Security Enhancement using Channel State Information for Multicarrier Modulation

by

Nidhi K. Sindhav
201915005

A Thesis submitted in partial fulfillment of the requirements of the degree of

MASTER OF TECHNOLOGY

in

ELECTRONICS AND COMMUNICATIONS

with specialization in

Wireless Communication and Embedded Systems

to

Dhirubhai Ambani Institute of Information and Communication Technology

A program jointly offered with

C.R.Rao Advanced Institute of Mathematics, Statistics and Computer Science

July, 2021

Declaration

I hereby declare that

i) the thesis comprises of my original work towards the degree of Master of Technology in Electronics and Communications at Dhirubhai Ambani Institute of Information and Communication Technology & C.R.Rao Advanced Institute of Applied Mathematics, Statistics and Computer Science, and has not been submitted elsewhere for a degree,

ii) due acknowledgment has been made in the text to all the reference material used.

Nidhi K. Sindhav

NIDHI K. SINDHAV

CERTIFICATE

This is to certify that the thesis work entitled **“Security Enhancement using Channel State Information for Multicarrier Modulation ”** has been carried out by **Nidhi K. Sindhav** for the degree of Master of Technology in Electronics & Communications Engineering at Dhirubhai Ambani Institute Of Information and Communication Technology & C.R.Rao Advanced Institute of Applied Mathematics, Statistics and Computer Science under the supervision of **Dr. Priyanka Mekala & Dr. Supriya Goel**.

M.Priya

Dr. Priyanka Mekala
Project Guide
Assistant Professor
C R Rao AIMSCS
Telangana-500046

supriya

Dr. Supriya Goel
Project Guide
Assistant Professor
C R Rao AIMSCS
Telangana-500046

ACKNOWLEDGEMENT

This project would not have been possible without the help and cooperation of many. I would like to thank the people who helped me directly and indirectly in the completion of this project work.

First and foremost, I would like to express my gratitude to our beloved **director Of C R Rao AIMSCS**, for providing his kind support in various aspects.

I would like to express my gratitude to my project guide **Dr. Priyanka Mekala & Dr. Supriya Goel**, Professor,for providing excellent guidance, encouragement, inspiration, constant and timely support throughout this M.Tech project phase II.

I would also like to thank Research Scholar **Mr.Goli Srikanth** in the Dept. of Wireless Communication for his guidance and help.

Finally, my deep and sincere gratitude to my family and friends for their continuous and unparalleled love, help and support. I am forever indebted to my parents for giving me the opportunities and experiences that have made me who I am.

Abbrevations

- **OFDM** : Orthogonal Frequency Division Multiplexing
- **GFDM** : Generalized Frequency Division Multiplexing
- **CSI** : Channel State Information
- **PLS** : Physical Layer Security
- **PLE** : Physical Layer Encryption
- **BER** : Bit Error Rate
- **FFT** : Fast Fourier Transform
- **IFFT** : Inverse Fourier Transform
- **IoT** : Internet of Things
- **SWIPT** : Simultaneous Wireless Information and Power Transfer
- **AN** : Artificial Noise
- **CS** : Compressive Sensing
- **VLC** : Visible Light Communication
- **IRS** : Intelligent Reflecting Surface

Abstract

Wireless technologies of the fifth generation (5G) are vital to advancing Internet-of-Things (IoT) networks in the future. Information security in wireless networks is one of the most difficult problems due to the open nature of the wireless medium. A promising approach to ensure strong security has been characterized as physical layer security, which exploits the differences between the physical properties of signal channels to provide a resilient and effectively degraded signal at an eavesdropper that cannot be recovered regardless of the processing of the signal. This thesis presents a coherent framework for a secure transmission and receiver for IoT devices. The proposed framework will operate only in the physical layer. A study of symbol shuffling using channel state information (CSI) in OFDM (Orthogonal Frequency Division Multiplexing) GFDM(Generalized Frequency Division Multiplexing) are presented here. BER simulations of the multi-carrier modulation schemes with proposed Physical Layer Security(PLS) technique. Further, simulations of OFDM with the proposed PLS technique have been performed in order to compare different equalizers, tap lengths, and modulations. Devices with limited resources can benefit from these proposed PLS technique.

Keywords : PLS, Symbol shuffling, CSI, OFDM, GFDM, Secrecy Capacity

TABLE OF CONTENTS

Abstract **i**

List of Figures **iv**

List of Tables **1**

1 Introduction **1**

1.1 Wireless Security 2

1.2 Multicarrier Modulation Scheme 4

1.3 Motivation & Goal 9

1.4 Thesis Outline 10

2 Literature Review **11**

2.1 Physical Layer Encryption(PLE) 12

2.2 Physical layer Security(PLS) 14

2.3 Existing IoT security technique 20

3 Methodology & Proposed Work **21**

3.1 System Model 21

3.2 Block Diagram 22

3.3 Proposed Physical Layer Security Method 23

4 Experimental Results **27**

4.1 Comparison Of Legitimate Channel and Eavesdropper Channel capacity . 28

4.2 Channel Secrecy Capacity 32

4.3 BER after PLS 33

4.4 Channel Knowledge Parameter 34

4.5 BER comparison in OFDM & GFDM after PLS Technique 35

4.6 Different Equalizer Comparison after PLS technique 37

4.7 Different Modulation(M) & Channel tap length(L) performance in terms of BER after PLS technique 39

5 Conclusion & Future work 40

5.1 Conclusion 40

5.2 Future Work 41

APPENDICES 41

A MATLAB Code 42

List of Figures

1.1 OSI model 3

1.2 OFDM block diagram 5

1.3 GFDM Block Diagram[11] 8

1.4 OFDM to GFDM symbol arrangement 9

2.1 Wireless Security Category 11

2.2 Shannon's cipher system[14] 13

2.3 Wyner's wiretap channel [14] 15

3.1 System Model 21

3.2 Physical Layer Block Diagram 22

3.3 Block diagram includes Proposed PLS technique 23

4.1 Multipath fading effect 28

4.2 Channel capacity comparison of Legitimate & Eavesdropper channel(without PLS) 29

4.3 OFDM channel capacity(N=28) 30

4.4 OFDM channel capacity(N=80) 30

4.5 OFDM channel capacity(L=2) 31

4.6 OFDM channel capacity(L=8) 31

4.7 Channel secrecy capacity 32

4.8 BER comparision Of BoB & Eave after PLS 33

4.9 BER in OFDM after PLS with channel knowledge parameter 34

4.10 α=0.1 34

4.11 α=0.01 34

4.12 α=0.001 34

4.13 BER in OFDM & GFDM after PLS 35

4.14 OFDM & GFDM symbol arrangement 36

4.15 Different equalizer 37

4.16 Different M 39

4.17 Different L 39

Chapter 1

Introduction

Wireless communication is everywhere in the world in modern technologies. Cellular communication alone is reachable to almost every part of the world. Applications of Wireless networks includes banking and other financial transactions, social networking, environmental monitoring and many others. So, the wireless network security is very important in today's scenario. Conventionally Security has been considered at upper layer of communication networks not at the physical layer. Cryptography based method is the very widely used method for security purpose and in current situation it works well. The encryption of data can become difficult in low-powered devices due to issues such as key management and computational complexity. A message can go through numerous intermediate terminals on its way from the source to the destination in an ad hoc network In sensors or Radio Frequency Identification (RFID) networks,in which the end devices are of very low complexity[1]. For these and other reasons, methods that are based on physical layer properties of channel takes appreciable interest to secure data transmission. These methods are based on information theoretic results which is related to Claude Shannon's early work on the mathematical theory of communication. Symmetric key encryption based method was Shannon's work, perhaps a more relevant development in this area was Aaron Wyner's work on the wiretap channel,which inaugurated the idea that communication channels themselves can impart confidentiality without using shared secret keys[1].

Wireless physical layer security has become a crucial research topic in modern technologies, and considerable improvement has been made in understanding the underlying ability of the physical layer to ensure secure communications and to find the successive limits of this ability. To mitigate the ability of potential eavesdroppers so that she could not able to gain information there has been two principle properties of radio transmission diffusion and superposition can be exploited to provide confidentiality. These mechanisms contains the exploitation of different properties which includes fading, interference, and path diversity(with the use of multiple antennas),this can be used to extract shared secret key from the physical layer properties.

1.1 Wireless Security

In terms of security wired communication is more secure compared to wireless communication. During wired communication, devices are linked through nodes and cables, so that unauthorized users are not able to see or access confidential messages. Furthermore, users are becoming increasingly concerned about security in wireless networks because of open communication. The OSI protocol architecture is typically used in wireless networks[2]. OSI model with transmitter(Node A), receiver(Node B) & wireless medium is as shown in Fig.1.1. The security threats and vulnerabilities at each layer of OSI are protected separately and are aligned to the wireless network's security requirements[3]. Security concerns are traditionally addressed over the physical layer(Lower layer) in the seven-layer OSI model of computer networking, such as with cryptography, which is used at the application layer if the physical layer has already enabled an error-free link [4]. Cryptographic methods usually encrypt plain texts using special algorithms that are computationally infeasible for the adversary(eavesdropper) to decrypt if they don't have access to the encryption keys. Despite this, security methods such as encryptions may no longer be sufficient due to the improvement of computers' computing abilities and methods of breaking encryption algorithms.

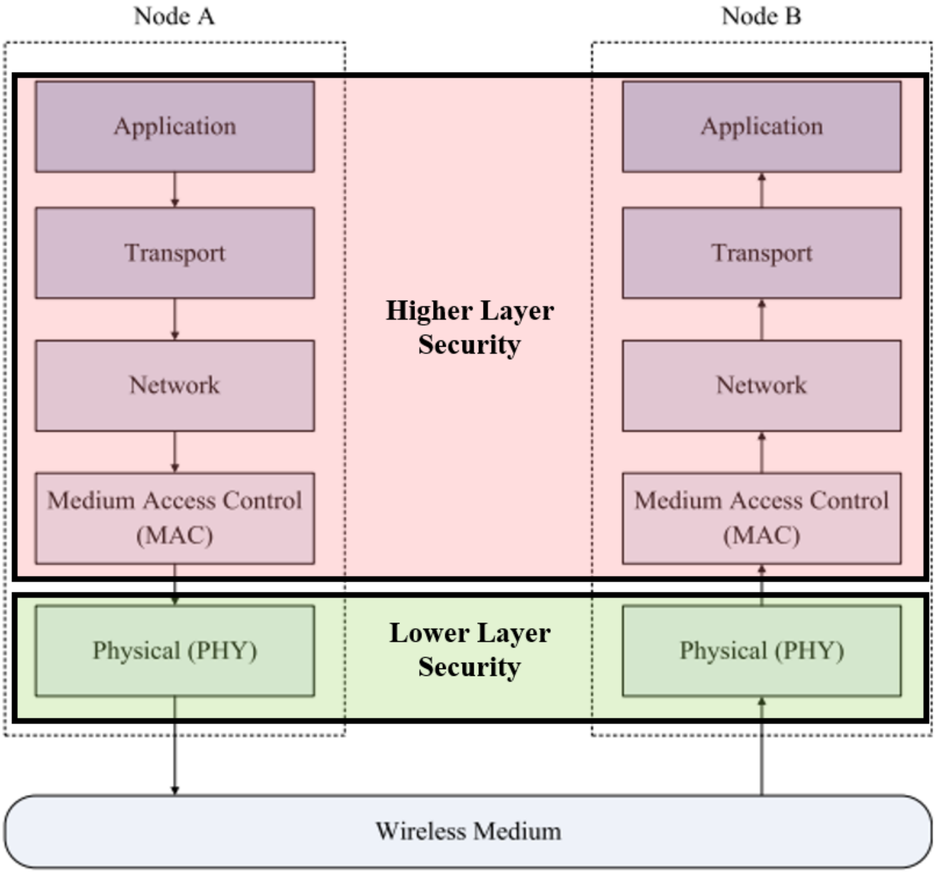

Figure 1.1: OSI model

A robust form of security for wireless networks has been studied at the physical layer as a promising approach. Essentially, physical layer security is achieved by exploring how various physical properties of signal channels affect the capability of achieving security, i.e., security without any limitations regarding the eavesdropper's computing power. Therefore, physical layer security is typically considered an information-theoretic security.

Different OSI layers use different authentication protocols. **Our focus is on Physical layer security** which is an emerging technique of securing the open communication environment against eavesdropping attacks at the physical layer. The study of models, methods, and algorithms that aim to reinforce the secure communication systems by utilizing the properties of the physical layer has been developed a dynamic research area,which is known as physical layer security[5]. For resource limited scenarios(IoT devices) encryption-based algorithms and standards are not perfectly appropriate because of the low computational cost and low powered devices. The physical layer security technologies, is believed to be effective supplementary over upper layer encryption based security for wireless network security.[6]

The physical layer security technologies have the following advantages[6].

- Attaining perfect secrecy [7, 8]. It has been demonstrated from the knowledge of information theory that even the eavesdropper is computationally powerful the physical layer security has the capability to reach perfect secrecy . In encryption based method eavesdropper can decrypt the message via brute-force calculation which is not in the case of physical layer security.
- Low computational complexity and resource consumption [7]. No need to manage key as physical layer security does not depend on the computing capability of hardware equipment,and it is lightweight in terms of computational complexity and resource requirements.
- By exploiting physical layer properties, such security technologies can accommodate the changes of wireless channel by optimizing the system parameters and transmission schemes.

1.2 Multicarrier Modulation Scheme

This choice of multi carrier techniques is motivated by the desire to fool an illegitimate user (an eavesdropper), so that the an eavesdropper is not able to untangle the information. The technique proposed in this thesis involves shuffling and reshuffling operations, which can be achieved if multiple options or multicarrier techniques are used.

1.2.1 OFDM(Orthogonal Frequency Division Multiplexing)

Orthogonal frequency-division multiplexing (OFDM) is a method of digital signal modulation in which a single data stream is split across several separate narrow band channels to reduce interference at different frequencies. Fig 1.2 represents block diagram of OFDM.

Detailed explanations are provided in this section.

In an OFDM system, Transmitted input bit stream is encoded into one data symbol. Such N symbols are modulated using any digital modulation technique which is known as bit mapping IFFT process maps N symbols onto N sub carriers and maintains orthogonality of each subcarrier.

$$x(n) = \frac{1}{\sqrt{N}} \sum_{k=0}^{n-1} X(k) e^{j2\pi nk} \tag{1.1}$$

One transmitted OFDM symbol contains such N number of IFFT processed samples.The transmitted OFDM symbol convoluted with channel taps h(l).

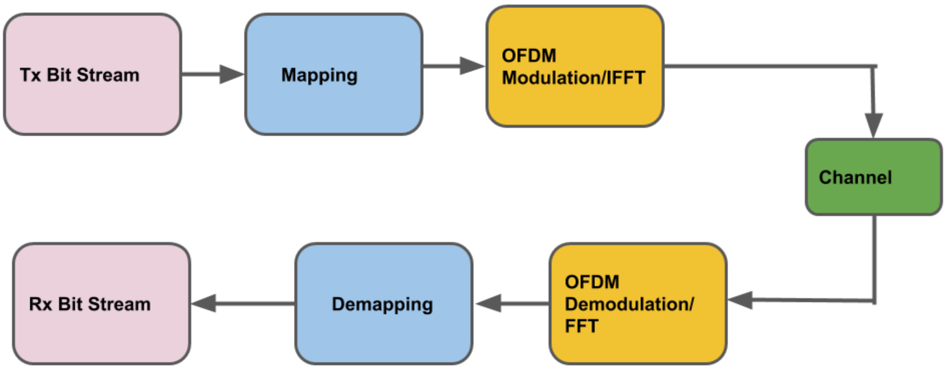

Figure 1.2: OFDM block diagram

At the receiver side FFT of y(n)

$$Y(k) = \frac{1}{\sqrt{N}} \sum_{n=0}^{n-1} y(n) e^{\frac{-j2\pi nk}{N}} \tag{1.2}$$

$$H(k) = \frac{1}{\sqrt{N}} \sum_{l=1}^{n-1} h(l) e^{\frac{-j2\pi lk}{N}} \tag{1.3}$$

Using demapping symbols convert into output bit stream.

The new encryption scheme is employed in OFDM at the physical layer[9]. The new scheme confuses the subcarrier for dummy data and reoredr the training symbol by a new secure sequence. The system is robust to various attacks with security analysis.

OFDM Modulation and Demodulation

- Let $\mathbf{h} = [h_0, h_1 \ldots h_{L-1}]$ are the L Gaussian $i.i.d$ fading channel coefficients with mean 0 and variance 1 .

$$y[k] = \sum_{l=0}^{L-1} h_l x[k-l] + n[k] \tag{1.4}$$

- Channel Model (Cyclic prefix based Transmission)[10]

$$\mathbf{y} = \mathbf{H}_{cir}\mathbf{x} + \mathbf{n} \tag{1.5}$$

  - $\mathbf{y} \in \mathbb{C}^{N\times 1}$ is the received vector.
  - $\mathbf{H}_{cir} \in \mathbb{C}^{N\times N}$ is the circulant matrix.
  - $\mathbf{x} = \mathbf{E}_t\mathbf{s}$ is the modulated transmitted data, where $\mathbf{s}$ is the conventional modulation symbols and $\mathbf{E}_t \in \mathbb{C}^{N\times N}$ is the modulation matrix .
  - $\mathbf{n} \in \mathbb{C}^{N\times 1}$ is the AWG noise with mean 0 and variance σ^2.

- Let $\mathbf{E}_r \in \mathbb{C}^{N\times N}$ be the demodulation matrix, than the effective channel becomes,

$$\overbrace{\mathbf{E}_r\mathbf{y}}^{\bar{\mathbf{y}}} = \overbrace{\mathbf{E}_r\mathbf{H}_{cir}\mathbf{E}_t}^{\mathbf{H}_d}\mathbf{s} + \overbrace{\mathbf{E}_r\mathbf{n}}^{\bar{\mathbf{n}}}$$

$$\mathbf{E}_t = \frac{1}{\sqrt{N}}[a_0, a_1, a_2, \ldots, a_k \ldots a_N]$$

- where a_k is k^{th} column vector of E_t containing the elements, $a_{N,k}[n] = exp(\frac{j2\pi kn}{N})for n = 0, \ldots, N-1$.

$$\mathbf{H}_d = \mathbf{E}_r\mathbf{H}_{cir}\mathbf{E}_t \tag{1.6}$$

$$\mathbf{H}_d = \begin{bmatrix} H_0 & 0 & \dots & 0 \\ 0 & H_2 & \dots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \dots & H_{N-1} \end{bmatrix} \tag{1.7}$$

- Therefore the effective channel is denoted as,

$$\bar{\mathbf{y}} = \mathbf{H}_d\mathbf{s} + \bar{\mathbf{n}} \tag{1.8}$$

- By applying inverse of the channel effect for each subcarrier,

$$\hat{s}[k] = \frac{\bar{y}[k]}{H_k} = s[k] + \frac{\bar{n}[k]}{H_k}\text{for}k = 0, \dots, N-1. \tag{1.9}$$

OFDM drawbacks

- As the phases of the subcarriers are independent of each other in OFDM, the modulation typically exhibits a large dynamic range. The phases may combine in constructive or destructive manner.
- High out of band leakage
- High PAPR.
- To overcome OFDM drawbacks new MCM(Multi Carrier Modulation) scheme is introduced it is known as GFDM(Generalized Frequency Devision Multiplexing).

1.2.2 GFDM(Generalized Frequency Division Multiplexing)

GFDM is used filtering method for each subcarrier. In a single processing unit, multiple symbols(sub symbols) across the whole frequency span is processed. Unlike OFDM subcarrier is no longer orthogonal in the case of GFDM and characteristics of each subcarrier can change, accordingly interleaving of different types of subcarrier is possible. It can still have satisfactory spectral efficiency and satisfactory out of band emission. It can have MIMO support as well. GFDM does not have good control of in band emission or spectral efficiency is not that much improved compared to other multicarrier modulation techniques. In GFDM pulse shaping filter is used as filter and applied on each subcarrier. In a single step multiple symbols(sub symbols) are processed per subcarrier[11].

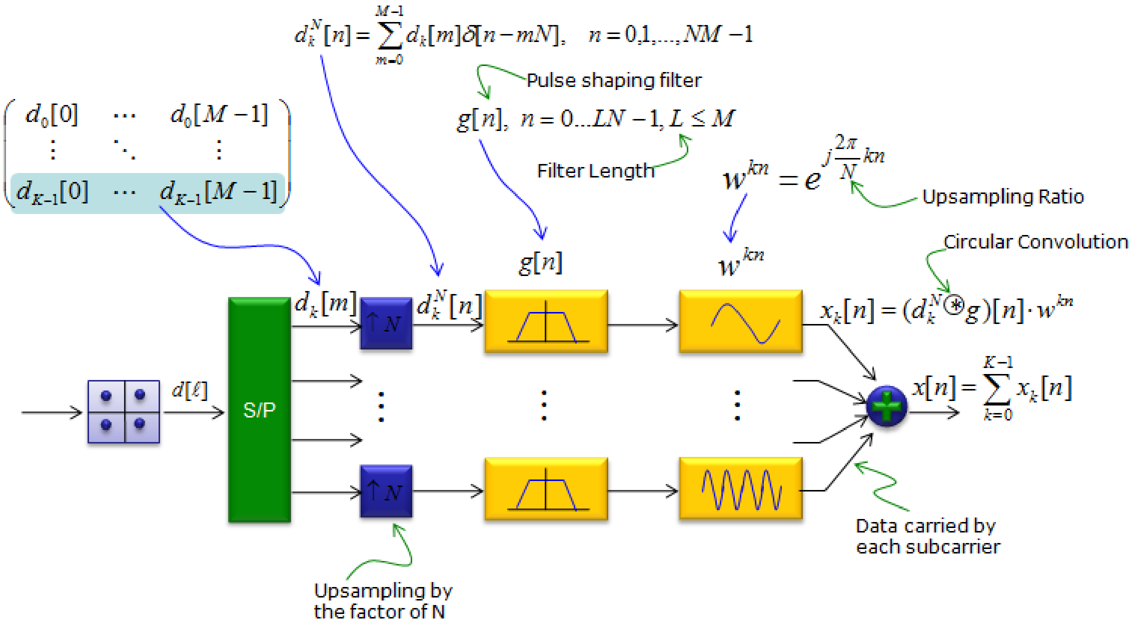
$d_k^N[n] = \sum_{m=0}^{M-1} d_k[m]\delta[n-mN], \quad n = 0,1,\ldots,NM-1$
Pulse shaping filter
$g[n],\ n = 0 \ldots LN-1, L \le M$
Filter Length
$w^{kn} = e^{j\frac{2\pi}{N}kn}$
Upsampling Ratio
$\begin{pmatrix} d_0[0] & \cdots & d_0[M-1] \\ \vdots & \ddots & \vdots \\ d_{K-1}[0] & \cdots & d_{K-1}[M-1] \end{pmatrix}$
Circular Convolution
$g[n]$
w^{kn}
$d_k[m]$
$\uparrow N$
$d_k^N[n]$
$x_k[n] = (d_k^N \circledast g)[n] \cdot w^{kn}$
$d[\ell]$
S/P
$x[n] = \sum_{k=0}^{K-1} x_k[n]$
$\uparrow N$
Data carried by each subcarrier
Upsampling by the factor of N

Figure 1.3: GFDM Block Diagram[11]

GFDM in IOT

In order to avoid the limitations of OFDM and extend the battery life of devices in the IoT, wireless data can be transmitted in a simultaneous manner through symbol allocation and joint subcarriers through multiuser GFDM for IoT[12]. IoT devices run on 5G networks have limited resources and are energy-constrained. The proposed scheme in[12] was termed as SWIPT.

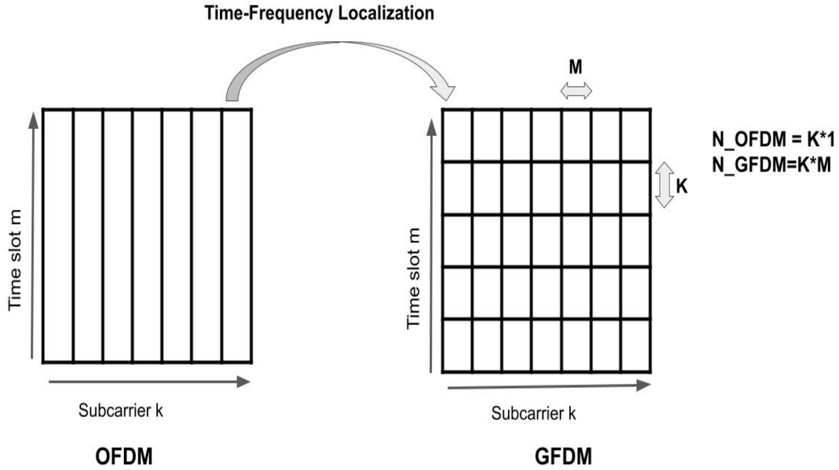

Figure 1.4: OFDM to GFDM symbol arrangement

In IoT, GFDM for multiuser downlink is analyzed based on its 2-D time-frequency block structure. Fig.1.4 represents OFDM & GFDM symbols/subsymbol arrangement where it could be noticed GFDM has frequency and time division(2-D structure) which increases transmission rate compare to OFDM. As a result of the numerous connections that will be present in future 5G scenarios, SWIPT scheme for GFDM , which can improve spectrum efficiency, higher transmission rate and battery life extension simultaneously, would be the qualified candidate for the 5G-based IoT[12].

1.3 Motivation & Goal

The key idea of physical layer security is to ensure security of information data at the physical layer by taking advantage of the difference between the legitimate(Alice to Bob) channels and eavesdropper channels which can be generated by the randomness of wireless mediums (such as channel fading and noises). As this technology does not excessively depends on computational capability of device it is more advantageous to resource limited devices. As a result of traditional upper layer cryptography, transmissions are vulnerable to a host of passive and active attacks. MAC headers and physical packet headers can be used as an attacker since they are in plain text and contain information such as data rates, mapping schemes, side channel information (SCI) and packet length.[13]. Physical layer security with low complexity can supplement or replace cryptography techniques.

As IoT devices are typically low-cost, their storage memory and processing power are fairly limited. Furthermore, most IoT devices use batteries for power, which puts significant strain on energy sources. A PLS strategy that is highly energy-efficient and can be implemented with low complexity is required to combine low-cost and low-power consumption features. In this thesis a secure way of transmission and receiver framework is proposed for these devices which will operate only in the physical layer. A study of symbol shuffling using (CSI) in OFDM & GFDM are implemented here. BER simulations of the multi-carrier modulation schemes with proposed Physical Layer Security(PLS) technique. Moreover, simulation of OFDM with proposed PLS technique in terms of secrecy capacity, a different equalizer comparison , channel tap length , different modulation are included. These techniques can augment conventional cryptography for devices with limited resources.

1.4 Thesis Outline

This thesis is organized as follows. Chapter 2 includes literature overview of physical layer Encryption(PLE)(Explained Shannon's cipher in detail), Physical Layer Security(PLS)(Explained Wyner's model in detail) and exciting IOT security technique. Chapter 3 includes methodology and proposed work with system model & mathematical equation. Chapter 4 includes experimental results of proposed PLS technique over different parameter(Modulation,channel tap length, equalizer,OFDM,GFDM) BER plot in MATLAB. Chapter 5 includes Conclusion of proposed PLS technique with its application future work.

Chapter 2

Literature Review

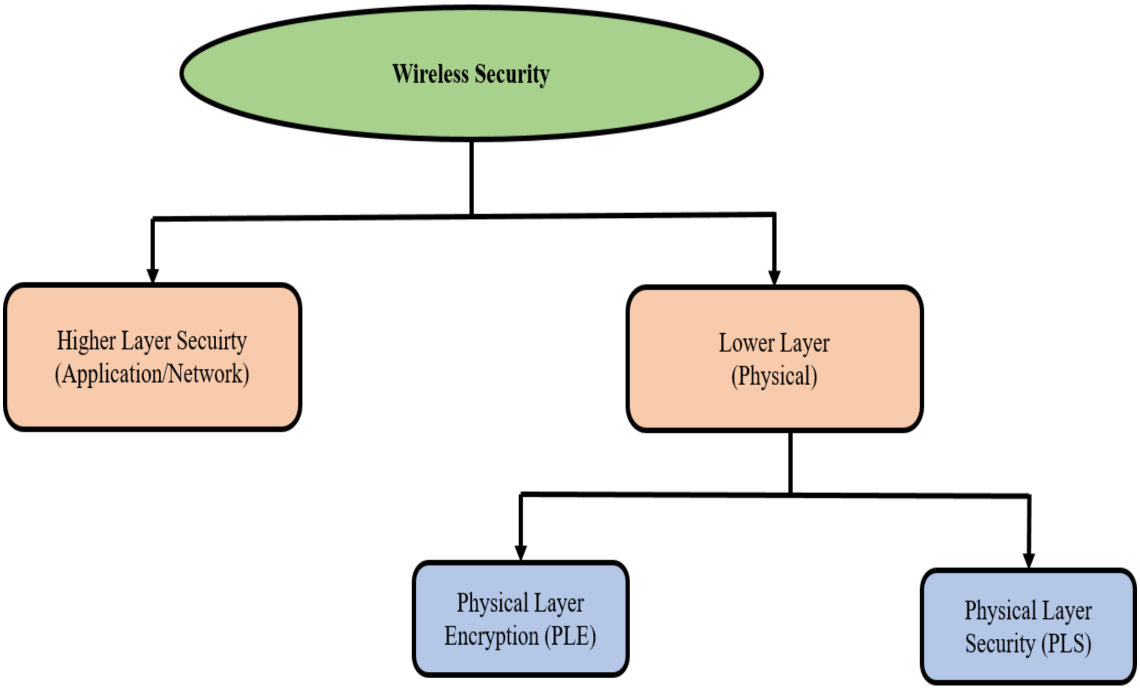
Wireless Security
Higher Layer Secuirty (Application/Network)
Lower Layer (Physical)
Physical Layer Encryption (PLE)
Physical Layer Security (PLS)

Figure 2.1: Wireless Security Category

There are two main section in literature: Physical layer security (without key) and Physical layer encryption (with key) as shown in fig. 2.1. Further also included existing IoT security techniques.

2.1 Physical Layer Encryption(PLE)

A discussion of wireless secret key generation techniques using physical layer characteristics is presented in this section. Shannon's cipher system, which can be seen in Fig 2.2, was used to pioneer the study of information theory.

As is depicted in Fig. 2.2, Shannon considered a noiseless cipher system. 2.1. A sender (Alice) sends a message M to a receiver (Bob) in secret, so as not to be intercepted by an Eavesdropper (Eve), who wants to intercept Alice and Bob's communication. Eave is unaware of the secret key K that Alice and Bob share. During encryption, Alice uses this key to encrypt the message M, and Bob uses this key to decrypt the message from codeword X. If the mutual information between the message M and the codeword X , which is overheard by Eve, is exactly zero then the communication scheme is considered to be secure.

$$I(M;X) = 0 \tag{2.1}$$

Mutual information in terms of entropy is

$$I(M;X) = H(M) - H(M/X) \tag{2.2}$$

$$H(M) = -\sum p(m)\log_2 p(m) \tag{2.3}$$

H(M) describes the entropy of M that describes the uncertainty about the random variable M in equation 2.3, where p(m) is the probability that M will take on the value m, while the conditional entropy H (M /X) describes the residual uncertainty in M after X has been observed. I(M ; X) = 0 thus infers that there is uncertainty H (M) is equal to the uncertainty H (M /X). That is to say, the message M and the codeword X should be

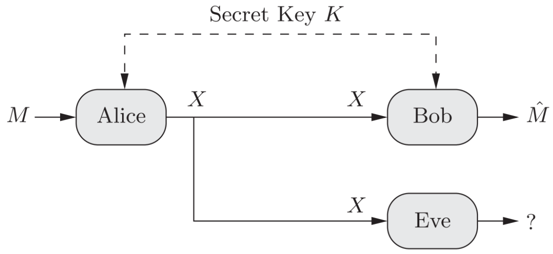

Figure 2.2: Shannon's cipher system[14]

statistically independent. This condition is known as perfect secrecy and cannot reveal any information about the message M based on the observed codeword X. Eve, though computationally superior, can still infer confidential information by simply guessing the transmitted message when the observed codeword is ignored. According to Shannon, perfect secrecy is achievable if the entropy of the secret key (K) H(K) is as large as the entropy of a message is H (M). i.e., H (K)≥H (M).

Based on the assumption that the message and the secret key are sequence of binary numbers, perfect secrecy is achieved by the one-time pad approach , where the codeword X is simply the binary addition [exclusive or (XOR) operation] of the message and the secret key; i.e., X = M ⊕ K. The concept extends beyond the binary case and the crypto lemma is true in a much more general setting [14].

Drawbacks of Shannon's Cipher system

- key management, distribution, and maintenance processes
- longer key length
- The conventional cryptography technique can be cracked by fast development and advances in computing power devices.
- New Wireless technologies are time delayed, limited in power and processing restricted and so cryptography technique are not much suitable to it.

Key management techniques must required in Physical Layer Encryption(PLE) methods. In[15] represents three unconventional approaches to keying variable management. Public key crypt system is utilized to transport keying variable for crypt system in first approach,UHF radio channel is used to determine crypt variable in second approach. Third approach is based on respective characteristics exhibited by convolution and deconvolution estimation. In Ref.[16] the pulse response of the legitimate channel is used as the random source to distill the keys and found the secret key generation issue for the ultra-wide band (UWB) channels. In Ref. [17] generated a key agreement strategy which is depends upon LLR thresholding. Ref[18] used the received signal strength as the common randomness for the legitimate users, which has not high computational complexity. probabilistic ciphering was explained in[19], It is also encryption based method ,the sensor outputs are randomly mapped to a set of discrete quantization levels,and the respective probabilities are only known to the Legitimate Fusion Center(LFC) but unknown the Eavesdropping Fusion Center(EFC). By optimizing the probability distribution, a high error floor is generated for the signal detection at the EFC,it is guaranteed transmission security. Probabilistic ciphering improves the system security performance in[20].

2.2 Physical layer Security(PLS)

Wyner introduced the wiretap channel as the first basic physical layer security model. A method to generalize Shannon's cipher is presented that considers reliable and secret communication over noisy channels [14].

In some ways, Wyner's wiretap channel task is similar to Shannon's cipher. As shown in Fig. 2.3, Wyner considered noisy channels. The objective is to reliably reconstruct the message at Bob's side (receiver) without a secret key, unlike Shannon's cipher system. Therefore, Alice has to convert M into codeword X^n and retrieve message from Y^n.
For reliable transmission
$P(\hat{M} \neq M)$
Codeword of length n makes use of the channel n times

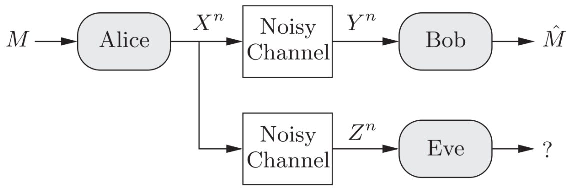

Figure 2.3: Wyner's wiretap channel [14]

Where $X^n = (X_1, ...X_n), Y^n = (Y_1, ...Y_n), Z^n = (Z_1, ...Z_n)$

Where Y^n and Z^n is channel output at Bob((legitimate receiver) side and Eve side(illegitimate user) respectively. There must be strict statistical independence between the message M and the channel output Z^n at Eve. Since communications channels are noisy, statistical independence can only be computed asymptotically in lengths of blocks n. Conditional entropy can be defined as:

$$\frac{1}{n}H(M/Z^n) \cong \frac{1}{n}H(M) \tag{2.4}$$

Weak secrecy is defined as:

$$\frac{1}{n}I(M; Z^n) \rightarrow_{n\rightarrow\infty} 0 \tag{2.5}$$

Weak secrecy has its vulnerabilities and can be strengthened by dropping the division by n.

I(M;Z^n)$\rightarrow_{n\rightarrow\infty}$ 0

The secrecy capacity of discrete memory less wiretap channel is given by:

$$C_s = \max_{V-X-(Y,Z)} (I(V;Y) - I(V;Z)) \tag{2.6}$$

V is artificial noise in system which make eavesdropper's channel noisier.

Drawbacks of Wyner's wiretap channel [14]:

- Typically, Eve's channel is assumed to be less effective than Bob's, which isn't always the case for practical purposes.
- There is a trade-off between capacity and secrecy.

In [21] presents a low density parity check code (LDPC) coding scheme for gaussian wiretap channels. To hide data from evesdropper the messages are transmitted over punctured bits. Alice and Bob must be able to communicate reliably to prevent eavesdropping by keeping the security gap $\mathrm{SNR}_B/\mathrm{SNR}_E$ as small as possible.o defend against eavesdropper.

Difference between Shannon's and Wyner's Model:

- Wyner's model consider presence of noise in communication channel which was not include in Shannon's model.
- Shannon's model has some secret key between Alice and Bob while in the case of Wyner's model local random number generator(key in one time pad) in Alice encoder which is known by Alice only. Wyner's model has not any secret key.

In some of the literature Lower(Physical) Layer security is categorized as follows[**2**]

i)SINR based (key less)approach: concept behind this approach is compare SNR_E(at eavesdropper side) $<$ SNR_B(at bob side).This approach does not require any secret key and can practically achieve perfect secrecy,most processing as at transmitter side and enhance Bob's performance. For better. It is recommended that Eve's SINR must be less than Bob's SINR and also Eve's fading must be more then Bob. Security is achieved at the cost of capacity.

ii)Complexity(key) based approach: Concept behind this approach is extracting the random keys from the channel of the legitimate user to manipulate data at the upper layer or physical layer. This approach solves the problem of key distribution. It also provide confidentiality even if Eve's channel is better than Bob's channel and provides authentication. It is assumed that Eve has limited computational power. Due to key approach computational power is essential element and so key must has limited length which effects perfect secrecy.Secrecy can not achieve if Eve is able to know Bob's channel. Most process are at transmitter and receiver both side which results in power,delay and overhead costs.Most commonly used.

In the literature, many PLS schemes have been developed. some of them are artificial noise injection, the secure beam forming/precoding, the anti-eavesdropping signal design, the cooperation-based secure transmission techniques, power allocation and resource allocation schemes, etc.

The Artificial Noise (AN) injection technique transmits the information-containing signal along with the AN, thus adversely affecting the performance of the eavesdropper. Information-bearing signals and ANs are injected into range space and null space of the legitimate user's channel matrix, respectively [22]. It is known that many AN-based PLS schemes require multiple antennas to be deployed at the transmitter[23, 24], which meets certain requirements for IoT devices such as low cost and small size. An OFDM system uses a wireless power jammer to improve secrecy. [25]. Power allocation policy was developed to maximize secrecy information rate while maintaining harvest energy requirements for the energy receiver[26, 27] . The above works are concerned about co-operative AN injection strategies are designed.

The Compressive Sensing (CS) technique compresses sparse signals with a lower sampling rate than Nyquist sampling. It was used to obtain physical layer security (PLS) in a recent study [28]. Linear transformation is used in CS to transform sparse information-bearing signals. The information-bearing signals are multiplied by a measurement matrix. If the measurement matrix is unknown to the eavesdropper the transmission secrecy can be achieved. In [29] proposed a method for constructing the measurement matrix using an m sequence. The m sequence is generated through the use of a random seed. This random seed is generated from RSSI values and RSSI values of packets exchanged between the legitimate user pairs. In ref [30], a CS-based encryption scheme was developed for multi-carrier systems. The bit flipping technique is applied to secure communications between massive sensor nodes and the legitimate fusion center (LFC). According to this method, nodes are divided into two groups based on the strength of their channel gains to the LFC.

Researchers have proposed a threshold-based bit-flipping scheme in Ref. [31]. In this scheme, LFC transmits two thresholds s and w to the sensors,to autonomously classify themselves into strong or weak groups sensors compare their channel gains with the thresholds s and w . In order to degrade the eavesdroppers' signal reception, Cooperative secrecy is a mechanism that lets friendly nodes create artificial interference by acting as a jammer. Conventionally encryption based method is used for wireless security. To achieve the comprehensive security requirements of authenticity, confidentiality, integrity, and availability different security mechanisms can be applied at each layer[1]. To prevent illegitimate access of illegitimate users, at the link layer, secure medium access control (MAC) can be used. To provide encrypted security service at the network layer Virtual Private Network(VPN) can be used.At the transport layer secure socket is deployed to authenticate legitimacy of user[6]. To encrypt user's confidential information at application layer Hyper Text Transfer Protocol can be deployed. Due to the heavy computation complexity and high resource cost, it is difficult for deploying the encryption-based security technologies into resource limited scenario, such as in low-end network in which the communication equipments may be low-cost with low battery capacity, and low complexity compatibility.

Almost every aspect of PLS for VLC is addressed in [32], including different channel models, input distributions, network configurations, precoding/signaling strategies, and confidentiality capabilities and information rates. A wireless communication system equipped with an intelligent reflecting surface (IRS) is examined to determine if artificial noise (AN) improves the secrecy rate [33]. Simulation results indicate that the new setup with IRS reflect beamforming benefits from the incorporation of AN in transmit beamforming. From the point of view of physical-layer security. In [34] investigated transmission optimization for IRS assisted multi-antenna systems. The design goal is to maximize the system secrecy rate subject to the source transmit power constraint and the unit modulus constraints imposed on phase shifts at the IRS.

2.2.1 Concluding remarks about some of the existing PLS techniques

Among the PLS methods mentioned above, each has its strengths and weaknesses. The artificial noises needed for AN injection can be generated using a pseudo-random number generator, for which a wide range of already existing algorithms can be used. While the AN injection approach provides secrecy benefits, it consumes more energy to send the artificial noise signal [22]. A secure transmission method based on CS does not require any additional power expenditure, thereby energy efficient [28]. Unlike CS-based approaches, bit flipping reduces implementation complexity and overcomes the weaknesses of CS based approach [31]. Bit flipping involves the transmission of false data by the sensors within the weak group to confuse the eavesdropper, which is a waste of power and bandwidth. Cooperative secrecy (CS) does have a major downside, namely the amount of signaling needed for devices to coordinate each other in a network, which makes the protocol design complicated. In Ref. [35] developed algorithms, respectively, to amplify-and-forward (AF) and decode-and-forward (DF) to worsen the eavesdropper channel by sending weighted artificial noises independently from the relay nodes. The enhancement of the physical layer is found in Ref. [26] where cooperative jamming and secure beamforming were combined to provide security.

2.3 Existing IoT security technique

In the context of sensing applications, IoT provides a vision of a future internet in which any object with computing, sensing, and communication capabilities can communicate with other devices using Internet protocols. Lightweight cryptography is an encryption method which is used for resource limited devices for low computational complexity. AES and SHA work Good together, they face issues in an Internet of things (IoT)/embedded world due to two much power consumption [36] and lightweight cryptography is less secured[37].

IoT devices are comprised of a variety of low-cost components. Most IoT devices have limited storage memory and rely on batteries for power, which results in very limited computing and communication capabilities. As a consequence, it is forbidden to use complicated cryptography protocols and sophisticated encryption and decryption algorithms. In contrast to traditional cryptography methods, Proposed Physical Layer Security (PLS) focuses on how wireless channels can enhance the performance at legitimate receivers.

Chapter 3

Methodology & Proposed Work

3.1 System Model

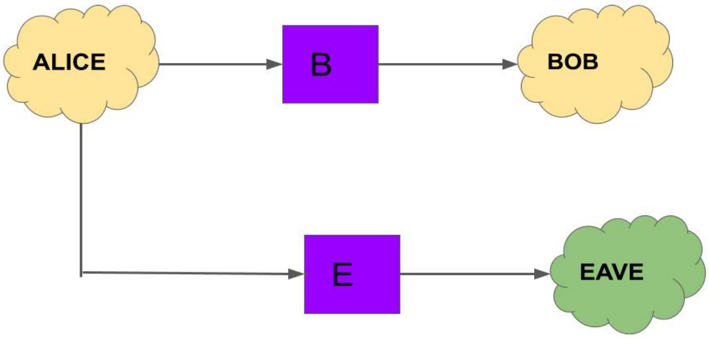

Figure 3.1: System Model

Fig. 3.1 illustrates this example of a three-node network where a third-party, Eave listens in on transmissions from Alice to Bob in order to intercept the transmissions. Communication channel from Alice to Bob is called the legitimate channel, between Alice to Eave is known as eavesdropper channel. Due to the different geographical locations of the two receivers, the signals received by them are usually different. Signals passing through the two channels are subject to different fading effects. B and E in fig. 3.1

represents channel model between Alice-Bob Alice-Eave respectively.

$$Y_B = H_B X + n_B \tag{3.1}$$

$$Y_E = H_E X + n_E \tag{3.2}$$

In equation 3.1 & 3.2 represents output at the Bob and Eave side respectively. H_B & H_E represents diagonal channel matrix. It is representation of channel fading co-efficient. X is input symbol. n_B & n_E is additive white Gaussian noise.

3.2 Block Diagram

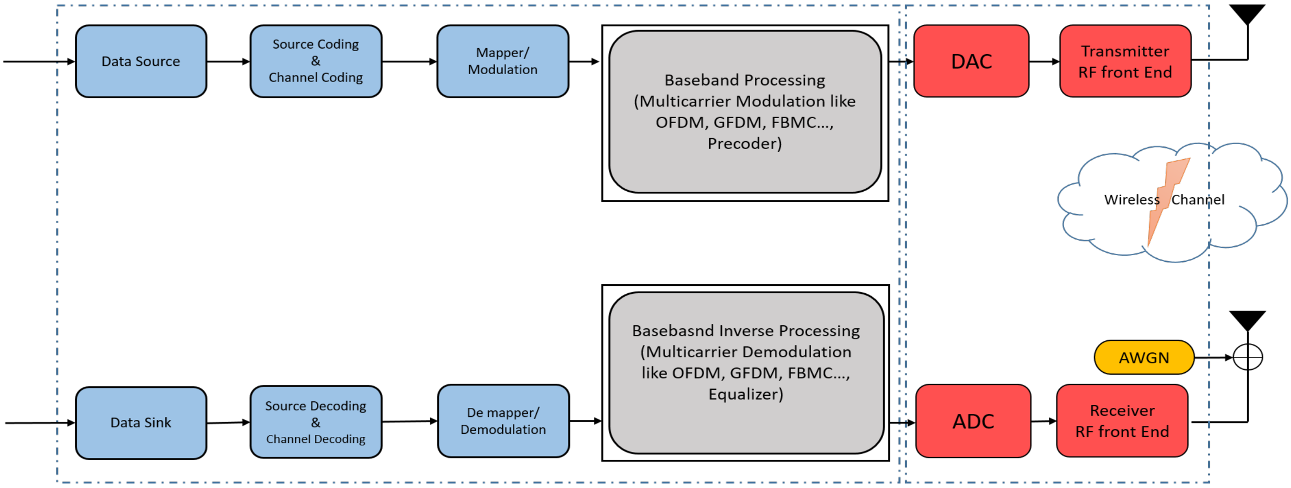
Data Source
Source Coding & Channel Coding
Mapper/ Modulation
Baseband Processing (Multicarrier Modulation like OFDM, GFDM, FBMC..., Precoder)
DAC
Transmitter RF front End
Wireless Channel
AWGN
Data Sink
Source Decoding & Channel Decoding
De mapper/ Demodulation
Basebasnd Inverse Processing (Multicarrier Demodulation like OFDM, GFDM, FBMC..., Equalizer)
ADC
Receiver RF front End

Figure 3.2: Physical Layer Block Diagram

Fig 3.2 represents Physical layer block diagram. The transmitter comprises of a source encoder,channel encoder and modulator. The information has been transmitted by data source. Analog to digital converter is used to digitized the data source. The purpose of the source encoder is to remove as much redundancy as possible from the (digitized) output of the information source. The channel encoder introduces controlled redundancy into the binary information sequence by applying error-correcting codes. The channel encoder introduces controlled redundancy into the binary information sequence by applying error-correcting codes. The primary purpose of the digital modulator is to map the binary information sequence into signal waveforms[38][39].Baseband processing includes Multi carrier Modulation scheme. Thesis focuses on OFDM & GFDM. Wireless channel introduces unintended distortion to the transmitted signal by, for example, adding noise and introducing fading . The receiver follows the reverse process of transmitter. It consists of Demodulator, Channel decoder, source decoder and DAC(Digital to Analog converter). Figure 3.3 is representation of system model in terms of block diagram. It includes proposed Physical Layer Security(PLS) technique. The green block is added in basic physical layer block diagram. It represents symbol shuffling and reshuffling according to Channel State Information(CSI) of legitimate user (Alice & Bob) channel.

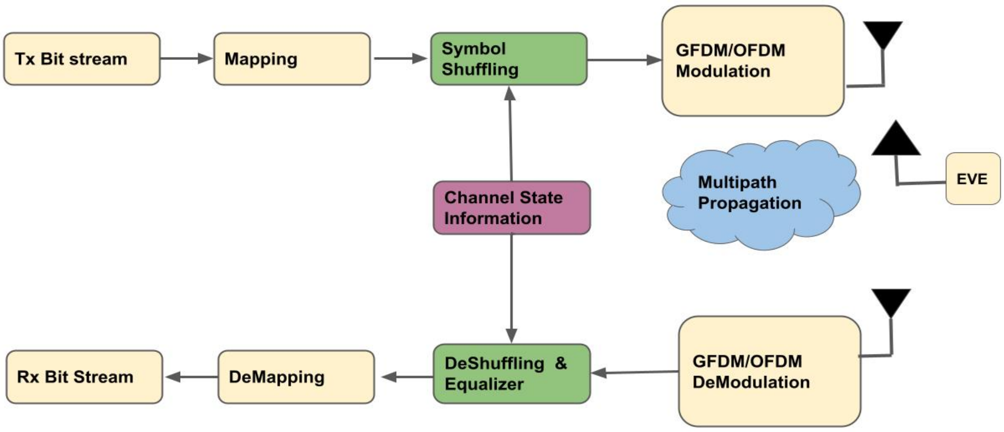

Figure 3.3: Block diagram includes Proposed PLS technique

3.3 Proposed Physical Layer Security Method

Channel matrix H$_d$ of the OFDM explained in section 1.2:

$$\mathbf{H}_d = \mathbf{E}_r \mathbf{H}_{cir} \mathbf{E}_t,$$

$$\mathbf{H}_d = \begin{bmatrix} H_0 & 0 & \dots & 0 \\ 0 & H_1 & \dots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \dots & H_{N-1} \end{bmatrix}$$

3.3.1 Methodology

High Level Idea: Input Symbols have been shuffled according to CSI of legitimate channel(Alice-Bob). So the real order of the symbol is completely unknown to eavesdropper and it is become difficult for eavesdropper to decode the information properly.

- Let's take an example for N subcarrier
- Output at Bob's side

$$Y_B = H_B X + n_B \tag{3.3}$$

$$\begin{bmatrix} Y_0 \\ Y_1 \\ Y_2 \\ \vdots \\ Y_N \end{bmatrix} = \begin{bmatrix} h_0 & 0 & \dots & 0 \\ 0 & h_1 & \dots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \dots & h_{N-1} \end{bmatrix} \begin{bmatrix} X_0 \\ X_1 \\ X_2 \\ \vdots \\ X_{N-1} \end{bmatrix} + \begin{bmatrix} n_0 \\ n_1 \\ n_2 \\ \vdots \\ n_{N-1} \end{bmatrix}$$

- Assume ascending order of CSI(Principle Diagonal elements of H$_B$)

  h$_5 < h_{17} < h_{N-2} < \dots < h_{N-4}$

- Now shuffled input symbol according to above CSI and named it as $X_{shuffle}$

$$\text{X}_{shuffle} = \begin{bmatrix} X_5 \\ X_{17} \\ X_{N-2} \\ \vdots \\ X_{N-4} \end{bmatrix}$$

$$\widetilde{Y_B} = H_B X_{shuffle} + n_B \tag{3.4}$$

$$\begin{bmatrix} Y_0 \\ Y_1 \\ Y_2 \\ \vdots \\ Y_{N-1} \end{bmatrix} = \begin{bmatrix} h_0 & 0 & \dots & 0 \\ 0 & h_1 & \dots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \dots & h_{N-1} \end{bmatrix} \begin{bmatrix} X_5 \\ X_{17} \\ X_{N-2} \\ \vdots \\ X_{N-4} \end{bmatrix} + \begin{bmatrix} n_0 \\ n_1 \\ n_2 \\ \vdots \\ n_{N-1} \end{bmatrix}$$

- Output at Eavesdropper side

$$\widetilde{Y_E} = H_E X_{shuffle} + n_E \tag{3.5}$$

- Shuffled location known to only legitimate receiver(Bob).

  – As the shuffled location is known to Legitimate receiver(Bob) only and so only Bob can decode the information with correct location.

$$\widetilde{Y_B} = \begin{bmatrix} \widetilde{Y_5} \\ \widetilde{Y_17} \\ \widetilde{Y_{N-2}} \\ \vdots \\ \widetilde{Y_{N-4}} \end{bmatrix}, \widetilde{Y_E} = \begin{bmatrix} \widetilde{Y_0} \\ \widetilde{Y_1} \\ \widetilde{Y_2} \\ \vdots \\ \widetilde{Y_{N-1}} \end{bmatrix}$$

where $\widetilde{Y_B}$ and $\widetilde{Y_E}$ is output at Bob and eavesdropper side after shuffling the input symbols.

The proposed PLS technique has been a shuffling of input symbols based on the CSI of legitimate channel (Alice-Bob) co-efficient. As per the user's preference, user can sort input symbols in ascending or descending order. Proposed PLS technique has been used legitimate channel co-efficient for shuffling order and therefore, the actual order(true order before shuffling) of the symbols is unknown to the eavesdropper, and therefore, it is difficult for the eavesdropper to decode the information properly. The effectiveness of this technique can increase as the number of sub carriers increases since eavesdroppers will have more difficulties decoding information even by brute force attack. So, proposed PLS technique is valid for multicarrier modulation schemes only. Eavesdropper is assumed to be less equipped than legitimate users here. There are some challenges in the proposed PLS technique. One of them is sharing the CSI order of legitimate channels with legitimate users (Alice & Bob) and protecting them from eavesdropping attacks.

Chapter 4

Experimental Results

The experimental setup consists of many parameters. It is vital for the experiment to consider the channel model. In this thesis, we mainly focus on the Rayleigh fading channel model, which is considered to be a reasonable assumption when the environment contains multiple objects that make the radio signal scatter before it reaches the receiver [40], like in densely populated urban areas where radio signals are likely to be scattered. Even though Rayleigh fading is important for physical layer studies, there are some other fading models, like Rician fading, Nakagami fading, Log-normal shadow fading, and Weibull fading, that are more suitable for some scenarios.

Rayleigh fading is a statistical model used to describe the effects of propagation environments on a radio signal, such as that used by wireless devices. According to Rayleigh fading models, the magnitude of a signal passing through such a medium (also known as a communication channel) will vary randomly in accordance with a Rayleigh distribution, the radial component of the sum of two uncorrelated Gaussian random variables. Rayleigh channel model used in experiments considered for multipath scenario so it is known as multipath (time delay) fading model. The detailed explanation is given in below fig. where the channel conditions for single transmitter and receiver was considered. This can be extended to multiple transmitter and multiple receiver.

CSI is one of the important parameter in the proposed PLS technique. CSI refers to channel state information (or channel properties), which describes how a signal prop-

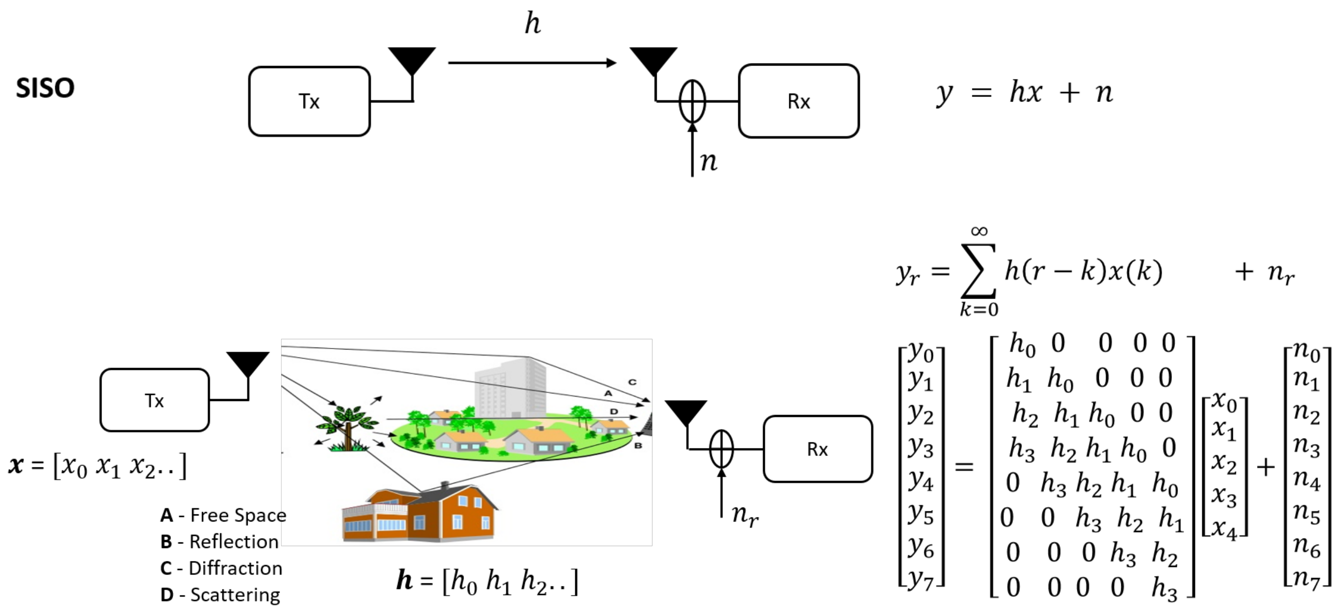
SISO
h
Tx
Rx
n
$y = hx + n$
$y_r = \sum_{k=0}^{\infty} h(r-k)x(k) \quad + n_r$
Tx
$\boldsymbol{x} = [x_0\ x_1\ x_2..]$
A - Free Space
B - Reflection
C - Diffraction
D - Scattering
A
B
C
D
$\boldsymbol{h} = [h_0\ h_1\ h_2..]$
Rx
n_r
$\begin{bmatrix} y_0\\ y_1\\ y_2\\ y_3\\ y_4\\ y_5\\ y_6\\ y_7 \end{bmatrix} = \begin{bmatrix} h_0 & 0 & 0 & 0 & 0\\ h_1 & h_0 & 0 & 0 & 0\\ h_2 & h_1 & h_0 & 0 & 0\\ h_3 & h_2 & h_1 & h_0 & 0\\ 0 & h_3 & h_2 & h_1 & h_0\\ 0 & 0 & h_3 & h_2 & h_1\\ 0 & 0 & 0 & h_3 & h_2\\ 0 & 0 & 0 & 0 & h_3 \end{bmatrix} \begin{bmatrix} x_0\\ x_1\\ x_2\\ x_3\\ x_4 \end{bmatrix} + \begin{bmatrix} n_0\\ n_1\\ n_2\\ n_3\\ n_4\\ n_5\\ n_6\\ n_7 \end{bmatrix}$

Figure 4.1: Multipath fading effect

agates from a transmitter to a receiver, such as channel gain, fading distribution, and noise strength. As a general rule, CSI can be broken down into two levels : instantaneous CSI and statistical CSI. The instantaneous CSI represents the current channel conditions, whereas the statistical CSI refers to the statistical characterizations of the channel, which can be determined by knowing the instantaneous CSI. With the instantaneous CSI, transmissions can be adjusted to the current channel conditions, which is crucial for reliable communication, whereas the statistical CSI does not have such a benefit. Other parameters used in experiment has been explained in inference section.

4.1 Comparison Of Legitimate Channel and Eavesdropper Channel capacity

Inference: Figure shows channel capacity of two different channels with eavesdropper channel being noisier than legitimate channel, which degrades eavesdropper channel performance. It could be understand by equation 4.1. The channel capacity C, is defined to

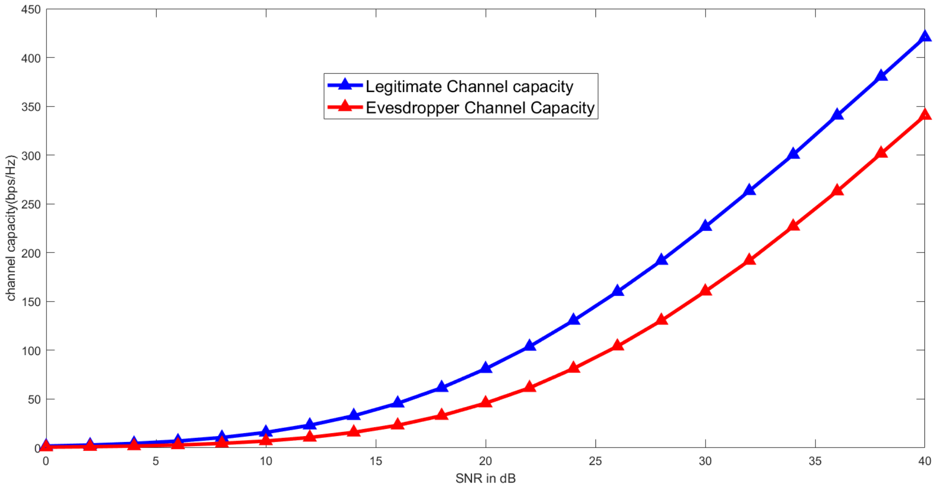

Figure 4.2: Channel capacity comparison of Legitimate & Eavesdropper channel(without PLS)

be the maximum rate at which information can be transmitted through a channel.

$$\frac{C}{W} = \log_2(1 + \frac{S}{N}) \tag{4.1}$$

where C = channel capacity

W = Bandwidth

$\frac{S}{N}$ = Signal to Noise ratio

Some of the was parameters used in Fig 4.2:

No of subcarrier = 64

Channel tap length =4

Noise variance of legitimate channel = 0.5

Noise variance of eavesdropper channel = 0.2

Modulation = OFDM

4.1.1 Effect of changing Number of subcarrier(N) & channel tap length(L) on channel capacity

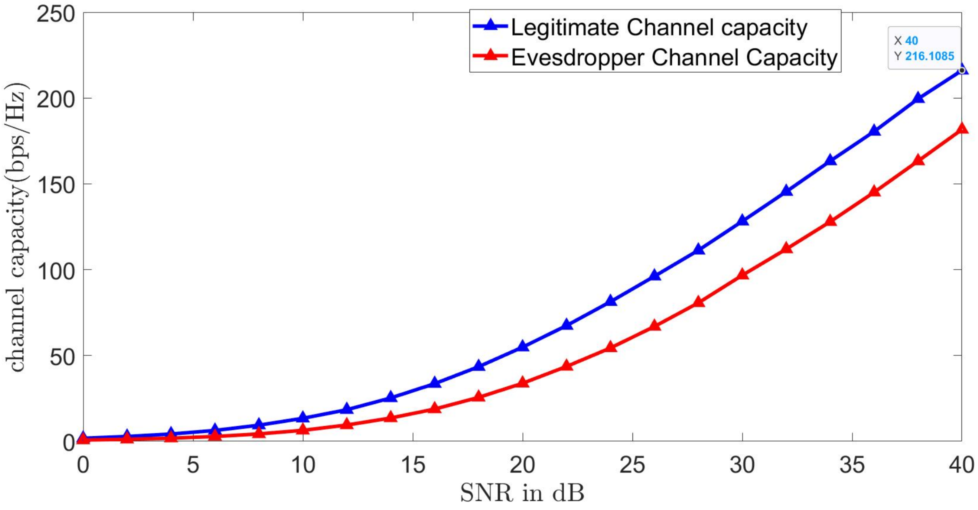

Figure 4.3: OFDM channel capacity(N=28)

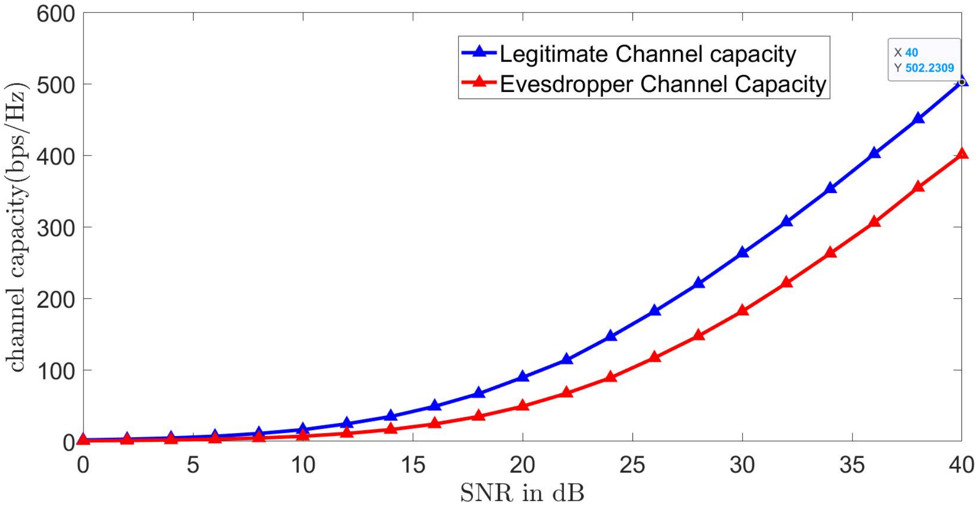

Figure 4.4: OFDM channel capacity(N=80)

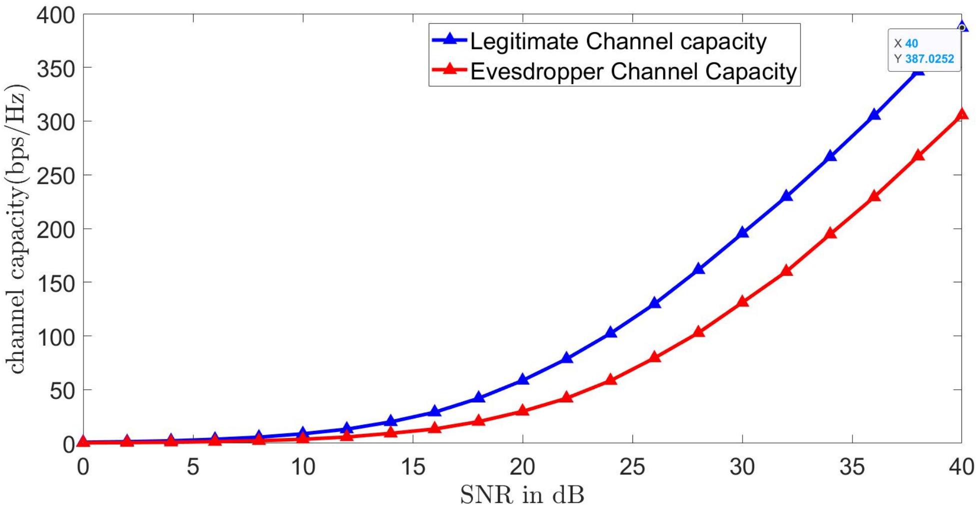

Figure 4.5: OFDM channel capacity(L=2)

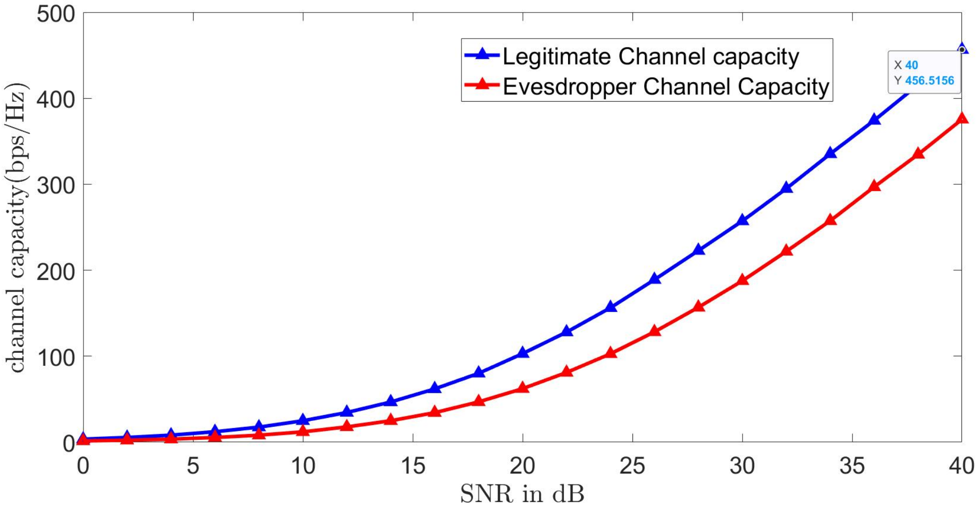

Figure 4.6: OFDM channel capacity(L=8)

Inference: Fig 4.3 , 4.4 , 4.5 & 4.6 shows the effect of changing N & L. By increasing the number of subcarriers and channel tap length, channel capacity is increased at higher value of SNR.For With a low SNR, there won't be much improvement.

4.2 Channel Secrecy Capacity

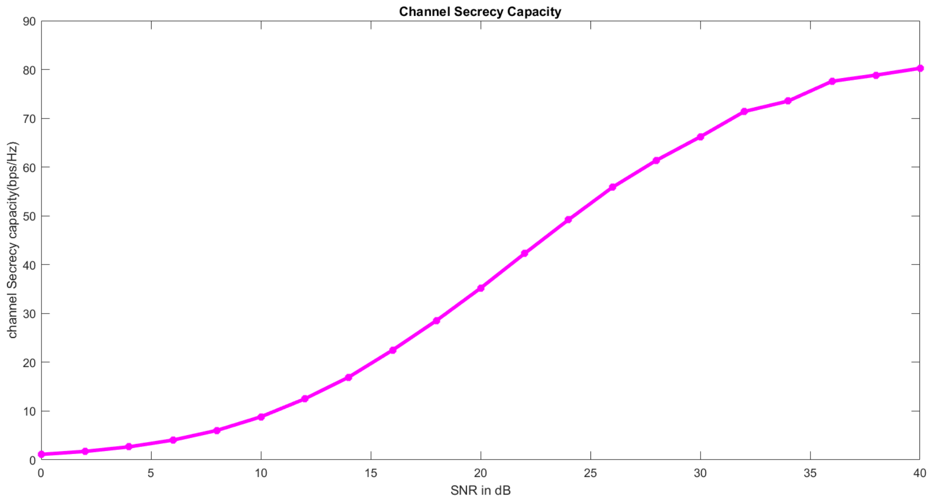

Figure 4.7: Channel secrecy capacity

Inference: The amount of confidentiality the channel is capable of preserving against eavesdroppers is its channel secrecy capacity. Channel Secrecy Capacity is difference between legitimate(between Alice & Bob) channel capacity and Eavesdropper Channel Capacity. From fig 4.7 it can be observed as SNR increases channel secrecy capacity also increases. Low SNR values could allow eavesdroppers to access confidential information(message). Secrecy capacity increases by increasing number of subcarrier(N) and channel tap length(L).

Channel Secrecy Capacity = Legitimate Channel Capacity - Eavesdropper Channel Capacity.

4.3 BER after PLS

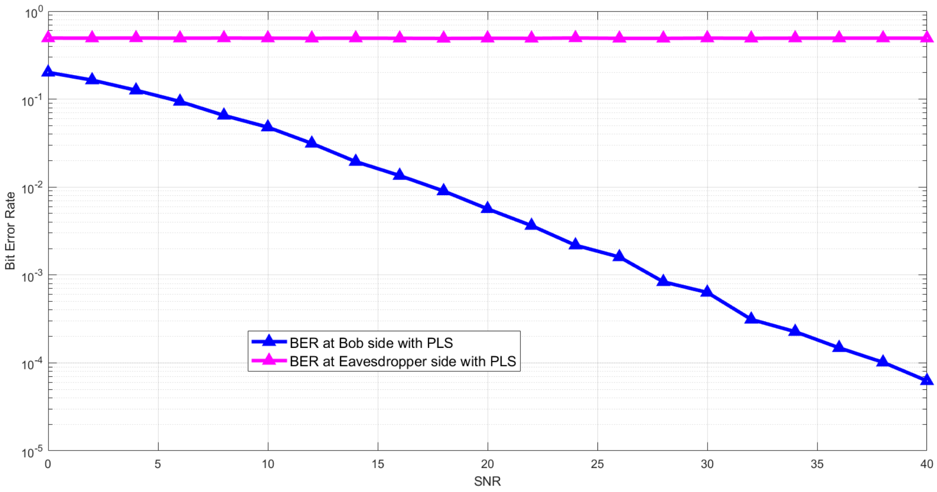

Figure 4.8: BER comparision Of BoB & Eave after PLS

Inference: It is become difficult for Eavesdropper to decode complete information. As CSI of Bob and Eavesdropper will not be same.So, even if Eavesdropper can find shuffling technique it has very less probability that ascending order of both of legitimate & eavesdropper channel will be same.

Fig 4.8 calculates BER after proposed PLS technique was applied . It was executed number of iteration times(itr).

BER_{BOB}=(1/itr)*sum(mean($Xb_{shuffle}\neq$Xb$_{hat}$))

BER_{EAVE}=(1/itr)*sum(mean($Xb\neq$Xe$_{hat}$))

In above equations comparison of symbol with shuffled location information($Xb_{shuffle}$) and received output at Bob side(Xb_{hat}) to calculate BER_{BOB}. To calculate BER_{EAVE} comparison of symbol without shuffled location information (Xb) and output received at Eave side (Xe_{hat}). As the shuffled location is only known to Bob $BER_{BOB}>BER_{EAVE}$ (in Fig 4.8).

In Fig. 4.8 signal is created with more confusion such that eavesdropper can't decode the information. In any of the cases eavesdropper error rate doesn't go beyond 0.5 as both the channel are completely different. We can consider output of fig.4.9 which is explained channel similarity with worst case scenario where error rate is approximatly 0.5

4.4 Channel Knowledge Parameter

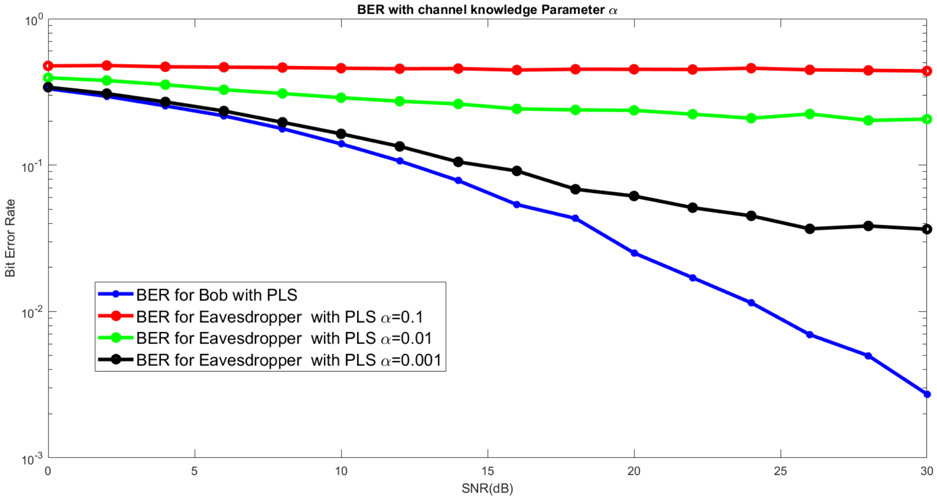

Figure 4.9: BER in OFDM after PLS with channel knowledge parameter

Inference: Here the graph represents parameter α which changes the variance of eavesdropper channel and this parameter effects the performance of Eavesdropper.The detailed case is explained in the following section.

Parameter based on channel knowledge

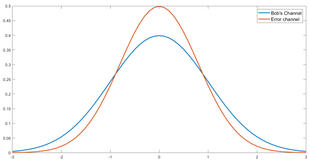

Figure 4.10: α=0.1

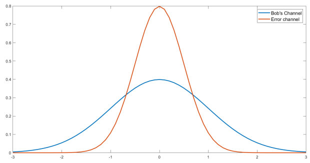

Figure 4.11: α=0.01

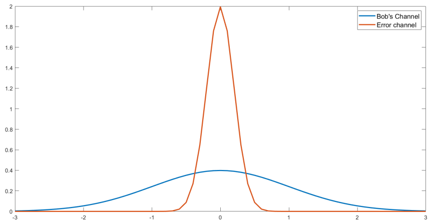

Figure 4.12: α=0.001

Inference: Eavesdropper channel is formulated using Bob's channel and error channel addition with parameter α.

Eavesdropper Channel = Bob's channel + α*Error channel.

Blue line indicates Bob's channel & Red line indicates α*Error channel

4.5 BER comparison in OFDM & GFDM after PLS Technique

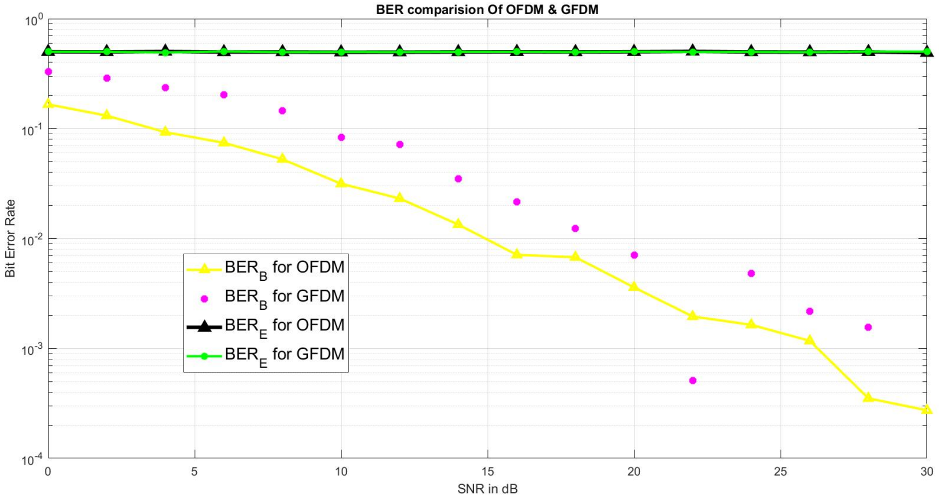

Figure 4.13: BER in OFDM & GFDM after PLS

Inference: Fig 4.13 represents BER comparison of OFDM & GFDM with the proposed PLS technique. It can be observed that OFDM outperforms compare to GFDM at legitimate(Bob) sid. At eavesdropper side both the modulation scheme perform equal because shuffelled location is unknown to it.

Some of the parameters used in this experiment(Fig. 4.13):

N_$OFDM$ = number of symbols in OFDM taken over one time period

N_$GFDM$ = number of subsymbols in GFDM taken over one time period

For the above parameter consider this below Fig. 4.14:

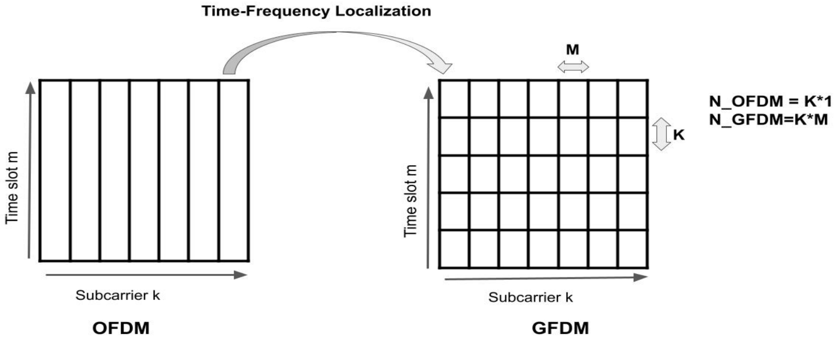

Figure 4.14: OFDM & GFDM symbol arrangement

Fig. 4.14 represents symbol arrangement in OFDM & GFDM. Where OFDM has division in frequency while GFDM has division in frequency as well as time. For the comparison purpose in this experiment both this quantity N_$OFDM$ & N_$GFDM$ should be equal.

N_$OFDM$ = 256

N_$GFDM$ = 64× 4 =256 where 4 represents number of time slot(m) in GFDM & 16 represents number of subcarriers in GFDM

4.6 Different Equalizer Comparison after PLS technique

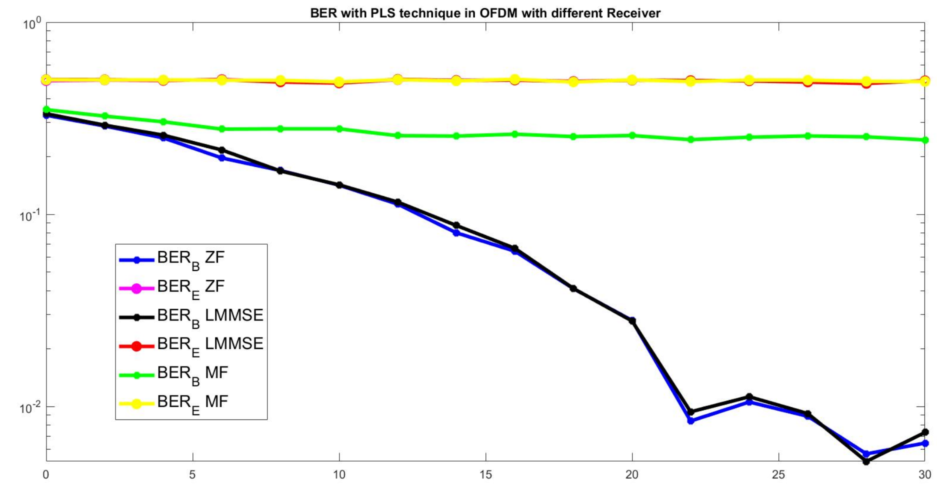

Figure 4.15: Different equalizer

Inference: From the above graph 4.15 performance of three equalizer(Zero Forcing-ZF, Linear Minimum Mean Square-LMMSE, Matched Filter-MF) have been compared interms of BER. At Bob side ZF and LMMSE(Black & Blue) coincides with each other and error decrease as SNR increases while MF gives almost constant output(Green line). In the eavesdropper all the equalizer performance is approximately constant w.r.t to SNR and it coincides(Yellow,Red & Pink).

In fig 4.15 comparison of different equalizer is shown. The mathematical equation for this three equalizer are as shown below:

Detection of input symbol using Different equalizer shown below:

1)Zero forcing(ZF)

$$\hat{X_b} = {H_b}^{-1} Y_B \tag{4.2}$$

$$\hat{X_E} = {H_E}^{-1} Y_E \tag{4.3}$$

2)Linear Minimum Mean Square Error(LMMSE)

$$\hat{X_b} = ((\frac{1}{SNR})^{-1}I + H_b^H H_b)H_b^H Y_B \tag{4.4}$$

$$\hat{X_E} = ((\frac{1}{SNR})^{-1}I + H_E^H H_E)H_E^H Y_E \tag{4.5}$$

3)Matched Filter(MF)

$$\hat{X_b} = (SNR){H_b}^H Y_B \tag{4.6}$$

$$\hat{X_E} = (SNR){H_E}^H Y_E \tag{4.7}$$

where

$\hat{X_b}$ = Detection of input symbol at Bob side

$\hat{X_E}$ = Detection of input symbol at Eaves side

Y_B = output at Bob side

Y_E = output at Eaves side

H_b & H_E = Legitimate & Eavesdropper channel matrix

4.7 Different Modulation(M) & Channel tap length(L) performance in terms of BER after PLS technique

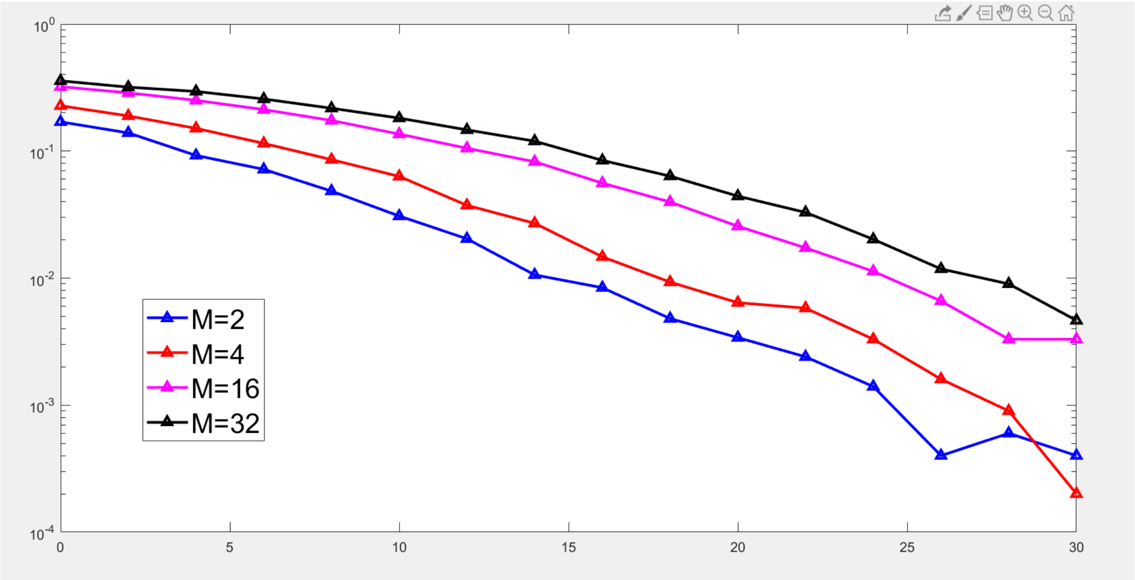

Figure 4.16: Different M

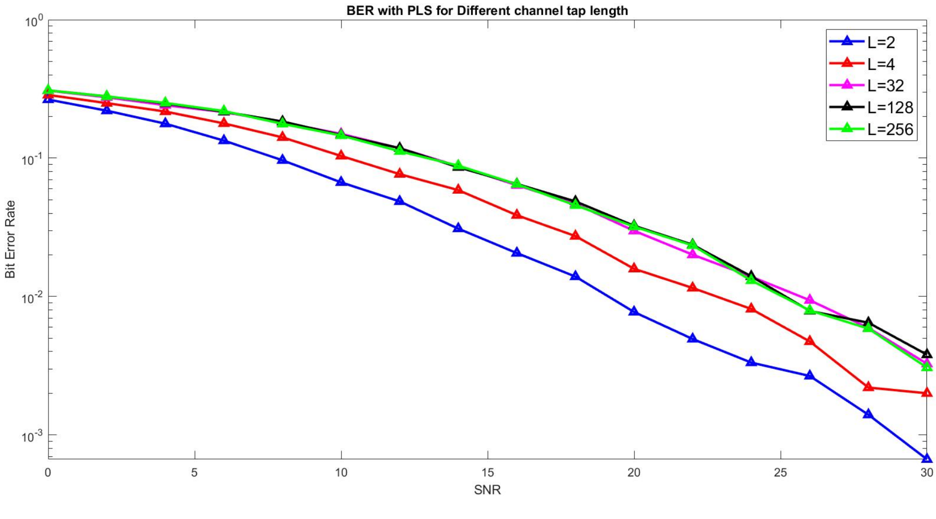

Figure 4.17: Different L

Inference: As M increases number of symbol increases and in constellation diagram distance between two symbol decreases which leads to increase in BER. As channel tap length increases BER also increases. At L=32,L=128 & L=256 almost coincides with each other.

Chapter 5

Conclusion & Future work

5.1 Conclusion

In this work, a novel Physical Layer Security(PLS) Scheme has been proposed and implemented specially for low category devices. PLS scheme has the advantages to use channel properties for the security purpose. In this thesis We have proposed PLS technique which is used Channel State Information(CSI) to shuffle the symbols.These proposed scheme is applied in Multi carrier Modulation scheme. Motive to choose multicarrier techniques is to confuse illegitimate user(eavesdropper) for security purpose so that illegitimate user(eavesdropper) can not decode the information properly. CSI of legitimate channel(between Alice & Bob) is ordered in ascending or descending order and according to that order symbols of the information(message) signal. At receiver side order of that is known to only legitimate receiver. It is unknown to illegitimate user(Eavesdropper). It is difficult to decode the information efficiently from eavesdropper side as the order of symbol is according to legitimate channel. It can be shown by experimental results of Channel capacity and Bit Error Rate(BER).Also comparison of two multicarrier modulation(GFDM & OFDM) in terms of BER compared.

IoT is composed of a large number of low-cost devices. The IoT devices are typically equipped with limited storage memory and powered with batteries, which in turn yield very limited capabilities in terms of computing and communications., complicated cryptography protocols and sophisticated encryption/decryption algorithms are prohibited from being used. This proposed PLS technique can be extend this proposed pto different multicarrier modulation scheme. This technique can be used as supplement to secure low category devices(i.e.IoT devices).

5.2 Future Work

This proposed PLS technique can be extended to different Multicarrier Modulation scheme like FBMC(Filter Bank Multicarrier) , UFMC(Universal Filter Multicarrier). This PLS technique is used CSI and so it should include more realistic and practical parameter(fading,interference & more no of eavesdropper) to observe the scenario in the practical devices. Also share the order of shuffled symbol with both legitimate users(Alice & Bob) is quite challenging in practical aspects. If eavesdropper will be strong(powered) candidate to crack this security technique then that is also future orienting problem to solve.

Appendix A

MATLAB Code

- **Comparison Of Legitimate Channel and Eavesdropper Channel capacity & Channel secrecy capacity**

```
clc;
clearvars;
close all;
set(0,'defaulttextinterpreter','Latex');
L=4;
SNRdB=0:2:40;  % SNR Range
SNR_lin=10.^(SNRdB/10);
%sigma=sqrt(
nbits=192000; % No of bits
%Xbins=60;
% hlen=4;
% h=randi([0 3],1,hlen);
%for jj=1:length(SNRdB)
%CDF=zeros(size(SNRdB));
N_itr=10000; % no of iteration
N=64;   %no of subcarriers
I=eye(N);
```

```
D = dftmtx(N)/sqrt(N);
 %Channel_capacity1=zeros(1,length(SNRdB));
 Channel_cap_main=zeros(1,length(SNRdB)); % Initialize legitimate Channel capacity matrix
Channel_cap_Eave=zeros(1,length(SNRdB));  % Intialize eavesdropper channel matrix
C_Eave=zeros(N_itr,length(SNRdB));
%C1=zeros(N_itr,length(SNRdB));
C_main=zeros(N_itr,length(SNRdB));

 for jj=1:length(SNRdB)
   for itr=1:N_itr
        %h1 = sqrt(1/2)*(rand(1,8)+1j*rand(1,8));

        %%%Main(Legitimate) channel%%%
        hm=sqrt(1/2)*(rand(1,L)+1j*rand(1,L)); % legitimate channel
        h_main = [hm zeros(1,N-L)];
        H_maincir = toeplitz(h_main,[h_main(1) fliplr(h_main(2:end))]);
        Hm=D*H_maincir*D';

        %%%eavesdropper channel%%%
        %h2=sqrt(0.1)*(rand(1,L)+1j*rand(1,L));
        h2=sqrt(0.2)*(rand(1,L)+1j*rand(1,L));
        h_eve=[h2 zeros(1,N-L)];
        H_eavecir=toeplitz(h_eve,[h_eve(1) fliplr(h_eve(2:end))]);
        He=D*H_eavecir*D';
% disp(Hcir);
%Hf = diag(fft(h_main,N));

% X=inv(SNR_lin)*Hd'*Hd;
%%% calculate Evesdropper channel capacity %%%
C_Eave(itr,jj)=log2(real(det(I + He'*He*SNR_lin(jj)/N)));
%C1(itr,jj) = log2(real(det(I + Hf'*Hf*(SNR_lin(jj)/1))));
%%%Calculate main channel capacity %%%
C_main(itr,jj)=log2(real(det(I + Hm'*Hm*SNR_lin(jj)/N)));
   end
   Channel_cap_Eave(jj)=sum(C_Eave(:,jj))/N_itr;
   %Channel_capacity1(jj)=sum(C1(:,jj))/N_itr;
   Channel_cap_main(jj)=sum(C_main(:,jj))/N_itr;
 %[pdf,rate]=hist(C,Xbins);
 %pdf=pdf/itr;

 end
 %y1=(2.^Channel_capacity1);
%semilogy(SNRdB,(2.^Channel_capacity1),'r  -*','linewidth',2); hold on
%%%plot channel capacity %%%
figure;
plot(SNRdB,(Channel_cap_main),'b  -^','linewidth',3); hold on;
plot(SNRdB,(Channel_cap_Eave),'r  -^','linewidth',3);
lgd=legend('Legitimate Channel capacity','Evesdropper
Channel Capacity');
lgd.FontSize=14;
xlabel('SNR in dB');
ylabel('channel capacity(bps/Hz)');
figure;
plot(SNRdB,(Channel_cap_main)-(Channel_cap_Eave),'m -*','linewidth',3);
xlabel('SNR in dB');
ylabel('channel Secrecy capacity(bps/Hz)');
title('Channel Secrecy Capacity');
% xlim([0 40]);
```

- **BER after PLS**

```
clc;
clearvars;
close all;
itr=1000;
N=128;
L=8;
SNRdB=0:2:48;
BER_BOB1=zeros(length(SNRdB),itr);
BER_EAVE1=zeros(length(SNRdB),itr);

BER_BOB=zeros(size(SNRdB));
BER_EAVE=zeros(size(SNRdB));
for ii=1:length(SNRdB)
    for jj=1:itr
%%%Channel coefficient from Alice to Bob channel %%%
```

```
hb=sqrt(1/2)*(rand(1,L)+1j*rand(1,L));  %randomly select channel coefficient
Hb=diag(fft(hb,N));
%Hb_diag=diag(Hb);
[Hb_diag,shuffleloc]=sort(diag(Hb),'descend'); % shuffleloc in descending order of channel co-efficient

 %%%Channel coefficient from Alice to Eavesdropper channel %%%
 he=sqrt(1/2)*(rand(1,L)+1j*rand(1,L));
 He=diag(fft(he,N));
 %Hb_diag=diag(He);

 Xb=sign(randn(N,1));   %BPSK input symbol

 %%%Initialize Variables%%%
Xb_shuffle=zeros(size(Xb));
Xb_hat=zeros(size(Xb));
Xe_hat=zeros(size(Xb));


Xb_shuffle=Xb(shuffleloc);   % shuffle input according to channel co-efficient descending order

%%% Randomly generate noise%%%
% nb=sqrt(1/2)*randn(N,1)+1i*randn(N,1);
% ne=sqrt(1/2)*rand(N,1)+1i*randn(N,1);

```

```
%%%Shuffled Output%%%
%  Yb=Hb*Xb_shuffle;%+nb; %Bob output
%  Ye=He*Xb_shuffle;%+ne; %Eavesdropper output
 Yb = awgn(Hb*Xb_shuffle,SNRdB(ii),'measured'); % Adding white Gaussian Noise
 Ye = awgn(He*Xb_shuffle,SNRdB(ii),'measured'); % Adding white Gaussian Noise
%for ii=1:L
%Xb_hat(ii)=sign(real((1/Hf_diag(ii))*Yb(ii)));
%Xe_hat(ii)=sign(real((1/Hf_diag(ii))*Ye(ii)));
%end

%%%Matched filter technique(Detection Method) %%%
Xb_hat=sign(real(Hb'*Yb)); %Detected input symbol at Bob side
Xe_hat=sign(real(He'*Ye));  %Detected input symbol at Eavesdropper side

%%%Calculating Error%%%
BER_BOB1(ii,jj)=mean(Xb_shuffle~=Xb_hat);
BER_EAVE1(ii,jj)=mean(Xb~=Xe_hat);


    end
    BER_BOB(ii)=(1/itr)*sum(BER_BOB1(ii,:));
    BER_EAVE(ii)=(1/itr)*sum(BER_EAVE1(ii,:));
end
figure;
```

```
semilogy(SNRdB,BER_BOB,'b -^','linewidth',3);grid on;
hold on;
semilogy(SNRdB,BER_EAVE,'m -^','linewidth',3);
xlim([0 40]);
lgd=legend('BER at Bob side with PLS','BER at Eavesdropper side with PLS');
lgd.FontSize=12;
xlabel('SNR');
ylabel('Bit Error Rate');
```

- **Channel Knowledge Parameter**

```
clc;
clear all;
close all;
M =  16;
N = 256;
nBits = N*log2(M);
ModType = 'QAM';      %Modulation Type
%l =[4 8 16];
l=4;
nItr = 100;          %no of iteration
BlkSize = 8;          %No of bits in one block for Encryption
SNRdB = 0:2:30;
ii=1;
 T=[0.1 0.01 0.001];
BER_PLS=zeros(length(T),length(SNRdB));
BERz_PLS=zeros(length(T),length(SNRdB));
```

```
%for l=1
for tt=T
for snr = 1:length(SNRdB)
TxBitsF = [];
RxBitsFB = [];
RxBitsFE = [];
EnBitsF = [];
RxBitsFB_PLS = [];
 RxBitsFE_PLS = [];

%y=length(TxBitsF);

for itr = 1:nItr

    TxBits=randi([0 1],nBits,1);   %randomly  input bit generated symbol
    TxBitsF = [TxBitsF; TxBits];  %

    %%%Modulation without Encryption%%%
    TxSym_PLS=Modulation(TxBits,ModType,M);


    %%%Channel co-efficient for Bob%%%
    hb=sqrt(1/2)*(rand(1,1)+1j*rand(1,1));  %randomly select channel coefficient
    Hb=diag(fft(hb,N));

    %%%shuffling%%%
    [HbS,shuffleloc]=sort(diag(Hb),'descend');

    %%%Channel co-efficient for Eavesdropper%%%
%     he=sqrt(1/2)*(rand(1,L)+1j*rand(1,L));  %randomly select channel coefficient
%     He=diag(fft(he,N));
%
errchan = sqrt(1/2)*(rand(1,1)+1j*rand(1,1));

        %for ii=1:length(tt)


    he=hb+tt*errchan;
    He=diag(fft(he,N));
    [HeS,shuffleloc1]=sort(diag(He),'descend');
    [~,ab] = sort(shuffleloc,'ascend');
    [~,ae] = sort(shuffleloc1,'ascend');

    %%%AWGN without Encryption%%%
    Yb_PLS = awgn(Hb*TxSym_PLS(shuffleloc),SNRdB(snr),'measured');
    Ye_PLS = awgn(He*TxSym_PLS(shuffleloc),SNRdB(snr),'measured');
    %%%Zero forcing Equalizer without Encryption%%%
    xb_PLS = inv(Hb)*Yb_PLS;
    xe_PLS = inv(He)*Ye_PLS;

      %%%Demodulation withput Encryption%%%
    RxBitsB1_PLS = DeModulation(xb_PLS(ab),ModType,M);
    RxBitsE1_PLS = DeModulation(xe_PLS(ae),ModType,M);

     %%%Rx bits without Encryption%%%
     RxBitsFB_PLS = [RxBitsFB_PLS; RxBitsB1_PLS];
    RxBitsFE_PLS = [RxBitsFE_PLS; RxBitsE1_PLS];

end
SNRdB(snr)

%%%Calculating Bit Error Rate without Encryption%%%
[~,BER_PLS(ii,snr)] = biterr(TxBitsF,RxBitsFB_PLS); %Ber for Bob
[~,BERz_PLS(ii,snr)] = biterr(TxBitsF,RxBitsFE_PLS);%BER for Eave

end
ii=ii+1;
end
%%%PLOT%%%
ii=1;
figure;
%semilogy(SNRdB,BER,'b -^','linewidth',2);grid on;
%hold on;
%title('

%semilogy(SNRdB,BERz,'r-^','linewidth',2);
%hold on;
```

```
semilogy(SNRdB,BER_PLS(ii,:),'b -*','linewidth',3);
hold on;
semilogy(SNRdB,BERz_PLS(ii,:),'r -o','linewidth',3);
%hold on;
%semilogy(SNRdB,BER_PLS(ii+1,:),'m -*','linewidth',2);
hold on;
semilogy(SNRdB,BERz_PLS(ii+1,:),'g -o','linewidth',3);
%hold on;
%semilogy(SNRdB,BER_PLS(ii+2,:),'y -*','linewidth',2);
hold on;
semilogy(SNRdB,BERz_PLS(ii+2,:),'k -o','linewidth',3);
%hold on;
lgd=legend('BER for Bob with PLS','BER for Eavesdropper with PLS \alpha=0.1','BER for Eavesdropper  with PLS \alpha=0.01','BER for Eavesdropper  with PLS \alpha=0.001');
lgd.FontSize = 14;
xlabel('SNR(dB)');
ylabel('Bit Error Rate');
title('BER with channel knowledge Parameter \alpha');
```

- **BER comparision in OFDM & GFDM after PLS technique**

```
clc;
clear all;
close all;
L=4;

M_OFDM  = 4;  %number of subsymbol in GFDM
```

```
N_OFDM = 64;
K = N_OFDM; % no of subcarriers in GFDM
N = 256; %Number of subcarriers in OFDM

M=2;
nBits = N*log2(M);
ModType = 'BPSK';     %Modulation Type
BlkSize = 8;
Kidx = 1:K;
SNRdB=0:2:30;
nitr=100;
%% GFDM Required Filters

% r = 0.2;
% CP = r*K;
a = 1; % Roll-Off
R=((0:(K-1))'-K/2-eps)/(a*K)+1/2;
R(R<0)=0;R(R>1)=1;
F=1-R;% Ramp rise/fall
R=R.^4.*(35 - 84*R+70*R.^2-20*R.^3);F=1-R;% Meyer auxiliary function
R=1/2*(cos(F*pi)+1);F=1-R;% Meyer RC rise/fall
R=sqrt(R);F=sqrt(F);%Meyer RRC
g=[F;zeros((M_OFDM-2)*K,1);R];

gi = g;
gq = ifft(circshift(fft(gi),M/2));
% figure;
% plot(real([gi gq]));
% Ai matrix
Ai = zeros(M_OFDM*K, M_OFDM*K);
n = 0:M_OFDM*K-1; n=n';
w = exp(1j*2*pi/K);

for k=0:K-1
 for m=0:M_OFDM-1
 Ai(:,m*K+k+1) = 1i^(mod(m,2))*circshift(gi, m*K) .* w.^(k*n);
 end
end



% Aq matrix
Aq = zeros(M_OFDM*K, M_OFDM*K);
for k=0:K-1
 for m=0:M_OFDM-1
 Aq(:,m*K+k+1) = 1i^(mod(m,2)+1)*circshift(gq, m*K) .* w.^(k*n);
 end
end

A = (Ai +Aq);


%%
```

```matlab


for snr=1:length(SNRdB)
    TxBitsF = [];
RxBitsFB = [];
RxBitsFE = [];
EnBitsF = [];
RxBitsFB_PLS = [];
 RxBitsFE_PLS = [];
 RxBitsFB_GFDM = [];
 RxBitsFE_GFDM = [];
    for ii=1:nitr
        TxBits=randi([0 1],nBits,1);   %randomly  input bit generated symbol
    TxBitsF = [TxBitsF; TxBits];  %

    TxSym  = Modulation( TxBits,ModType,N);

    %%%Modulation without Encryption%%%
    %TxSym_PLS=Modulation(TxBits,ModType,M_OFDM);


    %%%Channel co-efficient for Bob%%%
    hb=sqrt(1/2)*(rand(1,L)+1j*rand(1,L));  %randomly select channel coefficient
    Hb=diag(fft(hb,N));
    he=sqrt(1/2)*(rand(1,L)+1j*rand(1,L));  %randomly select channel coefficient
    He=diag(fft(hb,N));
    [HbS,shuffleloc_OFDM]=sort(diag(Hb),'descend');

    %%% Adding white Gaussian Noise%%%
    Yb = awgn(Hb*TxSym,SNRdB(snr),'measured');
    Ye = awgn(He*TxSym(shuffleloc_OFDM),SNRdB(snr),'measured');

    %%%Zero forcing Equalizer%%%
    xb = inv(Hb)*Yb;
    xe=inv(He)*Ye;
    %%%Demodulation%%%
    RxBitsB = DeModulation(xb,ModType,M);
    RxBitsE=DeModulation(xe,ModType,M);
    RxBitsFB = [RxBitsFB; RxBitsB];
    RxBitsFE = [RxBitsFE; RxBitsE];


     gfdm = A*TxSym;

    Hb_GFDM = kron(eye(M_OFDM),diag(fft(hb,N_OFDM))); %diag(fft(hb,M_OFDM*N_OFDM));%
    He_GFDM = kron(eye(M_OFDM),diag(fft(he,N_OFDM))); %diag(fft(he,M_OFDM*N_OFDM));%

    [HbS_GFDM,shuffleloc_GFDM]=sort(diag(Hb_GFDM),'descend');
%y = H*d;
```

```
yb_GFDM=awgn(Hb_GFDM*gfdm,SNRdB(snr),'measured');
ye_GFDM=awgn(He_GFDM*gfdm(shuffleloc_GFDM),SNRdB(snr),'measured');
dd = inv(Hb_GFDM *A)*yb_GFDM/norm(Hb_GFDM*A);
dde_GFDM=inv(He_GFDM*A)*ye_GFDM;
    RxBitsB_GFDM = DeModulation(dd,ModType,M);
    RxBitsE_GFDM=DeModulation(dde_GFDM,ModType,M);
    RxBitsFB_GFDM  = [RxBitsFB_GFDM; RxBitsB_GFDM];
    RxBitsFE_GFDM = [RxBitsFE_GFDM; RxBitsE_GFDM];

    end
    SNRdB(snr)
    %figure;
%BER_GFDM(snr)=mean(data~=data_demodulate);
[~,BER_OFDM(snr)] = biterr(TxBitsF,RxBitsFB); %Ber for Bob
[~,BERE_OFDM(snr)] = biterr(TxBitsF,RxBitsFE);
[~,BER_GFDM(snr)]=biterr(TxBitsF,RxBitsFB_GFDM);
[~,BERE_GFDM(snr)]=biterr(TxBitsF,RxBitsFE_GFDM);
end
figure;
semilogy(SNRdB,BER_OFDM,'y -^','linewidth',2);grid on;
hold on;
%xlabel('SNR');
%ylabel('Bit Error Rate');
%hold on;
semilogy(SNRdB,BER_GFDM,'m *','linewidth',3);
hold on;
```

```
semilogy(SNRdB,BERE_OFDM,'k -^','linewidth',3);
hold on;
semilogy(SNRdB,BERE_GFDM,'g -*','linewidth',2);
xlabel("SNR in dB");
ylabel("Bit Error Rate");
lgd=legend('BER_B for OFDM','BER_B for GFDM','BER_E for OFDM','BER_E for GFDM');
title('BER comparision Of OFDM & GFDM');
lgd.FontSize = 14;
%%
```

- **Different Equilizer Comparision after PLS technique**

```
clc;
clear all;
close all;
%hold on;
M =  16;
N = 256;
nBits = N*log2(M);
ModType = 'QAM';     %Modulation Type
L = 4;
nItr = 10;         %no of iteration
BlkSize = 8;         %No of bits in one block for Encryption
SNRdB = 0:2:30;
SNR_lin=10.^(SNRdB/10);
for snr = 1:length(SNRdB)
TxBitsF = [];
```

```
RxBitsFB = [];
RxBitsFE = [];
EnBitsF = [];
RxBitsFB_PLS = [];
 RxBitsFE_PLS = [];
%y=length(TxBitsF);
RxBitsB_PLS1=[];
RxBitsE_PLS1=[];
RxBitsFB_PLS1=[];
RxBitsFE_PLS1 = [];
RxBitsB_PLS2=[];
RxBitsE_PLS2=[];
RxBitsFB_PLS2=[];
RxBitsFE_PLS2 = [];


for itr = 1:nItr
    TxBits=randi([0 1],nBits,1);   %randomly  input bit generated symbol
    TxBitsF = [TxBitsF; TxBits];  %

    %%%Modulation with PLS%%%
    TxSym_PLS=Modulation(TxBits,ModType,M);


    %%%Channel co-efficient for Bob%%%
    hb=sqrt(1/2)*(rand(1,L)+1j*rand(1,L));  %randomly select channel coefficient
```

```matlab
    Hb=diag(fft(hb,N));

    %%%shuffling%%%
    [HbS,shuffleloc]=sort(diag(Hb),'descend');

    %%%Channel co-efficient for Eavesdropper%%%
%     he=sqrt(1/2)*(rand(1,L)+1j*rand(1,L));  %randomly select channel coefficient
%     He=diag(fft(he,N));
%
errchan = sqrt(1/2)*(rand(1,L)+1j*rand(1,L));
    %tt= 0.01;
    %he=hb+tt*errchan;
    he=sqrt(1/2)*(rand(1,L)+1j*rand(1,L));
    He=diag(fft(he,N));
    [HeS,shuffleloc1]=sort(diag(He),'descend');
    [~,ab] = sort(shuffleloc,'ascend');
    [~,ae] = sort(shuffleloc1,'ascend');

    %%%AWGN with PLS%%%
    Yb_PLS = awgn(Hb*TxSym_PLS(shuffleloc),SNRdB(snr),'measured');
    Ye_PLS = awgn(He*TxSym_PLS(shuffleloc),SNRdB(snr),'measured');

    %%%Zero forcing Equalizer with PLS%%%
     xb_PLS = inv(Hb)*Yb_PLS;
     xe_PLS = inv(He)*Ye_PLS;
```

```

 %%%LMMSE Receiver %%%
 xb_PLS1 = inv((1/SNR_lin(snr))*eye(N) + Hb'*Hb)*Hb'*
Yb_PLS;
  xe_PLS1 = inv((1/SNR_lin(snr))*eye(N) + He'*He)*He'*
Ye_PLS;

%%% Matched filter %%%
xb_PLS2 = SNR_lin(snr)*Hb'*Yb_PLS;
xe_PLS2 = SNR_lin(snr)*He'*Ye_PLS;

   %%%Demodulation with PLS Zero forcing%%%
 RxBitsB_PLS = DeModulation(xb_PLS(ab),ModType,M);
 RxBitsE_PLS = DeModulation(xe_PLS(ae),ModType,M);

  %%%Rx bits with PLS Zero forcing%%%
  RxBitsFB_PLS = [RxBitsFB_PLS; RxBitsB_PLS];
 RxBitsFE_PLS = [RxBitsFE_PLS; RxBitsE_PLS];

 %%%Demodulation with PLS LMMSE%%%
 RxBitsB_PLS1 = DeModulation(xb_PLS1(ab),ModType,M);
 RxBitsE_PLS1 = DeModulation(xe_PLS1(ae),ModType,M);

  %%%Rx bits with PLS LMMSE%%%
  RxBitsFB_PLS1 = [RxBitsFB_PLS1; RxBitsB_PLS1];
 RxBitsFE_PLS1= [RxBitsFE_PLS1; RxBitsE_PLS1];

  %%%Demodulation with PLS Matched Filter%%%
```

```
    RxBitsB_PLS2 = DeModulation(xb_PLS2(ab),ModType,M);
    RxBitsE_PLS2 = DeModulation(xe_PLS2(ae),ModType,M);

     %%%Rx bits with PLS Matched filter%%%
     RxBitsFB_PLS2 = [RxBitsFB_PLS2; RxBitsB_PLS2];
    RxBitsFE_PLS2= [RxBitsFE_PLS2; RxBitsE_PLS2];
end
SNRdB(snr)

%%%Calculating Bit Error Rate with PLS Zero forcing%%%
[~,BER_PLS(snr)] = biterr(TxBitsF,RxBitsFB_PLS); %Ber for Bob
[~,BERz_PLS(snr)] = biterr(TxBitsF,RxBitsFE_PLS);%BER for Eave
%%%Calculating Bit Error Rate with PLS LMMSE%%%
[~,BER_PLS1(snr)] = biterr(TxBitsF,RxBitsFB_PLS1); %Ber for Bob
[~,BERz_PLS1(snr)] = biterr(TxBitsF,RxBitsFE_PLS1);%BER for Eave
%%%Calculating Bit Error Rate with PLS Matched filter%%%
[~,BER_PLS2(snr)] = biterr(TxBitsF,RxBitsFB_PLS2); %Ber for Bob
[~,BERz_PLS2(snr)] = biterr(TxBitsF,RxBitsFE_PLS2);%BER for Eave
end
%%%PLOT%%%
%figure;
%semilogy(SNRdB,BER,'b -^','linewidth',2);grid on;
```

```
%hold on; xlabel('SNR');
ylabel('Bit Error Rate');
%semilogy(SNRdB,BERz,'r-^','linewidth',2);
%hold on;
semilogy(SNRdB,BER_PLS,'b -*','linewidth',3);
hold on;
semilogy(SNRdB,BERz_PLS,'m -o','linewidth',3);
hold on
semilogy(SNRdB,BER_PLS1,'k -*','linewidth',3);
hold on;
semilogy(SNRdB,BERz_PLS1,'r -o','linewidth',3);
hold on;
semilogy(SNRdB,BER_PLS2,'g -*','linewidth',3);
hold on;
semilogy(SNRdB,BERz_PLS2,'y -o','linewidth',3);
lgd=legend('BER_B ZF','BER_E ZF','BER_B LMMSE','BER_E LMMSE','BER_B MF','BER_E MF');
%legend('BER for Bob with symbol shuffling','BER for Eavesdropper  with symbol shuffling');
lgd.FontSize = 14;
title("BER with PLS technique in OFDM with different Receiver");
```

- **Different Modulation after PLS technique**

```
clc;
clear all;
close all;
M_matrix =  [2 4 16 32];
%M=8;
N = 5;

ModType = 'QAM';     %Modulation Type
L = 4;
nItr = 1000;         %no of iteration
BlkSize = 8;         %No of bits in one block for Encryption
SNRdB = 0:2:30;
BER_PLS=zeros(length(SNRdB),length(M_matrix));
BERz_PLS=zeros(length(SNRdB),length(M_matrix));
ii=1;
for M=M_matrix
    nBits = N*log2(M);
for snr = 1:length(SNRdB)
TxBitsF = [];
RxBitsFB = [];
RxBitsFE = [];
EnBitsF = [];
RxBitsFB_PLS = [];
 RxBitsFE_PLS = [];
%y=length(TxBitsF);

```

```
for itr = 1:nItr
    TxBits=randi([0 1],nBits,1);   %randomly  input bit generated symbol
    TxBitsF = [TxBitsF; TxBits];  %

    %%%Modulation with PLS%%%
    TxSym_PLS=Modulation(TxBits,ModType,M);


    %%%Channel co-efficient for Bob%%%
    hb=sqrt(1/2)*(rand(1,L)+1j*rand(1,L));  %randomly select channel coefficient
    Hb=diag(fft(hb,N));

    %%%shuffling%%%
    [HbS,shuffleloc]=sort(diag(Hb),'descend');

    %%%Channel co-efficient for Eavesdropper%%%
%     he=sqrt(1/2)*(rand(1,L)+1j*rand(1,L));  %randomly select channel coefficient
%     He=diag(fft(he,N));
%
errchan = sqrt(1/2)*(rand(1,L)+1j*rand(1,L));
    %tt= 0.01;
    %he=hb+tt*errchan;
    he=sqrt(1/2)*(rand(1,L)+1j*rand(1,L));
    He=diag(fft(he,N));
    [HeS,shuffleloc1]=sort(diag(He),'descend');
    [~,ab] = sort(shuffleloc,'ascend');
    [~,ae] = sort(shuffleloc1,'ascend');

    %%%AWGN with PLS%%%
    Yb_PLS = awgn(Hb*TxSym_PLS(shuffleloc),SNRdB(snr),'measured');
    Ye_PLS = awgn(He*TxSym_PLS(shuffleloc),SNRdB(snr),'measured');

    %%%Zero forcing Equalizer with PLS%%%
    xb_PLS = inv(Hb)*Yb_PLS;
    xe_PLS = inv(He)*Ye_PLS;

      %%%Demodulation with PLS%%%
    RxBitsB1_PLS = DeModulation(xb_PLS(ab),ModType,M);
    RxBitsE1_PLS = DeModulation(xe_PLS(ae),ModType,M);

     %%%Rx bits with PLS%%%
     RxBitsFB_PLS = [RxBitsFB_PLS; RxBitsB1_PLS];
    RxBitsFE_PLS = [RxBitsFE_PLS; RxBitsE1_PLS];

end
SNRdB(snr)

%%%Calculating Bit Error Rate with PLS%%%
[~,BER_PLS1(snr)] = biterr(TxBitsF,RxBitsFB_PLS); %Ber for Bob
[~,BERz_PLS2(snr)] = biterr(TxBitsF,RxBitsFE_PLS);%BER
```

```
    for Eave

end
BER_PLS(:,ii)=BER_PLS1;
BERz_PLS(:,ii)=BERz_PLS2;
ii=ii+1;
end
%%%PLOT%%%
figure;
%semilogy(SNRdB,BER_PLS,'b -^','linewidth',2);grid on;
%hold on; xlabel('SNR');
%ylabel('Bit Error Rate');
%semilogy(SNRdB,BERz_PLS,'r-^','linewidth',2);
%hold on;
semilogy(SNRdB,BERz_PLS(:,1),'b -^','linewidth',2);
hold on;
semilogy(SNRdB,BERz_PLS(:,2),'r -^','linewidth',2);
hold on;
semilogy(SNRdB,BERz_PLS(:,3),'m -^','linewidth',2);
hold on;
semilogy(SNRdB,BERz_PLS(:,4),'k -^','linewidth',2);
%semilogy(SNRdB,BERz_PLS,'r -o','linewidth',2);
%hold on;
%legend('BER for Bob with symbol shuffling','BER for
    Eavesdropper  with symbol shuffling');
lgd=legend('M=2','M=4','M=16','M=32');
lgd.FontSize = 14;
%title("BER with Symbol shuffling technique in OFDM fo")
```

- **Different Channel Tap Length after PLS technique**

```
clc;
clear all;
close all;
%M_matrix =  [2 4 16 32];
M=8;
N = 5;
L_matrix=[2 4 32 128 256];
ModType = 'QAM';     %Modulation Type
%L = 4;
nItr = 1000;         %no of iteration
BlkSize = 8;         %No of bits in one block for Encryption
SNRdB = 0:2:30;
BER_PLS=zeros(length(SNRdB),length(L_matrix));
BERz_PLS=zeros(length(SNRdB),length(L_matrix));
ii=1;
nBits = N*log2(M);
for L=L_matrix

for snr = 1:length(SNRdB)
TxBitsF = [];
RxBitsFB = [];
RxBitsFE = [];
EnBitsF = [];
RxBitsFB_PLS = [];
 RxBitsFE_PLS = [];
%y=length(TxBitsF);
```

```matlab

for itr = 1:nItr
    TxBits=randi([0 1],nBits,1);   %randomly  input bit generated symbol
    TxBitsF = [TxBitsF; TxBits];  %

    %%%Modulation with PLS%%%
    TxSym_PLS=Modulation(TxBits,ModType,M);


    %%%Channel co-efficient for Bob%%%
    hb=sqrt(1/2)*(rand(1,L)+1j*rand(1,L));  %randomly select channel coefficient
    Hb=diag(fft(hb,N));

    %%%shuffling%%%
    [HbS,shuffleloc]=sort(diag(Hb),'descend');

    %%%Channel co-efficient for Eavesdropper%%%
%     he=sqrt(1/2)*(rand(1,L)+1j*rand(1,L));  %randomly select channel coefficient
%     He=diag(fft(he,N));
%
errchan = sqrt(1/2)*(rand(1,L)+1j*rand(1,L));
    %tt= 0.01;
    %he=hb+tt*errchan;
    he=sqrt(1/2)*(rand(1,L)+1j*rand(1,L));
    He=diag(fft(he,N));
    [HeS,shuffleloc1]=sort(diag(He),'descend');
    [~,ab] = sort(shuffleloc,'ascend');
    [~,ae] = sort(shuffleloc1,'ascend');

    %%%AWGN with PLS%%%
    Yb_PLS = awgn(Hb*TxSym_PLS(shuffleloc),SNRdB(snr),'measured');
    Ye_PLS = awgn(He*TxSym_PLS(shuffleloc),SNRdB(snr),'measured');

    %%%Zero forcing Equalizer with PLS%%%
    xb_PLS = inv(Hb)*Yb_PLS;
    xe_PLS = inv(He)*Ye_PLS;

      %%%Demodulation with PLS%%%
    RxBitsB1_PLS = DeModulation(xb_PLS(ab),ModType,M);
    RxBitsE1_PLS = DeModulation(xe_PLS(ae),ModType,M);

     %%%Rx bits with PLS%%%
     RxBitsFB_PLS = [RxBitsFB_PLS; RxBitsB1_PLS];
    RxBitsFE_PLS = [RxBitsFE_PLS; RxBitsE1_PLS];

end
SNRdB(snr)

%%%Calculating Bit Error Rate with PLS%%%
[~,BER_PLS1(snr)] = biterr(TxBitsF,RxBitsFB_PLS); %Ber for Bob
```

```
[~,BERz_PLS2(snr)] = biterr(TxBitsF,RxBitsFE_PLS);%BER for Eave

end
BER_PLS(:,ii)=BER_PLS1;
BERz_PLS(:,ii)=BERz_PLS2;
ii=ii+1;
end
%%%PLOT%%%
figure;
%semilogy(SNRdB,BER_PLS,'b -^','linewidth',2);grid on;
%hold on;

%semilogy(SNRdB,BERz_PLS,'r-^','linewidth',2);
%hold on;
semilogy(SNRdB,BER_PLS(:,1),'b -^','linewidth',2);
hold on;
semilogy(SNRdB,BER_PLS(:,2),'r -^','linewidth',2);
hold on;
semilogy(SNRdB,BER_PLS(:,3),'m -^','linewidth',2);
hold on;
semilogy(SNRdB,BER_PLS(:,4),'k -^','linewidth',2);
hold on;
semilogy(SNRdB,BER_PLS(:,5),'g -^','linewidth',2);
%semilogy(SNRdB,BERz_PLS,'r -o','linewidth',2);
%hold on;
%legend('BER for Bob with symbol shuffling','BER for Eavesdropper  with symbol shuffling');
```

```
lgd=legend('L=2','L=4','L=32','L=128','L=256');
lgd.FontSize = 14;
xlabel('SNR');
ylabel('Bit Error Rate');
title("BER with PLS for Different channel tap length");
```

Bibliography

[1] Yulong Zou et al. "A Survey on Wireless Security: Technical Challenges, Recent Advances, and Future Trends". In: *Proceedings of the IEEE* 104.9 (2016), pp. 1727–1765. DOI: 10.1109/JPROC.2016.2558521.

[2] Mohammad M. Rashid, Ekram Hossain, and Vijay K. Bhargava. "Cross-layer analysis of downlink V-BLAST MIMO transmission exploiting multiuser diversity". In: *IEEE Transactions on Wireless Communications* 8.9 (2009), pp. 4568–4579. DOI: 10.1109/TWC.2009.080513.

[3] Constantinos Kolias, Georgios Kambourakis, and Stefanos Gritzalis. "Attacks and Countermeasures on 802.16: Analysis and Assessment". In: *IEEE Communications Surveys Tutorials* 15.1 (2013), pp. 487–514. DOI: 10.1109/SURV.2012.021312.00138.

[4] Paul C Van Oorschot Alfred J Menezes and Scott A Vanstone. *Handbook of applied cryptography*. CRC press, 2010.

[5] Yan Zhang Xiangyun Zhou Lingyang Song. *PHYSICAL LAYER SECURITY IN WIRELESS COMMUNICATIONS*.

[6] Dong Wang et al. "Enhancing Information Security via Physical Layer Approaches in Heterogeneous IoT With Multiple Access Mobile Edge Computing in Smart City". In: *IEEE Access* 7 (2019), pp. 54508–54521. DOI: 10.1109/ACCESS.2019.2913438.

[7] Yingbin Liang, H Vincent Poor, and Shlomo Shamai. *Information theoretic security*. Now Publishers Inc, 2009.

[8] Matthieu Bloch and João Barros. “Frontmatter”. In: *Physical-Layer Security: From Information Theory to Security Engineering*. Cambridge University Press, 2011, pp. i–vi.

[9] Junqing Zhang et al. “Design of an OFDM Physical Layer Encryption Scheme”. In: *IEEE Transactions on Vehicular Technology* 66.3 (2017), pp. 2114–2127. DOI: 10.1109/TVT.2016.2571264.

[10] Shaoshi Yang and Lajos Hanzo. “Fifty Years of MIMO Detection: The Road to Large-Scale MIMOs”. In: *IEEE Communications Surveys Tutorials* 17.4 (2015), pp. 1941–1988. DOI: 10.1109/COMST.2015.2475242.

[11] In: http://www.sharetechnote.com/html/5G/5G_Phy_Candidate_GFDM.html.

[12] Zhenyu Na et al. “Joint Subcarrier and Subsymbol Allocation-Based Simultaneous Wireless Information and Power Transfer for Multiuser GFDM in IoT”. In: *IEEE Internet of Things Journal* 6.4 (2019), pp. 5999–6006. DOI: 10.1109/JIOT.2018.2865248.

[13] Hanif Rahbari and Marwan Krunz. “Secrecy beyond encryption: obfuscating transmission signatures in wireless communications”. In: *IEEE Communications Magazine* 53.12 (2015), pp. 54–60. DOI: 10.1109/MCOM.2015.7355566.

[14] 1 H. Vincent Poora and Rafael F. Schaeferb. “Wireless physical layer security”. In: *PNAS* 114.1 (2017), pp. 19–26.

[15] J.E. Hershey, A.A. Hassan, and R. Yarlagadda. “Unconventional cryptographic keying variable management”. In: *IEEE Transactions on Communications* 43.1 (1995), pp. 3–6. DOI: 10.1109/26.385951.

[16] Robert Wilson, David Tse, and Robert A. Scholtz. “Channel Identification: Secret Sharing Using Reciprocity in Ultrawideband Channels”. In: *IEEE Transactions on Information Forensics and Security* 2.3 (2007), pp. 364–375. DOI: 10.1109/TIFS.2007.902666.

[17] Stefano Tomasin, Francesco Trentini, and Nicola Laurenti. "Secret Key Agreement by LLR Thresholding and Syndrome Feedback over AWGN Channel". In: *IEEE Communications Letters* 18.1 (2014), pp. 26–29. DOI: 10.1109/LCOMM.2013.112513.131744.

[18] Sriram Nandha Premnath et al. "Secret Key Extraction from Wireless Signal Strength in Real Environments". In: *IEEE Transactions on Mobile Computing* 12.5 (2013), pp. 917–930. DOI: 10.1109/TMC.2012.63.

[19] Reza Soosahabi and Mort Naraghi-Pour. "Scalable PHY-Layer Security for Distributed Detection in Wireless Sensor Networks". In: *IEEE Transactions on Information Forensics and Security* 7.4 (2012), pp. 1118–1126. DOI: 10.1109/TIFS.2012.2194704.

[20] Tuncer Can Aysal and Kenneth E. Barner. "Sensor Data Cryptography in Wireless Sensor Networks". In: *IEEE Transactions on Information Forensics and Security* 3.2 (2008), pp. 273–289. DOI: 10.1109/TIFS.2008.919119.

[21] Demijan Klinc et al. "LDPC Codes for the Gaussian Wiretap Channel". In: *IEEE Transactions on Information Forensics and Security* 6.3 (2011), pp. 532–540. DOI: 10.1109/TIFS.2011.2134093.

[22] Satashu Goel and Rohit Negi. "Guaranteeing Secrecy using Artificial Noise". In: *IEEE Transactions on Wireless Communications* 7.6 (2008), pp. 2180–2189. DOI: 10.1109/TWC.2008.060848.

[23] Xi Zhang et al. "Artificial-noise-aided secure multi-antenna transmission in slow fading channels with limited feedback". In: *2014 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP)*. 2014, pp. 3968–3972. DOI: 10.1109/ICASSP.2014.6854346.

[24] Gang Wang et al. "Secrecy Energy Efficiency Optimization in AN-Aided Distributed Antenna Systems With Energy Harvesting". In: *IEEE Access* 6 (2018), pp. 32830–32838. DOI: 10.1109/ACCESS.2018.2846689.

[25] Guangchi Zhang et al. “Wireless Powered Cooperative Jamming for Secure OFDM System”. In: *IEEE Transactions on Vehicular Technology* 67.2 (2018), pp. 1331–1346. DOI: 10.1109/TVT.2017.2756877.

[26] Lin Hu et al. “Cooperative Jamming for Physical Layer Security Enhancement in Internet of Things”. In: *IEEE Internet of Things Journal* 5.1 (2018), pp. 219–228. DOI: 10.1109/JIOT.2017.2778185.

[27] Mengyu Liu and Yuan Liu. “Power Allocation for Secure SWIPT Systems With Wireless-Powered Cooperative Jamming”. In: *IEEE Communications Letters* 21.6 (2017), pp. 1353–1356. DOI: 10.1109/LCOMM.2017.2672660.

[28] Amitav Mukherjee. “Physical-Layer Security in the Internet of Things: Sensing and Communication Confidentiality Under Resource Constraints”. In: *Proceedings of the IEEE* 103.10 (2015), pp. 1747–1761. DOI: 10.1109/JPROC.2015.2466548.

[29] Ruslan Dautov and Gill R. Tsouri. “Securing While Sampling in Wireless Body Area Networks With Application to Electrocardiography”. In: *IEEE Journal of Biomedical and Health Informatics* 20.1 (2016), pp. 135–142. DOI: 10.1109/JBHI.2014.2366125.

[30] Jinho Choi. “Secure Transmissions via Compressive Sensing in Multicarrier Systems”. In: *IEEE Signal Processing Letters* 23.10 (2016), pp. 1315–1319. DOI: 10.1109/LSP.2016.2595524.

[31] Hyoungsuk Jeon et al. “Secure Type-Based Multiple Access”. In: *IEEE Transactions on Information Forensics and Security* 6.3 (2011), pp. 763–774. DOI: 10.1109/TIFS.2011.2158312.

[32] Mohamed Amine Arfaoui et al. “Physical layer security for visible light communication systems: A survey”. In: *IEEE Communications Surveys & Tutorials* 22.3 (2020), pp. 1887–1908.

[33] Xinrong Guan, Qingqing Wu, and Rui Zhang. “Intelligent Reflecting Surface Assisted Secrecy Communication: Is Artificial Noise Helpful or Not?” In: *IEEE Wireless Communications Letters* 9.6 (2020), pp. 778–782. DOI: 10.1109/LWC.2020.2969629.

[34] Hong Shen et al. “Secrecy Rate Maximization for Intelligent Reflecting Surface Assisted Multi-Antenna Communications”. In: *IEEE Communications Letters* 23.9 (2019), pp. 1488–1492. DOI: 10.1109/LCOMM.2019.2924214.

[35] Lun Dong et al. “Improving Wireless Physical Layer Security via Cooperating Relays”. In: *IEEE Transactions on Signal Processing* 58.3 (2010), pp. 1875–1888. DOI: 10.1109/TSP.2009.2038412.

[36] William J Buchanan, Shancang Li, and Rameez Asif. “Lightweight cryptography methods”. In: *Journal of Cyber Security Technology* 1.3-4 (2017), pp. 187–201.

[37] Nicky Mouha. “The Design Space of Lightweight Cryptography”. In: *NIST Lightweight Cryptography Workshop 2015*. Gaithersburg, United States, July 2015. URL: https://hal.inria.fr/hal-01241013.

[38] S. Sampei. “Applications of digital wireless technologies to global wireless communications”. In: 1997.

[39] Michel C Jeruchim, Philip Balaban, and K Sam Shanmugan. *Simulation of communication systems: modeling, methodology and techniques*. Springer Science & Business Media, 2006.

[40] B. Sklar. “Rayleigh fading channels in mobile digital communication systems .I. Characterization”. In: *IEEE Communications Magazine* 35.7 (1997), pp. 90–100. DOI: 10.1109/35.601747.