ISSN 2047-3338

Comparative Analysis of Forward Error Correction Techniques with Direct Sequence Spread Spectrum for Secure Communication

Fabiha Hashmat[1], Fatima Hassan Butt[2] and M. Junaid Arshad[3]
[1,2,3]Department of Computer Science and Engineering, UET, Lahore-Pakistan

***Abstract*— Secure communication is one of the critical research area. A variety of techniques for secure communication are available. Communication insecurity result due to low transfer limit, no built-in redundancy or checking, jamming, interception, cross talk, interference, eavesdrop, masquerade, modification of messages, replay, denial of service and unauthorized traffic analysis. All of the above mentioned factors limit the performance of secure communication. We have addresses direct sequence spread spectrum (DSSS) for secure communication. Now for selecting best error correction technique to be used with direct sequence, analysis of different forward error correction techniques is necessary in order to determine which FEC technique will provide best results in terms of low noise. Firstly we have done Bit Error Rate (BER) analysis of Forward Error Correction (FEC) techniques namely Hamming Code, Reed-Solomon Code and Convolutional Code with the help of MATLAB/Simulink in order to determine the best error correction technique to be used with DSSS. Convolution Coding technique is used as it better withstand noise with low E_b/N_o as it gave us a BER=0 for E_b/N_o =12dB. It was also observed that due to spreading technique the signal was transmitted at strength lower than the noise floor of the system which makes it a secure communication without any unauthorized interceptions. We have analyzed the signal was retrievable at the receiver side with less error rate as result of Convolutional FEC technique used with DSSS and undetectable during transmission as it is transmitted below noise floor of the system. In the end we have calculated system budget from transmitter to the receiver separated by a distance of 1m by taking account of all the gain and losses from transmitter to the receiver end.**

***Index Terms*— DSSS, Secure, BER, FHSS and Spreading**

I. INTRODUCTION

COMMUNICATION security is applied to prevent intruders from unauthorized interceptions while still transmitting to the receiver. Communication security is a necessary requirement of defense communication systems, industrial automation systems, global positioning systems and avionics systems. Communication security in the above mentioned systems is to ensure sensitive data protection from unauthorized access, cyber threats and attacks, illegal interception, exploitation, eavesdropping, jamming, masquerade, modification of messages, replay, denial of service and unauthorized traffic analysis.

A variety of techniques for secure communication are available namely spread spectrum, digital signature, encipherment, authentication exchange, notarization, traffic padding, routing control and steganography. We have addressed spread spectrum technique in our research work for secure communication between transmitter and receiver. In Spread spectrum technique, greater bandwidth is used for transmission signal as compare to modulating signal. It is a digital modulation technique [1]. It spreads the transmitted signal on a wide frequency band. In this signal power is maintained while consuming more bandwidth than the modulated signal. The signal is buried in the noise floor of the system, therefore it does not have distinguishable peak like narrow band signal. Spread spectrum signal is difficult to detect, intercept, jam and distinguish because it is transmitted below noise level (Fig. 1).

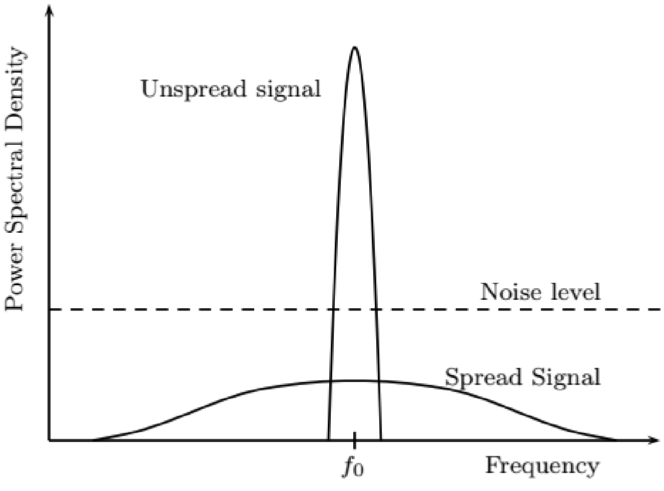

Fig. 1. Spread Signal [2]

There are two types of spread spectrum techniques.

1. FHSS: Frequency Hopping Spread Spectrum
2. DSSS: Direct Sequence Spread Spectrum

In frequency hopping spread spectrum signal is switched among different frequency channels rapidly. In direct sequence spread spectrum rapid phase transition is performed. Direct Sequence Spread Spectrum (DSSS) techniques have advantages over Frequency Hopping Spread Spectrum (FHSS). Frequency Hopping Spread Spectrum (FHSS) has low transfer limit as compare to Direct Sequence Spread Spectrum (DSSS) as well as it has no error checking mechanism. In this paper we are considering Direct Sequence Spread Spectrum (DSSS) as a secure communication technique.

The organization of this paper is as specified below. In Section II brief literature review of techniques used for secure communication is provided. Section III provides an overview of Direct Sequence Spread Spectrum (DSSS) as a secure communication technique. Mechanism of spreading and de-spreading of signal is discussed. In Section IV Bit Error Rate (BER) analysis of different Forward Error Correction (FEC) techniques namely Hamming Code, Reed-Solomon Code and Convolutional Code is done to determine the best error correction technique to be used with Direct Sequence Spread Spectrum (DSSS). Section V provides link budget analysis of the proposed secure communication system. Lastly the paper is summarized in Section VI.

II. LITERATURE REVIEW

The subject of secure communication is an active area of research. Although many techniques have been employed for communication but they have many pros and cons but this technique is under consideration due to its benefits over the others. Many researchers have done Bit Error Rate analysis of DSSS by applying different FEC techniques and other methods for efficient and secure communication system.

Jaorsa Sousa [3] has proposed a stochastic frequency hopping geometrical mathematical model that ensures secure packet transmission by eliminating the effect of jammers.

Song Fang's[4] has done wireless communication under broad band jamming attacks. According to his research DSSS and FHSS will eventually fail to provide communication under high transmitting power jammers. These jammers jam all the available transmission frequencies. He proposed an anti-jamming system which eliminates the effect of such jammers.

M.Hassan [5] presented implementation of Frequency hopping and Direct sequence for the purpose of secure transmission. Spread spectrum provides the advantage in security, message privacy, resolution, ranging and anti-jamming. PN sequence is used for secure data transmission. The longer the PN sequence spreading, harder it will be detected. Bit error analysis should be done before selecting a particular FEC technique for error checking as less BER results in higher SNR and better communication quality. FHSS has relatively low transfer limit as compare to DSSS since so much information can be sent over any given frequency it does not provide any built in mechanism for error checking or the redundancy.

Research on spread spectrum cryptography and information hiding was done by Laurent Dubreil and Thierey P. Berger [2]. They suggested that instead of using a cryptographically secure PN sequence, one should directly use a PN sequence. In practical applications there are some problems of synchronization with such a PN sequence because of large period sequence.

A survey of security mechanisms with DHSSS shows that the growing size of the wireless network demands the security to be made a part of the network layer. The immediate need of a solution for this problem lead to the introduction of spread spectrum. The paper in question has made a comparison of the two of the most famous spread spectrum the DSSS (direct sequence spread spectrum) and WDSSS (watermark direct spread spectrum) [6].

M.I. Yousef [7] used DSSS technique with residue number system. According to their analysis performance degradation occur at a rate of 31.5 dB with BER = 10^{-5}. The effected of noise generated by the jammer was eliminated by forward error correction techniques. There is an improvement in performance with a factor of 2 dB where BER = 10^{-5} using residue number system. They proved that residue number system improves SNR by decreasing the probability of BER.

Phongnauim Benprom and CharratPinthong [8] have done analysis of DSSS technique while using convolutional code as a FEC technique under the influence of BPSK jamming signal. With the help of convolutional code the BER of signal is improved at a rate of 4 dB with BER = 10^{-6}.

T.A. Shanmugasundarem and Alamelu Nachaiappan[9] have done BER analysis of DSSS-FEC. They have done performance analysis of BER for FEC coded coherent, non-coherent under Rayleigh fading channel and Non-coherent under Rician fading channel. According to their results, the Reed Solomon Code used for FEC gives good performance of BER when used with Rayleigh fading but on the other hand its performance is not suitable for Racian fading.

Sanjeev Kumar and Ragini Gupta [10] have done BER analysis by using Reed Solomon code in order to encode data streams in digital communication. They evaluated performance by BPSK modulation over AWGN channel. Performance analysis of RS code is done for different codes in MATLAB. Simulation of RS with Different code rate is being evaluated (i.e. 0.96, .878, .80 and .647) with constant block length which is 255. Results show that by decreasing code rate and keeping block length constant, BER performance improves.

III. DIRECT SEQUENCE SPREAD SPECTRUM (DSSS)

In DSSS data is made available in much greater bandwidth through rapid phase transition. Time period and bandwidth of signal are inversely proportional in relation. So as the time period reduces, the bandwidth increases which can be explained by Nyquist criteria.

$$R = \frac{1}{T} = 2B \qquad (1)$$

Where, T= Time Period of signal, B= Bandwidth of signal

To spread the frequency, signal is multiplied by pseudorandom binary waveform. Pseudorandom is a random noise signal which is called a PN signal. The output of the PN signal is called chip rate. Processing gain of signal is the ratio of chip rate to the bit rate of the signal. To retrieve the signal at the receiver end, spreading is removed by generating replica phase lock of pseudorandom spread signal.

IV. BIT ERROR RATE (BER) ANALYSIS AND SPREADING

In digital data transmission, performance criterion is determined by Bit Error Rate (BER) and Bit Energy to Noise Power Density Ratio E_b/ N_o.

$$BER = \frac{\text{Number of Error Bits}}{\text{Number of Total Bits}} \qquad (2)$$

Noise in the transmission channel causes error bits. Signal to Noise Ratio (SNR) describes the relation between noise and signal.

$$SNR = \frac{\text{Signal Power}}{\text{Noise Power}} \qquad (3)$$

SNR is inversely proportional to BER. For better communication quality, BER should be low as it results in high SNR. There are two types of Forward Error Correction (FEC) techniques: i) Block Codes, ii) Convolutional Codes

There are many types of block codes such as Hamming Code, Parity Code, Polynomial Code, Reed-Solomon Code, Reed Muller Code and Perfect Code. This section analyzes and simulates the performance of Quadrature Phase Shift Keying (QPSK) using three types of Forward Error Correction (FEC) techniques which are Hamming code, Reed-Solomon code and Convolutional code in order to yield the best performance criterion in terms of BER as well as E_b/N_o. Communication is said to be reliable if it has BER which lies in the range of less than or equal to 10^{-6}. Mathematical formula for calculating BER at certain signal power is as follows. Error Rate calculation is done over AWGN channel.

$$P_b = Q\sqrt{\frac{2E_b}{N_o}} \qquad (4)$$

A) Error Rate Calculation in QPSK Modulated Channel

Quadrature Phase Shift Keying is a type of digital modulation. In this scheme 2 bits are modulated out of 4 possible carrier shifts (0,90,180,270 degrees). Block Diagram of QPSK modulation is shown in Fig. 2.

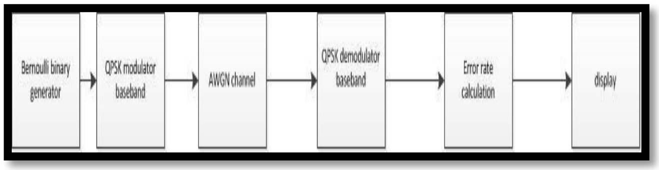

Fig. 2. Block Diagram of QPSK Modulation

For Error Rate Calculation of QPSK Modulated Channel below mentioned parameters in Table I are used.

TABLE I
FUNCTION BLOCK PARAMETERS: AWGN CHANNEL (QPSK)

Parameter	Value
Input Processing	Columns as channels (frame based
Initial Speed	67
Mode	Signal to Noise Ratio Eb/N_0
Eb/N_0	16
Number of Bits per symbol	1
Input Signal Power, referenced to 1 ohms (watts)	1

However in Simulink we can see the BER at the display block as shown below in Fig. 3.

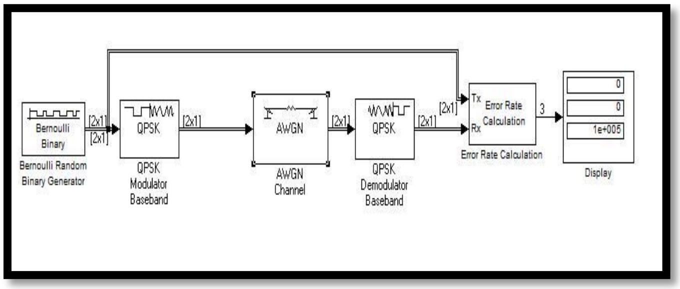

Fig. 3. Error Rate Calculation in QPSK Modulated Channel

The Simulink result shows that the BER = 0 for Eb/ N_o =16 dB. Graphical analysis of BER Vs SNR without coding is shown in Fig. 4.

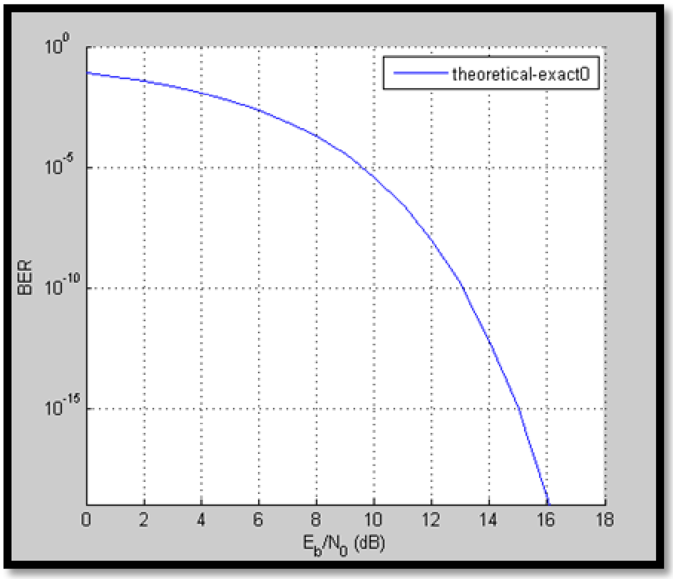

Fig. 4. Graphical Analysis of BER Vs SNR without Coding

B) Error Rate Calculation of Hamming Code

Hamming Code is a linear error correcting code. It's error detecting rate is up to 2 bit and correcting rate is up to 1 bit. . Block Diagram of Hamming Code is shown in Fig. 5.

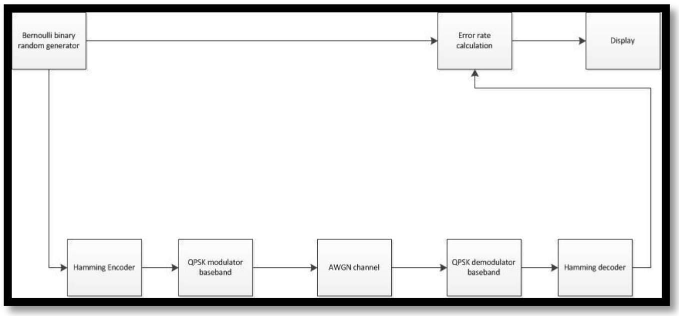

Fig. 5. Block Diagram of Hamming Code

For Error Rate Calculation of Hamming Code over AWGN channel below mentioned parameters in Table II are used.

TABLE II
FUNCTION BLOCK PARAMETERS: AWGN CHANNEL (HAMMING CODE)

Parameter	Value
Input Processing	Columns as channels (frame based
Initial Speed	67
Mode	Signal to Noise Ratio Eb/N$_0$
Eb/N$_0$	13
Number of Bits per symbol	1
Input Signal Power, referenced to 1 ohms (watts)	1
Symbol Period(s)	0.1

Model of Hamming Code using Simulink is shown in Fig. 6.

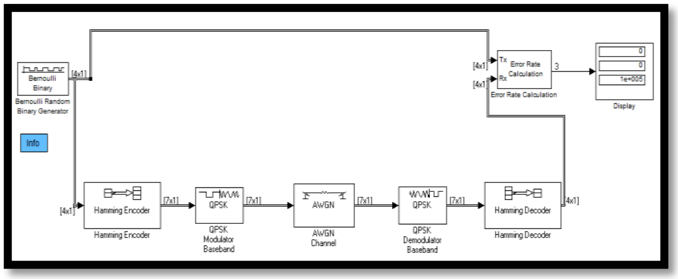

Fig. 6. Model of Hamming Code using Simulink

When channel encoder is not used the system provides us Eb/N$_o$= 16dB bearing no errors. Below this signal strength, the Gaussian noise of the channel starts effecting the transmitted signal. Since hamming encoder provides us Eb/N$_o$ of 13 dB with no errors, hence this channel encoding technique gives us the processing gain of 3 dB. This is shown in the plot of BER vs Eb/N$_o$ of Hamming (7,4) Code in Fig. 7.

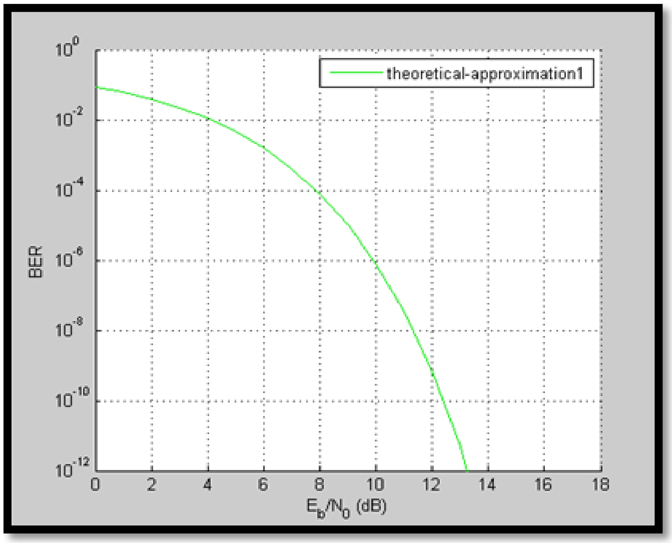

Fig. 7. Graphical Analysis of BER Vs SNR in Hamming Code

C) Error Rate Calculation in Reed-Solomon Code

Reed-Solomon Code is a non-binary cyclic error correcting code. In transmitted signal it adds t check symbols which have the capability to detect any error combination up to t. It's error correcting capability is [t/2] symbols. Block Diagram of Reed-Solomon Code is shown in Fig. 8.

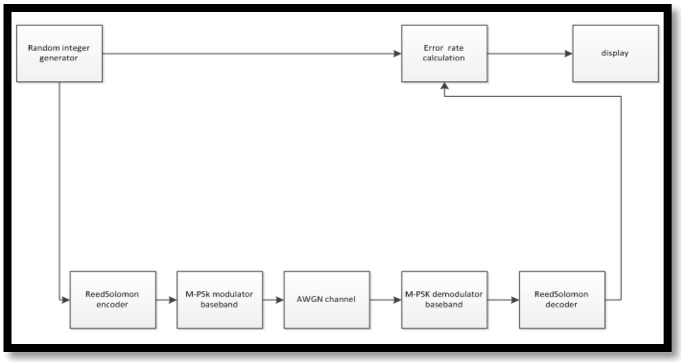

Fig. 8. Block Diagram of Reed-Solomon Code

TABLE III
FUNCTION BLOCK PARAMETERS: AWGN CHANNEL (REED-SOLOMON CODE)

Parameter	Value
Input Processing	Columns as channels (frame based
Initial Speed	67
Mode	Signal to Noise Ratio Eb/N$_0$
Eb/N$_0$	15
Number of Bits per symbol	1
Input Signal Power, referenced to 1 ohms (watts)	1
Symbol Period(s)	1

For Error Rate Calculation of Reed-Solomon Code over AWGN channel below mentioned parameters in Table III are used. Model of Reed-Solomon Code in Simulink is shown in Fig. 9.

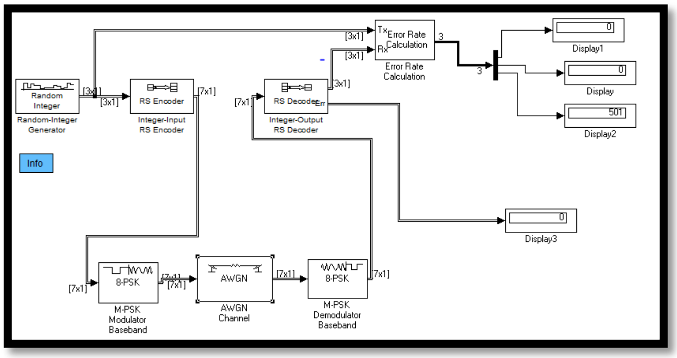

Fig. 9. Model of Reed-Solomon Code in Simulink

Since Reed-Solomon encoder provides us Eb/N$_o$ of 15 dB with no errors, hence this channel encoding technique gives us the processing gain of 1 dB only. This is shown in the plot of BER Vs Eb/N$_o$ of Reed-Solomon Code in Fig. 10.

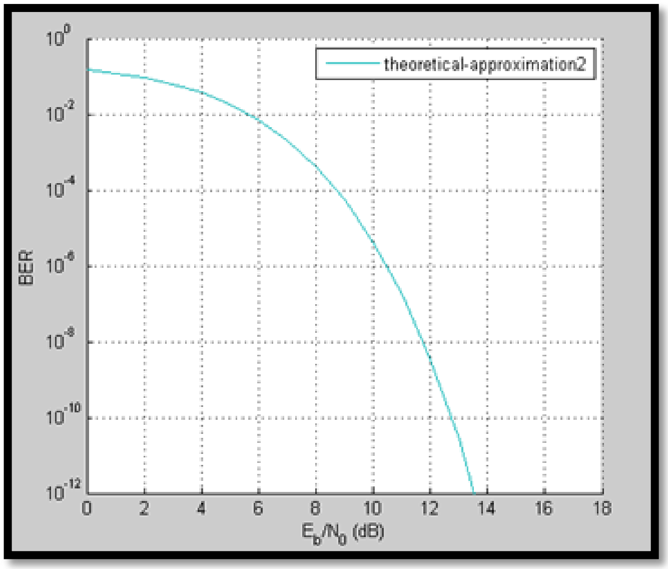

Fig. 10. Graphical Analysis of BER Vs SNR in Reed-Solomon Code

D) Error Rate Calculation of Convolutional Code

Convolutional Code generates parity check symbols by Boolean polynomial functions. Block Diagram of Convolutional Code is shown in Fig. 11.

For Error Rate Calculation of Convolutional Code over AWGN channel below mentioned parameters in Table IV are used. Model of Convolutional Code in Simulink is shown in Fig. 12.

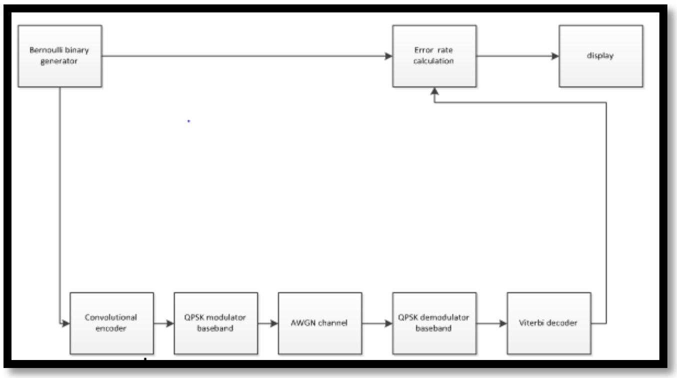

Fig. 11. Block Diagram of Convolutional Code

TABLE IV
FUNCTION BLOCK PARAMETERS: AWGN CHANNEL (REED-SOLOMON CODE)

Parameter	Value
Input Processing	Columns as channels (frame based
Initial Speed	67
Mode	Signal to Noise Ratio Eb/N$_0$
Eb/N$_0$	12
Number of Bits per symbol	1
Input Signal Power, referenced to 1 ohms (watts)	1
Symbol Period(s)	0.1

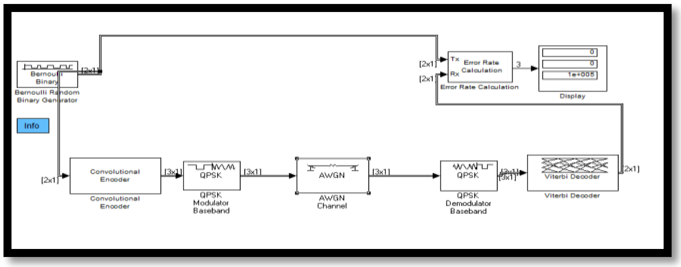

Fig. 12. Model of Convolutional Code in Simulink

Since convolutional encoder provides us Eb/N$_o$ of 12 dB with no errors, hence this channel encoding technique gives us the processing gain of 4 dB only. This is shown in the plot of BER Vs Eb/N$_o$ of Convolutional Code in Fig. 13.

Convolutional Coding technique is the one which better withstand noise with lower E$_b$/ N$_o$. Hence we have used this technique for error correction.

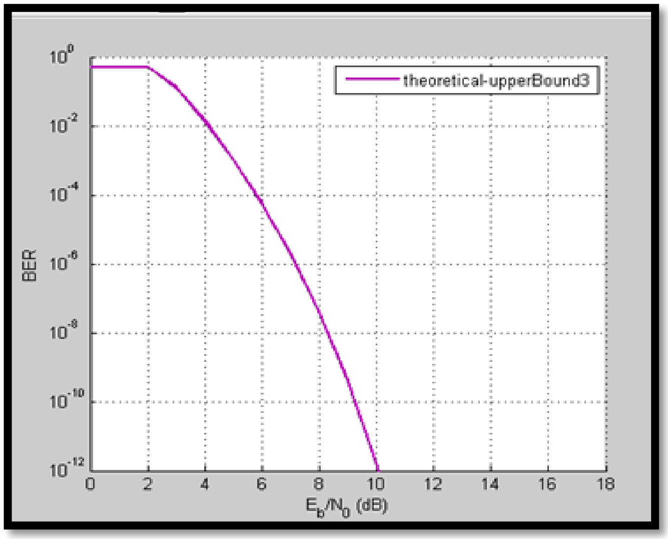

Fig. 13. Graphical Analysis of BER Vs SNR in Convolutional Code

E) Spreading of Signal

Now using spreading technique, we had again observed the processing gain of the signal. As we know that, the message signal is spreaded through mapping onto a random sequence, hence, we are using pseudorandom sequence generator. Block Diagram of DSSS is shown in Fig. 14.

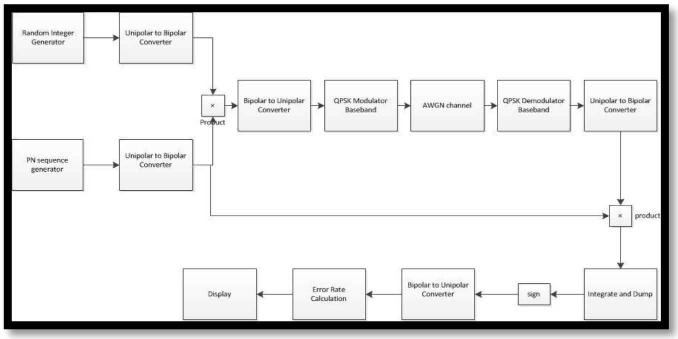
Random Integer Generator
Unipolar to Bipolar Converter
×
Product
Bipolar to Unipolar Converter
QPSK Modulator Baseband
AWGN channel
QPSK Demodulator Baseband
Unipolar to Bipolar Converter
PN sequence generator
Unipolar to Bipolar Converter
×
product
Display
Error Rate Calculation
Bipolar to Unipolar Converter
sign
Integrate and Dump

Fig. 14. Block Diagram of DSSS

For Error Rate Calculation using spreading (DSSS) over AWGN channel below mentioned parameters in Table V are used.

TABLE V
FUNCTION BLOCK PARAMETERS: AWGN CHANNEL (DSSS)

Parameter	Value
Input Processing	Columns as channels (frame based
Initial Speed	67
Mode	Signal to Noise Ratio Eb/N$_0$
Eb/N$_0$	5
Number of Bits per symbol	1
Input Signal Power, referenced to 1 ohms (watts)	1
Symbol Period(s)	0.1

The model of DSSS in Simulink is shown in Fig. 15.

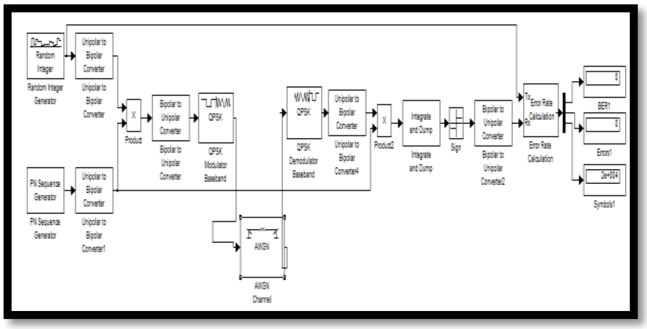
Random Integer
Random Integer Generator
Unipolar to Bipolar Converter
Unipolar to Bipolar Converter
X
Product
Bipolar to Unipolar Converter
Bipolar to Unipolar Converter
QPSK
QPSK Modulator Baseband
QPSK
QPSK Demodulator Baseband
Unipolar to Bipolar Converter
Unipolar to Bipolar Converter4
X
Product2
Integrate and Dump
Integrate and Dump
Sign
Bipolar to Unipolar Converter
Bipolar to Unipolar Converter2
Tx
Rx
Error Rate Calculation
Error Rate Calculation
0
BER1
0
Errors1
2e+004
Symbols1
PN Sequence Generator
PN Sequence Generator
Unipolar to Bipolar Converter
Unipolar to Bipolar Converter1
AWGN
AWGN Channel

Fig. 12. DSSS in Simulink

Using spreading technique, the processing gain we obtain from the above specified parameters, is 11dB. Hence, it is concluded that the signal transmitted through DSSS has its strength lower than the noise floor of the system. Therefore, such signal is neither detectable nor jammed.

F) Processing Gain Comparison

Processing gain comparison of above mentioned FEC techniques and DSSS (spreading) is represented by Table VI.

From Table VI results of processing gains, we have analyzed that the Convolutional Coding technique us the one which better withstand noise with lower E$_b$/ N$_{o.}$ Hence we have used this technique for error correction with DSSS.

TABLE VI
PROCESSING GAIN COMPARISON

Signal Transmission Technique	Eb/N$_o$	Processing Gain
QPSK Modulation	16 dB	-
Hamming Code	13 dB	3 dB
Reed-Solomon Code	15 dB	1 dB
Convolutional Code	12 dB	4 dB
Spreading (DSSS)	5 dB	11 dB

TABLE VII
BER VERSUS SNR COMPARISON

Forward Error Correction Technique	(SNR) Eb/N$_o$	BER
Hamming Code	13 dB	0
Reed-Solomon Code	15 dB	0
Convolutional Code	12 dB	0

V. LINK BUDGET ANALYSIS

Communication system link budget is calculated by considering all the gains, losses, attenuation of transmitted signal, antenna gain, feed line and miscellaneous losses from the transmitter to the receiver. It is calculated in order to meet the available bandwidth and radio frequency power of the system under consideration. Following is the simple link budget equation.

Received power (dBm) = transmitted power (dBm) + Gains (dBm) - losses (dBm) (5)

Following are the key considerations while calculating system link budget. We have calculated system link budget with a distance of 1m between transmitter and the receiver.

A) Channel Noise

For channel noise power calculation in watts following formula is used.

$$N = KTB \tag{6}$$

N is the noise power, T is the temperature of the system which is 290 K approximately and K is the Boltzman's constant whose value is 1.38 x 10^{-23} J/K.
B = channel bandwidth (Hz) = 614.4kHz
By putting the above mentioned values:
N = (1.38 x 10-23) (290) (614.4k)
N = 2.45*10-15 W (lowest possible noise level)
According to the above stated equations we have to tradeoff between power and bandwidth in order to attain a certain performance criterion of signal transmission.

B) Range and Path Loss

Transmission range and power of received signal are inversely proportional to each other. Path Loss is calculated by the below stated formula.

$$L = 20\log_{10}(D) + 20\log_{10}(f) + 20\log_{10}\frac{4\Pi}{C} - G_t - G_r \tag{7}$$

Where
D = distance between receiver and transmitter = 1m
λ = free space wavelength = c/f = 〚3*10〛^8/2.4G
c = speed of light (〚3*10〛^8m/s)
f = frequency (Hz) = 2.4G
Gt = 2.14dB
Gr = 2.14dB
By putting the values the end result is:
= 35.76dB

C) Spread Spectrum

$$Processing\ Gain = 10log_{10}(\frac{C}{R}) \tag{8}$$

Where
C= chip rate = 32000
R= bit rate = 1000
By putting the values we obtain:
= 15 dB
A typical link budget equation for radio communication system is:

$$P_{R_x} = P_{T_x} + G_{T_x} + G_{R_x} - L_{T_x} - L_{R_x} - FSPL - L_p \tag{9}$$

Where
P_{T_x} = Transmitted power = 10mW = 10dBm=-20dBW
G_{T_x} = Transmitter antenna gain = 2.14dB
G_{R_x} = Receiver antenna gain = 2.14dB
L_{T_x} = Transmitter losses = ignored
L_{R_x} = Receiver losses = ignored
$FSPL$ = Free Space Path Loss = 35.76dB
L_p = Miscellaneous losses = 1dB
Hence, by putting these values in above equation we obtain
P_{R_x} = Received power = -22.48dBm=0.0056493697481mW
By adding the processing gain of the encoder and the spreader, i.e:
Processing gain of convolutional encoder = 4dB
Processing gain of spreader = 15dB
We get
P_{R_x} = -22.48dB + 4dB + 15dB
P_{R_x} =-3.48dB = 0.44874538993mWb

VI. CONCLUSION

A Direct Sequence Spread Spectrum (DSSS) was modeled using MATLAB/ Simulink. The simulation was done over AWGN channel. Bit Error Rate (BER) analysis of Hamming Code , Reed-Solomon Code and Convolutional Code was done to obtain best error correction and detection technique. Relationship curves of BER over Eb/N_o were obtained and it was concluded that Convolutional Code technique was the best Forward Error Correction (FEC) technique to be used with DSSS. It gives us BER = 0 for Eb/N_o = 12dB. Communication system is implemented in MATLAB using Convolutional Code, DSSS and pseudo random noise generator. It was observed that due to DSSS technique the signal was transmitted at strength lower than the noise floor of the system. The value of Eb/N_o for the system is 5dB and processing gain is 11dB. The signal was completely retrievable, undetectable and unable to get jammed as it is transmitted below the noise level of the system. In the end key considerations to calculate the system link budget are stated. Finally path loss is calculated between transmitter and receiver which are separated by a distance of 1m.

REFERENCES

[1] R. E. Ziemer, "Fundamentals of spread spectrum modulation," Synthesis Lectures on communications, Vol. 2, pp. 1-79, 2007.

[2] L. Dubreuil and T. P. Berger, "Spread Spectrum, Cryptography and Information Hiding," in Proceedings of ACCT'9, 2004.

[3] J. S. Sousa and J. P. Vilela, "Uncoordinated Frequency Hopping for Wireless Secrecy Against Non-degraded Eavesdroppers," IEEE Transactions on Information Forensics and Security, Vol. 13, pp. 143-155, 2017.

[4] S. Fang, Y. Liu, and P. Ning, "Wireless communications under broadband reactive jamming attacks," IEEE Transactions on Dependable and Secure Computing, Vol. 13, pp. 394-408, 2016.

[5] M. M. Hasan, J. M. Thakur, and P. Podder, "Design & Implementation of FHSS and DSSS for Secure Data

Transmission," International Journal of Signal Processing Systems, Vol.4, No. 2, 2014.

[6] T. Kang, X. Li, C. Yu, and J. Kim, "A survey of security mechanisms with direct sequence spread spectrum signals," Journal of Computing Science and Engineering, vol. 7, pp. 187-197, 2013.

[7] Youssef, M. I., Emam, A. E., & Elghany, M. A., "Direct sequence spread spectrum technique with residue number system. International Journal of Electrical, Computer and Systems Engineering, Vol, 3, No. 4, pp. 223-230, 2009.

[8] Benprom, P., Pinthong, C., & Kanprachar, S. (2011, May). Analysis of convolutional coded direct sequence spread spectrum CDMA system with a BPSK jamming signal. In Electrical Engineering/Electronics, Computer, Telecommunications and Information Technology (ECTI-CON), 2011 8th International Conference on (pp. 268-271). IEEE.

[9] Shanmugasundaram, T., & Nachiappan, A. "Bit Error Rate (Ber) Performance Analysis Of Dsss-Fec Coherent And Non-Coherent Mfsk Under Rayleigh And Rician Fading Channels," i-manager's Journal on Wireless Communication Networks Vol. 1 l, No. 4, March 2013.

[10] Kumar, S., & Gupta, R. Bit error rate analysis of Reed-Solomon code for efficient communication system. International Journal of Computer Applications, 30(12), pp.11-15, 2011.