Physical layer security based on chaotic maps applied to OFDM systems

Abdelkader.Saadi[1,1], Adda.Ali Pacha[2,1], and Naima.Hadj Said[3,1]
[1]Laboratory of Coding and Security of Information, University of Sciences and Technology Mohamed Boudiaf,Pobox 1505, Oran M‟Naouer 31000, Algeria

Abstract

Recently, physical layer security (PLS) has attracted widespread attention to improve security in networks without focusing on encryption techniques at the higher layers. This paper proposes a PLS scheme through an orthogonal frequency division multiplexing (OFDM) system based on chaotic maps. An OFDM wave is securedby mixing its modulated symbols and encoding information bits at the same time. Informationis encoded by generating a stream of bits by chaotic maps. To build a secure OFDM wave, the modulated symbols are shuffled by a scrambling matrix that is created by chaotic maps. Their initial conditions act as a secret shared key. We send only one key to encrypt the first OFDM signal at the beginning of the transmission. After the first transmission, the received information, after its decryption, serve as the key to the next information. In other word, the information itself is the key to the next information to be received. Meanwhile, we do not have to send the encryption key on every transmission.

Keywords: OFDM, chaotic maps, Logistic map, Cryptography, Physical layer security.

1 Introduction

Information security has become a real concern in recent years due to the broadcast nature of communications that implement a point-to-multipoint architecture as Passive Optical Net- works (PON) [1] for wired networks and cellular communication for wireless networks. Whereas, traditional encryption methods have been widely adopted in the upper layers to ensure information security. These methods are designed on the assumption that the computational power and resources of an eavesdropper will not be sufficient for information intrusions. The massive processing power that we have today has not yet satisfied our needs for speed and computing power. Quantum computing has emerged that harness the energy of atoms and molecules to perform memory and processing tasks. These de vices have the ability to perform specific calculations much faster than any silicon-based processor. With the increase in computing power, the computational rigidity of some mathematical problems may not persist, which leads to the failure of many traditional cryptosystems. Recently, physical layer security (PLS) has been traded as a promising proposal for ensuring the security of communication systems through several technical keys in the physical layer such as Code division multiple access (CDMA), Multiple Input Multiple Output (MIMO) and OFDM [2]. Due to the ease of digital processing of the OFDM signal, the data of this signal can be encoded on the physical layer [3]. The security of this system can be efficiently improved by using chaos theory. It is a way to make a secure communication due to its sensitivity to initial conditions [4, 5]. Based on the chaotic permutation of data in the OFDM signal, it is one of the simple ways to secure the physical layer [6]. This is done by scrambling the signal in the time and/or frequency domain through a chaotic map [7]. It can be performed before and after the IFFT block in OFDM system [8, 9] .That means in frequency domain as in [10] or in time domain as in [11]. All of the above protection schemes are based on pre-shared keys whether they are represented in the initial conditions of the chaotic maps used or some method is used to create them. This means that the transmitter must send these keys on every transmission. In this paper, we designed a security system based on sending one key to encrypt only the beginning of the transmission, while the rest of the keys will be generated from the received information to decrypt the incoming information. Hence, the sent message itself represents the key to

[1] abdelkader.saadi@univ-usto.dz
[2] a.alipacha@gmail.com
[3] naima.hadjsaid@univ-usto.dz

the next message. This makes it more difficult for an eavesdropper to extract any useful information. Therefore, the proposed scheme could obtain a powerful security capability. Thus, it can be achieve almost the perfect secrecy that Shannon indicated in his famous paper [12] with good transmission performance.

The remainder of this paper is organized in 5 sections as follows: Section 2 an introductory background to OFDM and Chaos systems. Section 3 describes the algorithm proposed to secure the OFDM system. Section 4 describes security analysis of the proposed system through evaluating the results simulated for the BER (Bit Error Rate) performance. The last section is concluding the paper.

2 Background and preliminaries

2.1 OFDM

The selective fading environment, or known as the use of broadband for wireless communications, leads to deterioration of system performance through Inter symbol interference (ISI)phenomenon. To avoid that, OFDM appeared, this technology divides the bandwidth into a large number of narrow bands, sub channels or sub carriers instead of using the entire bandwidth at once, this is the meaning of 'Frequency Division'. The information is modulate across each sub-carrier using a specific modulation scheme (suchas BPSK, QPSK, QAM. . .). The modulateddata on each subcarriers are transmitted simultaneously (a kind of Multiplexing) and termed as OFDM symbols. It increases spectrum efficiency, due to multiple overlapping and orthogonal small/narrow frequencies, which explains the name orthogonal frequency division multiplexing [13, 14].

Figure 1 illustrates the basic principles be-hind OFDM system ,including a complete block diagram of the typical OFDM transmitter and receiver[15]. It is difficult to generate this signal because of the large number of subcarriers that means you need a large number of oscillators, instead of using modulators , an IFFT transformation is performed on the modulated data across each subcarrier in the frequency domain to pro- duce an OFDM symbol in the time domain, this is one of the key principles behind the use of OFDM. For N parallel data streams, N - point IFFT is performed on the complex digital modulated signal X(n). The time domain signal x(n), can be expressed as:

$$x[n] = IFFT(X[n]) = \sum_{i=1}^{N-1} X(i)\exp\frac{j2\pi in}{N} \quad (1)$$

Then in the time domain, to prevent ISI at the receiver caused by multipath delay spread in the channel, cyclic prefixes or guard intervals of length Ncp are inserted between each symbols after the IFFT operation ,which result N+Ncp samples transmitted in serial through the channel.At the receiver, the cyclic prefix is removed, and the N received symbols are demodulated, using an FFT operation on the OFDM symbols to re- cover the original information bits. The received frequency domain signal Y (n) is given by:

$$Y[n] = FFT(y[n]) = \sum_{i=1}^{N-1} y(i)\exp\frac{-j2\pi in}{N} \quad (2)$$

Where y is the received OFDM symbol in thetime domain.

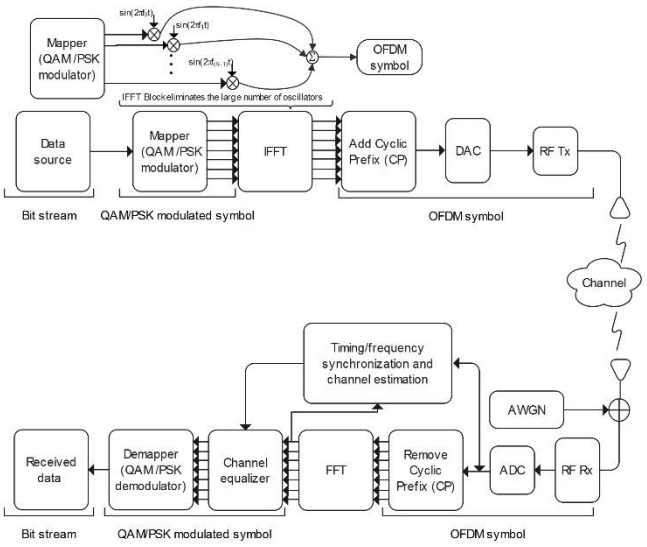

Figure 1: Block diagram of transmitter and receiver in an OFDM system.

2.2 Chaos system and chaotic maps

In common usage, Chaos means " a state of disorder, confusion, havoc, madness,. . . ", but chaos theory in mathematics is the study of nonlinear dynamical systems that are very

sensitive to initial conditions. Although there is no universally accepted mathematical definition of chaos, a commonly used definition says that for a dynamical system to be classified as chaotic, it must have the following properties: Deterministic, Nonlinear, Sensitive dependence to initial condition. Chaotic maps have been attracted the attention of cryptographers designers, as many chaotic cryptosystems have been proposed in the last years [5]. A chaotic map is a mathematical function that produces some kind of chaotic behavior. It can be characterized by discrete time parameter such as Logistic map, Baker's map or continuous time parameter like Lorenz system. It can be one dimensional space as Tent maps or multidimensional space like Hénon map.

2.2.1 The logistic map

The logistic map is a one dimensional discrete time map that often used to describe the growth of biological populations [16]. The mathematical simplicity of the logistic map has made it a useful and practical base for new ideas in chaos theory and their application in cryptography [17].

The logistic map is defined by the following equation [18]:

$$x_{n+1} = \lambda x_n(1 - x_n) \quad (3)$$

with n=1,2,3,...

Given a starting value or initial condition $0 \leq x_0 \leq 1$ and positive parameter $0 < \lambda < 4$ the map produces a sequence of values: $x_0, x_1, x_2, x_3, \ldots$ that you get by iterating it, e.g.

$x_1 = \lambda x_0(1 - x_0)$
$x_2 = \lambda x_1(1 - x_1)$
$x_3 = \lambda x_2(1 - x_2)$
...

Figure 2 shows the logistic map function as function of x for multiple values of parameter λ. The symmetry of the map function around the midpoint of the interval [0, 1] is obvious. For parameters values λ superior than 3.5699 the iterative map shows a strange complex behavior, where the map function never repeats its values history. The expression "sensitivity on initial conditions" might be used to describe this chaotic behavior. Figure 3 shows two signs of the logistic map with an initial value, the first sign with $x_0 = 0.0000000001$, the second with values $x_0 = 0.00000000011$, and $\lambda = 3.9999$. It seems that with a small difference in initial condition it gives us two different signals with no correlation between them.

Figure 4 shows a bifurcation diagram that summarizes the dynamic behavior of the logistic mapwhen the parameter value λ lies between 0 and 4.

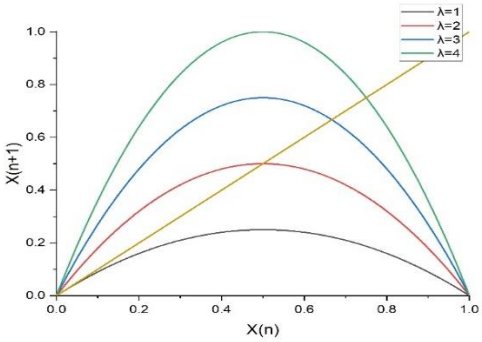

Figure 2: Logistic map function for different values of parameter λ.

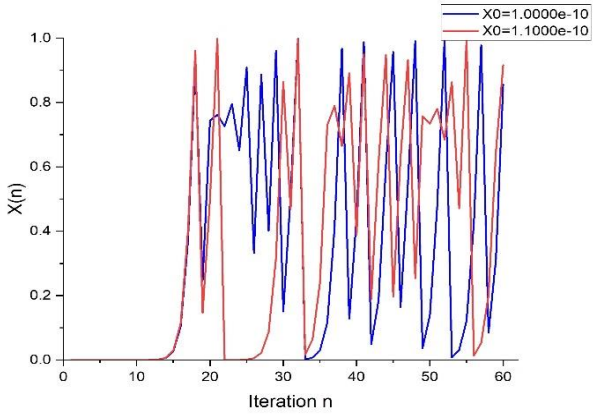

Figure 3: Sensitivity on initial conditions for λ=3.9999.

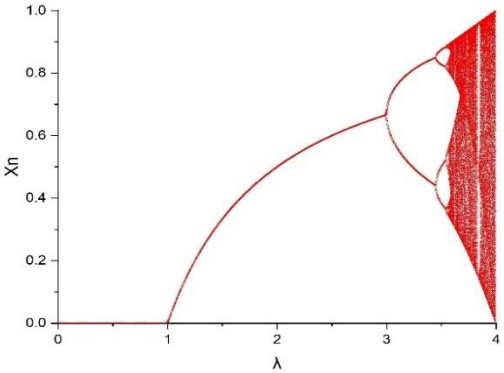

Figure 4: Bifurcation diagram of the logistic mapfor $\lambda = [0 - 4]$.

Figure 5 illustrate the Lyapunov exponent which is a powerful tool that characterizes dynamical processes and measures the sensitivity to initial conditions. The Lyapunov exponent L computed using the derivative method is defined by [19]:

$$L = \lim_{n\to\infty} \frac{1}{n} \left(\sum_{i=1}^{n} \left(\ln\left|\frac{df_\lambda}{dx_i}\right|\right)\right) \quad (4)$$

Where $\frac{df_\lambda}{dx_i}$ represents differentiation with respect to x and $x_0; x_1; x_2, \ldots; x_n$ are successive iterates. For a positive Lyapunov exponent shows a chaotic behavior but if it is negative, it indicates a fixed point or stable periodic orbit, in the case of zero it indicates the occurrence of bifurcation [20].

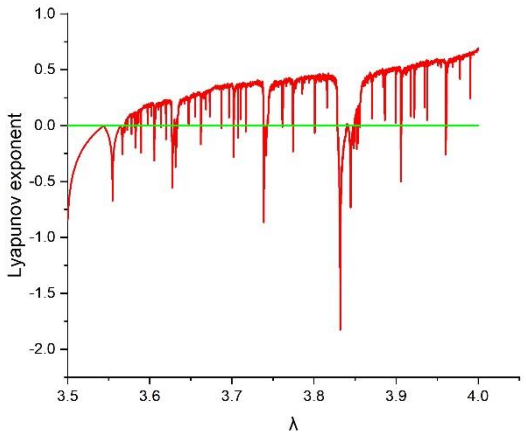

Figure 5: Values of estimated Lyapunov exponent for logistic map for $\lambda = 3.5...4$.

3 Proposed Algorithm

3.1 Matrix generation algorithm

In order to secure the data to be transmitted, we can use permutation methods, which are famous for their simplicity, as one of the strengths of these methods is their low computational complexity. The positions of the input data are changed by the permutation matrix. One way to create this matrix is to use chaotic maps. In, the Logistic map was used to create the permutation matrix, which changes the positions of N input information, this matrix with dimension size of $N \times N$, and each row of this matrix contains only a unique one '1' and the rest elements of the row are zeros '0', and every row differs from the rest rows of the matrix. Lets denotes by P the permutation matrix:

$$P = (R_1; R_2; R_3; \ldots; R_N)$$

Where R_i is a row vector with $i = 1,2,..,N$, which contains $(N-1)$ zeros and only a unique one. The place of this one '1' in row $R_i(j) = 1$ is created by iterating the Logistic map.

In order to get the position of the unique one in each row vector of the permutation matrix to be created, we follow the steps bellow:

The first step: We enter and read the input data number and the initial condition value, as well as the parameter value λ which is greater than 3.5699 in order to achieve the chaotic behavior of the logistic map.

The second Step: We divide the interval [0-1] by the same number of input data so that we get N sub-intervals spaced by $\frac{1}{N}$.

The third step: We map these subintervals in ascending order with natural numbers, starting with 1 until N, which means that the first subinterval $[0 - \frac{1}{N}[$ is mapped by 1 and the second subinterval $[\frac{1}{N} - \frac{2}{N}[$ is mapped by 2 until the N subinterval.

Fourth step: Iterating the chaotic map using the value of the initial condition entered in the first step. Each iteration result belongs to one of the subintervals mapped in the previous step with numbers from 1 to N. This number specifies the place of '1' in each row vector. Every position is preserved to each row vector ,and will be excluded for the rest rows vector in all future iterations. Which means that the corresponding sub-interval is excluded from the future iterations results. That means, if each future iterated value of the logistic map corresponds to one of the preselected intervals it will be ignored by another iteration until all the different positions of the one '1' in each row vector of this matrix are determined. This matrix can be inverted to recover the data correctly using a symmetric key.

3.2 Binary numbers generation algorithm

Using a logistic map, we can create a series of pseudo-random bits that may be used as a key for an encryption process [21]. To convert a real number xi, which is an output of the logistic map iteration, to a bit symbol bi we use a threshold function [22] :

$$b_i = f(x_i) = \begin{cases} 1 & if\ x_i < c \\ 0 & otherwise \end{cases} \quad (5)$$

c is a specific threshold value, this value is chosen such that the probability of $x_i < c$ is equal to the probability of $x_i > c$ in order to generate an unbiased random sequence ($Prob(x_i < c) = Prob(x_i > c)$). b_i and b_{i+1} are statistically independent and the probability that b_i is 0 or 1 is the same $\forall i, x_0$.

3.3 OFDM encrypted system

The main idea of our proposed OFDM system is to shuffle the generated symbols throughout one of the used mapping modulation schemes (BPSK, QPSK,QAM, ...). This is done by adding permutation matrix block to produce scrambled symbols in the frequency domain, before the IFFT block as shown in Figure 6. As result, the OFDM properties will be distorted. That means, the level of security will be enhanced in the physical layer. It has been done by using permutation matrix suggested in section 3.1. In order to construct this permutation matrix we also need the value of the initial condition and it must be also known at both sides, the transmitter and receiver. The initial condition is the symmetric key used to encrypt and decrypt the OFDM symbol during each transmission or reception operation.

The encryption and decryption algorithms are known to the eavesdropper in a brute force attack, but the key is unknown. To decrypt the cipher data via a brute-force attack, the eavesdropper attempts exhaustively access to all possible keys $L = N!$, where N is the size of the FFT block. To complicate the task of the eavesdropper's brute-force attack, the information bits can be encrypted by generating a sequence of random bits by the algorithm described in section 3.2. It can be acted as key with same length of the information bits. The information bits will be encrypted by adding this key as a xor process before the modulation block. This means that even if the eavesdropper has strong computational power to decrypt the proposed OFDM system by applying a brute force attack, he will still get an encrypted information bits.

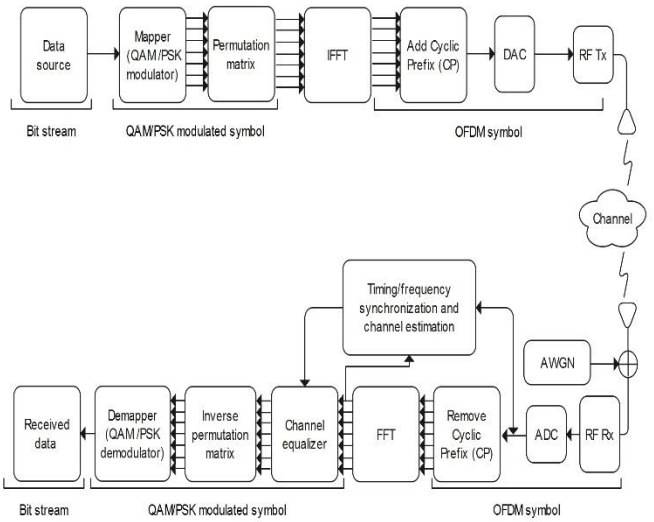

Figure 6: Block diagram of transmitter and receiver in the proposed OFDM system.

3.4 Initial condition IC

The key point in the encryption process in the frequency domain is how to create the initial condition value at both sides, the receiver and the transmitter, without sending it through the transmission channel. Our idea is divided into two parts, the first part is to send the value of the first initial condition (IC_0) to encrypt/decrypt the first OFDM symbol only on the two sides (Transmitter and receiver) . This first initial condition is created and distributed based on Key generation and distribution techniques . To generate our first key, the legitimate users exploit the unexpected (random) properties of their shared wireless channel. The second part is the method to generate the initial condition values to encrypt/decrypt the rest OFDM symbols by generating them from the information previously sent. Since the source of the information to be transmitted is a random source of bits, that is, each transmitted bit stream is different from the next bit stream. Therefore, We can take advantage of the randomness of the source in order to generate the remaining initial conditions without sending them on the channel to encrypt/decrypt the remaining OFDM symbols in the two sides. The rest initial conditions is created by calculating the probability of transmitting bit 1 or 0 of the bit stream. generate the remaining initial conditions withoutsending them

on the channel to encrypt/decrypt the remaining OFDM symbols in the two sides . The rest initial conditions is created by calculating the probability of transmitting bit 1 or 0 of the bit stream.

As illustrated in Figure 7,the first OFDM symbol is transmitted in application of the first part with computing the probability of bit 1 or 0 from the bit stream carried in the this symbol. This probability will be used as the initial condition to encrypt/ decrypt the next OFDM symbol.

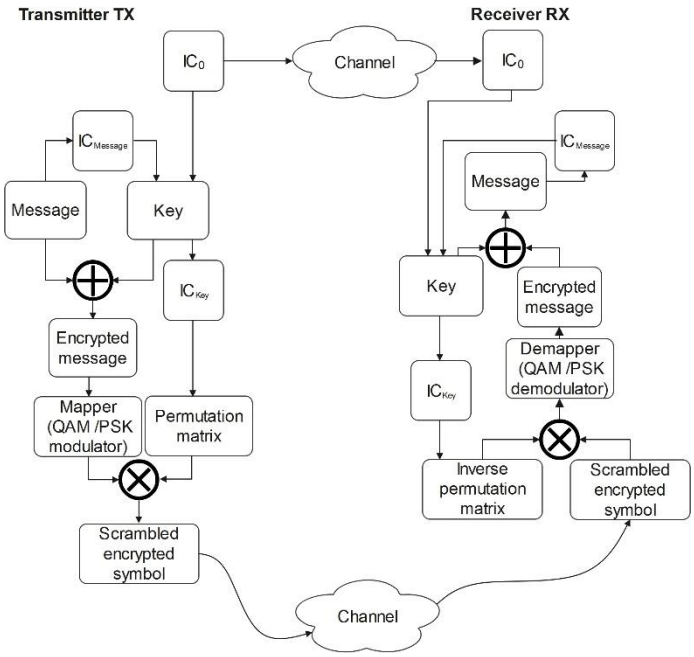

Figure 7: An illustrative diagram of the processof generating initial conditions.

For each transmission, the probability of bit 1or 0 is computed as the initial condition for encrypt/decrypt the next OFDM symbol until the end of the transmission.

4 Simulation results and Discussion

In this section, we present the performance of the proposed scheme evaluated by the BER analysis over both AWGN channels and Rayleigh flat fading channels. We have used two types of digital modulation techniques (PSK, QAM) in different modulation order to see the robustness of our system in terms of security. The OFDM system in this paper is based on the IEEE 802.11a specification shown in Table 1 [25]. The analysis was performed by observing the simulation results executed by Matlab R2018b installed on a computer with Intel(R) Core(TM) i76820HQ CPU@2.70 GHz with 8.00 GHz RAM and OS Microsoft Windows 10 Pro.

The BER curves of our secure OFDM system compared with standard OFDM system over both AWGN channels and Rayleigh flat fading channels are plotted in Figure 8 and 9 respectively. From the Figures 8-9 (a),(b),(c),(d),(e),(f),and (g), It is obvious that the proposed schemes has the same BER performance as that of conventional OFDM systems for the legitimate receiver (Bob side). Unlike the BER performance of the illegitimate receiver (Eve side) remains constant and never decreases even at high SNR. It is owing to the fact that the original message cannot be correctly recovered without keys represented in the initial condition values of the chaos map. This key changes every transmission operation based on our proposed scheme which achieves al- most the perfect secrecy according to Shannon secrecy through the equal key size to the data symbols size. Our proposed scheme ensures that the encryption key is sent only once during the first transmission session, unlike other security schemes [6, 7, 8] that need to share the encryption key in every transmission session.

Parameter	Value
FFT size. nFFT	64
Number of used subcarriers. nDSC	52
FFT Sampling frequency	20MHz
Subcarrier spacing	312.5kHz (=20 MHz/64)
Used subcarrier index Cylcic prefix duration, Tcp	{-26 to -1, +1 to +26} 0.8μs
Data symbol duration, Td	3.2 μs
Total Symbol duration, Ts	4μs

Table 1: Parameters of the OFDM PHY

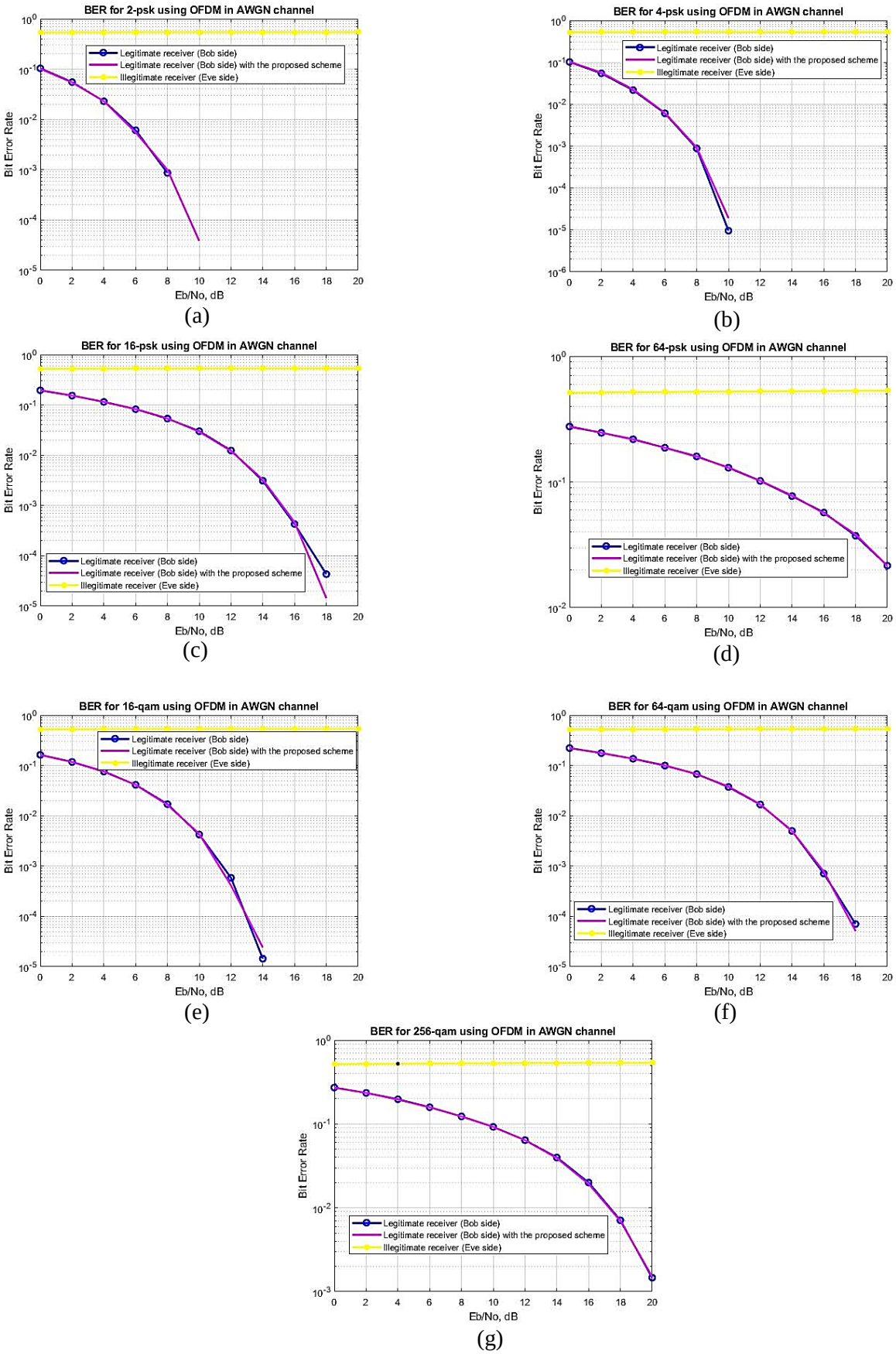

Figure 8: BER performance over AWGN channel

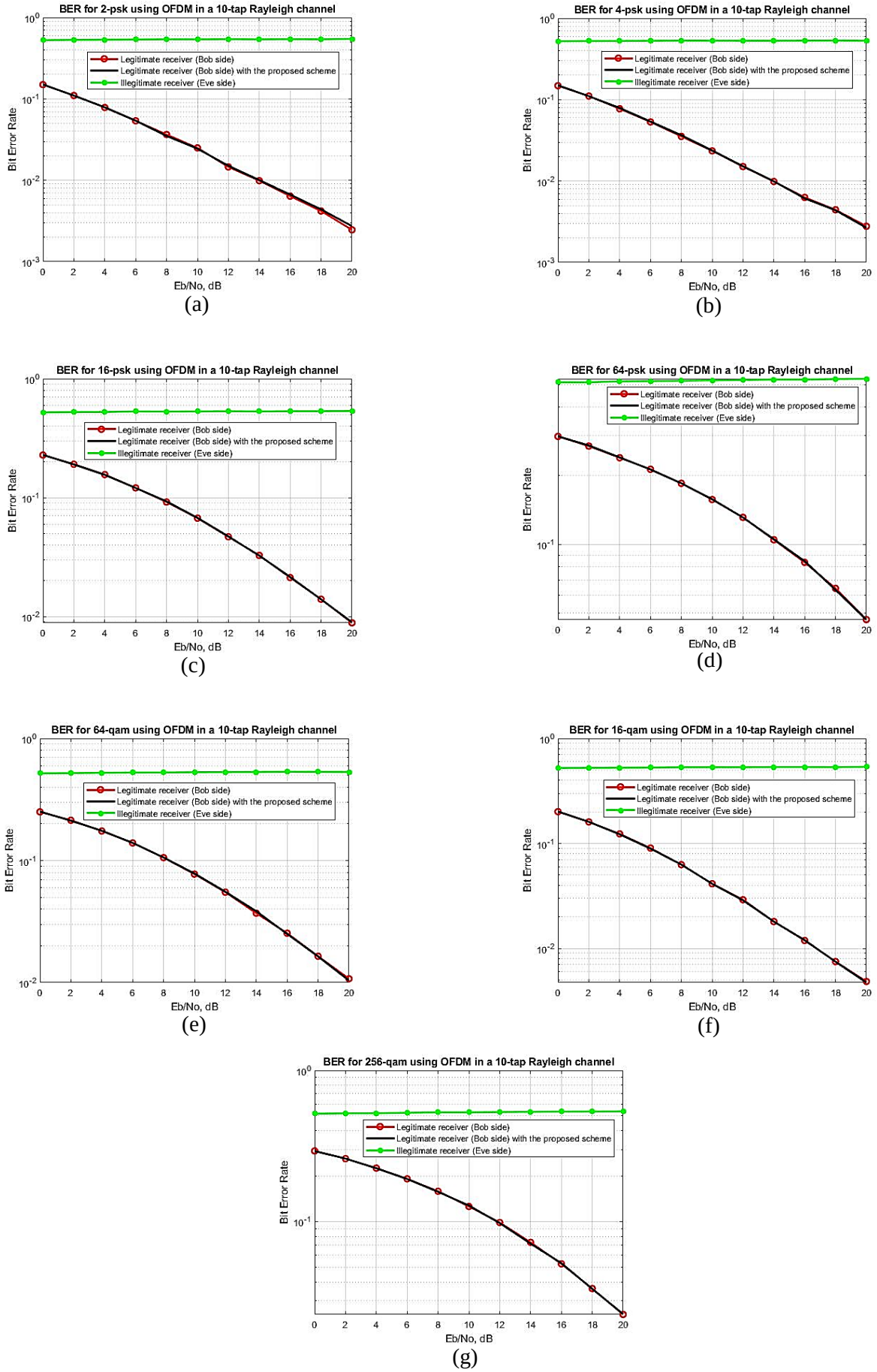

Figure 9: BER performance over 10-tap Rayleigh flat fading channel

5 Conclusion

In this paper, we present a secure OFDM system based on permutation using logistic map in the frequency domain. Where its initial condition is used as a secret key shared between the transmitter and receiver. Which is sent once during the entire transmission process. The rest of the initial conditions are generated by the information transmitted itself. Logistic map work by using these initial conditions to generate a stream of bits that act as a key to encrypt the information. This key has the same length as the information and no need to be sent. Since the source of the information is random, the rest initial conditions is generated by computing the probabilitythat bit 0 or 1 exist in the information. Then the OFDM symbol is scrambled by a permutation matrix. Which is generated using Logistic map and its initial condition is computed with the same method from the generated key stream.

6 Future work

In future work, the initial encryption key for transmission is generated using the random coefficients estimated at receiver and transmitter as channel state information CSI or RSSI (Received Signal Strength Indicator).

References

[1] Group 15 ITU-T, Study. *ITU-T Rec. G.984.1 (03/2008) Gigabit-capable passive optical networks (GPON): General characteristics*. ITU-T, 2008.

[2] Yi Sheng Shiu, Shih Yu Chang, Hsiao Chun Wu, Scott C.H. Huang, and Hsiao Hwa Chen. Physical layer security in wireless networks: A tutorial. *IEEE Wireless Communications*, 18(2):66–74, 2011.

[3] Reem Melki, Hassan N. Noura, Moham- mad M. Mansour, and Ali Chehab. A sur- vey on ofdm physical layer security. *Physical Communication*, 32:1–30, 2019.

[4] Ljupčo Kocarev. Chaos-based cryptography: A brief overview. *IEEE Circuits and Systems Magazine*, 1(3):6–21, 2001.

[5] Ljupco Kocarev and Shiguo Lian. *Chaos-based cryptography: Theory, algorithms and applications*, volume 354. Springer Berlin, Heidelberg, 2011.

[6] Lijia Zhang, Xiangjun Xin, Bo Liu, and Yongjun Wang. Secure ofdm-pon based on chaos scrambling. *IEEE Photonics Technology Letters*, 23(14):998–1000, 2011.

[7] Adnan A.E. Hajomer, Xuelin Yang, and Weisheng Hu. Secure ofdm transmission precoded by chaotic discrete hartley transform. *IEEE Photonics Journal*, 10(2):1–9, 2018.

[8] Wei Zhang, Chongfu Zhang, Wei Jin, Kun Qiu, and Chen Chen. Hybrid time-frequency domain chaotic interleaving for physical-layer security enhancement in ofdm-pon systems. *2016 IEEE/CIC International Conference on Communications in China, ICCC 2016*, pages 1–4, 2016.

[9] Lijia Zhang, Bo Liu, Xiangjun Xin, Qi Zhang, Jianjun Yu, and Yongjun Wang. Theory and performance analyses in secure co-ofdm transmission system based on two-dimensional permutation. Journal of Lightwave Technology, 31(1):74–80, 2013.

[10] Muhammad Asif Khan, Varun Jeoti, and Rana Shahid Manzoor. Secure interleaving - physical layer security enhancement of ofdm based system. *Communications in Computer and Information Science*, 171 CCIS:349–361, 2011.

[11] Hao Li, Xianbin Wang, and Weikun Hou. Secure transmission in ofdm systems by us- ing time domain scrambling. *IEEE Vehicular Technology Conference*, pages 1–5, 2013.

[12] C. E. Shannon. Communication theory of se- crecy systems. *Bell System Technical Jour- nal*, 28(4):656–715, 1949.

[13] Mathuranathan Viswanathan. *Simulation of digital communication systems using Matlab*. 2013.

[14] Mathuranathan Viswanathan. *Wireless Communication Systems in Matlab*. Inde- pendent, 2020.

[15] Yong Soo Cho, Jaekwon Kim, Won Young Yang, and Chung G. Kang. *MIMO-OFDM Wireless Communications with MATLAB®*. John Wiley & Sons, 2010.

[16] Robert M. May. Simple mathematical mod- els with very complicated dynamics. *Nature*, 261(5560):459–467, 1976.

[17] N. K. Pareek, Vinod Patidar, and K. K. Sud. Discrete chaotic cryptography using exter- nal key. *Physics Letters, Section A: General,Atomic and Solid State Physics*, 309(1-2):75–82, 2003.

[18] V. Patidar, K.K. Sud, and N.K. Pareek. A pseudo random bit generator based on chaotic logistic map and its statistical test- ing. *Informatica*, 33(4):441–452, 2009.

[19] Stephen Lynch. Dynamical systems with ap- plications using MATLAB®, second edition. Springer International Publishing, 2014.

[20] Ahmed Sahnoune and Daoud Berkani. On the correlation of chaotic signals generated by multimodal skew tent map. Signal, Im- age and Video Processing, 12(7):1273–1278, 2018.

[21] Madhu Sharma, Ranjeet Kumar Ranjan, and Vishal Bharti. A pseudo-random bit gener- ator based on chaotic maps enhanced witha bit-xor operation. Journal of Information Security and Applications, 69:103299, 9 2022.

[22] Ali Kanso and Nejib Smaoui. Logis- tic chaotic maps for binary numbers gen- erations. Chaos, Solitons & Fractals, 40(5):2557–2568, 2009.

[23] Ahmed Badawy, Tarek Elfouly, Tamer Khat- tab, Amr Mohamed, and Mohsen Guizani. Unleashing the secure potential of the wire- less physical layer: Secret key generation methods. Physical Communication, 19:1–10, 2016.

[24] Junqing Zhang, Alan Marshall, Roger Woods, and Trung Q. Duong. Efficient key generation by exploiting randomness from channel responses of individual ofdm sub- carriers. IEEE Transactions on Communi- cations, 64(6):2578–2588, 2016.

[25] IEEE Computer Society LAN MAN Stan- dards Committee et al. Part 11: Wireless lan medium access control (mac) and physical layer (phy) specifications: High- speed physi- cal layer in the 5ghz band. *IEEE std 802.11 a-1999*, 1999.