Physical Layer Security Using Chaotic Communication

Abdullah Irfan

Department of Electronics

Quaid-i-Azam University, Islamabad
Pakistan

A Thesis Submitted in Partial Fulfillment of the Requirements
for the Degree of

Master of Philosophy
in
Electronics

Aug, 2023

DEPARTMENT OF ELECTRONICS
QUAID-I-AZAM UNIVERSITY
ISLAMABAD

This is to certify that the research work described in this thesis entitled "Physical layer Security Using Chaotic Communication" in fulfillment of the requirement for the award of degree of MPhil Electioncs is the original work of the author and has been carried out under my direct supervision. I have personally gone through all the research/data/results reported in this manuscript and hence certify its correctness and authenticity. I also certify that the thesis has been prepared under my supervision according to the prescribed format of the institution and I endorse its evaluation for the award of MPhil degree through the official procedures of the institute QAU.

Adviser
Prof. Dr. Muhammad Zia
Department of Electronics
Quaid-i-Azam University, Islamabad
Pakistan

Chairman
Prof. Dr. Qaisar Abbas Naqvi
Department of Electronics
Quaid-i-Azam University, Islamabad
Pakistan

Dedicated to my parents and siblings who have always been a source of inspiration and strength for me

Acknowledgements

First and foremost, I praise and acknowledge Allah Almighty, the Lord, and creator of the heavens and earth. All respect and gratitude go to the Holy Prophet Muhammad (Peace be upon him) who enlightens our hearts with the light of Islam and whose way of life has been a continuous guide for us.

I would like to express my heartiest appreciation and gratitude to my research adviser, Dr. Muhammad Zia, for providing his valuable time in spite of hectic schedule; for enlightening me with research ideas, for having insightful conversations, for his extraordinary attitude towards research and inspiring me in the times of need. I am certain that experiences gained by working under his supervision will play a crucial role in shaping my professional career.

Secondly, I am grateful to all the teachers of the Department of Electronics for their encouragement, and assistance, and entertaining my questions. I will never forget their help in clearing my thoughts on diverse topics.

I would like to acknowledge my parents and siblings for their sacrifice and assistance. This is their motivation that has allowed me to keep pushing forward. I am also thankful to all my friends for their cooperation, encouragement, and guidance throughout my university life. Finally, I would say thanks to all who have been supportive and cooperative during the research work.

Abdullah Irfan

Abstract

Wireless communication is vulnerable to active and passive eavesdropping due to its broadcast nature. Conventional security measures such as cryptography-based approaches are employed to secure data at the upper network layers. However, such security techniques may not be viable for future networks supporting internet of things (IoT) and large number of sensors due to the high cost, high implementation complexity and limited computational power. In this thesis, for physical layer security, we used chaotic maps to secure wireless communication. For the security of physical layer, two different techniques are proposed to secure data. In first technique, a non-OFDM waveform transmission is proposed with rake receiver to decode data over multipath Rayleigh fading channel. In second method, OFDM waveform is transmitted over a multipath Rayleigh channel. In proposed work, differential encoded information is spreaded with chaotic sequence and than transmitted over wireless channel. We used two different modulation techniques which are differential binary phase shift keying (DBPSK) and differential Quadrature phase shift keying (DQPSK). We observe that both transceiver designed achieve promising performance.

Contents

List of Figures

Chapter 1

Introduction

In modern era, contemporary communication links are established over the wireless channel for the variety of networks such as internet of things (IoT), devices and wireless sensor networks [1]. Due to the nature of the wireless medium, information security is a major challange [2]. Privacy of personal information and sensitive data is always major concern for the individuals, groups and companies. Conventional methods to secure private information such as cryptography provides data security at upper layers of the network model. The conventional cryptographic methods have severe drawbacks such as complexity and are feasible for systems with energy and comutational power constraints. Thus, low-power IoT devices can not work with conventional cryptographic methods due to power constraints and execution power of the systems. There are several alternate solutions such as physical layer security [2, 3] and chaos-based physical layer communication [4].

Wyner introduced the physical layer security (PLS) of the wiretap channels in [5]. PLS for wired networks can be easily established as compared to the wireless networks. The use of wireless networks has increased significantly and growing exponentially. The broadcast nature of wireless communication makes the wireless networks more vulnerable to eavesdropping [3]. Moreover, malicious attackers can also stage aggressive attempts to obstruct or tamper with illegitimate signals. There are several threats to the wireless communication links including eavesdropping, jamming, network infiltration, identity theft, and many more. Therefore, it is essential to protect the wireless transmis-

sion from the eavesdropper. PLS exploits channel resources to ensure secure communication from the eavesdropper, which may have unlimited computational power [2]. By exploiting diversity techniques, the security of the physical layer can be improved [6]. The randomness and diversity approaches for the physical layer equilibrize the limitations brought by standardized cipher-based encryption on the upper layer. PLS gained much attention in recent years [3, 7]. In particular, channel reciprocity of time-division duplex (TDD) networks exploits channel reciprocity to achieve PLS [8]. In many wireless communication systems, physical layer security is used generate encryption key by exploiting channel reciprocity TDD systems. Key generation rate is a bottleneck for the key generation from the channel randomness [9] and references therein.

Chaotic communication is an alternate choice to achieve physical layer security. The transmitter and receiver generate chaotic signal from the same map with same precision to encode and decode data, respectively. Transmitter and receiver can generate synchronzised chaotic sequences using same initial state and parameters. Note that initial state and parameter can be generated from channel reciprocity and both nodes can stay synchronized for much longer duration [10] and references therein.

1.1 Literature Review

The bit error rate for the chaos based DS-CDMA communication system over slow fading multipath channel is presented in [11]. The receiver in [11] uses simple rake receiver for decoding. The bit error rate is performed using the bit energy distribution, noise variance, and number of paths.

In [12], the author proposed a novel approach, which uses chaotic direct sequence Spread spectrum (DSSS) to improve the security of the physical layer. In this work, the symbol period changes in accordance with the chaotic spreading sequence behaviour. Consequently, the spreading pattern and symbol period changed chaotically at the same time. The primary objective is to protect data against blind estimate attacks on the DSSS-based communication system. Through computer simulation, the performance of the proposed approach in

the presence of additive white Gaussian noise (AWGN) is evaluated. The improvement in physical layer security is also assessed using numerical results.

In [13], a study of the performance evaluation of chaotic direct-sequence code-division multiple access (CDS-CDMA) and differential chaos shift keying (DCSK), both of which are used for wireless low-data rate applications. A wireless channel that is affected by noise, fading, multipath and spread delay for low chaotically spreading signal is mathematically modeled and described. BER performance for low-power chaos-based systems in wireless multipath channels is improved. This indicates that implementing chaos-based communication systems can improve physical layer security in low-rate wireless networks.

In [14], the author proposed a novel chaotic modulation based on the symbolic sequence connected to the chaotic map because most chaotic communication systems show poor performance under noise and Rayleigh fading. In this technique, instead of the typical BPSK or QAM, chaotic modulated signals are transmitted in each subcarrier of the conventional OFDM system. In the receiver, the Viterbi algorithm is used to estimate the transmitted sequence in the frequency domain.

In [15], the auther explained the drawbacks of conventional cryptographic security used for securing data which is affected in the wireless domain. In this work, a novel security technique is proposed to protect the physical layer in a wireless medium as radio channels' quick spatial, spectral, and temporal decorrelation features can improve the ability to provide secrecy authentication services.

Physical layer security (PLS) is a new method that can improve wireless security without depending on higher-layer encryption methods. From PLS legitimate users can transmit confidential information over wireless channel in the presence of an eavesdropper. In [16], the author provides a thorough analysis of OFDM-based PLS methods that offer security services such as key generation and distribution, authentication, secrecy, integrity, and availability. In this survey, the author explained different PLS techniques in literature, challenges, their current limitations and countermeasures.

In [17], physical layer security (PLS) scheme through Orthogonal frequency

division multiplexing (OFDM) based on the chaotic maps. In this work, the OFDM waveform is secured by mixing its modulated symbols and encoded information bits at the same time. A stream of bits is generated by a chaotic map from which the information is encoded. To secure of OFDM waveform, the modulated symbol is mixed up by the scrambling matrix which is created with chaotic maps. Initial conditions of the chaotic signal act as a shared secret key. For that purpose, only one key is encrypted in the first OFDM symbol as a preamble of the transmission. After the decryption of the first information at the receiver end, this information acts as a key for the next information decryption. The main advantage of this approach is that the encryption key is not sent for every transmission.

1.2 Motivation and Objective

Advancements in computing technologies bring numerous risks in cryptographic techniques because eavesdroppers can launch brute force attacks having infinite computing capabilities [18]. PLS can be achieved by implementing several convenient techniques without consuming massive communication resources and the infrastructure that shares cryptographic systems among legitimate users [19]. For the security of information mostly chaotic signals are used in which information is directly mapped and transmitted in the wireless channel. Chaotic communication is the study of chaotic dynamical systems. Chaotic signals are aperiodic, irregular and impossible to predict [20]. Due to these properties, chaotic signal enhance the security of data during wireless transmission [21].

The main objective of our research is to provide PLS utilizing chaotic maps. Because chaotic maps are highly sensitive to initial state and control parameters. Low-power IoT devices need security since cryptographic security approaches are inapplicable to them due to resource constraints and high computational complexity. The other objective of this work is our signal transmission is free of interference and antijamming.

In our proposed work, we used chaos-based OFDM and non-OFDM waveform for transmission. OFDM technology is widely used because of easy im-

plementation and has high spectral efficiency, suitable bandwidth scalability and robustness to multipath fading. Due to these properties the security of the OFDM system is more important [22]. Inter-symbol interference (ISI) is no longer an issue when utilising OFDM, and the technique is much less sensitive to synchronization errors in time.

The differential encoding technique is used to encode information bits. In differential encoding rather than transmitting absolute values themselves the difference between the consecutive symbol is transmitted and at the receiver end the first symbol is considered as reference and calculating the difference between the reference and the next symbol information is differentially decoded. In our case, we used differential phase shift keying (DPSK) to encode the information in terms of difference in phases [23]. We used DBPSK and DQPSK modulation techniques and evaluate the BER performance. The main advantage of differential encoding decoding is that the system is more robust against multipath fading and noise [24].

To get PLS, seed sharing is done through channel reciprocity in Time division duplex (TDD) mode. The main advantage of using TDD mode is that the radio propagation channel between two antennas is reciprocal and both channels have the same frequency response [25]. In simple words, the downlink and uplink transmission share the same frequency band in TDD wireless communication mode. So, this research shows that the PLS using chaotic communication in which the information bits are differentially encoded and spreaded with baseband chaotic signal. At receiver end, for chaos-based non-OFDM waveform Rake receiver is used to decode the information bits. For chaos-based OFDM waveform OFDM demodulator is used to decode the information bits over multipath Rayleigh fading channel.

1.3 Contribution

The contribution of this work is as follow:

- We proposed physical layer security using chaotic maps. The bit error rate for multipath Rayleigh channels is calculated using the proposed

method.

- We used chaos-based non-OFDM waveform transmission of signal for the information security in multipath Rayleigh fading channel and in order to remove the inter-symbol interference Rake receiver is used.
- We used chaos-based OFDM waveform transmission of signal for information security in multipath Rayleigh fading channel.

1.4 Dissertation Outline

The organization of the remaining dissertation is as follows: **Chapter 2** introduces chaos theory, chaotic maps and types of chaotic maps. Two main types of chaotic maps such as continuous-time chaotic maps and discrete-time chaotic maps are discussed. Application of finite precision chaotic maps, such as S-box and secure wireless communication are also discussed in this chapter. Different types of secure chaotic communication which are chaotic masking, Chaos shift keying (CSK), Differential chaos shift keying (DCSK) are also discussed in Chapter 2. **Chapter 3** discuss the proposed system model based on non-OFDM waveform and OFDM waveform transmission for the security of physical layer using rake and OFDM demodulator respectively. In addition, simulation results for bit error rate performance in Rayleigh fading channel are also discussed in chapter 3. **Chapter 4** concludes this work by providing a summary of our main work and contributions and also suggests possible extensions for future work.

Chapter 2

Chaos and Chaotic Communication

In this chapter, we present chaos theory, continuous-time chaotic maps and finite precision chaotic maps. We also discuss applications of finite precision chaotic maps such as S-box and chaotic communication. In this chapter, main focus is the application of discrete-time chaotic maps with finite precision to secure wireless communication link.

2.1 Chaos Theory

Chaos theory deals with study of non-linear dynamic systems, which are apparently random and are evolved from simple equation as a deterministic non-linear system. The examples of such dynamic non-linear systems are weather, turbulence, bahaviour of stock market, and human brain state. American metrologist Edward Lorenz is poineer of chaos theory in 1963. Lorenz introduced a three-dimensional non-linear first-order differential equation, which is a well-known example of chaos theory and has many applications. He observed that a small change in the initial condition of the chaotic system brings an exceptionally large difference in the states of the chaotic system [26]. Thus, chaos theory deals with non-linear deterministic systems, which are impossible to predict without the knowledge of the initial state of the system and chaotic system parameters. Chaos theory has its many application such as secure communication, image encryption and cryptography. Next, we discuss

chaotic maps and its types.

2.2 Chaotic maps

Chaotic maps are non-linear dynamical system which exhibit irregular, unpredictable and uncertain behaviour. Chaotic maps are modeled with simple equation with complex behaviour. Chaotic maps are highly sensitive to initial condition and control parameters due to the fact that a small change in parameters and initial state leads to different tracjectries. Chaotic maps evolve iteratively such that current state generate the next state.

The state of the chaotic map and paramters are represented by high precision real-numbers. However, realization of the chaotic maps on computer or embedded systems has limitation of finite precision. This leads to either convergence of map or small period of the map attributed to the finite precision [27]. In finite precision, each state of the chaotic map is represented by few number of bits. For example, under 8-bit finite precision representation has 256 possible states. Thus, repetetion of state of map or convergence has high probability. Encryption and secure wireless communication are two main applications of the chaotic maps. In cryptography, cipher text is obtained from the chaotic map, which evolves from the iterative chaotic sequence generation. For the long chaotic map, encryption and decryption function are makes it difficult for the eavesdropper to break the cryptosystem [28]. The two main types of chaotic maps are

- Continuous-time chaotic maps
- Discrete-time chaotic maps

2.2.1 Continuous-time Chaotic maps

The continuous-time chaotic maps are dynamic systems, which use differential equations to generate chaos. These maps are realized using analog circuit [29]. Furthermore, continous-time chaotic maps are sensitive to the initial state

and parameters. That is, small changes in the initial condition can lead to different trajectories with respect to time. The trajectories of the continous-time chaotic maps highly depend on the parameter selection. The general equation of continuous chaotic system is

$$\frac{du}{dt} = F(u, t), \tag{2.1}$$

where $u(t)$ is continuous-time chaotic signal. The most common examples of continuous-times chaotic maps are Lorenz system, Chua system, Rösssler system and Duffing oscillator. Lorenz system is a well-known example of the continuous chaotic map, which produces complex structures, unexpected real-valued sequences of the system variable. Lorenz system consist of three initial values and three system parameters [30]. The equation of three-dimensional dynamic Lorenz system is

$$\begin{aligned} \frac{dx}{dt} &= \sigma(y - x) \\ \frac{dy}{dt} &= x(\rho - z) - y \\ \frac{dz}{dt} &= xy - \beta z \end{aligned} \tag{2.2}$$

where, σ, ρ and β are the system parameter and x, y and z is the initial state of Lorenz system.

2.2.2 Discrete-time Chaotic maps

Discrete-time chaotic systems are used to generate discrete chaotic sequence by non-linear difference equation [29]. The application of discrete-time chaotic maps with finite precision are S-box generation, pseudo random number generation and secure wireless communication. The most widely used discrete-time chaotic maps are logistic map, tent map, quadratic map, and Henon map. The general equation of the discrete chaotic system is

$$u_{n+1} = F(u_n), \tag{2.3}$$

where u is an initial seed value and u_n are iterated value for discrete-time chaotic system. $F(.)$ is the function of chaotic map in which u_n is the present state and u_{n+1} is the next state. In discrete system, present value acts as a seed for the next value.

Logistic map is an example of discrete-time chaotic map and most widely used due to its simple mathematical equation, complex dynamics and behaviour [31]. Logistic map is one-dimensional map which exhibits chaotic behaviour under infinite precision. The mathematical equation of logistic map is

$$u_{n+1} = \lambda u_n(1 - u_n), \tag{2.4}$$

where λ is the control parameter which can have any value between $[0\ 4]$, u_n is an current state and u_{n+1} is the next value. Note that $0 \leq u_n \leq 1$. Realization of discrete chaotic maps such as logistic map on computer systems or microcontroller has limitation of finite precision. The finite precision of the states of chaotic map leads to either periodic behavior of the chaotic map or convergence. Thus, short cycle of the discrete-time chaotic map is a major for the secure system. Many works has been published to enhance periodic length of the discrete-time chaotic map [32, 33].

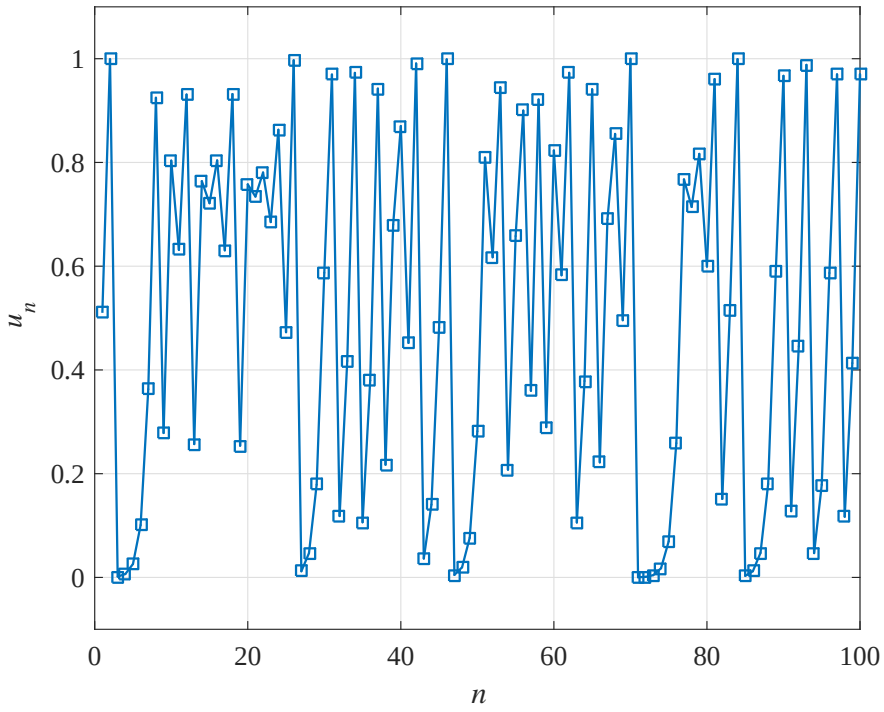

Figure 2.1: Logistic map with parameter value $\lambda = 4$ and initial value $u_0 = 0.5101$

In Fig 2.1, logistic map is generated for 100 iteration, which shows different values at different points. If we change the value of control parameter and initial value, then result will be completely different due to sensitivity of the chaotic maps to the initial state.

2.3 S-Box

The substitution box is used in crptosystem to provide confusion property described by Shannon in his work [34]. S-box is basic component of symmetric key algorithms in crptography used in block ciphers to create confusion. Strong block ciphers is resistant to linear and differential crptanalysis. S-box is used in almost all conventional cryptographic systems, such as the Advanced Encryption standard (AES), the Data Encrption standard (DES) and

many more. In terms of mathematical representation, the nonlinear mapping of S-box is $S(x) = (f_{n-1}(x), \ldots, f_0(x)) : F_2^n \rightarrow F_2^n$ for $n \times n$ matrix. Where, $\{0,1\}^n$ denotes the vector spaces of n elements from $GF(2)$ and $f_i(0 \leq i \leq n-1)$ is boolean function [35]. Different discrete-time chaotic maps are used to generate S-box because of sensitivity to initial conditions and random behaviour [36]. S-box generation is tested on the different number of criteria to exhibits good cryptographic properties, such as nonlinearty, bijection, output bits independence criterion, strict avalanche criterion and maximum expected linear probability [37].

2.4 Chaotic Communication

Chaotic communication in which chaotic signal is used for transmiting and receiving information. Chaotic communication is used to secure the transmission of data for different telecommunication technologies and used chaotic systems to produce complex dynamic behaviour. Since 1990, the chaotic secure communication becomes hot topic for researchers. Chaotic communication signals are spread spectrum signals which have large bandwidth. In conventional communication systems, the analog signal is sent through the channel consists of sums of sinusoid waveforms which is linear. However, in chaotic communication, chaotic waveform consists the segments of samples which is non-linear. Chaotic communication has numerous advantages which makes it more attractive for communication due to its non-linear behaviour, unstable and aperiodic characteristics. Chaotic signals are wide-band signals which offer cheaper solutions as compared to conventional spread spectrum systems and are resistant to multipath fading [38]. There are different chaotic communication techniques used for secure communication and the most frequently used techniques are

- Chaotic masking
- Chaos shift keying communication
- Chaotic parameter modulation

2.4.1 Chaotic Masking

Chaotic masking is a technique used for chaotic analog communication. In chaotic masking a signal which is generated from a chaotic system is superimposed on the message signal directly means a noise-like signal is added to the information-bearing signal. At receiver, the information is obtained by subtracting the chaotic masked signal from message signal [39, 40]. In chaotic masking technique, the transmitter and receiver are synchronized with each other to produce the same chaotic sequence otherwise the decoding of correct information is difficult [41].

2.4.2 Chaos Shift Keying Communication

Chaos Shift Keying (CSK) technique is used for chaotic digital communication. In selective application domains, chaotic modulation scheme shows unique features of chaotic basis function [42]. There are several modulation techniques are used in CSK. The most commons are

- Chaos shift keying (CSK)
- Differential chaos shift keying (DCSK)

2.4.2.1 Chaos Shift Keying (CSK)

Chaos shift keying is a digital modulation technique [43] use to mapped each symbol in different chaotic attractor explain in Fig 2.2. In transmitter, two chaos sequence generators z and v produces chaotic signal z_t and v_t respectively. If the information bit is $+1$ then z_t is transmitted for specified time interval and for -1 v_t is transmitted for specified time interval. CSK system works on the basis of self synchronization in which receiver and transmitter are synchronized with each other. The same sequence is generated in transmitter and receiver for different bit. In receiver, the received signal is correlated with the reference signal produced at receiver side to decide whether the bit 1 or -1 [44].

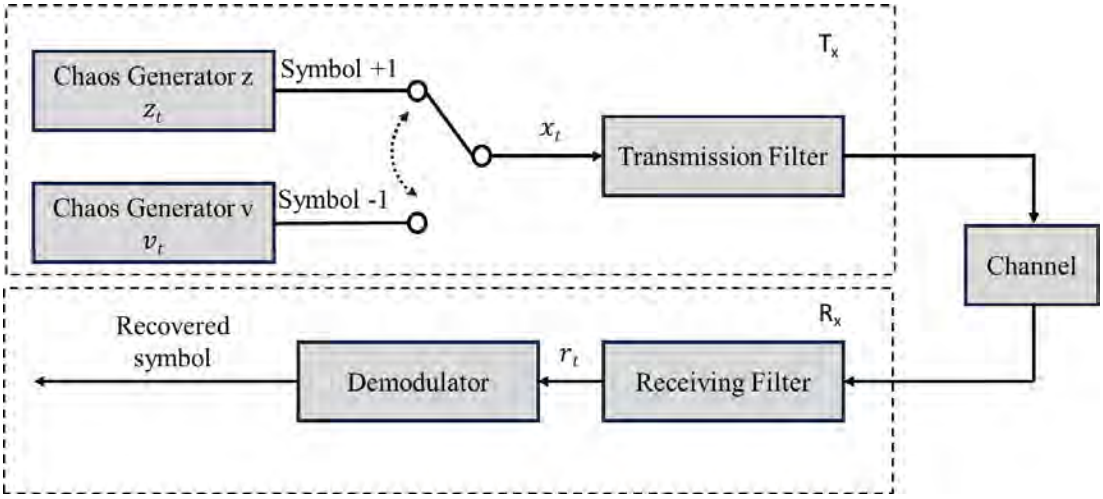

Figure 2.2: Block Representation of transmitter and receiver for CSK

2.4.2.2 Differential Chaos Shift Keying (DCSK)

DCSK in Fig 2.3 explains, every information-carrying bit consists of two chaotic sample slots. The first one represents reference signal and second one contains information [45]. In second slot, if the transmitted bit is $+1$ then the transmitted signal is same as the reference signal and if the transmitted bit is -1 the transmitted signal is inverse of reference signal [46]. For every bit, the transmitted output of the chaotic sequence u_n of length K followed by the same sequence multiplied by the information signal $\mathrm{b}_i = \pm 1$.

$$x_n = \begin{cases} u_n & 0 < n \leq K \\ \mathrm{b}_i u_{n-K} & K < n \leq 2K \end{cases} \tag{2.5}$$

Furthermore, the transmitted signal pass through flat fading channel and additive white Gaussian noise is added to received signal. The mathematical representation of received signal is

$$r_n = h x_n + w_n \tag{2.6}$$

In order to recover the information, the received signal r_n is passed through

the correlator. In correlator, the reference samples and information samples are correlated and the output of the correlator for i-th bits is [46]

$$\alpha_i = T_c \sum_{n=1}^{K} r_n r_{n+K}, \tag{2.7}$$

where T_c is chip time. The output for i-th bit is decoded by comparing the α_i to threshold value which is zero.

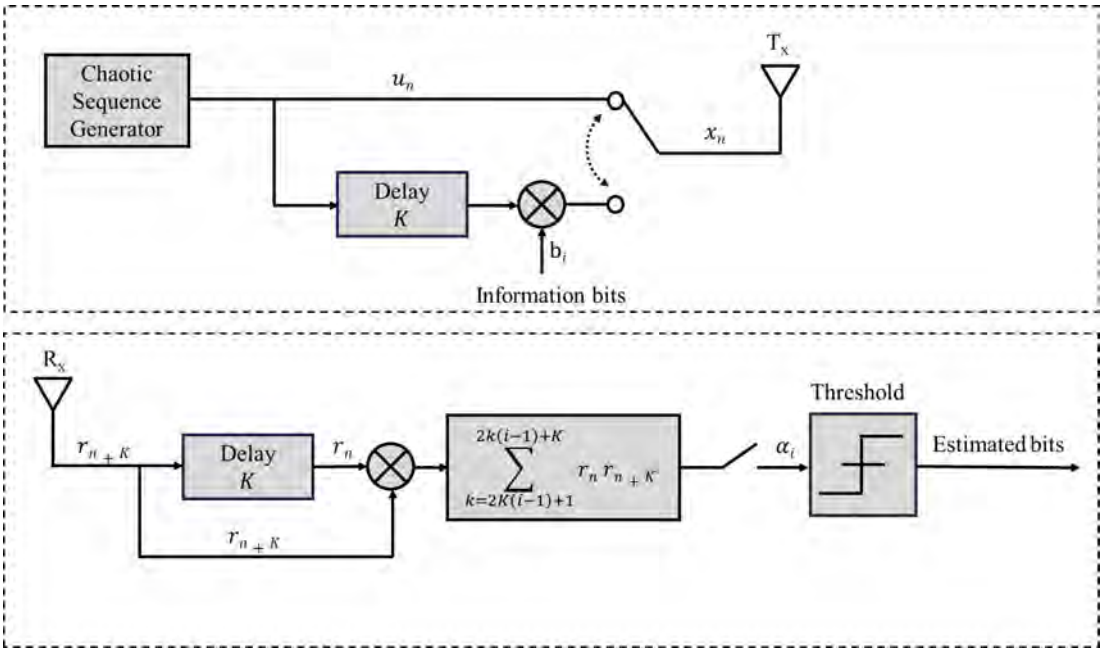

Figure 2.3: Block Representation of transmitter and receiver for DCSK

2.4.3 Chaotic Parameter Modulation

Chaotic parameter modulation is also known as chaotic switching. Chaotic switching is one of the simplest form of chaotic parameter modulation. In this scheme, the information signal consists of binary data. Binary data is used to modulate one or more parameters of the chaotic system for transmisssion. At transmitter, for both 1 and 0, there are different sets of parameters for modulation. At receiver, the information is decoded by using the synchronization

error to decode the data and the received signal corresponds to which set of parameter [47].

2.5 Summary

In this chapter, we briefly discussed chaos theory, chaotic maps. We focused on the two main types of chaotic maps, which are continuous-time chaotic map and discrete-time chaotic map. Application of discrete-time chaotic maps such as S-box and chaotic communication is also discussed in this chapter. Different types of chaotic communication such as chaotic masking, chaos shift keying (CSK), differential chaos shift keying (DCSK) and chaotic parameter modulation are discussed in this chapter.

Chapter 3

Physical layer security and Chaotic Maps

In this chapter, we discuss the proposed method for the physical layer security using chaotic maps for communication. The logistic map is used to generate a chaotic sequence, which is discrete in nature and highly sensitive to the initial conditions. For physical layer security, we used differentially encoded data, which is spreaded with the specified length of chaotic sequence. In the proposed model, a chaotic modulated non-OFDM waveform and chaotic modulated OFDM waveform is transmitted over the flat-fading and multipath Rayleigh fading channel. OFDM is widely employed in broadband wireless communication systems, mainly due to the fact that it offers high data rates with low computational complexity. OFDM is resistant to multipath fading. The proper use of chaotic maps in OFDM can enhance the security at the physical layer level.

3.1 System Model

In the proposed system model for physical layer security (PLS) in fig 3.1, the chaotic sequence is generated by the logistic map, which is discrete in nature. The transmitter and receiver are synchronized with each other by using the same initial state and parameters. Both communicaion nodes can gener-

ate the same initial states and parameters from the channel reciprocity under TDD mode [8]. Thus, initial state and parameters are not shared over wireless medium. In TDD mode, uplink and downlink share the same frequency band during the wireless transmission. In the system model, transmitter spreads information bits with the dynamic spreading code generated from the discrete-time chaotic map such as logistic map and quadratic map. In low signal-to-noise ratio (SNR) regime, acquiring channel state information is not reliable. Thus, receive signal strength (RSS) can be used to acquire partial channel state information [48, 49].

Acquisition of the channel state information (CSI) is not viable in low SNR regime and differential encoder encodes the information in terms phase difference between the neighbouring symbols of the M-PSK. The differentially encoded data is spreaded by the dynamic spreading code generated from the chaotic sequence. We propose OFDM based and non-OFDM transmission modes to transmit a differentially encoded information symbols along with dynamic spreading codes. At the receiver end, interoperable receive chain is enabled to decode the transmitted information bits. Next, we discuss the two aforementioned transceiver separately in the following sections.

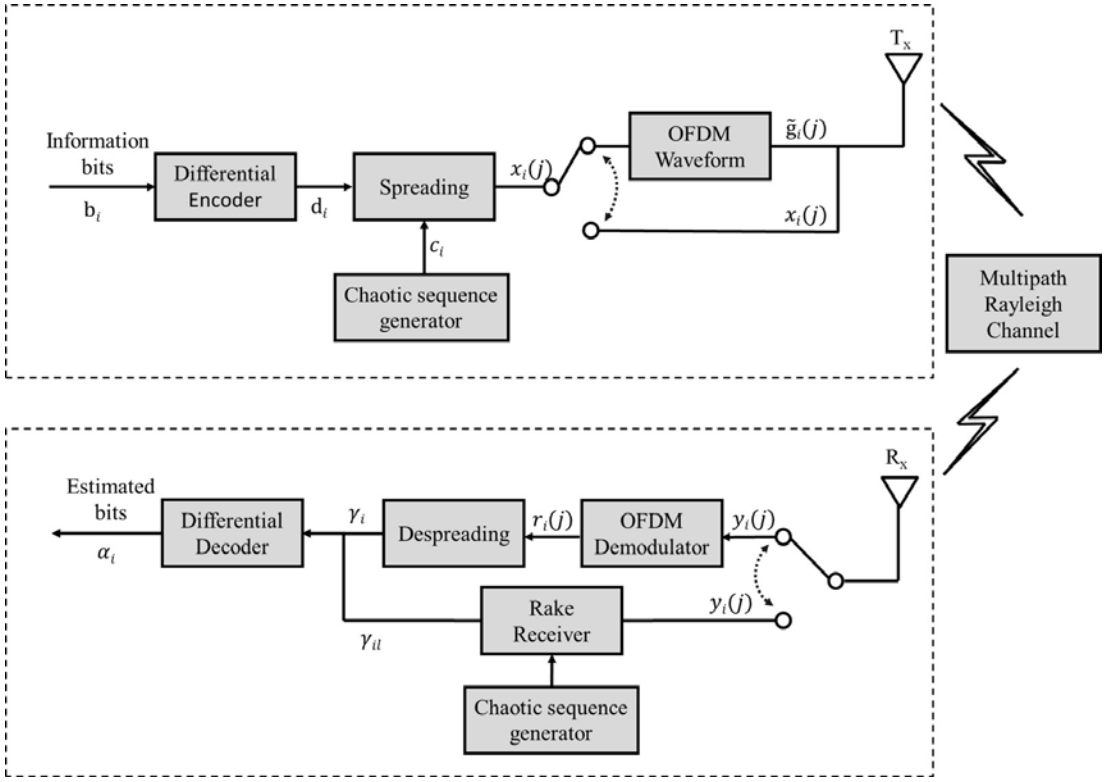

Figure 3.1: System model for the chaos based communication to secure information

3.1.1 Non-OFDM Transceiver Design

In non-OFDM proposed transmission method, chaotic sequence spreads differentially encoded data using logistic or quadratic map. In the proposed approach, we use logistic map to generate a discrete-time chaotic signal. Each differentially encoded information symbol is spreaded with a dynamic chaotic code (sequence) of length K. Finally, the spreaded message signal is transmitted over the dynamic flat-fading or frequency selective wireless Rayleigh fading channel. We assume additive white Gaussian noise (AWGN) for the system.

In receiver, the multiple signals from the each path is combined to achieve

better performance. To recover the information, we design rake receiver, where different sub-receivers are used to counter multipath fading also called fingers. Each finger is used to decode the information independently and the received signal with a different delay is correlated with the reference chaotic signal. The superpositon of the correlation of the fingers provides good estimate of the angle, which is used to decode transmitted bits.

In the proposed transmitter for non-OFDM waveform in fig 3.2, we spread basedband signal with spreading code $\mathbf{c}_i \in \mathcal{R}^{K\times 1}$ generated from the chaotic map. We use logistic map, which is an one-dimensional discrete-time map. The mathematical representation of the unipolar logistic map is

$$u_{n+1} = \lambda\ u_n\ (1 - u_n). \tag{3.1}$$

The biase of unipolar logistic map is -0.5. The bipolar chaotic spreading code for the i-th information symbol is

$$\mathbf{c}_i = u_{iK:(i+1)K-1} - 0.5, \tag{3.2}$$

where, $i = 0, 1, 2, 3, \ldots, \infty$ and K is spreading factor. Thus, spreaded baseband signal is

$$\mathbf{x}_i = \mathrm{d}_i \mathbf{c}_i. \tag{3.3}$$

Note that the $\mathbf{x}_i \in \mathcal{C}^{K\times 1}$ and $x_i(j)$ is the j-th element of $\mathbf{x}_i$ where, $j = 0, 1, 2, \ldots, K-1$. Here d_i is differentially encoded data and $\mathbf{c}_i$ is spreading sequence from chaotic map u_n. The output of channel is

$$y_i(j) = \sum_{l=0}^{L-1} h_l x_i(j-l) + w(j), \tag{3.4}$$

where l represent sample delay of l-th path, h_l is path gain and L is a total number of paths and $w(j)$ is additive white Gussain noise. In the proposed receiver, for non-OFDM waveform in fig 3.4, the received signal encounters multipath channel effect. To mitigate the channel impact from multipath sig-

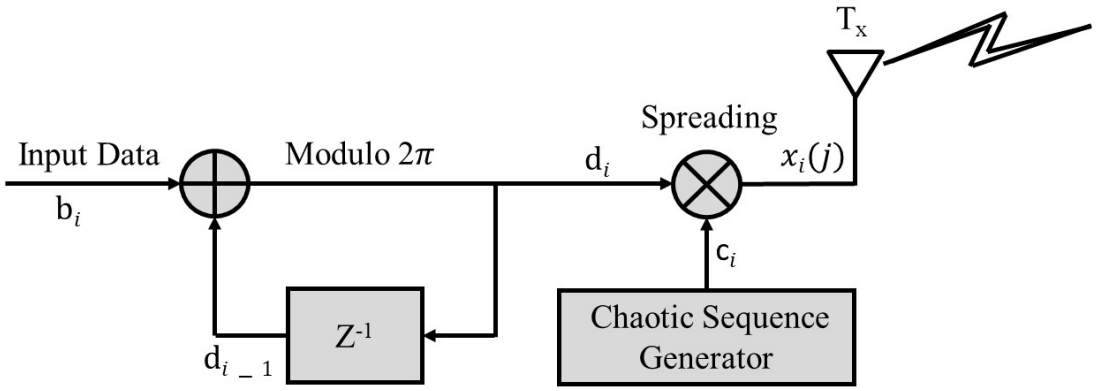

Figure 3.2: Block representation of Transmitter for non-OFDM Waveform Transmission

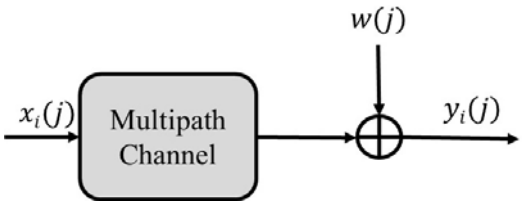

Figure 3.3: Channel For Transmission

nal, the received signal is separately correlated with the reference chaotic sequence in each finger of rake receiver for L number of paths. In the first finger , the received signal without any delay is correlated with the reference chaotic sequence. Thus, ℓ-th finger correlates reference signal with the received signal delayed by $\ell - 1$ samples. The mathematical representation for multiple fingers of the rake receiver is

$$\begin{aligned} \gamma_{i1} &= \mathbf{c}_i \mathbf{y}_{i0}^{\mathsf{T}} \\ \gamma_{i2} &= \mathbf{c}_i \mathbf{y}_{i1}^{\mathsf{T}} \\ &\vdots \\ \gamma_{i\ell} &= \mathbf{c}_i \mathbf{y}_{i\ell-1}^{\mathsf{T}} \end{aligned} \tag{3.5}$$

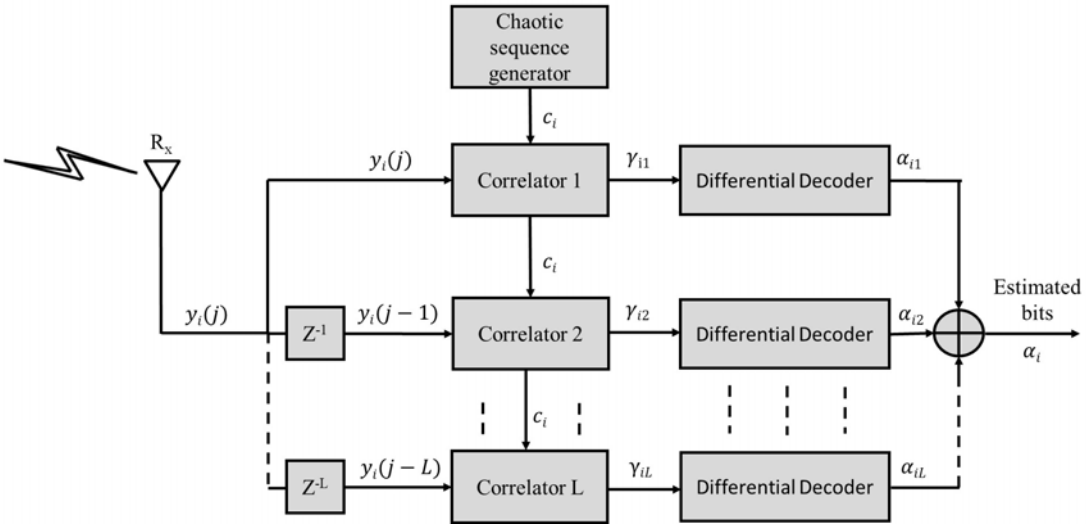

Figure 3.4: Block representation of receiver for non-OFDM Waveform Transmission

The general equation for ℓ-th correlator is

$$\gamma_{i\ell} = \mathbf{c}_i \mathbf{y}_{i\ell-1}^{\mathsf{T}} \quad l = 1, 2, \ldots, L-1 \tag{3.6}$$

Thus, we have correlation vector $\mathbf{a}_i = [\gamma_{i1} \quad \ldots \quad \gamma_{iL}]^T$ for the L paths corresponding to the i-th differentially encoded information symbol. The differential decoder for the L-path channel is

$$\alpha_i = \mathbf{a}_i^H \mathbf{a}_{i-1} \tag{3.7}$$

The information is enoded in angle of α_i.

3.1.2 OFDM Transceiver Design

Figure 3.5 presents the proposed chaos-based OFDM communication model. Instead of transmitting differentially encoded information spread by dynamic chaotic code, we design OFDM waveform. OFDM waveform mitigates the inter-symbol interference and converts single frequency selective channel into

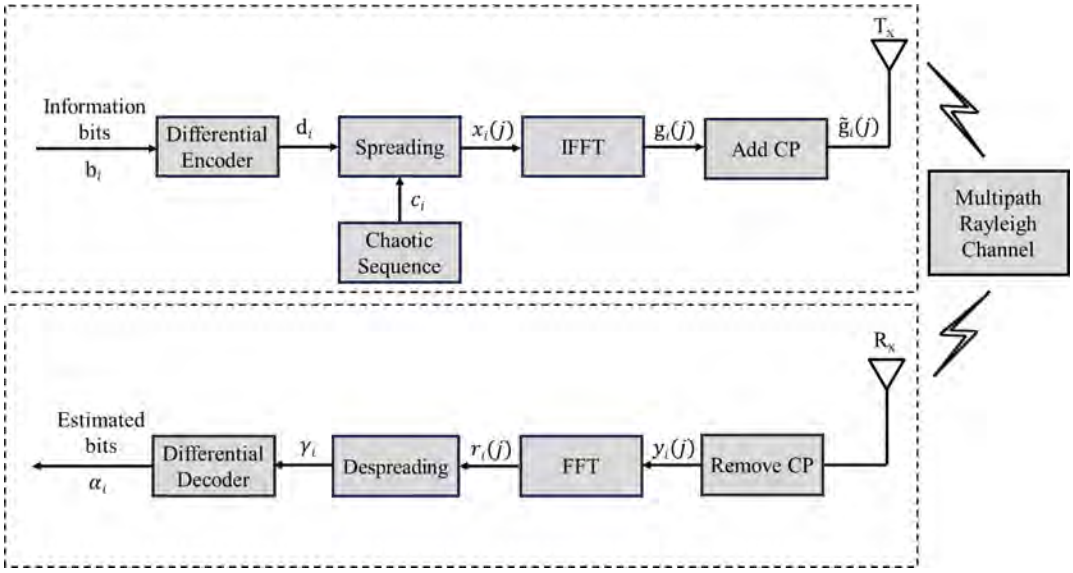

Figure 3.5: The proposed block representation of chaos-based OFDM Model for transmitter and receiver

N parallel flat-fading channels [50]. In the proposed transmitter with OFDM waveform, the code $\mathbf{c}_i$ of length N from the discrete-time logistic map spreads differentially encoded bit d_i. The chaotic spreading code for the i-th information symbol is given in (3.2). Thus, spreaded baseband signal is

$$\mathbf{x}_i = \mathrm{d}_i \mathbf{c}_i. \tag{3.8}$$

Note that the $\mathbf{x}_i \in \mathcal{C}^{K\times 1}$ and $x_i(j)$ is the j-th element of $\mathbf{x}_i$ where, $j = 0, 1, 2, \ldots, K-1$. Here d_i is encoded data and $\mathbf{c}_i$ is spreading sequence. OFDM-modulated signal is

$$\begin{aligned} g_i(j) &= \frac{1}{\sqrt{N}} \sum_{k=0}^{N-1} \mathbf{x}_i(k) e^{i2\pi kj/N} \qquad j = 0, 1, 2, \ldots, N-1 \\ \mathbf{g}_i &= \mathrm{IFFT}(\mathbf{x}_i). \end{aligned} \tag{3.9}$$

By adding the CP, the transmitted signal extended to $N + L - 1$, where $L - 1$ is the memory of the channel. The CP appended OFDM waveform is $\tilde{\mathbf{g}}_i$. The

output of frequency selective channel is

$$y_i(j) = \sum_{l=0}^{L-1} h_l \tilde{g}_i(j-l) + w(j) \tag{3.10}$$

where, $w(j)$ is additive white Guassian noise. The receiver of the proposed OFDM system performs FFT on the received signal after removing CP as follows

$$\begin{aligned} r_i(j) &= \frac{1}{\sqrt{N}} \sum_{k=0}^{N-1} \tilde{y}_i(k) e^{-i2\pi kj/N} \quad 0 < j \leq N-1 \\ \mathbf{r}_i &= \text{FFT}(\tilde{\mathbf{y}}_i). \end{aligned} \tag{3.11}$$

The despreading of OFDM-demodulated waveform is

$$\gamma_i = \mathbf{r}_i^H \mathbf{c}_i. \tag{3.12}$$

The differential decoder is

$$\alpha_i = \gamma_i^* \gamma_{i-1}. \tag{3.13}$$

The angle of α_i represent transmitted bits.

3.2 Performance Evaluation

In this section, we present the performance of the proposed approach for non-OFDM and OFDM waveform transmission over the multipath Rayleigh fading channel. We used chaotic spreading code to spread the differentially encoded information over the wireless channel. We use bit error rate (BER) to measure the performance for DBPSK and DQPSK modulations for the proposed models. We present impact of channel diversity and spreading code length on the non-OFDM and OFDM based transceivers for DBPSK and DQPSK modulations.

3.2.1 Simulation Setup

In the simulation setup, for both OFDM and non-OFDM transceivers presented in Fig 3.1 in Section 3.1, we used MATLAB enviornment for the simulation. We perform BER evaluation for the OFDM and non-OFDM waveforms using DBPSK and DQPSK modulation. The transmitted signal encounters Rayleigh fading frequency selective channel with L independent and identically distributed (i.i.d.) paths. The dynamic spreading codes of length n is generated from the discrete-time logistic map with initail state $u_0 = 0.5101$ and parameter $\lambda = 4$. We assume no channel knowledge and receivers of the OFDM and non-OFDM waveforms perform non-coherent detection. Furthermore, we assume that transmitter and receivers are equipped with single antenna. That is, single-input single-output (SISO) system. Now, we present BER performance of the proposed non-OFDM transceiver.

3.2.2 Non-OFDM Transmission results

For non-OFDM transmission, we evaluate BER performance over the multipath Rayleigh fading channel for DBPSK and DQPSK modulations.

In Fig. 3.6, we investigate impact of number of paths on the BER performance on the non-OFDM receiver with DBPSK modulation. We compare BER for $L = 2, 4, 8$ and 16 paths and the spreading factor $K = 64$. The performance of the BER for the proposed approach improves as the number of paths increases. Fig. 3.6 reveals that the receiver achieves higher diversity when number of paths are increaded from $L = 2$ to 8. However, diversity gain is not observed when number of paths are increased from 8 to 16. In the rake receiver, the number of fingers increases with respect with the number of paths. Each addition path induces inter-symbol interference to the other fingers of the rake receivers. When number of paths increaded to 16, inter-symbol interference diminishes diversity gain.

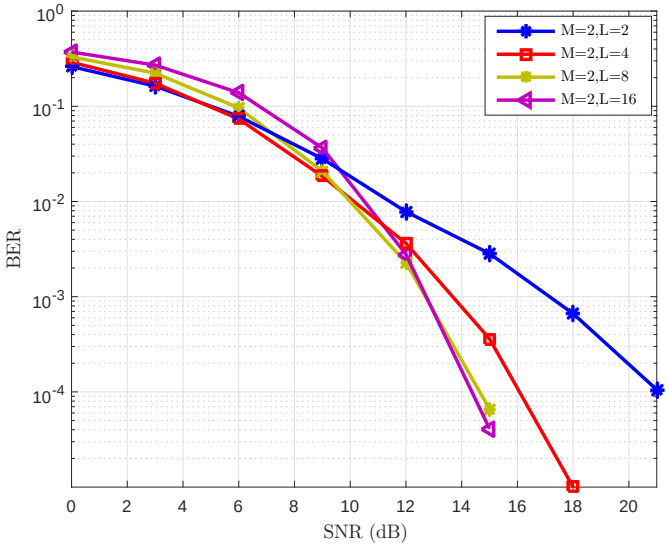

Figure 3.6: BER performance for DBPSK in multipath Rayleigh fading channel for $K = 64$

In Fig. 3.7, we investigate impact of number of paths on the BER performance on the non-OFDM receiver with DQPSK modulation. We compare BER for $L = 2, 4, 8$ and 16 paths and the spreading factor $K = 64$. We observed the same behaviour for DQPSK as for DBPSK in fig. 3.6.

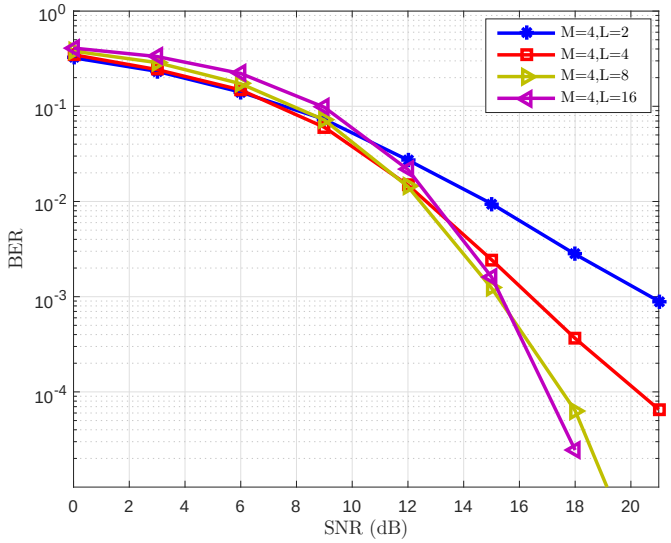

Figure 3.7: BER performance for DQPSK in multipath Rayleigh fading channel for $K = 64$

In Fig. 3.8, we investigate the BER comparison for DBPSK and DQPSK modulation on non-OFDM receiver. For $L = 2$ and 4 DBPSK exhibits good BER performance as compared to DQPSK modulation. The main reason DBPSK shows good performance is that each symbol has one bit spreaded across the dynamic chaotic code under unit energy. Each symbol in DQPSK has two bits that are spread out using the dynamic chaotic code. The difference in BER performance between DBPSK and DQPSK modulation is determined by the number of bits in each transmitted symbol per unit of energy.

In Fig. 3.9, we investigate the BER comparison for DBPSK and DQPSK modulation on non-OFDM receiver. For $L = 8$ and 16 gives the same behaviour as above in fig. 3.8.

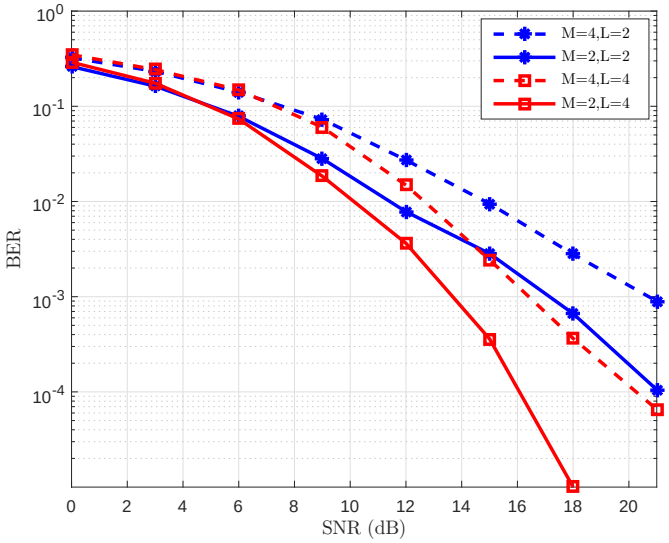

Figure 3.8: BER performance comparison of DQPSK and DBPSK in multipath Rayleigh fading channel for two and four paths

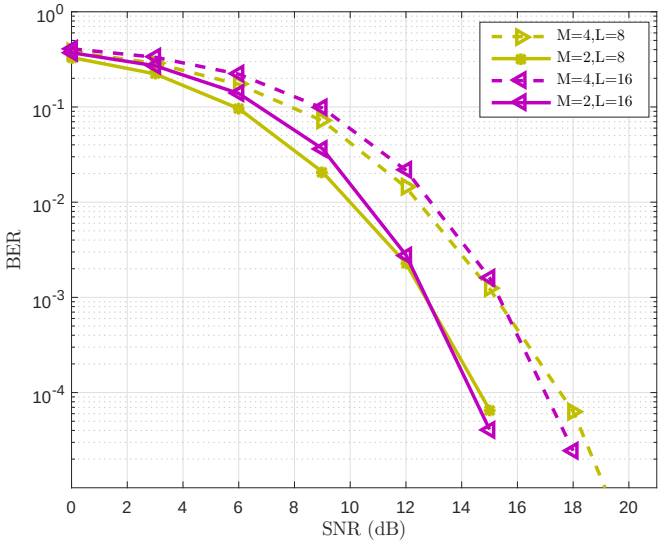

Figure 3.9: BER performance comparison of DQPSK and DBPSK in multipath Rayleigh fading channel for eight and sixteen paths

In Fig. 3.10, we investigate impact of number of paths on the BER performance on the non-OFDM receiver with DBPSK modulation for $K = 32$. We compare BER for $L = 2, 4, 8$ and 16 paths for the spreading factor $K = 32$. By decreasing the spreading length for large number of paths BER perfromance is degraded because Inter-symbol interference becomes prominent due to decrease in spreading length which impact the BER performance.

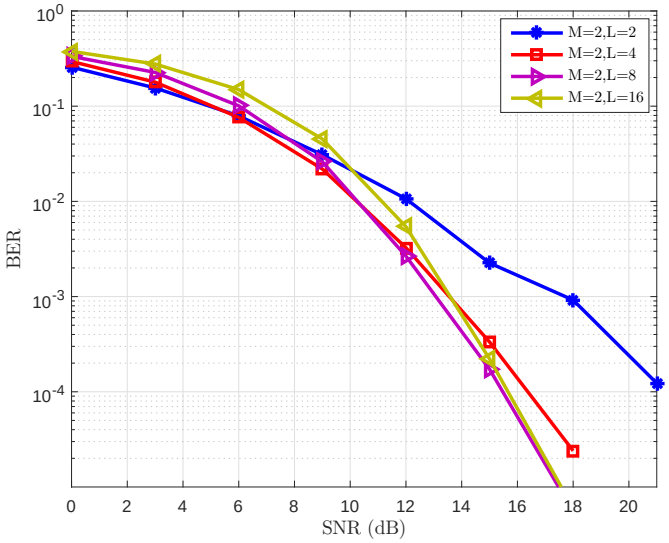

Figure 3.10: BER performance for DBPSK in multipath Rayleigh fading channel for $K = 32$

In Fig. 3.11, we investigate impact of number of paths on the BER performance on the non-OFDM receiver with DQPSK modulation. We compare BER for $L = 2, 4, 8$ and 16 paths and the spreading factor $K = 32$. We observed the same behaviour for DQPSK as for DBPSK in fig. 3.10.

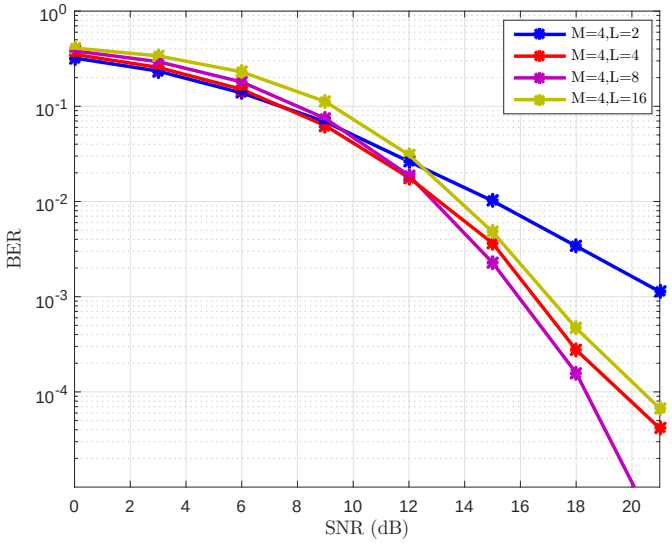

Figure 3.11: BER performance for DQPSK in multipath Rayleigh fading channel for $K = 32$

3.2.3 OFDM Transmission results

For OFDM transmission, we present BER performance of proposed model over the multipath Rayleigh fading channel. DBPSK and DQPSK modulation techniques are used to evaluate the BER performance.

In Fig. 3.12, we investigate impact of number of paths on the BER performance on the OFDM receiver with DBPSK modulation. We calculated the BER for paths $L = 2, 4, 8, 16$ and the spreading factor is $K = 64$ in a multipath Rayleigh fading channel. The performance of the BER for the proposed approach improves as the number of paths increases. OFDM completely removes the inter-symbol interference from the signal. The increase in numbers of paths in OFDM increases the BER performance due to higher diversity gain.

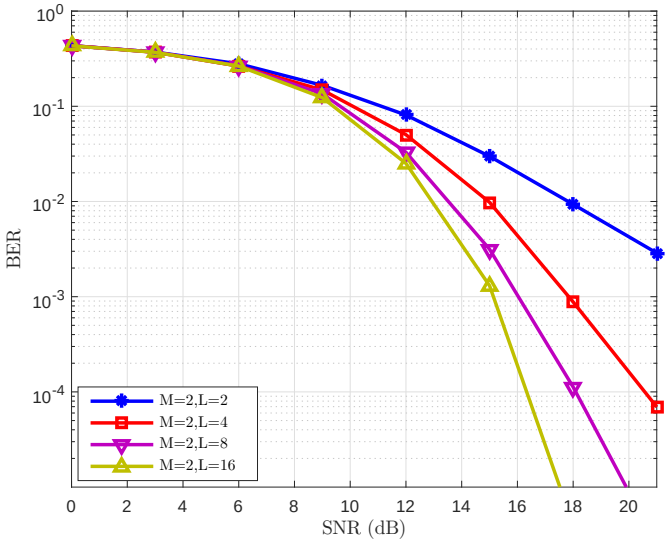

Figure 3.12: BER performance for DBPSK using OFDM in multipath Rayleigh fading channel for $K = 64$

In Fig. 3.13, we investigate impact of number of paths on the BER performance on the OFDM receiver with DQPSK modulation. We calculated the BER for paths $L = 2, 4, 8, 16$ and the spreading factor is $K = 64$ in a multipath Rayleigh fading channel. We observed the same behaviour as in fig. 3.12 for DBPSK.

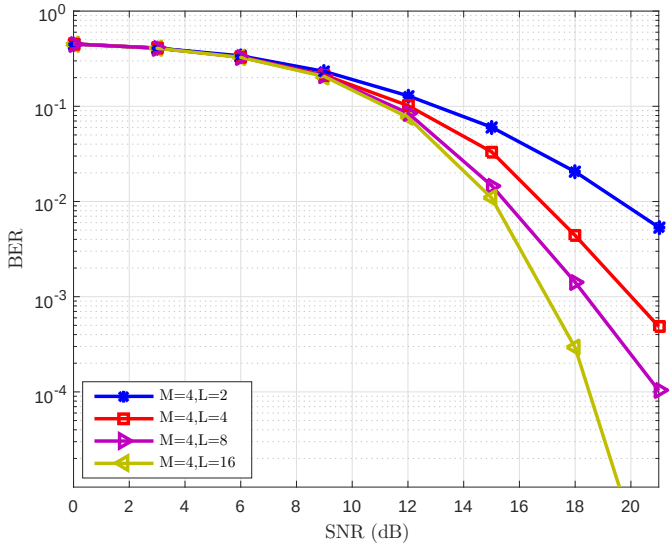

Figure 3.13: BER performance for DQPSK using OFDM in multipath Rayleigh fading channel for $K = 64$

In Fig. 3.14, we investigate the BER comparison for DBPSK and DQPSK modulation on OFDM receiver. For $L = 2$ and 4 DBPSK exhibits good BER performance as compared to DQPSK modulation. In DBPSK one information symbol cantain only one bit per unit energy for transmission. In DQPSK one information symbol contains two bits per unit energy for transmission. Due to energy difference between bits, DBPSK exhibits good BER performance as compared to DQPSK.

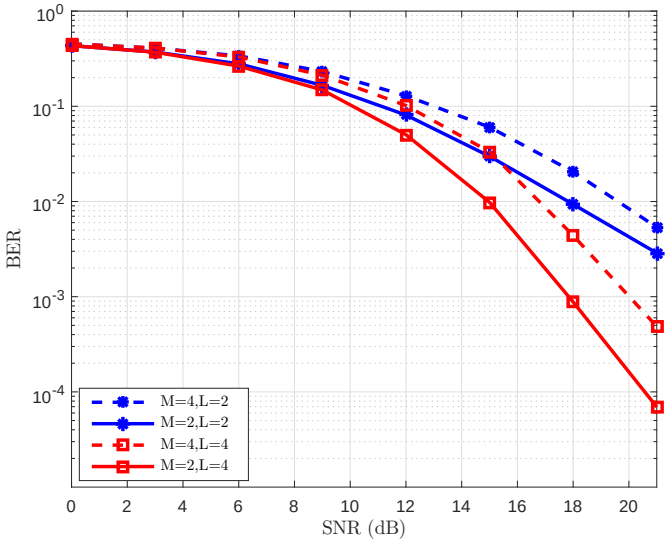

Figure 3.14: BER performance comparison of DQPSK and DBPSK Using OFDM in multipath Rayleigh fading channel for two and four paths

In Fig. 3.15, we investigate the BER comparison for DBPSK and DQPSK modulation on OFDM receiver for $L = 8$ and 16. These paths gives the same behaviour as in fig. 3.14

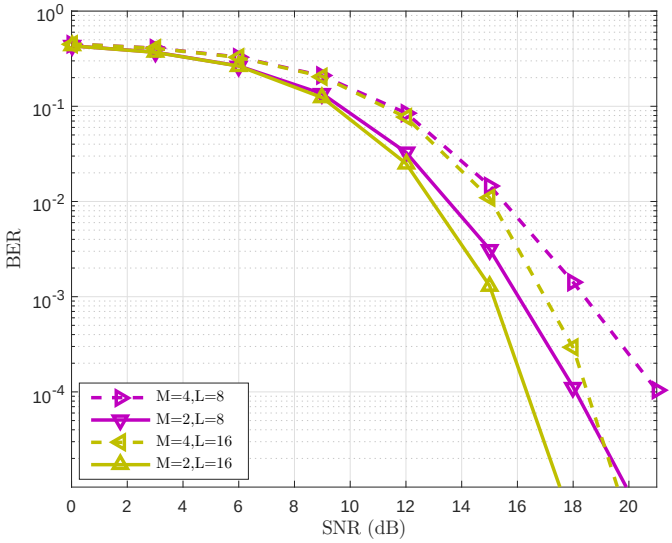

Figure 3.15: BER performance comparison of DQPSK and DBPSK using OFDM in multipath Rayleigh fading channel for eight and sixteen paths

In Fig. 3.16, we investigate impact of number of paths on the BER performance on the OFDM receiver with DBPSK modulation. We calculated the BER for paths $L = 2, 4, 8, 16$ and the spreading factor is $K = 32$ in a multipath Rayleigh fading channel. We observed the same behaviour as in fig. 3.12.

In Fig. 3.17, we investigate impact of number of paths on the BER performance on the OFDM receiver with DQPSK modulation for $K = 32$. We calculated the BER for paths $L = 2, 4, 8,$ and16. We observed the same behaviour as in fig. 3.16 for Rayleigh fading channel.

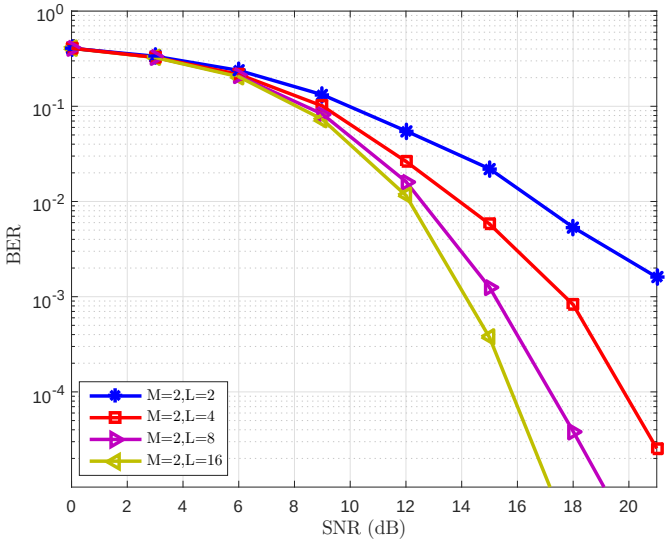

Figure 3.16: BER performance for DBPSK using OFDM in multipath Rayleigh fading channel for $K = 32$

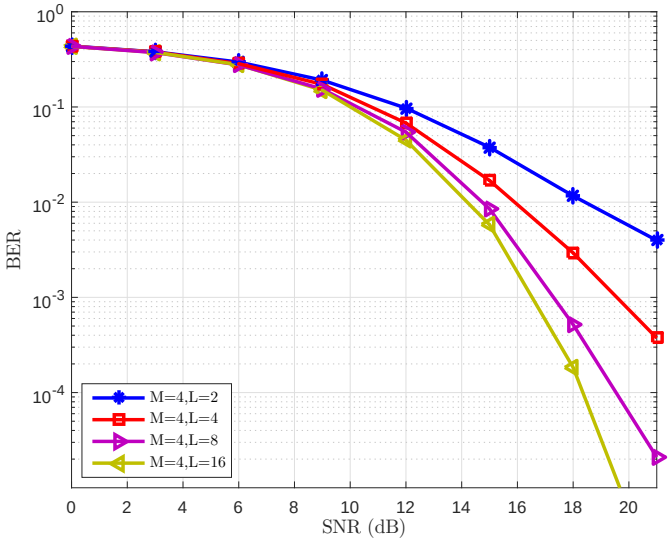

Figure 3.17: BER performance for DQPSK using OFDM in multipath Rayleigh fading channel for $K = 32$

3.2.4 Impact of spreading factor on BER performance

We compared the BER performance of proposed model by changing the spreading factor for both OFDM and non-OFDM transceiver over the multipath Rayleigh fading channel. We investigated the impact of spreading factor on BER performance for DBPSK and DQPSK modulation techniques.

In Fig. 3.18, we investigate impact of spreading factor on the BER performance for non-OFDM receiver with DBPSK modulation. We calculated the BER for paths $L = 2, 4, 8,$ and 16 for spreading factor $K = 32$ and 64 and compare the results in a multipath Rayleigh fading channel. The performance of BER in Fig. 3.18 is the same for $L = 2$ and 4 for spreading factor $K = 32$ and 64, and the change in spreading length has no effect on the BER performance. For $L = 8$ and 16, the BER performance is poor for $K = 32$ due to increased residual interference, and the correlation of the transmitted signal will also increase due to a decrease in the spreading length of the chaotic spreading code.

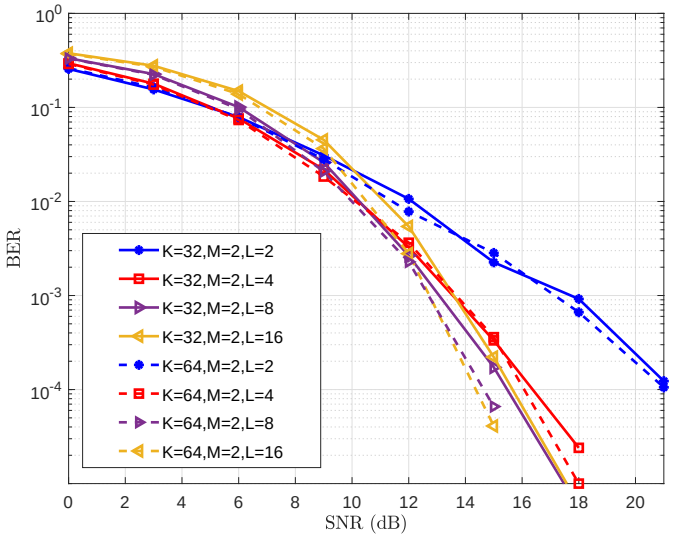

Figure 3.18: BER performance for DBPSK using non-OFDM transceiver in multipath Rayleigh fading channel for $K = 32$ and 64

In Fig. 3.19, we investigate impact of spreading factor on the BER performance for OFDM receiver with DBPSK modulation. We calculated the BER for paths $L = 2, 4, 8,$ and 16 for spreading factor $K = 32$ and 64 and compare the results in a multipath Rayleigh fading channel. In OFDM transceiver, by decreasing the spreading length the BER performance for $K = 32$ is sligthly better than $K = 64$ for all number of paths.

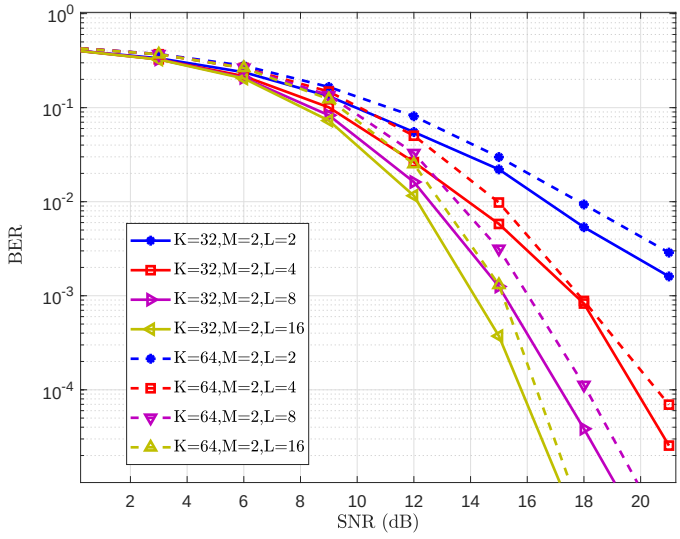

Figure 3.19: BER performance for DBPSK using OFDM transceiver in multipath Rayleigh fading channel for $K = 32$ and 64

3.2.5 Comparison of OFDM and non-OFDM Transceivers

We compared the performance of OFDM and non-OFDM transceivers in multipath Rayleigh fading channel. Chaos-based non-OFDM transceivers gives better performance up to a certain number of paths as compared to chaos-based OFDM transceivers. In OFDM transimission, BER improved by the increase in number of paths without any performance degradation. In non-OFDM transmission method at the receiver end, we performed a correlation of the received signal and the reference signal. In OFDM transmission at the receiver end, OFDM demodulater is used to demodulate information.

In Fig. 3.20, we compare the results of OFDM and non-OFDM receiver for spreading factor $K = 64$ with DBPSK modulation. For non-OFDM transceiver, the BER performance is better than OFDM transceiver because non-OFDM receiver is optimal and OFDM receiver is suboptimal.

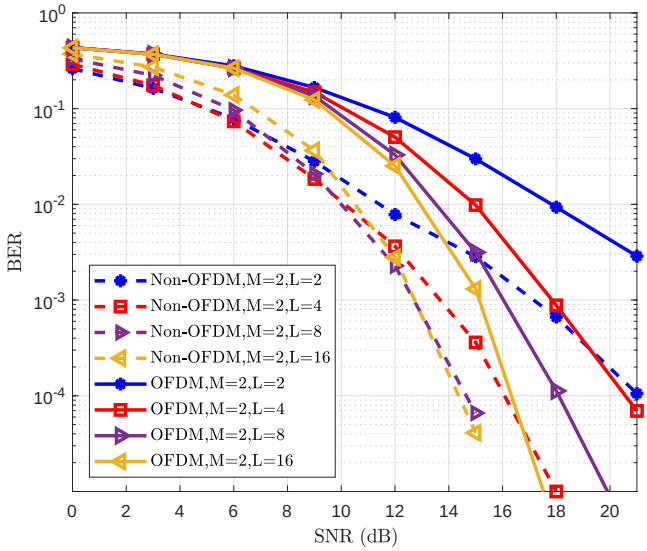

Figure 3.20: BER performance comparison of OFDM and non-OFDM transceiver for DBPSK in multipath Rayleigh fading channel for $K = 64$

In Fig. 3.21, we compare the results of OFDM and non-OFDM receiver for spreading factor $K = 32$ with DBPSK modulation. We observed that the BER performance for $L = 2, 4,$ and 8 is better for non-OFDM transceiver and for $L = 16$ the performance of both OFDM and non-OFDM transceiver is same. So for small number of paths the BER performance for non-OFDM transceiver is better than OFDM transceiver.

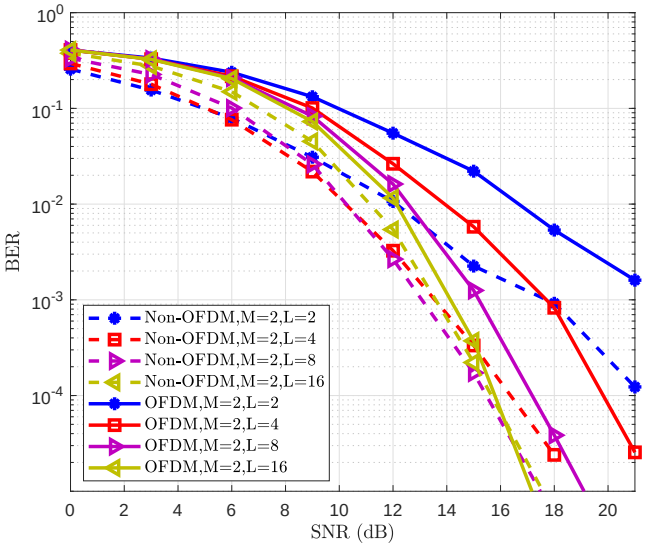

Figure 3.21: BER performance comparison of OFDM and non-OFDM transceiver for DBPSK in multipath Rayleigh fading channel for $K = 32$

3.3 Summary

In this chapter, we discussed the proposed system model used for the physical layer security. For PLS, we used a chaos-based non-OFDM transmission model and chaos-based OFDM transmission model. We discussed these two models in details. Other section of this chapter contains simulation results. In simulation results, we calculated the BER for non-OFDM transmission and OFDM transmission across the multipath Rayleigh fading channel. We calculated the BER of DBSPK and DQPSK for both propsoed methods.

Chapter 4

Conclusion and Future Work

In the proposed work, for physical layer security, we used the chaotic map to generate the spreading sequence and the encoded information is spreaded with baseband chaotic sequence. For signal transmission, we employed two alternative techniques. First, a non-OFDM baseband signal is transmitted, and the data is decoded in a multipath environment using a rake receiver. In the second, the OFDM baseband waveform is broadcast and the OFDM demodulator is used to decode the data after it has been sent across a Rayleigh fading channel. The performance of both methods is evaluated in terms of bit error rate (BER) in the proposed study. The BER performance for non-OFDM is improved by the Rake receiver's removal of the ISI from received signals for several pathways and the combination of these paths signals for decoding. OFDM is used to reduce the ISI from signals in order to enhance the BER performance during OFDM waveform transmission. The followings are possible future extensions of this work.

- In this work, logistic map is generated using floating point approach, which has high precision. Chaotic maps have short period with finite precision, which results in poor security due to periodicity. Behavior of the proposed method should be investigated with finite precion as future work.
- Performance evaluation of the proposed transceivers with different chaotic maps.

- Implementation of the proposed methods on software define radio (SDR) to evaluate the performance gap between simulation and actual impementation.

Bibliography

[1] Zhihong Yang, Yingzhao Yue, Yu Yang, Yufeng Peng, Xiaobo Wang, and Wenji Liu. Study and application on the architecture and key technologies for IOT. In *2011 International Conference on Multimedia Technology*, pages 747–751. IEEE, 2011.

[2] Aylin Yener and Sennur Ulukus. Wireless physical-layer security: Lessons learned from information theory. *Proceedings of the IEEE*, 103(10):1814–1825, 2015.

[3] Xiangyun Zhou, Lingyang Song, and Yan Zhang. *Physical layer security in wireless communications*. Crc Press, 2013.

[4] Long Kong, Georges Kaddoum, and Mostafa Taha. Performance analysis of physical layer security of chaos-based modulation schemes. In *2015 IEEE 11th international conference on wireless and mobile computing, networking and communications (WiMob)*, pages 283–288. IEEE, 2015.

[5] AD Wyner. The wire-tap channel. *The Bell System Technical Journal*, 54(8):1355–1387, 1975.

[6] Yulong Zou, Jia Zhu, Xianbin Wang, and Victor CM Leung. Improving physical-layer security in wireless communications using diversity techniques. *IEEE Network*, 29(1):42–48, 2015.

[7] Matthieu Bloch and Joao Barros. *Physical-layer security: from information theory to security engineering*. Cambridge University Press, 2011.

[8] Yiliang Liu, Hsiao-Hwa Chen, and Liangmin Wang. Physical layer security for next generation wireless networks: Theories, technologies, and challenges. *IEEE Communications Surveys & Tutorials*, 19(1):347–376, 2016.

[9] Guyue Li, Yinghao Xu, Wei Xu, Eduard Jorswieck, and Aiqun Hu. Robust key generation with hardware mismatch for secure mimo communications. *IEEE Transactions on Information Forensics and Security*, 16:5264–5278, 2021.

[10] Najme Ebrahimi, Hun-Seok Kim, and David Blaauw. Physical layer secret key generation using joint interference and phase shift keying modulation. *IEEE Transactions on Microwave Theory and Techniques*, 69(5):2673–2685, 2021.

[11] Georges Kaddoum, Daniel Roviras, Pascal Chargé, and Daniele Fournier-Prunaret. Accurate bit error rate calculation for asynchronous chaos-based ds-cdma over multipath channel. *EURASIP Journal on Advances in Signal Processing*, 2009:1–12, 2009.

[12] Nguyen Xuan Quyen, Chuyen T Nguyen, Pere Barlet-Ros, and Reiner Dojen. A novel approach to security enhancement of chaotic dsss systems. In *2016 IEEE Sixth International Conference on Communications and Electronics (ICCE)*, pages 471–476. IEEE, 2016.

[13] Nguyen Xuan Quyen and Kyandoghere Kyamakya. Chaos-based digital communication systems with low data-rate wireless applications. *Recent Advances in Nonlinear Dynamics and Synchronization: With Selected Applications in Electrical Engineering, Neurocomputing, and Transportation*, pages 239–269, 2018.

[14] David Luengo and I Santamaria. Secure communications using ofdm with chaotic modulation in the subcarriers. In *2005 IEEE 61st Vehicular Technology Conference*, volume 2, pages 1022–1026. IEEE, 2005.

[15] Suhas Mathur, Alex Reznik, Chunxuan Ye, Rajat Mukherjee, Akbar Rahman, Yogendra Shah, Wade Trappe, and Narayan Mandayam. Exploiting

the physical layer for enhanced security [security and privacy in emerging wireless networks]. *IEEE Wireless Communications*, 17(5):63–70, 2010.

[16] Reem Melki, Hassan N Noura, Mohammad M Mansour, and Ali Chehab. A survey on ofdm physical layer security. *Physical Communication*, 32:1–30, 2019.

[17] Abdelkader Saadi, Adda Pacha, Naima Said, et al. Physical layer security based on chaotic maps applied to ofdm systems. *International Journal of Advanced Studies in Computer Science & Engineering*, 12(1), 2023.

[18] Bruce Schneier. Description of a new variable-length key, 64-bit block cipher (blowfish). In *International workshop on fast software encryption*, pages 191–204. Springer, 1993.

[19] Bruce Schneier. *Applied cryptography: protocols, algorithms, and source code in C*. john wiley & sons, 2007.

[20] Andreas Abel and Wolfgang Schwarz. Chaos communications-principles, schemes, and system analysis. *Proceedings of the IEEE*, 90(5):691–710, 2002.

[21] Eiji Okamoto. A chaos mimo-ofdm scheme for mobile communication with physical-layer security. In *International Conference on Theory and Application in Nonlinear Dynamics (ICAND 2012)*, pages 203–212. Springer, 2013.

[22] Xiaozhong Zhang, Ying Wang, Juan Zeng, and Yongming Wang. A secure ofdm transmission scheme based on chaos mapping. In *2015 IEEE 34th International Performance Computing and Communications Conference (IPCCC)*, pages 1–6. IEEE, 2015.

[23] Vahid Tarokh and Hamid Jafarkhani. A differential detection scheme for transmit diversity. In *WCNC. 1999 IEEE Wireless Communications and Networking Conference (Cat. No. 99TH8466)*, volume 3, pages 1043–1047. IEEE, 1999.

[24] John G Proakis. *Digital communications*. McGraw-Hill, Higher Education, 2008.

[25] Jiann-Ching Guey and L Daniel Larsson. Modeling and evaluation of mimo systems exploiting channel reciprocity in tdd mode. In *IEEE 60th Vehicular Technology Conference, 2004. VTC2004-Fall. 2004*, volume 6, pages 4265–4269. IEEE, 2004.

[26] Edward N Lorenz. Deterministic nonperiodic flow. *Journal of atmospheric sciences*, 20(2):130–141, 1963.

[27] Chunguang Huang, Qun Ding, et al. Performance of finite precision on discrete chaotic map based on a feedback shift register. *Complexity*, 2020, 2020.

[28] Toshiki Habutsu, Yoshifumi Nishio, Iwao Sasase, and Shinsaku Mori. A secret key cryptosystem by iterating a chaotic map. In *Advances in Cryptology—EUROCRYPT'91: Workshop on the Theory and Application of Cryptographic Techniques Brighton, UK, April 8–11, 1991 Proceedings 10*, pages 127–140. Springer, 1991.

[29] Kehui Sun. *Chaotic secure communication: principles and technologies*. Walter de Gruyter GmbH & Co KG, 2016.

[30] R Anandkumar and R Kalpana. Analyzing of chaos based encryption with lorenz and henon map. In *2018 2nd International Conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud)(I-SMAC) I-SMAC (IoT in Social, Mobile, Analytics and Cloud)(I-SMAC), 2018 2nd International Conference on*, pages 204–208. IEEE, 2018.

[31] Shaoqiu Chen, Shiya Feng, Wenjun Fu, and Yingying Zhang. Logistic map: Stability and entrance to chaos. In *Journal of Physics: Conference Series*, volume 2014, page 012009. IOP Publishing, 2021.

[32] Shihong Wang, Weirong Liu, Huaping Lu, Jinyu Kuang, and Gang Hu. Periodicity of Chaotic Trajectories in Realizations of Finite Computer Precisions and its Implication in Chaos Communications. *International Journal of Modern Physics B*, 18(17n19):2617–2622, Jul. 2004.

[33] Fahad A Munir, Muhammad Zia, and Hasan Mahmood. Designing multi-dimensional logistic map with fixed-point finite precision. *Nonlinear Dynamics*, 97:2147–2158, 2019.

[34] Claude E Shannon. Communication theory of secrecy systems. *The Bell system technical journal*, 28(4):656–715, 1949.

[35] Gang Xu, Geng Zhao, and Lequan Min. A method for designing dynamical s-boxes based on discrete chaos map system. In *2009 International Conference on Communications, Circuits and Systems*, pages 876–880. IEEE, 2009.

[36] Dragan Lambić. A novel method of s-box design based on chaotic map and composition method. *Chaos, Solitons & Fractals*, 58:16–21, 2014.

[37] Dragan Lambić. A novel method of s-box design based on discrete chaotic map. *Nonlinear dynamics*, 87:2407–2413, 2017.

[38] Anjam Riaz and Maaruf Ali. Chaotic communications, their applications and advantages over traditional methods of communication. In *2008 6th International Symposium on Communication Systems, Networks and Digital Signal Processing*, pages 21–24. IEEE, 2008.

[39] Kevin M Cuomo and Alan V Oppenheim. Chaotic signals and systems for communications. In *1993 IEEE international conference on acoustics, speech, and signal processing*, volume 3, pages 137–140. IEEE, 1993.

[40] Veljko Milanovic and Mona E Zaghloul. Synchronization of chaotic neural networks for secure communications. In *1996 IEEE International Symposium on Circuits and Systems (ISCAS)*, volume 3, pages 28–31. IEEE, 1996.

[41] Ömer Morgül and Moez Feki. A chaotic masking scheme by using synchronized chaotic systems. *Physics Letters A*, 251(3):169–176, 1999.

[42] Michael Peter Kennedy, Géza Kolumbán, and Gábor Kis. Chaotic modulation for robust digital communications over multipath channels. *International Journal of Bifurcation and Chaos*, 10(04):695–718, 2000.

[43] Herve Dedieu, Michael Peter Kennedy, and Martin Hasler. Chaos shift keying: modulation and demodulation of a chaotic carrier using self-synchronizing chua's circuits. *IEEE Transactions on Circuits and Systems II: Analog and Digital Signal Processing*, 40(10):634–642, 1993.

[44] CK Tse and F Lau. Chaos-based digital communication systems. *Operating Principles, Analysis Methods and Performance Evaluation (Springer Verlag, Berlin, 2004)*, 2003.

[45] Jianbo Liu, Chunfei Ye, Shujing Zhang, and Wentao Song. The improved differential chaos shift keying scheme. In *WCC 2000-ICCT 2000. 2000 International Conference on Communication Technology Proceedings (Cat. No. 00EX420)*, volume 2, pages 1361–1363. IEEE, 2000.

[46] Georges Kaddoum, Pascal Chargé, Daniel Roviras, and Daniele Fournier-Prunaret. Performance analysis of differential chaos shift keying over an awgn channel. In *2009 International Conference on Advances in Computational Tools for Engineering Applications*, pages 255–258. IEEE, 2009.

[47] Tao Yang and Leon O Chua. Secure communication via chaotic parameter modulation. *IEEE Transactions on Circuits and Systems I: Fundamental Theory and Applications*, 43(9):817–819, 1996.

[48] Amang Sudarsono and Mike Yuliana. An anonymous authentication with received signal strength based pseudonymous identities generation for vanets. *IEEE Access*, 11:15637–15654, 2023.

[49] Weitao Xu, Sanjay Jha, and Wen Hu. Lora-key: Secure key generation system for lora-based network. *IEEE Internet of Things Journal*, 6(4):6404–6416, 2019.

[50] Yiming Zhu, Gangle Sun, Wenjin Wang, Li You, Fan Wei, Lei Wang, and Yan Chen. Ofdm-based massive grant-free transmission over frequency-selective fading channels. *IEEE Transactions on Communications*, 70(7):4543–4558, 2022.