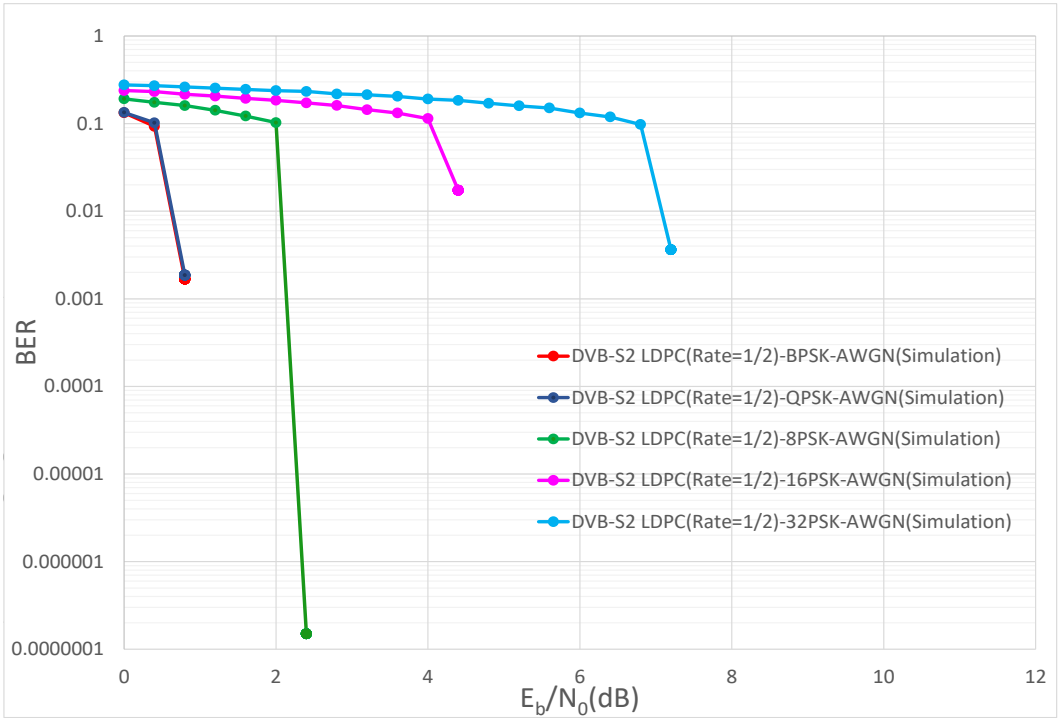

Figure 4.10: BER vs E_b/N_0 graph of DVB-S.2 standard Rate=1/2 LDPC coded AWGN channel for MPSK

The graph(Fig. 4.10) shows how bit error rate(BER) is changed with E_b/N_0 for various MPSK when DVB-S.2 standard Rate 1/2 LDPC channel coding is used and the channel is affected by AWGN. It can be seen from graph(Fig. 4.10) that BER performance of DVB-S.2 standard Rate 1/2 LDPC coded channel is similar for BPSK and QPSK modulation. The BER performance is degraded as modulation order M of MPSK modulation is increased further.

Now, QPSK can considered as two independent BPSK signals. They can be demodulated independently also. As a result, BER performance is similar for BPSK and QPSK modulation. Now, the number of symbols are increased for higher order modulation. The symbols are situated in a circle for MPSK. So, if modulation order

M of MPSK is increased the distance between constellation points are decreased. So there is higher chance of data errors. So BER performance of DVB-S.2 standard Rate 1/2 LDPC coded channel with AWGN is degraded if modulation order of MPSK is increased.

The graph(Fig. 4.10) shows BER performance of DVB-S.2 $rate = 1/2$ LDPC coded channel is improved as E_b/N_0 is increased for any particular modulation order of MPSK. The BER performance is far better than BER performance of uncoded channel after a certain E_b/N_0 and high coding gain can be achieved. So BER performance of DVB-S.2 $rate = 1/2$ LDPC coded channel is far better than uncoded channel(BER performance of uncoded communication channel with AWGN for MPSK has been shown in Fig. 3.2).

Now if E_b/N_0 is increased, the message points corresponding to symbols are moved further apart. So if E_b/N_0 is increased the distance between constellation points are increased.

Now, the block length of codeword of DVB-S.2 $rate = 1/2$ LDPC code is 64800. The number of low weight codewords are very small. So, There are small number of codewords which are undesirably close to any other codewords. So, BER performance is improved as a result.

Here belief propagation decoding in logarithm domain has been used in LDPC decoder. The decoding is performed iteratively. The noise corrupted code blocks are decoded more successfully with the large number of iterations. The iteration is stopped when a valid codeword is achieved or the number of iteration reaches its maximum value.

DVB-S.2 standard $rate = 1/2$ LDPC code is an irregular LDPC code. The degree of the bit nodes of the LDPC code are varying. Now bit nodes which have higher degrees collect more information from their adjacent check nodes and they get corrected first after happening small number of iterations. Then they helps other bit nodes get corrected through the iterative decoding process. It is similar to wave effect. As the degree of bit nodes of the LDPC code are varying, this wave effect is present. So it helps to improve BER performance.

So, for the above reasons, BER performance is improved very much when E_b/N_0 is increased for any particular modulation order of MPSK.

4.1.6 AWGN Channel with DVB-S.2 Standard Rate 1/2 LDPC Channel Coding and M-ary QAM Modulation

BER performance of DVB-S.2 standard Rate 1/2 LDPC Coded communication channel with AWGN noise for M-ary quadrature amplitude modulation(MQAM) has been discussed.

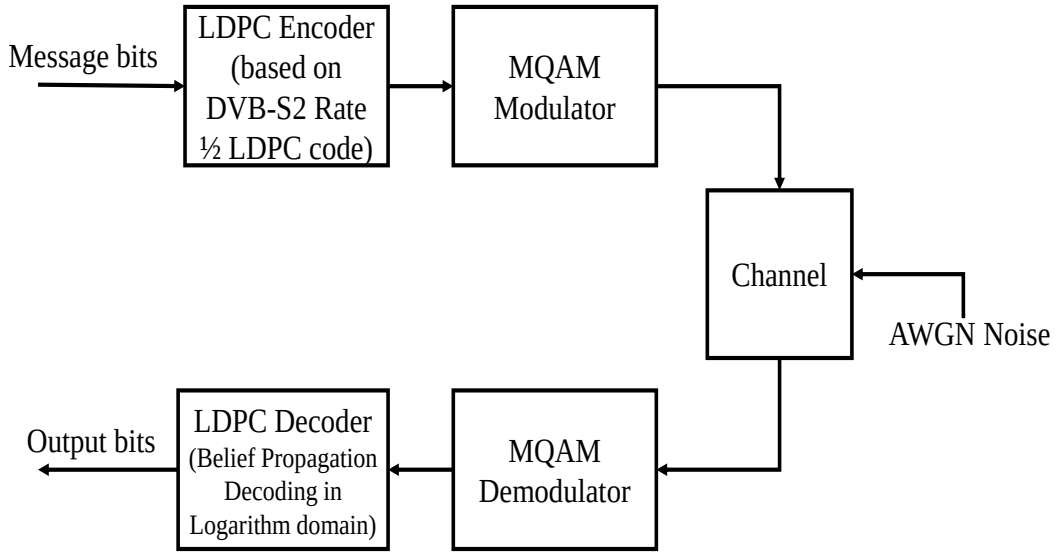

Figure 4.11: Block diagram of DVB-S.2 standard Rate=1/2 LDPC coded AWGN channel for MQAM

DVB-S.2 $rate = 1/2$ LDPC code has been used in this experiment. The length of the information block is 32400 bits and the length of the codeword block is 64800 bits. BER performance analysis of DVB-S.2 standard Rate 1/2 LDPC Coded communication channel has been conducted. The modulation scheme which has been considered here is M-ary quadrature amplitude modulation(MQAM). Additive white gaussian noise(AWGN) has been considered as channel noise. The experiment has been simulated in MATLAB.

The information block of length 32400 bits has been passed through LDPC encoder based on DVB-S.2 standard Rate 1/2 LDPC Code. 64800 bits block length

codeword has been generated. Then the encoded signal has been passed through MQAM modulator. The modulated signal has been sent through the communication channel. AWGN noise has been added to the signal in the channel. So the modulated signal has been noise corrupted when passing through the channel. Then noise affected signal has been received by MQAM demodulator. Then the demodulated signal has been passed through LDPC decoder based on belief propagation algorithm in logarithm domain. The decoder has corrected some errors. Now by comparing decoded bits with the original message bits, BER is calculated. The measured BER values in this experiment have been shown in the Table 4.6.

E_b/N_0(dB)	BER(QAM)	BER(8QAM)	BER(16QAM)	BER(32QAM)	BER(64QAM)
0	0.12608	0.198704	0.206759	0.242407	0.269784
0.2	0.121204	0.18821	0.202377	0.244815	0.261512
0.4	0.0981173	0.184259	0.193735	0.236327	0.260123
0.6	0.0930247	0.177994	0.198704	0.23142	0.255617
0.8	0.000691358	0.176049	0.183148	0.224815	0.247191
1	0	0.17213	0.17966	0.219444	0.244259
1.2	0	0.163642	0.172469	0.216235	0.240988
1.4	0	0.154537	0.16392	0.21037	0.236049
1.6	0	0.14358	0.156543	0.209475	0.22787
1.8	0	0.137222	0.147253	0.20321	0.222531
2	0	0.129167	0.14713	0.195062	0.213642
2.2	0	0.113642	0.12716	0.18713	0.216481
2.4	0	0.101235	0.122191	0.186049	0.207407
2.6	0	0.0144444	0.112654	0.181296	0.201728
2.8	0	8.10185e-05	0.104784	0.174877	0.200833
3	0	0	0.0315278	0.16321	0.195556
3.2	0	0	7.90895e-05	0.152315	0.18716
3.4	0	0	0	0.152623	0.178827
3.6	0	0	0	0.149043	0.178272
3.8	0	0	0	0.135926	0.167531
4	0	0	0	0.13179	0.165741
4.2	0	0	0	0.116327	0.161698
4.4	0	0	0	0.102006	0.146512
4.6	0	0	0	0.0908642	0.143642
4.8	0	0	0	0.00393659	0.138333
5	0	0	0	0	0.129846
5.2	0	0	0	0	0.118241
5.4	0	0	0	0	0.106111
5.6	0	0	0	0	0.0887654
5.8	0	0	0	0	0.00593542
6	0	0	0	0	0

Table 4.6: BER measurement of DVB-S.2 standard Rate=1/2 LDPC coded AWGN channel for MQAM

Based on simulation result, a graphical representation of BER vs E_b/N_0 has been shown in Fig. 4.12.

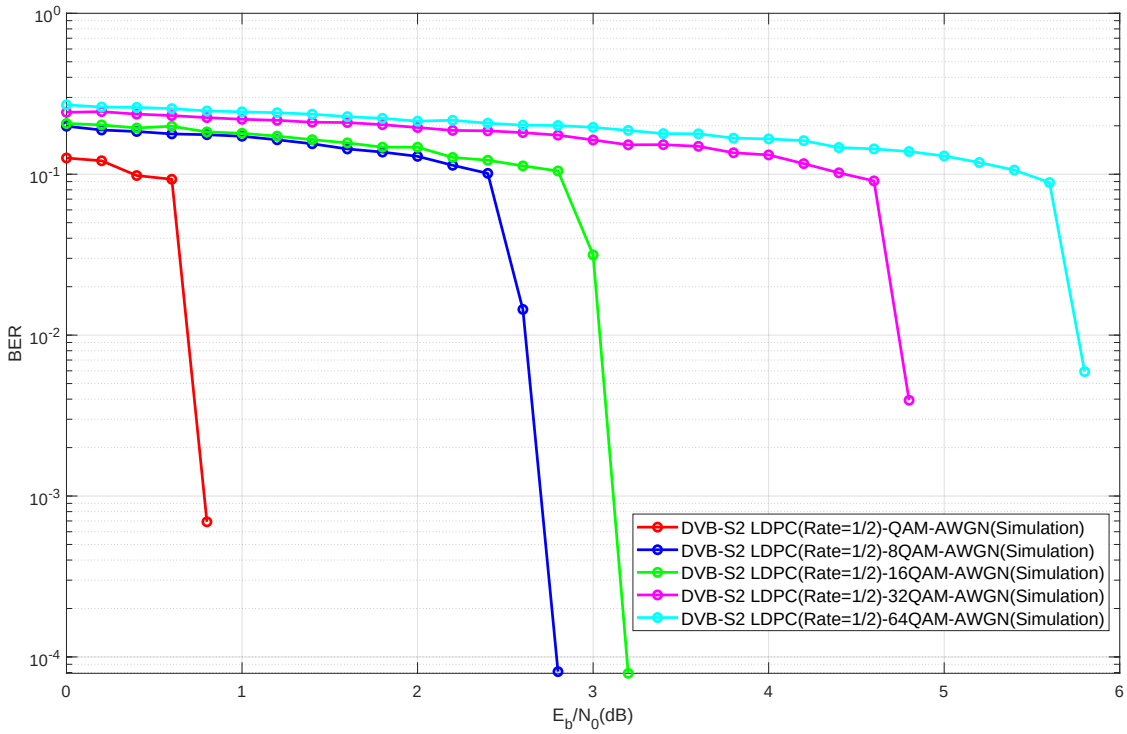

Figure 4.12: BER vs E_b/N_0 graph of DVB-S.2 standard Rate=1/2 LDPC coded AWGN channel for MQAM

The graph(Fig. 4.12) shows how BER is changed with E_b/N_0 for various MQAM when DVB-S.2 standard Rate 1/2 LDPC channel coding is used and AWGN is the channel noise. It can be seen from the graph(Fig. 4.12) that BER performance is degraded with increasing the modulation order of MQAM.

MQAM modulation technique modulates both phase and amplitude of carrier signal. So, both amplitude and phase are varied for various constellation points in MQAM modulation. The constellation points in the constellation diagram are situated in a square lattice structure. Now, the number of symbols is increased in constellation diagram when modulation order of MQAM is increased . As a result, the distances between constellation points are decreased. So there is higher possibility of data errors. So in DVB-S.2 $rate = 1/2$ LDPC coded channel, BER performance is

degraded when modulation order M of MQAM is increased.

It can be seen in graph(Fig. 4.12) that BER performance of DVB-S.2 $rate = 1/2$ LDPC coded channel is improved as E_b/N_0 is increased for any particular modulation order of MQAM. The BER performance is far better than BER performance of uncoded channel after a certain E_b/N_0 and the coding gain is high. So BER performance of DVB-S.2 $rate = 1/2$ LDPC coded channel is far better than uncoded channel(BER performance of uncoded communication channel with AWGN noise for MQAM has been shown in Fig. 3.4).

The message points corresponding to symbols are moved further apart when E_b/N_0 is increased. So if E_b/N_0 is increased the distances between constellation points are increased. As a result BER performance is improved.

The decoder mistakes to find the actually transmitted codeword due to noise when codewords weights are close to each other. The block length of codeword of DVB-S.2 $rate = 1/2$ LDPC code is 64800. The number of low weight codewords are very small. So There are small number of codewords which are undesirably close to any other codewords. So There will be less mistakes in decoding.

Belief propagation decoding in logarithm domain has been used in LDPC decoder and the decoding is performed iteratively. The decoder decodes noise corrupted code blocks more successfully with large number of iterations. The iteration is stopped when a valid codeword is achieved or the number of iteration reaches its maximum value.

DVB-S.2 standard $rate = 1/2$ LDPC code is an irregular LDPC code. The degree of the bit nodes of the LDPC code are varying. Now bit nodes which have higher degrees collect more information from their adjacent check nodes and they get corrected after happening small number of iterations. Then they helps other bit nodes get corrected through the iterative decoding process. It is similar to wave effect. So it helps to improve BER performance.

So , BER performance of DVB-S.2 standard Rate 1/2 LDPC Coded communication channel is improved very much when E_b/N_0 is increased for any particular modulation order of MQAM and the BER performance of this DVB-S.2 standard Rate 1/2 LDPC Coded case is better than uncoded channel.

4.2 Rayleigh Fading Channel with AWGN, Channel Coding and Modulation Schemes(M-ary PSK & M-ary QAM Modulation)

In this section, BER performance of coded Rayleigh fading communication channel with AWGN noise for M-ary phase shift keying(MPSK) and M-ary quadrature amplitude modulation(MQAM) has been discussed.

4.2.1 Rayleigh Fading Channel with AWGN, RS(255,239) Channel Coding and M-ary PSK Modulation

BER performance analysis of RS(255,239) coded Rayleigh fading communication channel has been conducted. The channel which has been considered here is wireless. M-ary phase shift keying(MPSK) has been considered as Modulation scheme. Rayleigh fading has been considered as the fading technique. Additive white gaussian noise(AWGN) has been considered as channel noise. The experiment has been simulated in MATLAB.

Input message symbols, which have been considered in this experiment, are random in nature. The RS channel encoder maps each 239 information symbols into 255 symbols length codeword. The codeword has been passed through MPSK modulator. Here BPSK, QPSK, 8PSK, 16PSK and 32PSK modulation schemes have been considered under MPSK. The MPSK modulator maps the information sequence into signal waveform. Now the modulated signal has been sent through Rayleigh fading communication channel. Additive white gaussian noise(AWGN) has been added. So the Rayleigh faded signal has been affected by AWGN noise. After that the noise corrupted signal waveform has been received by MPSK demodulator and the demodulator has demodulated it. Then the RS decoder has received the demodulated symbols and decoded it. The decoder has corrected some errors from the received symbols. Now original message symbols have been compared with the decoded information symbols. BER has been computed here. The measured BER values have been shown in Table 4.7.

E_b/N_0(dB)	BER(BPSK)	BER(QPSK)	BER(8PSK)	BER(16PSK)	BER(32PSK)
0	0.365536	0.366599	0.390882	0.407822	0.418072
1	0.349664	0.351471	0.378456	0.396386	0.408965
2	0.332075	0.334807	0.362342	0.385213	0.399138
3	0.313466	0.316827	0.34716	0.372229	0.388305
4	0.292798	0.297106	0.3293	0.358827	0.376076
5	0.270473	0.276229	0.311066	0.344616	0.364878
6	0.246096	0.253963	0.291141	0.329737	0.353458
7	0.220645	0.230473	0.271464	0.315606	0.342447
8	0.19373	0.207265	0.251085	0.301344	0.331703
9	0.166217	0.183156	0.231908	0.287474	0.322632
10	0.138672	0.15956	0.213598	0.275131	0.314786
11	0.111512	0.136547	0.197653	0.264787	0.310215
12	0.0851951	0.115117	0.184149	0.256094	0.305938
13	0.0622971	0.0953787	0.173452	0.249692	0.306088
14	0.0424435	0.0773363	0.165765	0.244131	0.308169
15	0.0265769	0.0612542	0.160459	0.240234	0.311587
16	0.0151752	0.0472103	0.156506	0.238819	0.317253
17	0.00738651	0.0342605	0.154088	0.237297	0.323838
18	0.000959728	0.0239639	0.152525	0.237535	0.330998
19	2.09205e-06	0.0153033	0.150181	0.23785	0.33784
20	0	0.00891632	0.148552	0.239279	0.344
21	0	0.00323379	0.14629	0.240375	0.350719
22	0	0.00013546	0.143887	0.242255	0.356434
23	0	6.10181e-07	0.141401	0.244279	0.362314
24	0	0	0.138271	0.246146	0.368035
25	0	0	0.134746	0.247702	0.373677
26	0	0	0.130649	0.248887	0.378996
27	0	0	0.126197	0.249559	0.384177
28	0	0	0.121721	0.249855	0.388611
29	0	0	0.116582	0.249966	0.392161
30	0	0	0.110869	0.249994	0.395051

Table 4.7: BER measurement of RS(255,239) coded Rayleigh fading channel with AWGN for MPSK

E_b/N_0(dB)	BER(BPSK)	BER(QPSK)	BER(8PSK)	BER(16PSK)	BER(32PSK)
31	0	0	0.104441	0.249999	0.397198
32	0	0	0.0977829	0.249999	0.398595
33	0	0	0.0898295	0.25	0.399246
34	0	0	0.0822306	0.25	0.399574
35	0	0	0.0733143	0.25	0.399671
36	0	0	0.0644236	0.25	0.399692
37	0	0	0.0552186	0.25	0.399727
38	0	0	0.0458421	0.25	0.399711
39	0	0	0.0368672	0.25	0.399724
40	0	0	0.0281878	0.25	0.399721
41	0	0	0.020749	0.25	0.399707
42	0	0	0.0140303	0.25	0.399713
43	0	0	0.00879132	0.25	0.399706
44	0	0	0.0038614	0.25	0.399712
45	0	0	0.000230649	0.25	0.399722
46	0	0	7.84519e-07	0.25	0.399707
47	0	0	0	0.25	0.399702
48	0	0	0	0.25	0.399717
49	0	0	0	0.25	0.399703
50	0	0	0	0.25	0.399708

Table 4.7: BER measurement of RS(255,239) coded Rayleigh fading channel with AWGN for MPSK

BER vs E_b/N_0 graph, based on simulation result, has been shown in Fig. 4.13.

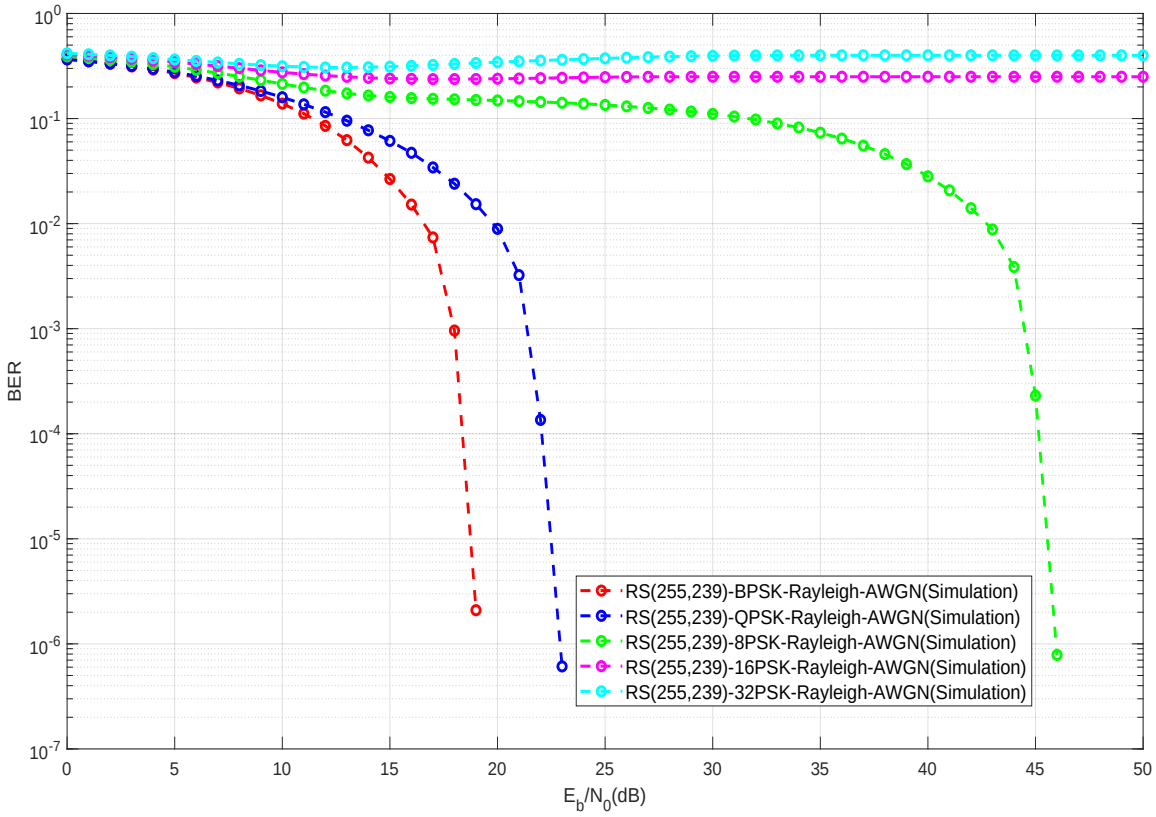

Figure 4.13: BER vs E_b/N_0 graph of RS(255,239) coded Rayleigh fading channel with AWGN for MPSK

The graph(Fig. 4.13) shows how BER is changed with E_b/N_0 for various MPSK when RS(255,239) coded Rayleigh fading communication channel is affected by AWGN noise. It can be seen in graph that BER performance is degraded with increasing modulation order(M) of MPSK.

If modulation order(M) of MPSK is increased, the number of symbols is increased in the constellation diagram. So, the symbols come closer to each other. As a result the distances between the constellation points are reduced. As a result, effect of noise will be more. So, BER performance is degraded when modulation order of MPSK is increased.

It can also be seen from the graphs(Fig. 4.13 and Fig. 3.5) that BER performance

of RS(255,239) coded Rayleigh fading communication channel with AWGN noise is better than BER performance of uncoded Rayleigh fading communication channel with AWGN noise for any particular modulation order of MPSK.

RS(255,239) code can correct errors in any eight symbols in the block of 255 symbols. Now, let there exists a burst of noise which lasts for duration 8 symbols. Now RS(255,239) decoder replaces the incorrect symbols with correct symbols. RS(255,239) decoder replaces one incorrect symbol with correct symbol whether one bit or all eight bits in a symbol are corrupted. So, RS(255,239) decoder performs very well against burst noise. As a result, BER performance is improved for the considered RS(255,239) coded Rayleigh fading communication channel.

It can also be seen from the graphs(Fig. 4.2 and Fig. 4.13) that BER performance of RS(255,239) coded communication channel with AWGN noise is better than BER performance of RS(255,239) coded Rayleigh fading communication channel with AWGN noise for any particular modulation order of MPSK.

Rayleigh fading channel has been considered in this experiment. Line-of-sight path has not been existed between the transmitter and receiver. Only non-line-of-sight path has been existed between the transmitter and receiver. The path between transmitter and receiver has been blocked by various obstacles. So, those obstacles reflect, refract, diffract and attenuate the signal. The signal has undergone flat fading. As a result, all frequency components of the signal experience same or equal magnitude of fading. Now, the magnitude of the signal that has passed through the Rayleigh fading communication channel is varied randomly according to the Rayleigh distribution. The probability density function(pdf) of Rayleigh distribution can be defined as shown in equation 2.13. Now, rapid amplitude fluctuation is induced in the received signal by Rayleigh fading channel and as a result performance degradation occurs seriously. Now, the Rayleigh faded signal has been corrupted by the AWGN noise in channel. As a result, BER performance is not good for the case Rayleigh fading channel.

4.2.2 Rayleigh Fading Channel with AWGN, RS(255,239) Channel Coding and M-ary QAM Modulation

BER performance analysis of RS(255,239) coded Rayleigh fading communication channel has been conducted. The modulation scheme ,which has been considered here, is M-ary quadrature amplitude modulation(MQAM). Here QAM, 8QAM, 16QAM, 32QAM and 64QAM modulation schemes have been considered under MQAM. Rayleigh fading has been considered as the fading technique. Additive white gaussian noise(AWGN) has been considered as channel noise here. MATLAB has been used for this experiment.

Input message symbols considered in this experiment are random in nature. The RS channel encoder maps each 239 information symbols into 255 symbols length codeword. The codeword has been passed through MQAM modulator. Now the modulated signal has been sent through Rayleigh fading communication channel. Additive white gaussian noise(AWGN) has been added. So the Rayleigh faded signal has been noise affected by AWGN noise. MQAM demodulator has received the noise corrupted signal and demodulated it. Then the RS decoder has received the demodulated symbols and decoded it. Some errors have been corrected by the decoder from the received symbols. Now, to calculate BER, original message bits have been compared with the decoded information bits. The measured BER values have been shown in Table 4.8

E_b/N_0(dB)	BER(QAM)	BER(8QAM)	BER(16QAM)	BER(32QAM)	BER(64QAM)
0	0.36637	0.399147	0.405832	0.417333	0.432385
1	0.353143	0.392045	0.397735	0.410533	0.429351
2	0.334566	0.379869	0.387683	0.405408	0.424529
3	0.315513	0.372652	0.380628	0.396449	0.419226
4	0.297767	0.363049	0.373849	0.389503	0.417233
5	0.275737	0.352259	0.368368	0.384571	0.413002
6	0.255737	0.341778	0.36012	0.378201	0.409236
7	0.231841	0.329289	0.352877	0.374399	0.404294
8	0.206632	0.318169	0.344733	0.369153	0.401736
9	0.181946	0.306961	0.336046	0.366109	0.399603
10	0.160058	0.295696	0.328954	0.358379	0.39682
11	0.13602	0.285601	0.323389	0.360633	0.393358
12	0.114603	0.27681	0.318028	0.355387	0.394393
13	0.0952563	0.26897	0.311104	0.353044	0.391025
14	0.0783839	0.260968	0.3084	0.350968	0.389838
15	0.0615743	0.255089	0.304184	0.348499	0.388896
16	0.0471757	0.248828	0.302401	0.346485	0.392045
17	0.0348222	0.242306	0.29989	0.346857	0.38739
18	0.0235042	0.239304	0.298515	0.345209	0.388933
19	0.015251	0.236961	0.296742	0.343823	0.387897
20	0.00879707	0.232929	0.29806	0.344038	0.387155
21	0.00345188	0.230068	0.294158	0.342798	0.388985
22	0.000108787	0.230445	0.29455	0.341904	0.387688
23	0	0.229597	0.297008	0.343311	0.387233
24	0	0.230664	0.295654	0.342762	0.387249
25	0	0.229451	0.296287	0.343248	0.388039
26	0	0.23159	0.297699	0.342317	0.38876
27	0	0.235476	0.301072	0.346899	0.389017
28	0	0.23626	0.302463	0.343949	0.387599
29	0	0.239195	0.304174	0.34602	0.386255
30	0	0.243724	0.305403	0.345235	0.388776

Table 4.8: BER measurement of RS(255,239) coded Rayleigh fading channel with AWGN for MQAM

E_b/N_0(dB)	BER(QAM)	BER(8QAM)	BER(16QAM)	BER(32QAM)	BER(64QAM)
31	0	0.244932	0.307348	0.345329	0.388133
32	0	0.245654	0.307646	0.346569	0.387191
33	0	0.246172	0.310089	0.349038	0.389053
34	0	0.246757	0.313133	0.347694	0.387845
35	0	0.248651	0.311266	0.347819	0.385037
36	0	0.24829	0.310622	0.347976	0.389854
37	0	0.250058	0.312374	0.350309	0.387788
38	0	0.249712	0.314127	0.350805	0.385978
39	0	0.250978	0.311757	0.350136	0.388164
40	0	0.250528	0.311292	0.351234	0.387008
41	0	0.250528	0.312897	0.349911	0.386668
42	0	0.249205	0.311742	0.351726	0.387249
43	0	0.250251	0.313525	0.350764	0.38624
44	0	0.251919	0.312338	0.35136	0.387578
45	0	0.250188	0.311867	0.349665	0.385779
46	0	0.249969	0.312348	0.350277	0.385434
47	0	0.249038	0.312814	0.350429	0.384074
48	0	0.250288	0.311062	0.350058	0.384409
49	0	0.249388	0.311412	0.349754	0.386088
50	0	0.248551	0.311862	0.3508	0.384969

Table 4.8: BER measurement of RS(255,239) coded Rayleigh fading channel with AWGN for MQAM

A graphical representation of BER vs E_b/N_0 has been shown in Fig. 4.14 which is based on simulation result.

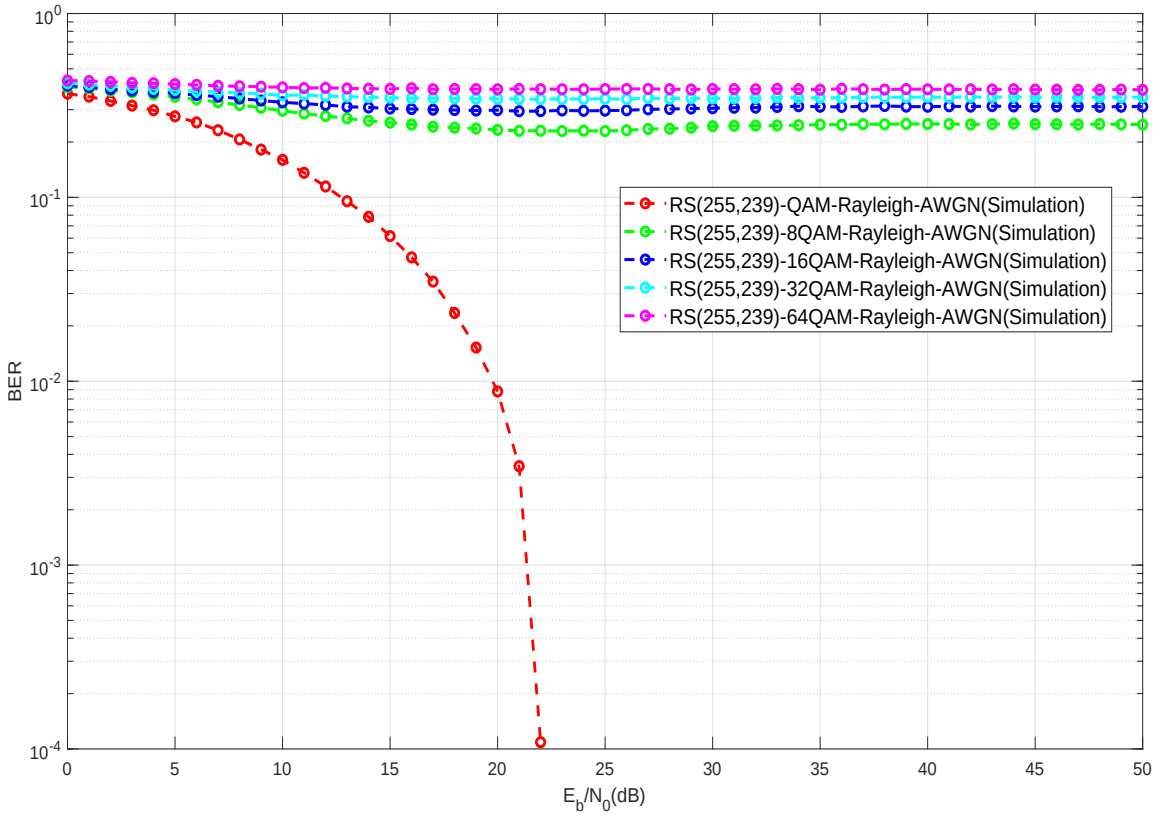

Figure 4.14: BER vs E_b/N_0 graph of RS(255,239) coded Rayleigh fading channel with AWGN for MQAM

The graph (Fig. 4.14) shows how BER is changed with E_b/N_0 for various orders of MQAM modulation scheme when RS(255,239) coded Rayleigh fading communication channel is affected by AWGN noise. It can be seen in graph(Fig. 4.14) that BER performance is degraded with increasing modulation order(M) of MQAM.

The carrier experiences phase as well as amplitude modulation in MQAM modulation. The constellation diagram of MQAM modulation scheme consists of a square lattice of symbol points. The energy per symbol of MQAM is not constant. If modulation order of MQAM is increased the number of symbols is increased in constellation diagram. So, the amplitude variation will be more for higher order modulation. Also, the distances between constellation points are decreased when modulation order of

MQAM is increased. So there is a higher possibility of data errors. As a result, BER performance is degraded when modulation order of MQAM is increased.

It can be seen from the graphs(Fig. 4.14 and Fig. 3.6) that BER performance of RS(255,239) coded Rayleigh fading communication channel with AWGN noise is better than BER performance of uncoded Rayleigh fading communication channel with AWGN noise for any particular modulation order of MQAM.

RS code has capability of correcting burst error. RS(255,239) code can correct errors in any eight symbols in the block of 255. Let there exists a burst of noise which lasts for duration 8 symbols. Now RS(255,239) decoder replaces the incorrect symbols with correct symbols. RS(255,239) decoder replaces one incorrect symbol with correct symbol whether one bit or all eight bits in a symbol are corrupted. So, RS(255,239) decoder performs very well against burst noise. As a result, BER performance of RS(255,239) coded Rayleigh fading communication channel with AWGN noise is better than BER performance of uncoded Rayleigh fading communication channel with AWGN noise for any particular modulation order of MQAM.

It can be seen from the graphs(Fig. 4.4 and Fig. 4.14) that BER performance of RS(255,239) coded communication channel with AWGN noise is better than BER performance of RS(255,239) coded Rayleigh fading communication channel with AWGN noise for any particular modulation order of MQAM.

Rayleigh fading channel has been considered in this experiment. The probability density function(pdf) of Rayleigh distribution can be defined as shown in equation 2.13. The path between transmitter and receiver has been blocked by various obstacles. Those obstacles attenuate the signal, reflect it, refract it, also diffract the signal. Only non-line-of-sight path has been existed between the transmitter and receiver. The signal has undergone flat fading. As a result, all frequency components of the signal experience equal magnitude of fading. Now, the magnitude of the signal that has passed through the Rayleigh fading communication channel is varied randomly according to the Rayleigh distribution. Now, rapid amplitude fluctuation is induced in the received signal by Rayleigh fading channel and as a result, serious BER performance degradation occurs. The Rayleigh faded signal has been also affected by the AWGN noise in channel. As a result, BER performance is degraded for the case Rayleigh fading channel here.

4.2.3 Rayleigh Fading Channel with AWGN, (7,1/2) Convolutional Channel Coding and M-ary PSK Modulation

BER performance analysis of (7,1/2) convolutional coded Rayleigh fading communication channel has been conducted. Modulation scheme, which has been considered here, is M-ary phase shift keying(MPSK). Rayleigh fading has been considered as the fading technique. Additive white gaussian noise(AWGN) has been considered as channel noise. The experiment has been simulated in MATLAB.

Let an infinite bitstream has come to the encoder. The $(7, 1/2)$ convolutional encoder has $rate = 1/2$. So, for every one bit of input the $(7, 1/2)$ convolutional encoder gives two bits output. Now encoded signal has been passed through MPSK modulator. Here BPSK, QPSK, 8PSK, 16PSK and 32PSK modulation schemes have been considered under MPSK. The MPSK modulated signal has been sent through Rayleigh fading communication channel. AWGN has been considered as the channel noise. So the passed Rayleigh faded signal has been affected by AWGN noise. Then the MPSK demodulator has received the noise corrupted signal and demodulated it. The demodulated signal has been passed through hard decision based Viterbi decoder. The Viterbi decoder has corrected some errors from the received bits. Now the decoded information bits has been compared with the original message bits and BER has been calculated. The measured BER values have been shown in Table 4.9.

E_b/N_0(dB)	BER(BPSK)	BER(QPSK)	BER(8PSK)	BER(16PSK)	BER(32PSK)
0	0.500013	0.50001	0.499856	0.499169	0.500112
1	0.50025	0.499666	0.499812	0.499625	0.49923
2	0.499577	0.499783	0.499744	0.500239	0.499916
3	0.499419	0.50002	0.499807	0.501232	0.499976
4	0.498948	0.499172	0.49969	0.500532	0.500209
5	0.496295	0.497653	0.499729	0.499809	0.500396
6	0.492228	0.495365	0.498534	0.499603	0.500316
7	0.47923	0.488621	0.499001	0.499143	0.500352
8	0.453414	0.474093	0.497242	0.498731	0.499337
9	0.398019	0.444322	0.493779	0.499156	0.499722
10	0.297606	0.390896	0.489387	0.499022	0.499416
11	0.156195	0.295645	0.481524	0.49939	0.500309
12	0.0515599	0.180469	0.473676	0.49939	0.49993
13	0.00996408	0.0830266	0.46049	0.499786	0.499857
14	0.00117947	0.0278694	0.448861	0.500031	0.500185
15	0.000100558	0.00721403	0.438072	0.500188	0.499874
16	6.01854e-06	0.00150225	0.427071	0.499892	0.499194
17	0	0.000255005	0.419359	0.500231	0.497667
18	0	3.02781e-05	0.412001	0.498667	0.498259
19	0	1.20371e-06	0.406454	0.497207	0.498661
20	0	2.77779e-07	0.395458	0.494485	0.497324
21	0	0	0.384521	0.493368	0.498089
22	0	0	0.373911	0.490963	0.49815
23	0	0	0.356797	0.490894	0.499031
24	0	0	0.33951	0.489471	0.500419
25	0	0	0.320721	0.488591	0.501149
26	0	0	0.297344	0.488001	0.502728
27	0	0	0.267815	0.488231	0.503456
28	0	0	0.237469	0.488194	0.504838
29	0	0	0.198886	0.488092	0.506293
30	0	0	0.160115	0.488206	0.506187

Table 4.9: BER measurement of (7,1/2) convolutional coded Rayleigh fading channel with AWGN for MPSK

E_b/N_0(dB)	BER(BPSK)	BER(QPSK)	BER(8PSK)	BER(16PSK)	BER(32PSK)
31	0	0	0.120997	0.488146	0.507266
32	0	0	0.0857228	0.487727	0.50682
33	0	0	0.0548561	0.488038	0.507746
34	0	0	0.0317734	0.488653	0.507412
35	0	0	0.015917	0.488021	0.507346
36	0	0	0.00712347	0.488877	0.507117
37	0	0	0.0025356	0.487859	0.50708
38	0	0	0.00081946	0.488645	0.507319
39	0	0	0.000227227	0.488822	0.50763
40	0	0	4.91671e-05	0.488461	0.508484
41	0	0	6.29632e-06	0.48793	0.508505
42	0	0	9.25929e-07	0.487198	0.507035
43	0	0	5.55557e-07	0.487741	0.507862
44	0	0	0	0.488718	0.506857
45	0	0	0	0.488067	0.507459
46	0	0	0	0.488154	0.507345
47	0	0	0	0.487964	0.507904
48	0	0	0	0.488995	0.507822
49	0	0	0	0.487819	0.507755
50	0	0	0	0.488176	0.507557

Table 4.9: BER measurement of (7,1/2) convolutional coded Rayleigh fading channel with AWGN for MPSK

Based on simulation result, a graphical representation of BER vs E_b/N_0 has been shown in Fig. 4.15

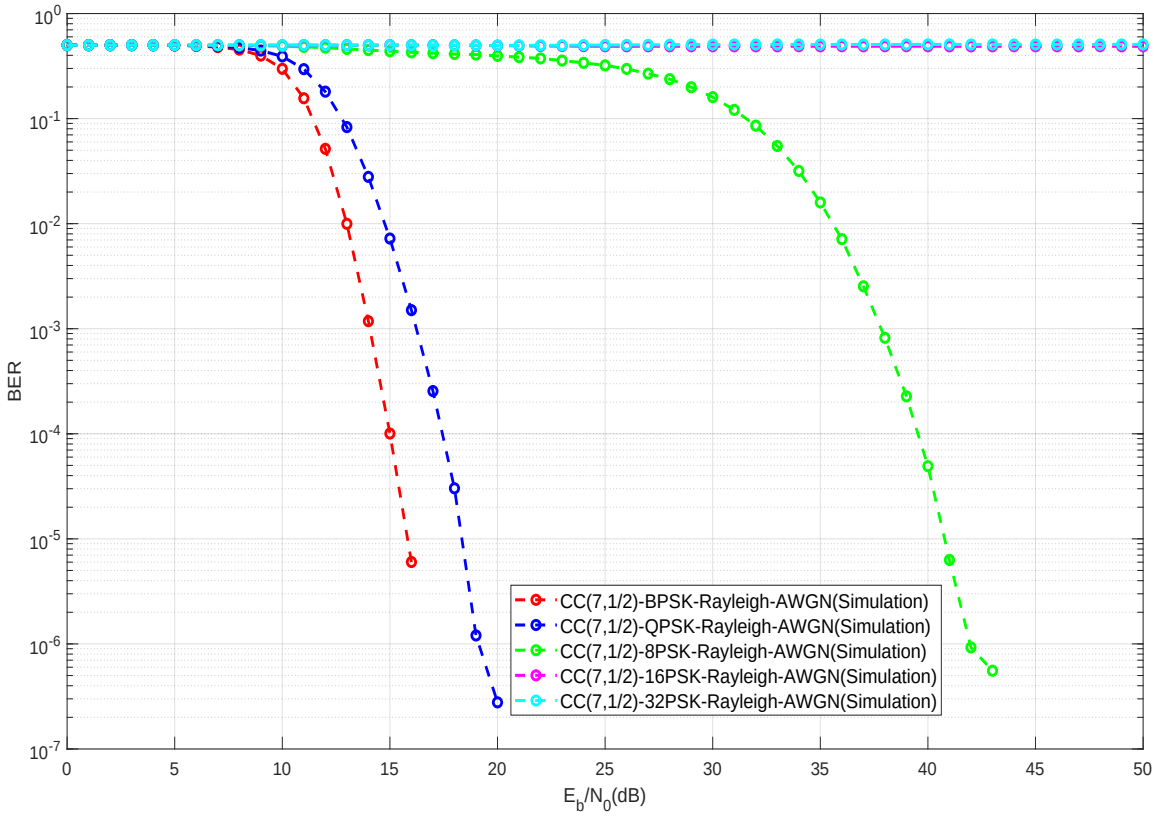

Figure 4.15: BER vs E_b/N_0 graph of (7,1/2) convolutional coded Rayleigh fading channel with AWGN for MPSK

The graph(Fig. 4.15) shows how BER is changed with E_b/N_0 for various MPSK when (7,1/2) convolutional coded Rayleigh fading communication channel is affected by AWGN noise. It can be seen in graph(Fig. 4.15) that the BER performance is degraded as modulation order M of MPSK modulation is increased.

The symbols are situated in a circle for MPSK. The number of symbols is increased when modulation order is increased. So, if modulation order M of MPSK is increased, the distance between constellation points are decreased. So, there is higher chance of data errors. So, BER performance of $(7, 1/2)$ convolutional coded Rayleigh fading channel with AWGN is degraded if modulation order of MPSK is increased.

It can also be seen from the graphs(Fig. 4.15 and Fig. 3.5) that BER performance of $(7, 1/2)$ convolutional coded Rayleigh fading communication channel with AWGN noise is better than BER performance of uncoded Rayleigh fading communication channel with AWGN noise for any particular modulation order of MPSK.

Bit error probability for the given convolutional code is bounded as shown in equation 4.1. Now, the minimal Hamming distance between different encoded sequences is called free distance which is represented by d_{free}. For high value of SNR, the lowest order term is the dominating term in bit error probability. In the lowest order dominating term d is equal to d_{free} i.e $d = d_{free}$. The $(7, 1/2)$ convolutional code is able to achieve free distance $d_{free} = 10$. Maximization of free distance is an important thing to improve BER performance. The bit error rate falls of exponentially with d_{free} at low error rates when maximum likelihood(ML) decoding is used. So BER performance is better for the $(7, 1/2)$ convolutional coded case.

It can be seen from the graphs(Fig. 4.6 and Fig. 4.15) that BER performance of $(7, 1/2)$ convolutional coded communication channel with AWGN noise is better than BER performance of $(7, 1/2)$ convolutional coded Rayleigh fading communication channel with AWGN noise for any particular modulation order of MPSK.

Rayleigh fading channel has been considered in this experiment. Line-of-sight path has not been existed between the transmitter and receiver. Only non-line-of-sight path has been existed between the transmitter and receiver. The path between transmitter and receiver has been blocked by various obstacles. So, those obstacles has attenuated the signal and also reflected, refracted, diffracted the signal. The signal has undergone flat fading. As a result, all frequency components of the signal experience same or equal magnitude of fading. Now, the magnitude of the signal that has passed through the Rayleigh fading communication channel is varied randomly according to the Rayleigh distribution. The probability density function(pdf) of Rayleigh distribution can be defined as shown in equation 2.13. Now, rapid amplitude fluctuation is induced in the received signal by Rayleigh fading channel and as a result huge BER performance degradation occurs.Now, the Rayleigh faded signal has been also corrupted by the AWGN noise in channel. As a result, BER performance is degraded for the case Rayleigh fading channel.

4.2.4 Rayleigh Fading Channel with AWGN, (7,1/2) Convolutional Channel Coding and M-ary QAM Modulation

BER performance analysis of (7,1/2) convolutional coded Rayleigh fading communication channel has been conducted. M-ary quadrature amplitude modulation(MQAM) modulation scheme has been considered here . Here QAM, 8QAM, 16QAM, 32QAM and 64QAM modulation schemes have been considered under MQAM. Rayleigh fading has been considered as the fading technique. Additive white gaussian noise(AWGN) has been considered as channel noise.

Let an infinite bitstream has come to the encoder. The $(7, 1/2)$ convolutional encoder has $rate = 1/2$. So, for every one bit of input the $(7, 1/2)$ convolutional encoder gives two bits output. The encoded signal has been passed through MQAM modulator. Now the modulated signal has been sent through Rayleigh fading communication channel. AWGN has been added. As a result, the Rayleigh faded signal has been noise affected by AWGN noise. MQAM demodulator has received the noise corrupted signal and demodulated it. The demodulated signal has been passed through hard decision based Viterbi decoder. The Viterbi decoder has corrected some errors from the received bits. Now, to calculate BER, the decoded information bits have been compared with the original message bits. The measured BER values have been shown in Table 4.10

E_b/N_0(dB)	BER(QAM)	BER(8QAM)	BER(16QAM)	BER(32QAM)	BER(64QAM)
0	0.500353	0.499845	0.499989	0.499266	0.499646
1	0.500093	0.500365	0.499727	0.500359	0.49973
2	0.500091	0.499067	0.499986	0.500218	0.500229
3	0.499727	0.49964	0.499795	0.500291	0.500182
4	0.498951	0.499572	0.499609	0.500518	0.499907
5	0.497471	0.500443	0.500807	0.500038	0.500255
6	0.494216	0.500325	0.499299	0.500207	0.500029
7	0.488126	0.500105	0.499322	0.499745	0.500264
8	0.474022	0.499695	0.499144	0.499611	0.499802
9	0.445841	0.499985	0.499411	0.499607	0.500499
10	0.389637	0.499579	0.499294	0.499766	0.50095
11	0.299069	0.500084	0.49848	0.50034	0.499929
12	0.181162	0.498923	0.498495	0.500128	0.499595
13	0.0820422	0.498509	0.498129	0.499899	0.500555
14	0.0271416	0.497485	0.499057	0.500429	0.499921
15	0.00724403	0.497179	0.499776	0.500426	0.500053
16	0.00142781	0.494544	0.499811	0.499962	0.500458
17	0.00026445	0.49202	0.499251	0.500206	0.500384
18	2.70372e-05	0.489328	0.499129	0.499937	0.500776
19	2.5926e-06	0.486486	0.499569	0.500547	0.500813
20	2.77779e-07	0.483525	0.499912	0.499985	0.500086
21	0	0.480368	0.499244	0.500371	0.499854
22	0	0.477809	0.499711	0.499566	0.500334
23	0	0.476086	0.500451	0.499971	0.499656
24	0	0.473678	0.499212	0.499976	0.50036
25	0	0.474036	0.50045	0.499671	0.50001
26	0	0.474016	0.500063	0.500445	0.499594
27	0	0.474268	0.499772	0.500285	0.500396
28	0	0.47474	0.499611	0.500438	0.500196
29	0	0.474422	0.500051	0.500193	0.500324
30	0	0.474602	0.500225	0.499779	0.500306

Table 4.10: BER measurement of (7,1/2) convolutional coded Rayleigh fading channel with AWGN for MQAM

E_b/N_0(dB)	BER(QAM)	BER(8QAM)	BER(16QAM)	BER(32QAM)	BER(64QAM)
31	0	0.474143	0.500064	0.499909	0.500613
32	0	0.474004	0.499716	0.500372	0.500303
33	0	0.475391	0.499102	0.499345	0.500458
34	0	0.474186	0.500241	0.500419	0.500194
35	0	0.475755	0.49924	0.49952	0.500471
36	0	0.474757	0.499656	0.50015	0.500184
37	0	0.47507	0.499476	0.499656	0.500353
38	0	0.475684	0.499489	0.500548	0.500234
39	0	0.474692	0.498909	0.500176	0.500231
40	0	0.474835	0.499677	0.50006	0.499683
41	0	0.475112	0.499344	0.500156	0.50068
42	0	0.474512	0.499281	0.500217	0.500175
43	0	0.476592	0.499875	0.49934	0.500343
44	0	0.474709	0.49937	0.499331	0.499559
45	0	0.474831	0.499619	0.500008	0.500219
46	0	0.474374	0.499238	0.499921	0.5007
47	0	0.474537	0.499938	0.499918	0.49988
48	0	0.474487	0.499509	0.499549	0.500296
49	0	0.475004	0.50007	0.500455	0.500212
50	0	0.474988	0.499822	0.500008	0.50029

Table 4.10: BER measurement of (7,1/2) convolutional coded Rayleigh fading channel with AWGN for MQAM

BER vs E_b/N_0 graph has been shown in Fig. 4.16. The graph is based on simulation result.

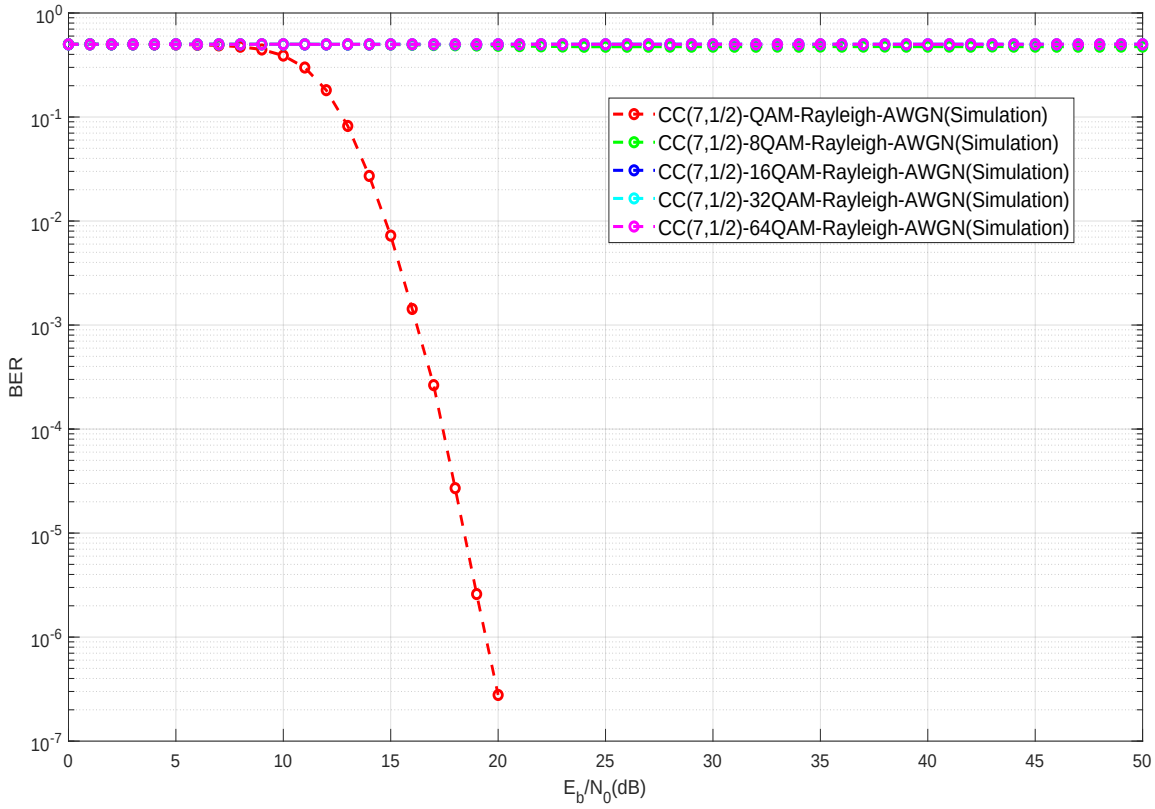

Figure 4.16: BER vs E_b/N_0 graph of (7,1/2) convolutional coded Rayleigh fading channel with AWGN for MQAM

The graph(Fig. 4.16) shows how BER is changed with E_b/N_0 for various orders of MQAM modulation scheme when (7,1/2) convolutional coded Rayleigh fading communication channel is affected by AWGN noise. It can be seen in graph(Fig. 4.16) that BER performance is degraded with increasing modulation order(M) of MQAM.

The constellation points are situated in square grid in MQAM modulation. The distance between symbol points are also not constant in MQAM. Now the number of symbols is increased in constellation diagram when modulation order of MQAM is increased. As a result, the distances between constellation points are decreased. The amplitude variation will also be more for higher order modulation. So the possibility

of data errors is more. So, BER performance is best for 4QAM and BER performance is degraded with increasing the modulation order further.

It can be seen from the graphs(Fig. 4.8 and 4.16) that BER performance of $(7, 1/2)$ convolutional coded communication channel with AWGN noise is better than BER performance of $(7, 1/2)$ convolutional coded Rayleigh fading communication channel with AWGN noise for any particular modulation order of MQAM.

Rayleigh fading channel has been considered in this experiment. Only non-line-of-sight path has been existed between the transmitter and receiver. The path between transmitter and receiver has been blocked by various obstacles. So, those obstacles has attenuated the signal and also reflected, refracted, diffracted the signal. The signal has undergone flat fading. As a result, all frequency components of the signal experience same or equal magnitude of fading. Now, the magnitude of the signal that has passed through the Rayleigh fading communication channel is varied randomly according to the Rayleigh distribution. The probability density function(pdf) of Rayleigh distribution can be defined as shown in equation 2.13. Now, rapid amplitude fluctuation is induced in the received signal by Rayleigh fading channel and as a result serious BER performance degradation occurs. Now, the Rayleigh faded signal has been noise corrupted by the AWGN noise in channel. As a result, BER performance is degraded for the case Rayleigh fading channel.

It can also be seen from the graphs(Fig. 4.16 and Fig. 3.6) that BER performance of $(7, 1/2)$ convolutional coded Rayleigh fading communication channel with AWGN noise is better than BER performance of uncoded Rayleigh fading communication channel with AWGN noise for any particular modulation order of MQAM.

Bit error probability for the given convolutional code is bounded as shown in equation 4.1. Now the minimal Hamming distance between different encoded sequences is called free distance which is represented by d_{free}. For high value of SNR, the lowest order term is the dominating term in bit error probability. In the lowest order dominating term d is equal to d_{free} i.e $d = d_{free}$. The $(7, 1/2)$ convolutional code is able to achieve free distance $d_{free} = 10$. Maximization of free distance is an important thing to improve BER performance. The bit error rate falls of exponentially with d_{free} at low error rates when maximum likelihood(ML) decoding is used. So BER performance is better for the $(7, 1/2)$ convolutional coded case.

4.3 Conclusion

In the first part of this chapter, BER performance analysis of coded communication channel with AWGN noise for MPSK and MQAM has been done where RS(255,239) code, CC(7,1/2) code and DVB-S.2 standard rate=1/2 LDPC error correcting codes are considered. In the second part of this chapter, BER performance analysis of coded communication channel considering both Rayleigh fading and AWGN noise has been done for MPSK and MQAM modulation techniques. It can be seen from the experiments results that BER performance of coded communication channel with AWGN noise is better than BER performance of uncoded communication channel with AWGN noise. It can also be seen from the graph that BER performance of coded communication channel with AWGN noise is better than BER performance of coded Rayleigh fading communication channel with AWGN noise. In the next chapter, block cipher based various modes of operations will be considered for coded communication channel with AWGN. Then it will be very much interesting to see what will be the impact of block cipher based various modes of operations on BER performance of the channel.

Chapter 5

BER Performance of Communication Channel with Encryption and Channel Coding

In the experiments, Consultative Committee for Space Data Systems(CCSDS) standard LDPC(k=1024, rate=1/2) code has been considered as error correcting code. Block cipher based various modes of operations have been considered. Here block cipher based electronic codebook(ECB) mode, counter(CTR) mode and cipher block chaining(CBC) mode of operation have been used in the experiments. Two block ciphers have been considered in the experiments shown in this chapter. The considered block ciphers are AES and HDNM8. BER performance of LDPC(k=1024, rate=1/2) coded communication channel with AWGN for BPSK modulation has been discussed. Then BER performance of the communication channel with AES based various modes(ECB, CTR and CBC) of operations and LDPC(k=1024, rate=1/2) coding has been discussed. Here also AWGN has been considered as channel noise and BPSK has been considered as the modulation technique in the experiments. After that, BER performance of the communication channel with HDNM8 based CTR mode of operation and LDPC(k=1024, rate=1/2) coding has been discussed. All the experiments have been simulated in MATLAB.

5.1 AWGN Channel with LDPC(with Information Block Length k=1024, Rate=1/2) Channel Coding and BPSK Modulation

BER performance of LDPC(k=1024, rate=1/2) coded communication channel with AWGN for BPSK modulation has been discussed in this section.

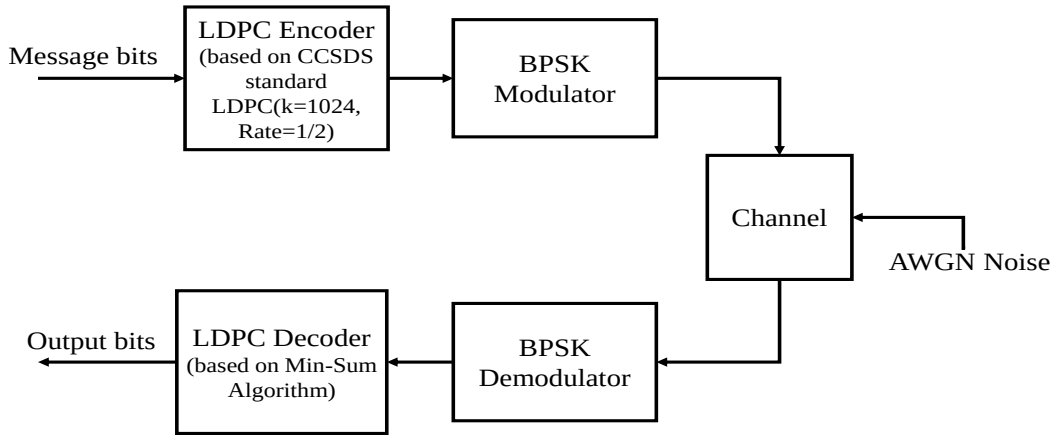

Figure 5.1: Block diagram of CCSDS standard LDPC(k=1024, Rate=1/2) coded AWGN channel for BPSK modulation

Here CCSDS standard low density parity check code(LDPC) has been used in this experiment. The CCSDS standard LDPC code which has been used here has information length(k) is 1024 bits and rate is 1/2. Binary phase shift keying(BPSK) has been considered here as the modulation scheme. Additive white gaussian noise(AWGN) has been considered as the channel noise. The experiment has been simulated in MATLAB.

The information block of length 1024 bits has been passed through LDPC encoder and the encoder gives codeword block of length 2048 bits. Then the encoded signal has been passed through BPSK modulator and the modulator has modulated it. The modulated signal has been sent through the communication channel. AWGN has been considered as the channel noise. Then noise corrupted signal has been received by BPSK demodulator and demodulated by the demodulator. The demodulated signal has been passed through LDPC decoder based on Min-Sum algorithm. Then BER

has been calculated by comparing decoded bits with the original message bits. The measured BER values have been shown in Table 5.1.

E_b/N_0(dB)	BER(BPSK)
0	0.1815
0.2	0.1778
0.4	0.1738
0.6	0.1671
0.8	0.1621
1	0.1547
1.2	0.1503
1.4	0.1438
1.6	0.1384
1.8	0.1339
2	0.1169
2.2	0.09879
2.4	0.05945
2.6	0.02903
2.8	0.01035
3	0.002422
3.2	0.0008008

Table 5.1: BER measurement of LDPC(k=1024, Rate=1/2) coded communication channel with AWGN for BPSK modulation

Based on simulation result, BER vs E_b/N_0 graph has been shown in Fig. 5.2.

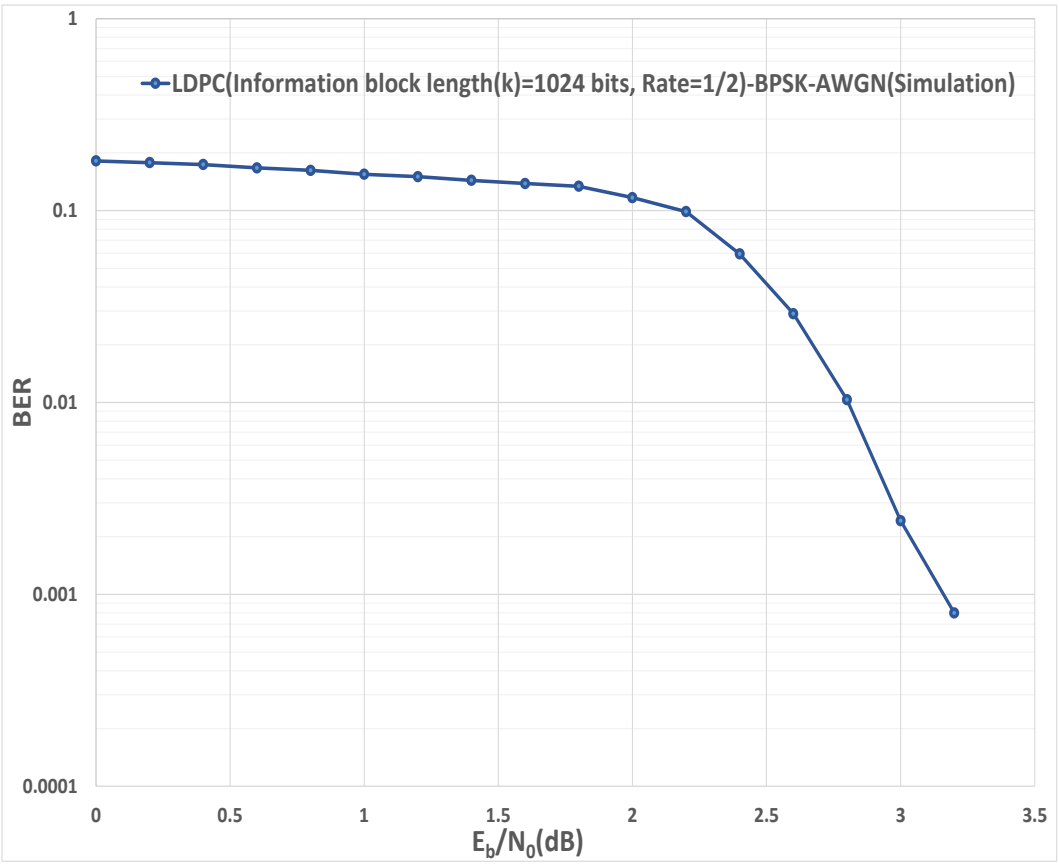

Figure 5.2: BER vs E_b/N_0 graph for LDPC(k=1024, Rate=1/2) coded communication channel with AWGN for BPSK modulation

The graph(Fig. 5.2) shows BER performance of LDPC(with k=1024 bits, Rate=1/2) coded channel is improved when E_b/N_0 is increased for BPSK modulation. The BER performance is far better than BER performance of uncoded channel after a certain E_b/N_0 and there is a high coding gain. So BER performance of rate 1/2 LDPC coded channel with information block length k=1024 bits is far better than uncoded channel(BER performance of uncoded communication channel with AWGN for BPSK modulation has been shown in Fig. 3.2).

There are only two constellation points present in BPSK modulation scheme. Now if E_b/N_0 is increased the the constellation points are moved further apart. So the distance between constellation points are increased. As a result, effect of noise will be less.

LDPC code is a capacity approaching code i.e the practical construction allows the noise threshold set to be very close to Shannon limit. Now, noise threshold is upper bound of channel noise and the probability of lost information can be made small up to noise threshold.

Now, if there are closeness of weight of codewords, the decoder mistakes to find the actually transmitted codeword due to noise. One advantage of LDPC code(k=1024, rate=1/2) is that the low weight codewords are nearly absent. So There are small number of codewords which are undesirably close to any other codewords. So BER performance is improved as a result.

There is an advantage of using LDPC decoding based on min-sum algorithm. The computational complexity is less in the decoding process. The decoding is performed iteratively. The corrupted LDPC code blocks are decoded more successfully with the greater number of iterations. The iteration is stopped when a valid codeword is achieved or the number of iteration reaches its maximum value. So, for the above described reasons, BER performance is improved very much.

5.2 AWGN Channel with AES Based Electronic Codebook(ECB) Mode Operation, CCSDS Standard LDPC(k=1024, Rate=1/2) Channel Coding and BPSK Modulation

In this section, BER performance of the communication channel with AES based ECB mode of operation and LDPC(k=1024, rate=1/2) coding has been discussed. Here AWGN has been considered as channel noise and BPSK has been considered as the modulation technique in the experiment.

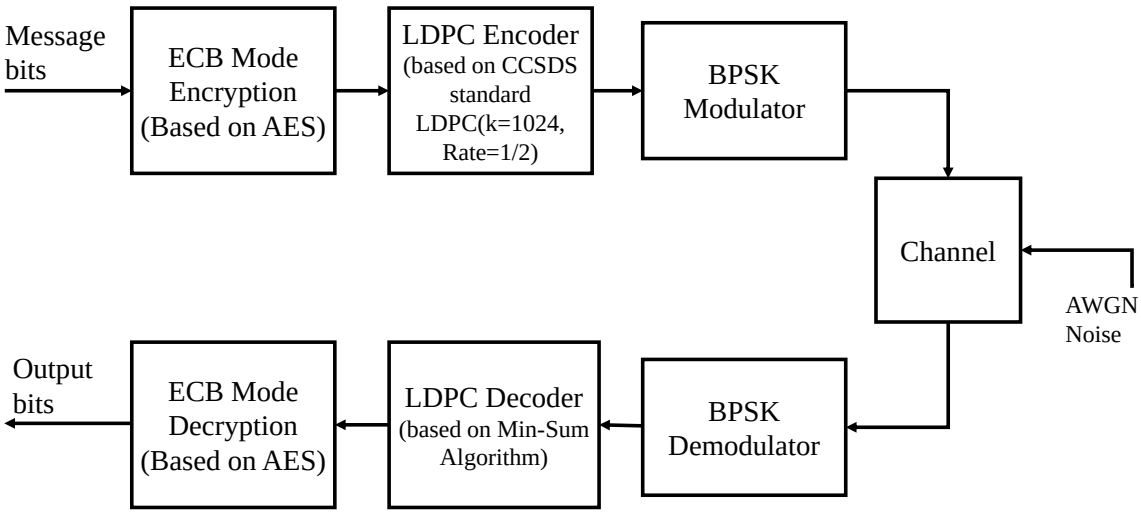

Figure 5.3: Block diagram for the AWGN channel with AES based ECB mode operation, LDPC(k=1024, Rate=1/2) coding and BPSK modulation

Advanced encryption standard(AES) encryption algorithm has been used here. The AES encryption algorithm takes block of length 128 bits as input. The 128 bits input is called plaintext. There are three different key lengths 128 bits, 192 bits and 256 bits are available in AES encryption. But 128 bits key has been used in this experiment.

Here, message bits come to the input. Now, the plaintext of block length 128 bits has been passed through AES encryption method one after another. The 128 bits

plaintext has been encrypted to 128 bits ciphertext through various rounds of AES encryption algorithm using 128 bits length keys. Then ciphertexts have been stored. After that total 1024 bits length encrypted message has been passed through LDPC encoder. The Rate 1/2 LDPC encoder with information block length(k) 1024 bits has been used in this experiment. The LDPC code has been used here is CCSDS standard. Then the encoded signal has been passed through BPSK modulator and the modulator has modulated it. The modulated signal has been sent through communication channel. The communication channel has been affected by AWGN noise. At the receiver end, the noise corrupted signal has been detected by BPSK demodulator. Then the demodulated signal has been passed through LDPC decoder which is based on min-sum algorithm and some errors have been corrected by the LDPC decoder. After that the decoded data block of length 1024 bits has been stored. Then 128 bits block from decoded data has been passed through AES decryption method one after another. They can be stored. Then the decrypted output bits have been compared with the original message bits and BER has been calculated. The measured BER values have been shown in Table 5.2.

E_b/N_0(dB)	BER(BPSK)
0	0.5001
0.2	0.4975
0.4	0.5012
0.6	0.5004
0.8	0.5005
1	0.5021
1.2	0.4986
1.4	0.4993
1.6	0.4993
1.8	0.4939
2	0.4732
2.2	0.4296
2.4	0.2703
2.6	0.1601
2.8	0.0253
3	0.005313

Table 5.2: BER measurement for the AWGN channel with AES based ECB mode operation, LDPC(k=1024, Rate=1/2) coding and BPSK modulation

A graphical representation of BER vs E_b/N_0, based on simulation result, has been shown in Fig. 5.4.

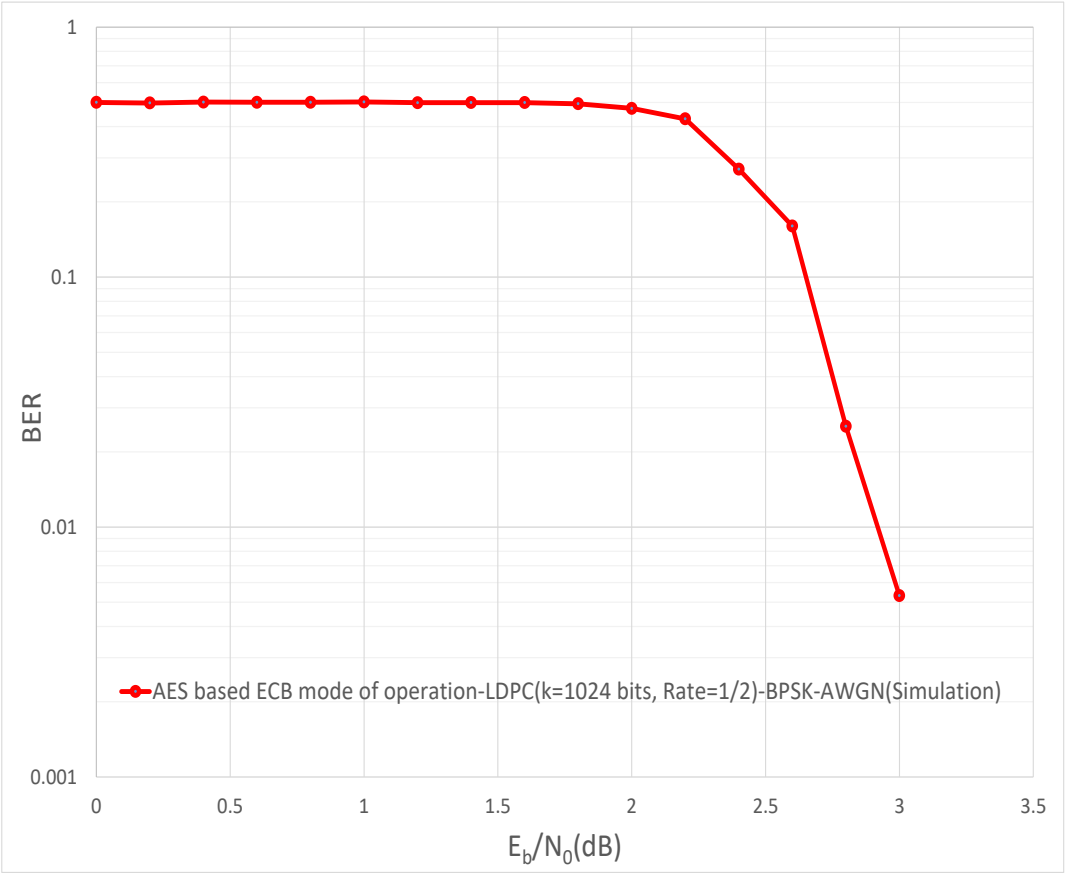

Figure 5.4: BER vs E_b/N_0 graph for the AWGN channel with AES based ECB mode operation, LDPC(k=1024, Rate=1/2) coding and BPSK modulation

It can be seen from the graphs(Fig. 5.2 and Fig. 5.4) that the BER performance of only LDPC(K=1024, rate=1/2) coded channel is better than BER performance of the channel with AES based ECB mode operation and LDPC(K=1024, rate=1/2) coding. BPSK modulation has been considered as the modulation scheme and AWGN noise has been considered as the channel noise in both the cases.

Message bits are encrypted by AES algorithm and then the encrypted bits are

encoded by the LDPC encoder. The encoded signal has been modulated by BPSK modulator. The modulated signal has been sent through the communication channel and noise corrupted by AWGN. The noise corrupted signal has been demodulated by BPSK demodulator. Then demodulated signal has been decoded by the LDPC decoder. The LDPC decoder tries to correct errors. Now, after decoding if there are some errors present in the decoded data, the erroneous data block is passed through the AES decryption. There are ten rounds in AES decryption. First nine rounds each consists of the following four subprocesses as shown below.

- Inv-ShiftRows
- Inv-SubBytes
- AddRoundKey
- Inv-MixColumns

Now Inv-MixColumns is not present in the tenth round of AES decryption. Tenth round consists of the following subprocesses.

- Inv-ShiftRows
- Inv-SubBytes
- AddRoundKey

So the errors propagates through the subprocesses in the rounds. The errors are increasing by propagating through the rounds. Finally there are large number of errors present in the recovered plaintext. So BER is increased. As a result BER performance is degraded. So, BER performance of only LDPC(K=1024, rate=1/2) coded channel is better than BER performance of the channel with AES based ECB mode operation and LDPC(K=1024, rate=1/2) coding.

5.3 AWGN Channel with AES Based Counter (CTR) Mode of Operation, CCSDS Standard LDPC(k=1024, Rate=1/2) Channel Coding and BPSK Modulation

BER performance of the communication channel with AES based CTR mode of operation and LDPC(k=1024, rate=1/2) coding has been discussed. Here AWGN has been considered as channel noise and BPSK has been considered as the modulation technique in this experiment.

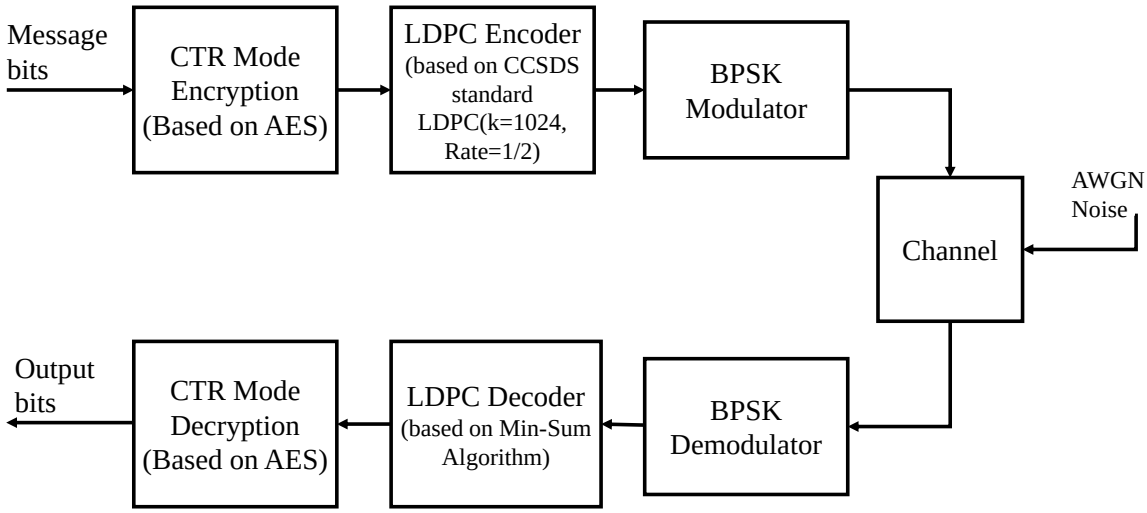

Figure 5.5: Block diagram for the AWGN channel with AES based CTR mode operation, LDPC(k=1024, Rate=1/2) coding and BPSK modulation

Advanced encryption standard(AES) encryption algorithm has been used in this experiment. 128 bits, 192 bits and 256 bits length keys are available in AES encryption. But 128 bits key has been used in this experiment. The AES encryption algorithm takes block of length of 128 bits as input.

In counter(CTR) mode operation, the counter initiates 128 bits value every time of operation. The 128 bits counter value has been encrypted by AES encryption first. Then the encrypted block of length 128 bits has been XORed with 128 bits plaintext block and 128 bits ciphertext has been produced. The ciphertexts have been

stored. Then 1024 bits encrypted message has been passed through the LDPC encoder. CCSDS standard LDPC($rate = 1/2$, k=1024) code based LDPC encoder has been used here. Then the encoded signal has been passed through BPSK modulator. The BPSK modulated signal has been sent through AWGN noise affected communication channel. So the signal has been corrupted by AWGN noise. The noise corrupted signal has been received by BPSK demodulator at the receiver side and then the demodulator has demodulated the signal. The BPSK demodulated signal has been passed through LDPC decoder which is based on min-sum algorithm. Then decoded information block of 1024 bits has been stored. Now 128 bits data block has been passed through counter(CTR) mode decryption one after another. Here in counter mode decryption, the counter has initiated same 128 bits values initiated at the time of counter mode encryption process every time of operation. Now the 128 bits counter value has been passed through AES encryption block first in counter mode decryption. Then the 128 bits output of the AES encryption block has been XORed with 128 bits of LDPC decoder decoded data. The XORed output has been considered as the counter mode decryption output. Now the counter mode decrypted output bits have been compared with the original message bits to find BER. The measured BER values have been shown in Table 5.3.

E_b/N_0(dB)	BER(BPSK)
0	0.1865
0.2	0.1768
0.4	0.1703
0.6	0.1656
0.8	0.1597
1	0.1564
1.2	0.1515
1.4	0.1448
1.6	0.1383
1.8	0.1312
2	0.1216
2.2	0.09144
2.4	0.05456
2.6	0.03204
2.8	0.01388
3	0.005381

Table 5.3: BER measurement for the AWGN channel with AES based CTR mode operation, LDPC(k=1024, Rate=1/2) coding and BPSK modulation

BER vs E_b/N_0 graph has been shown in Fig. 5.6. The graph is based on simulation result.

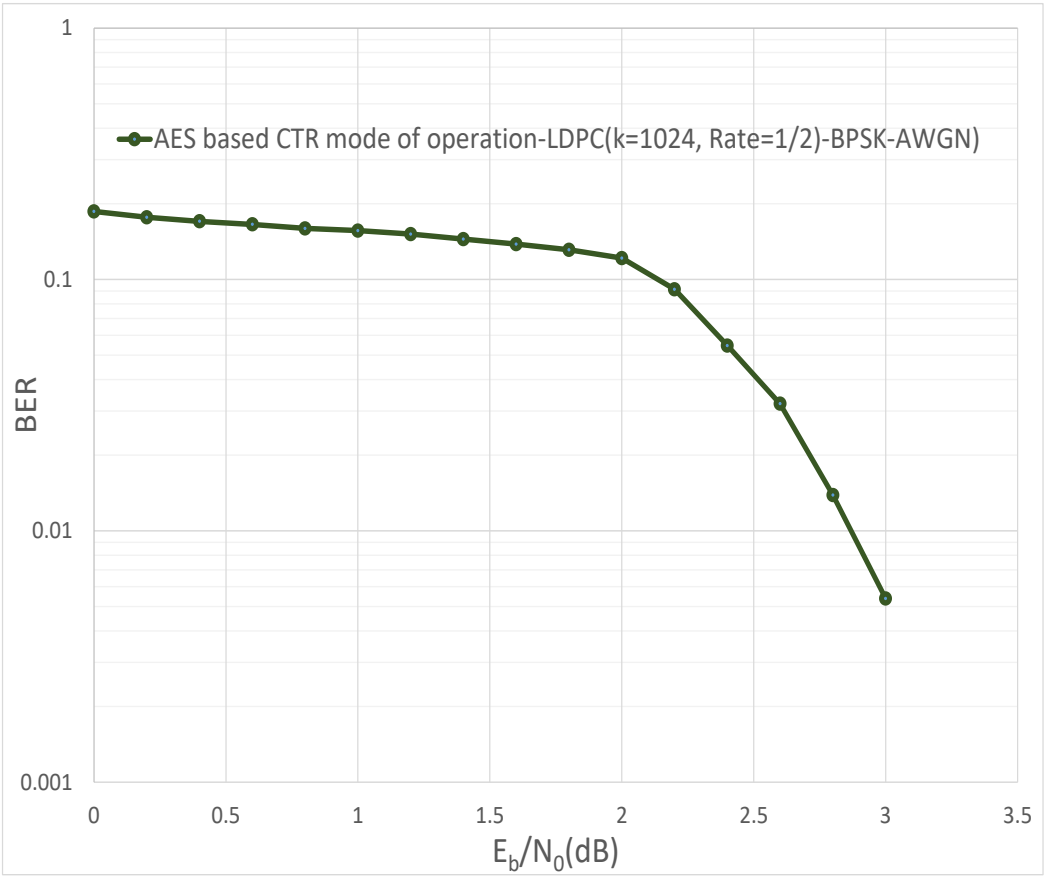

Figure 5.6: BER vs E_b/N_0 graph for the AWGN channel with AES based CTR mode operation, LDPC(k=1024, Rate=1/2) coding and BPSK modulation

It can be seen from the graphs(Fig. 5.2 and Fig. 5.6) that there is no big difference between BER performance of only LDPC(K=1024, rate=1/2) coded channel and BER performance of the channel with AES based CTR mode operation and LDPC(K=1024, rate=1/2) coding. BPSK modulation has been considered as the modulation scheme in both the cased and AWGN noise has been considered as the channel noise in both the cases.

When the AWGN noise corrupted signal has come to BPSK demodulator, the demodulator has demodulated the noise corrupted signal. Then the demodulated signal has been passed through LDPC min-sum based decoder. The LDPC decoder has decoded the demodulated signal. Here the LDPC min-sum decoder tries to correct some errors from the corrupted data. After that the decoded data has been passed through AES based counter(CTR) mode decryption. Here in AES based counter mode decryption, one AES encryption block presents. the counter initiated values goes through the AES encryption block and the subprocesses of AES encryption. After that AES encrypted data has been XORed with decoded data and the output is the AES based counter(CTR) mode decryption output. So the LDPC decoded data only goes through XOR operation in AES based counter mode decryption. The errors present in LDPC decoded data are not distributed through the counter mode decryption process. As a result there is no big difference between the BER performance of this case and BER performance of only LDPC case.

5.4 AWGN Channel with AES Based Cipher Block Chaining(CBC) Mode of Operation, CCSDS Standard LDPC(k=1024, Rate=1/2) Channel Coding and BPSK Modulation

BER performance of the communication channel with AES based CBC mode of operation and LDPC(k=1024, rate=1/2) coding has been discussed. Here AWGN has been considered as channel noise and BPSK has been considered as the modulation technique in this experiment.

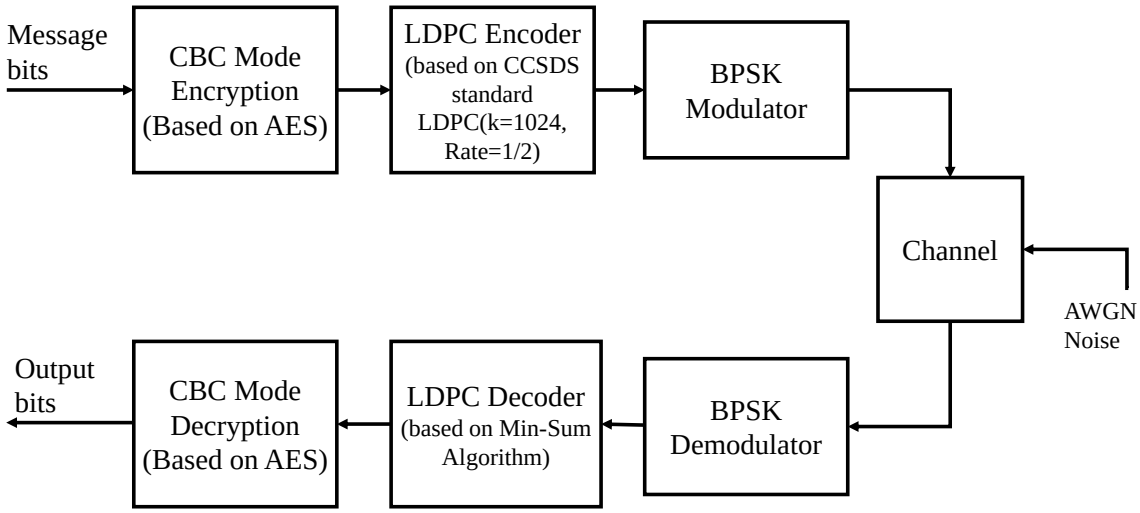

Figure 5.7: Block diagram for the AWGN channel with AES based CBC mode operation, LDPC(k=1024, Rate=1/2) coding and BPSK modulation

Advanced encryption standard(AES) encryption algorithm has been used in this experiment. There are three types of keys 128 bits, 192 bits and 256 bits are available in AES encryption. But 128 bits key has been used in this experiment. The AES encryption algorithm takes block of length 128 bits as input.

In AES based cipher block chaining(CBC) mode encryption an 128 bits initial vector has been considered at first. Then the initial vector has been XORed with 128 bits plaintext block. The XORed output value has been passed through AES encryption block. The first ciphertext block of length 128 bits has been produced at the

output of the AES encryption block. Then the first 128 bits ciphertext block has been XORed with the next 128 bits plaintext block and the XORed output has been passed through AES encryption block to get the second cipher text block. Each plaintext is XORed with the previous ciphertext block and the output has been passed through the AES encryption block to get the next ciphertext block and encrypted blocks are stored. After that total 1024 bits length encrypted message has been passed through LDPC encoder. The Rate 1/2 LDPC encoder with information block length(k) 1024 bits has been used in this experiment. Then the encoded signal has been modulated using BPSK modulator and the output has been sent through communication channel. AWGN noise has been added with the signal in the communication channel. After that the noisy signal has been detected by BPSK demodulator. Then the demodulated signal has been passed through LDPC decoder which is based on min-sum algorithm. Here some errors have been corrected by the LDPC decoder. After that the decoded data block of length 1024 bits has been stored. Then, in AES based CBC mode decryption, first 128 bits block of LDPC decoder decoded data has been passed through AES decryption block. Output of length 128 bits of the AES decryption block has been XORed with the 128 bits initial vector and first 128 bits AES based CBC mode decrypted plaintext block has been received. Now next 128 bits LDPC decoder decoded block has been passed through AES decryption block and the output of the AES decryption block has been XORed with previous 128 bits LDPC decoder decoded data and the second 128 bits AES based CBC mode decrypted output has been produced. To get plaintext blocks further, the 128 bits LDPC decoded data blocks has been passed through AES decryption block and the output of the AES decryption block has been XORed with the previous 128 bits block of LDPC decoder decoded data. After that BER has been computed by comparing the original message bits with the AES based CBC mode decrypted output bits. The measured BER values have been shown in Table 5.4.

E_b/N_0(dB)	BER(BPSK)
0	0.5
0.2	0.4994
0.4	0.4993
0.6	0.4964
0.8	0.4999
1	0.5001
1.2	0.5008
1.4	0.5002
1.6	0.4995
1.8	0.4988
2	0.4643
2.2	0.4177
2.4	0.2442
2.6	0.1281
2.8	0.05539
3	0.02497

Table 5.4: BER measurement for the AWGN channel with AES based CBC mode operation, LDPC(k=1024, Rate=1/2) coding and BPSK modulation

Based on simulation result, a graphical representation of BER vs E_b/N_0 graph has been shown in Fig. 5.8.

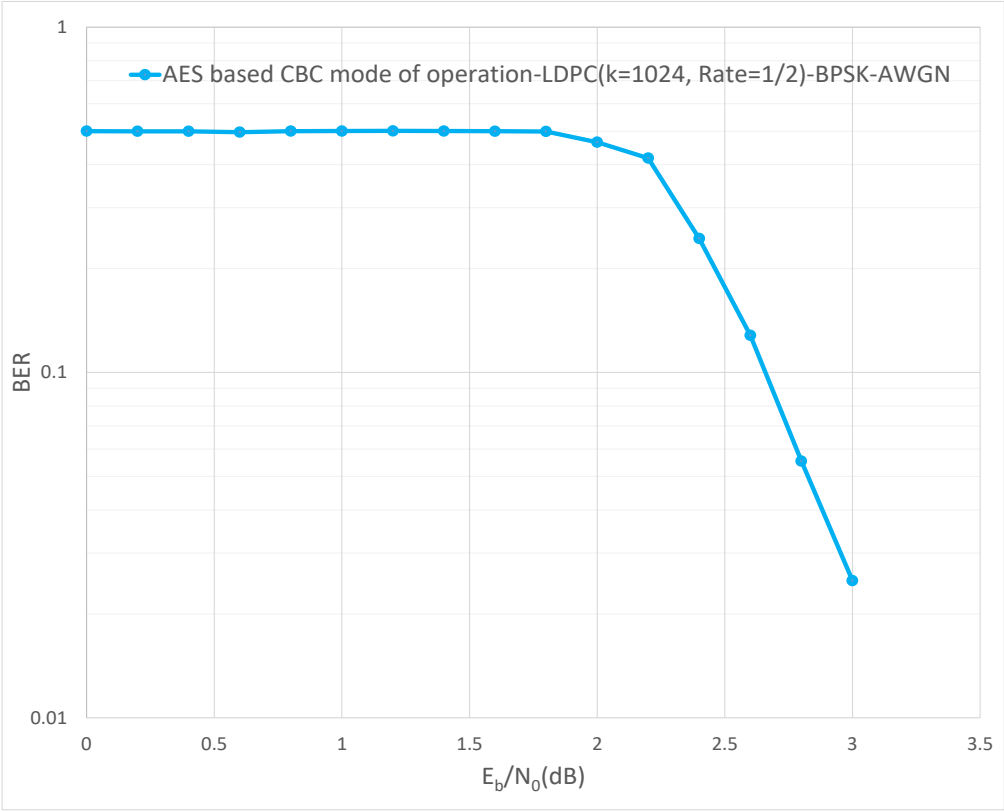

Figure 5.8: BER vs E_b/N_0 graph for the AWGN channel with AES based CBC mode operation, LDPC(k=1024, Rate=1/2) coding and BPSK modulation

It can be seen from the graphs(Fig. 5.2 and Fig. 5.8) that the BER performance of only LDPC(K=1024, rate=1/2) coded channel is better than BER performance of the channel with AES based CBC mode operation and LDPC(K=1024, rate=1/2) coding. In both the cases, BPSK modulation has been considered as the modulation scheme and AWGN noise has been considered as the channel noise .

The AWGN noise corrupted signal has been detected by the BPSK demodulator. Then the LDPC decoder has decoded the demodulated signal. The decoder tries to correct some errors here. The LDPC decoder decoded data has been passed through

the AES based CBC mode decryption process. At first, 128 bits LDPC decoded data goes through the AES decryption block in CBC mode decryption. The LDPC decoded data goes through the subprocesses of AES decryption block. So if some errors are present in LDPC decoded data, errors are increased after goes through the subprocesses. After that the output of AES decryption block has been XORed with initial vector to get the first 128 bits AES based CBC mode decrypted data block.
To get the second AES based CBC mode decrypted data block, next 128 bits LDPC decoded data blocks has been passed through various subprocesses of AES decryption block and as a result of errors are increased. Then the output of AES decryption block has been XORed with the previous 128 bits LDPC decoded data. So if there are errors present in the decoded blocks, the errors are increased further. This process will go on. So the errors propagate through the whole process of AES based CBC mode decryption and the errors are increased. So BER performance of only LDPC(K=1024, rate=1/2) coded channel is better than BER performance of the channel with AES based CBC mode operation and LDPC(K=1024, rate=1/2) coding.

5.5 AWGN Channel with HDNM8 Based Counter (CTR) Mode of Operation, CCSDS Standard LDPC (k=1024, Rate=1/2)Channel Coding and BPSK Modulation

BER performance of the communication channel with HDNM8 based CTR mode of operation and LDPC(k=1024, rate=1/2) coding has been discussed. Here AWGN has been considered as channel noise and BPSK has been considered as the modulation technique in this experiment.

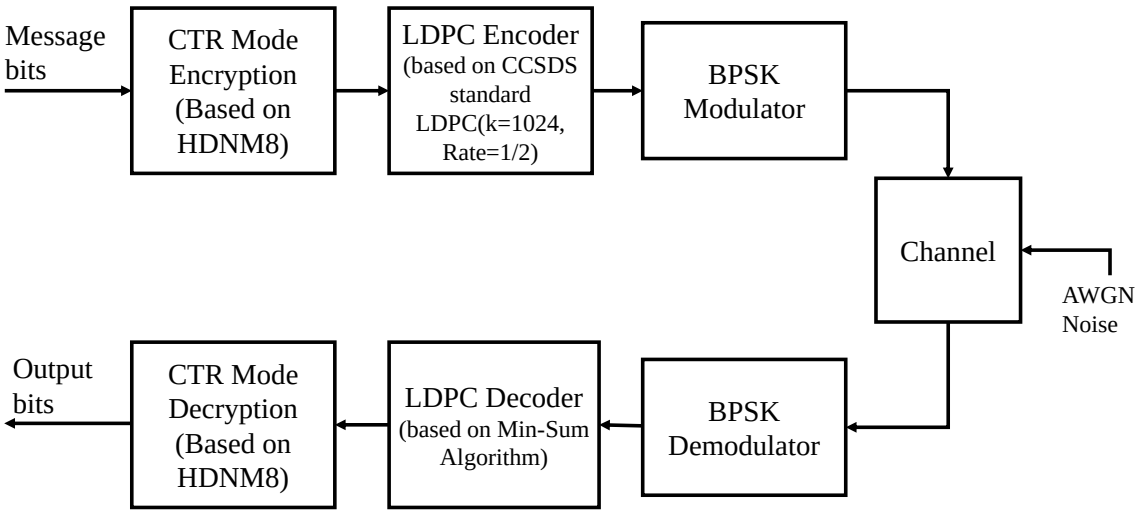

Figure 5.9: Block diagram for the AWGN channel with HDNM8 based CTR mode operation, LDPC(k=1024, Rate=1/2) coding and BPSK modulation

In HDNM8 based counter(CTR) mode operation, the counter initiates 128 bits value every time of operation. Now, the 128 bits counter value has been encrypted by HDNM8 encryption algorithm. Then the encrypted block of length 128 bits has been XORed with 128 bits plaintext block and 128 bits ciphertext has been produced and stored. Then 1024 bits encrypted message has been passed through the LDPC encoder. Here CCSDS standard LDPC($rate$ = 1/2, k=1024) code based LDPC encoder has been considered. Then the encoded signal has been passed through BPSK

modulator. Then BPSK modulated signal has been sent through communication channel and corrupted by AWGN noise. Then BPSK demodulator has received the noisy signal at the receiver side. The BPSK demodulated signal has been passed through LDPC decoder which is based on min-sum algorithm. Then decoded information block of 1024 bits has been stored and divided into 128 bits data block for decryption. Here in counter mode of decryption, the counter has initiated same 128 bits values initiated at the time of counter mode encryption process every time of operation. Now the 128 bits counter value has been passed through HDNM8 encryption block first in counter mode decryption. Then the 128 bits output of the HDNM8 encryption block has been XORed with block of 128 bits LDPC decoder output data. Now, decrypted output bits have been compared with the original message bits to find BER. The measured BER values have been shown in Table 5.5.

E_b/N_0(dB)	BER(BPSK)
0	0.1825
0.2	0.1775
0.4	0.1729
0.6	0.1685
0.8	0.1613
1	0.1583
1.2	0.1531
1.4	0.1431
1.6	0.139
1.8	0.1306
2	0.1185
2.2	0.0953
2.4	0.06023
2.6	0.03081
2.8	0.008203
3	0.002432

Table 5.5: BER measurement for the AWGN channel with HDNM8 based CTR mode operation, LDPC(k=1024, Rate=1/2) coding and BPSK modulation

A graphical representation of BER vs E_b/N_0, based on simulation result, has been shown in Fig. 5.10.

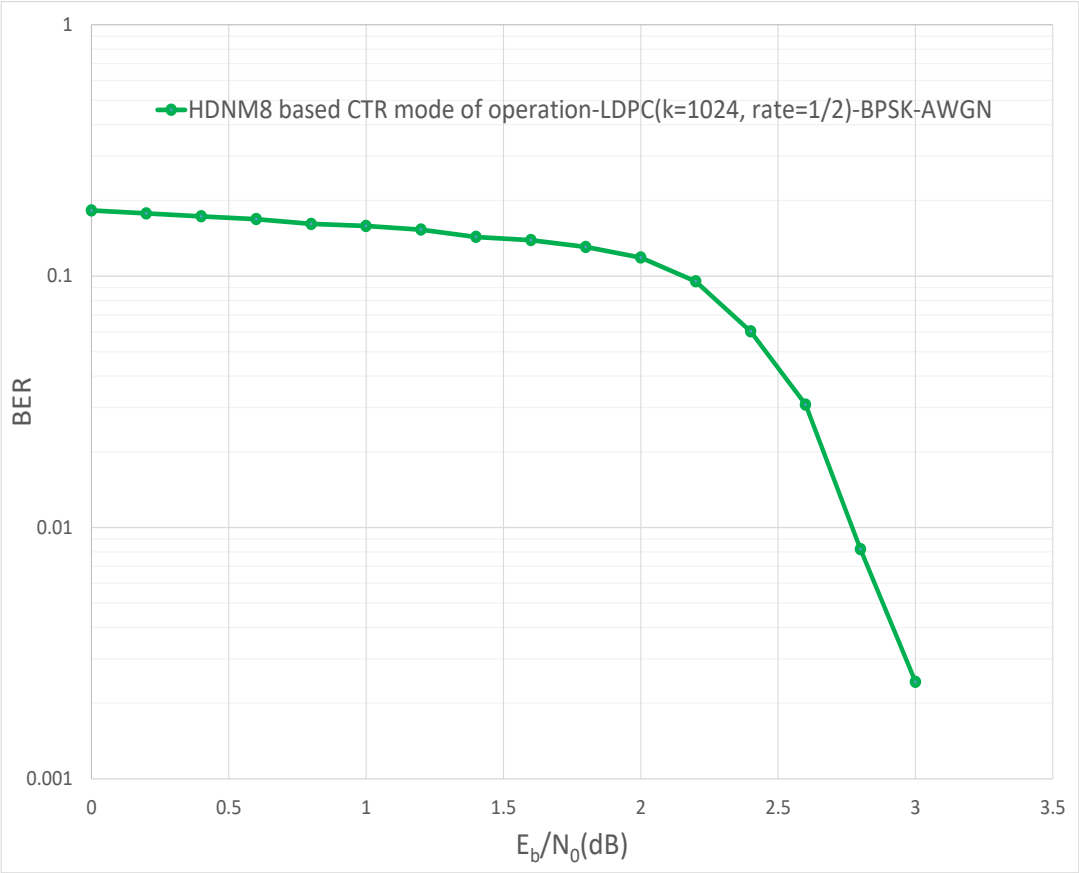

Figure 5.10: BER vs E_b/N_0 graph for the AWGN channel with HDNM8 based CTR mode operation, LDPC(k=1024, Rate=1/2) coding and BPSK modulation

It can be seen from the graphs(Fig. 5.2 and Fig. 5.10) that there is small difference between BER performance of only LDPC(K=1024, rate=1/2) coded channel and BER performance of the channel with HDNM8 based CTR mode operation and LDPC(K=1024, rate=1/2) coding. In both the cases, BPSK modulation has been considered as the modulation scheme and AWGN noise has been considered as the channel noise

Here BPSK demodulator has demodulated the AWGN noise corrupted signal after receiving the signal. Then the demodulated signal has been passed through LDPC min-sum based decoder. The LDPC decoder has decoded the demodulated signal. Here the LDPC min-sum decoder tries to correct some errors from the corrupted data. After that the decoded data has been passed through HDNM8 based CTR mode decryption. Now, HDNM8 encryption block is used in HDNM8 based CTR mode decryption. Now, the counter initiated values goes through the HDNM8 encryption block in the CTR mode decryption process. After that HDNM8 encrypted data has been XORed with decoded data and the output is the counter(CTR) mode HDNM8 decryption output. So, the LDPC decoded data only goes through XOR operation in HDNM8 based CTR mode decryption. The errors present in LDPC decoded data are not distributed through the counter mode decryption process. As a result, the BER performance of this case and BER performance of only LDPC case are nearly similar.

5.6 Conclusion

BER performance analysis of LDPC(k=1024, rate=1/2) coded communication channel with AWGN for BPSK modulation has been done. Then BER performance analysis of the communication channel with AES based various modes(ECB mode,CTR mode,CBC mode) of operations and LDPC(k=1024, rate=1/2) coding has been done, where also AWGN has been considered as channel noise and BPSK has been considered as the modulation technique in the experiments. Then BER performance analysis of the communication channel with HDNM8 based CTR mode of operation and LDPC(k=1024, rate=1/2) coding has been done. Now, it can be seen from the experiments results that BER performance of only LDPC coded communication channel is better than uncoded channel BER performance for BPSK modulation. There is no big difference between BER performance of only LDPC case and BER performance of the case where AES based CTR mode of operation has been used. Now, BER performance of the case where AES based CTR mode of operation has been used is better than the BER performance of the case where ECB mode of operation has been used. Now, BER performance of the case where AES based CTR mode of operation has been used is also better than the BER performance of the case where CBC mode of operation has been used. BER performance of the case where HDNM8 based CTR mode of operation has been used is also very good and comparable to AES based CTR mode case.

Ning et al. [27] proposed a joint encryption and error correction model where they considered first nine rounds of AES algorithm as it is and in the tenth round they considered LDPC encoding instead of ShiftRows operation. They showed BER performance for their model is better than some old methods. However, if channel encoding is used after completing the encryption process, there is no significant difference between the BER performances of this case and their proposed model. So, it is advantageous to use the two schemes separately because any one of the schemes can be changed without affecting other scheme and this is also more flexible.

Chapter 6

Summary and Future Work

All the experiments have been simulated in MATLAB. The channels have been considered in experiments are wireless. First AWGN has been considered as channel noise and BER performance has been evaluated for MPSK and MQAM modulations. Then Rayleigh fading and AWGN noise has been considered and BER performance has been evaluated for MPSK and MQAM modulations.
BER performance of coded communication channel with AWGN noise for MPSK and MQAM has been evaluated. In this thesis, RS(255,239) code, CC(7,1/2) code and DVB-S.2 standard rate=1/2 LDPC code are considered in the experiments. Then BER performance of coded communication channel considering both Rayleigh fading and AWGN noise has been evaluated for MPSK and MQAM modulation techniques. Also, BER measurement of LDPC(k=1024, rate=1/2) coded communication channel with AWGN for BPSK modulation has been done. Then BER performance of the communication channel has been evaluated with AES based various modes(ECB mode,CTR mode and CBC mode) of operations and LDPC(k=1024, rate=1/2) coding where AWGN has been considered as channel noise and BPSK has been considered as the modulation technique in the experiments.
Another block cipher HDNM8 has also been considered. BER performance of the AWGN channel with HDNM8 based counter(CTR) mode of operation and LDPC(k=1024, rate=1/2) coding has been evaluated and here BPSK modulation has been considered.

It can be seen from experiments results, BER performance of uncoded communication channel with AWGN noise for BPSK and QPSK is same and BER performance is degraded when modulation order is increased further for MPSK modulation. For MQAM modulation, BER performances of uncoded communication channel with AWGN noise is best for QAM modulation and BER performance is degraded when

modulation order of MQAM is increased further. It is found that BER performance of communication channel with AWGN noise is better than BER performance of communication channel with Rayleigh fading and AWGN noise.
There is no significant difference between BER performance of only LDPC case and BER performance of the case where AES based CTR mode of operation has been used. Experimental results show that BER performance of the case where AES based CTR mode of operation has been used is better than the BER performance of the case where ECB mode of operation has been used. BER performance of the case where AES based CTR mode of operation has been used is also better than the BER performance of the case where CBC mode of operation has been used. BER performance of the case where AES based ECB mode of operation has been used is better than the BER performance of the case where AES based CBC mode of operation has been used. BER performance of the AWGN channel with HDNM8 based counter(CTR) mode of operation and LDPC(k=1024, rate=1/2) coding for BPSK modulation is also very good.

There are other error correcting codes also available. So, BER performance of the coded communication channel can be evaluated for them and can be compared with the used error correcting codes in the experiments. Here some experiments have been done considering Rayleigh fading channel with AWGN noise. Now other types of fading channels can be considered with AWGN noise and BER performance analysis of communication channel can be done for them. In this thesis, BER performance analysis of the communication channel with three modes of encryption has been performed. So there is a scope to measure BER considering the other mode of operations and other block and stream ciphers.

Bibliography

[1] *TM synchronization and channel coding*. CCSDS Secretariat, National Aeronautics and Space Administration, Washington, DC, USA, 2022.

[2] Hnady Mohammed Almaktof, Amer R Zerek, Amer M Daeri, and Fatima LAAS-SIRI. Ber performance comparison of m-pam over awgn and fading channels. In *2021 IEEE 1st International Maghreb Meeting of the Conference on Sciences and Techniques of Automatic Control and Computer Engineering MI-STA*, pages 802–806. IEEE, 2021.

[3] Jaydeb Bhaumik and Dipanwita Roy Chowdhury. Hdnm8: A round-8 high diffusion block cipher with nonlinear mixing function. In *Mathematics and Computing 2013*, pages 41–55. Springer, 2014.

[4] Ranjan Bose. *Information theory, coding and cryptography*. McGraw Hill Education (India) Private Limited, 2016.

[5] Franco Chiaraluce. Error correcting codes in telecommand and telemetry for european space agency missions: An overview and new perspectives. In *2014 22nd International Conference on Software, Telecommunications and Computer Networks (SoftCOM)*, pages 233–240. IEEE, 2014.

[6] CKP Clarke. Reed-solomon error correction. *BBC R&D White Paper, WHP*, 31, 2002.

[7] Lasseni Coulibaly, Fethi Ouallouche, and Vitalice Oduol. Joint cryptography and channel-coding based on low-density parity-check codes and advanced encryption standard for 5g systems. *International Journal of Electrical and Electronic Engineering & Telecommunications*, 2021.

[8] Xinyu Da, Yanling Wang, and Tiecheng Xie. Performance of ldpc codes for satellite communication in ka band. In *2009 5th International Conference on Wireless Communications, Networking and Mobile Computing*, pages 1–4. IEEE, 2009.

[9] Joan Daemen and Vincent Rijmen. *The design of Rijndael*, volume 2. Springer, 2002.

[10] Zhongliang Deng, Yanyue Yang, Ke Wang, Wenliang Lin, Ruiliang Song, and Xiaotian Zhou. A novel adaptive rate matching algorithm based on ldpc for satellite communication. In *2020 IEEE 3rd International Conference on Electronics Technology (ICET)*, pages 799–803. IEEE, 2020.

[11] Morris Dworkin. Recommendation for block cipher modes of operation. methods and techniques. Technical report, National Inst of Standards and Technology Gaithersburg MD Computer security Div, 2001.

[12] William J Ebel and William H Tranter. The performance of reed-solomon codes on a bursty-noise channel. *IEEE Transactions on Communications*, 43(2/3/4):298–306, 1995.

[13] Ranya Salah Elagooz, Ashraf Mahran, Safa Gasser, and Mohamed Aboul-Dahab. Efficient low-complexity decoding of ccsds reed–solomon codes based on justesen's concatenation. *IEEE Access*, 7:49596–49603, 2019.

[14] Yi Fang, Pingping Chen, Guofa Cai, Francis CM Lau, Soung Chang Liew, and Guojun Han. Outage-limit-approaching channel coding for future wireless communications: Root-protograph low-density parity-check codes. *IEEE Vehicular Technology Magazine*, 14(2):85–93, 2019.

[15] Robert Gallager. Low-density parity-check codes. *IRE Transactions on information theory*, 8(1):21–28, 1962.

[16] Nathaly Orozco Garzon, Henry Carvajal Mora, and Celso de Almeida. An opportunistic system to counteract fading and gaussian interference effects under different modulation schemes. *IEEE Latin America Transactions*, 16(11):2716–2721, 2018.

[17] Simon Haykin. *Digital Communication Systems* . Wiley India Pvt. Ltd., 2021.

[18] Xin Huang, Li Chen, Wenjun Chen, and Ming Jiang. Design of multilevel reed–solomon codes and iterative decoding for visible light communication. *IEEE Transactions on Communications*, 67(7):4550–4561, 2019.

[19] Yasmeen M Hussein, Ammar H Mutlag, and Basman M Al-Nedawe. Comparisons of soft decision decoding algorithms based ldpc wireless communication system. In *IOP Conference Series: Materials Science and Engineering*, volume 1105, page 012039. IOP Publishing, 2021.

[20] Suhyeon Jeon, Jeongho Kwak, and Jihwan P Choi. Cross-layer encryption of cfb-aes-turbo for advanced satellite data transmission security. *IEEE Transactions on Aerospace and Electronic Systems*, 58(3):2192–2205, 2021.

[21] Min W Kang. An exploration of error-correcting codes for use in noise-prone satellite environments. 2018.

[22] M Michael Kobayashi, Frank Stocklin, Michael Pugh, Igor Kuperman, David Bell, Salem El-Nimri, Brad Johnson, Nancy Huynh, Shane Kelly, James Nessel, et al. Nasa's high-rate ka-band downlink system for the nisar mission. *Acta Astronautica*, 159:358–361, 2019.

[23] BP Lathi and Zhi Ding. Modern digital and analog communication systems, 2010.

[24] Yong Li, Xiang Huang, Jiguang He, Hongqing Liu, and Trieu-Kien Truong. On soft-information-based error and erasure decoding of reed–solomon codes in burst rayleigh fading channels. *IEEE Transactions on Communications*, 67(1):50–60, 2018.

[25] Ranjan Kumar Mahapatra, Saritha Sairupa, and Ravi Prasad. Performance analysis of modulation schemes for wireless sensor networks. *Journal homepage: www. ijrpr. com ISSN*, 2582:7421, 2022.

[26] Masataka Nakazawa, Toshihiko Hirooka, Masato Yoshida, and Keisuke Kasai. Extremely higher-order modulation formats. *Optical Fiber Telecommunications VIB*, pages 297–336, 2013.

[27] Li Ning, Lin Kanfeng, Lin Wenliang, and Deng Zhongliang. A joint encryption and error correction method used in satellite communications. *China communications*, 11(3):70–79, 2014.

[28] Prashnatita Pal, Bikash Chandra Sahana, Jayanta Poray, and Aditi Bal. Error-control coding algorithms and architecture for modern applications powered by ldpc codes and belief propagation. In *2022 9th International Conference on Computing for Sustainable Global Development (INDIACom)*, pages 238–243. IEEE, 2022.

[29] Vinay Panwar and Sanjeet Kumar. Bit error rate (ber) analysis of rayleigh fading channels in mobile communication. *International Journal of Modern Engineering Research (IJMER) Vol*, 2, 2012.

[30] John G Proakis and Masoud Salehi. *Communication systems engineering*. 2nd edition, 2002.

[31] P Rajagopalan, Pradeesh Madavan, H Ramamurthy, and S Sudhakar. Performance analysis of ldpc decoding algorithms for ccsds telecommand space data link protocol. In *2021 2nd International Conference for Emerging Technology (INCET)*, pages 1–5. IEEE, 2021.

[32] Theodore S Rappaport et al. *Wireless communications: principles and practice*. prentice hall PTR, 2nd edition, 2010.

[33] Irving S Reed and Gustave Solomon. Polynomial codes over certain finite fields. *Journal of the society for industrial and applied mathematics*, 8(2):300–304, 1960.

[34] CCSDS Secretariat. Tm synchronization and channel coding—summary of concept and rationale. *Green Book*, 2020.

[35] Geo Niju Shanth and Saru Priya. Low complexity implementation of ldpc decoder using min-sum algorithm. *International Journal of Computer Applications*, 975:8887, 2013.

[36] Vineet Sharma, Anuraj Shrivastav, Anjana Jain, and Alok Panday. Ber performance of ofdm-bpsk,-qpsk,-qam over awgn channel using forward error correcting code. volume 2, pages 1619–1624, 2012.

[37] Bernard Sklar et al. *Digital communications*. Prentice hall Upper Saddle River, NJ, USA:, 2001.

[38] SM Usha and KR Nataraj. Bit error rate analysis using qam modulation for satellite communication link. *Procedia Technology*, 25:456–463, 2016.

[39] Bingrui Wang and Qingli Zhang. Study of performance comparison of satellite error correction codes for correcting big burst data errors. In *2018 IEEE 3rd International Conference on Big Data Analysis (ICBDA)*, pages 254–258. IEEE, 2018.

[40] Keping Yu, Takuro Sato, et al. Modeling and analysis of error process in 5g wireless communication using two-state markov chain. *IEEE Access*, 7:26391–26401, 2019.