TELKOMNIKA Telecommunication Computing Electronics and Control
Vol. 22, No. 1, February 2024, pp. 42~54
ISSN: 1693-6930, DOI: 10.12928/TELKOMNIKA.v22i1.25167

Analysis of PLS enhancement using permutation index based OFDM-DCSK system over multipath Rayleigh fading channel

Dhuha Hussein Hameed, Fadhil S. Hasan
Department of Electrical Engineering, Faculty of Engineering, Al-Mustansiriyah University, Baghdad, Iraq

Article Info

Article history:

Received Mar 17, 2023
Revised Dec 5, 2023
Accepted Dec 11, 2023

Keywords:

Multipath Rayleigh fading channel
Orthogonal frequency division multiplexing-differential chaos shift keying
Permutation index
Physical layer security
Secrecy analysis

ABSTRACT

This paper presented the performance of physical layer security of permutation index (PI) with modulating bits-based orthogonal frequency division multiplexing differential chaos shift keying system (PIM-OFDM-DCSK), the objective behind PIM-OFDM-DCSK is to improve and increase the information rate, spectral, and energy efficiencies. In PIM-OFDM-DCSK, the (M) subcarriers, each carry (n+1) bits. The n bits are index bits utilized to choose one permutation of the chaotic reference. On the receiver, after OFDM demodulation, the correlation is made between the permuted versions of the chaotic reference and the received bearing sequence of data. Then the received bits are assessed by determining the maximum correlator outputs via which the n bits are detected. Then the maximum output correlator sign is utilized to detect the modulating bit. The performance of the PIM-OFDM-DCSK is tested under additive white gaussian noise and multipath fading channel. Furthermore, the bit error rate is derived based on the wiretap system for the proposed PIM-OFDM-DCSK and compared with other DCSK modulations. The results show that the proposed PIM-OFDM-DCSK scheme is promising and competitive compared with other DCSK system, and the best BER performance is as an increase in the value of n and a decrease in the value of β.

Corresponding Author:

Dhuha Hussein Hameed
Department of Electrical Engineering, Faculty of Engineering, Al-Mustansiriyah University
Baghdad, Iraq
Email: eeph006@uomustansiriyah.edu.iq

1. INTRODUCTION

The services of wireless communication are extremely increasing in modern-day life due to the significance of the enormous spread of wireless devices, distinguished by their ease of use and high mobility. Furthermore, the increase in wireless data communication is mainly driven by the number of useful applications specified for mobile used users. Therefore, wireless media is becoming the foremost access for furthermost communication-based services that convey wireless signals and waves. Therefore, earnest security dangers are conspicuous in such services due to the nature of the broadcast. Consequently, novel security necessities have immediately been required. As a matter of fact, a communication system's strong security needs to be executed without just depending on the conventional cryptographic methods, which generally rely on the security model of Shannon's [1]. To this end, physical layer security (PLS) [2], the key powerful matter for research in addition to reliability, capacity, and delay, is apparently the same as a capable and developing idea to solve the problem of eavesdropping security [3]–[6]. Therefore, the PLS is utilized in a wireless environment to enhance reliability and improve security against eavesdropping attacks. The PLS is dissimilar to the cryptography method. The open system interconnects model upper layers are exercised to treat any inconsistencies associated with the attributes of cryptography methods, authenticity, privacy, and confidentiality of data transmission.

These features generally rely on cryptographic procedures, which consist of the distribution of secret-key, public-key, and symmetric encryption. This arrangement is the most successful and practical, but more complexity is added to the communication system. In contrast, these procedures are independent of the physical layer [7], [8].

Shannon [1] had the first investigation on the security of information-theoretic by describing the wiretap channel. The next work was by Wyner [2] that presented a further general noisy wiretap channel and exposed that without using any secret keys, the secure communication of information-theoretic can be accomplished by keeping the 3rd party unaware of the secure message. From that point forward, to concentrate on the study of information-theoretic secrecy performance viewpoint, sufficient attention from both academia and industry was attracted. Furthermore, there exists a multitude of research concentrating on wireless communication schemes utilizing chaos as carrier sequence because of their beneficial characteristics of wideband [9].

On another hand, the spread spectrum communication system that uses the chaotic signal has the most significant increasing acceptance because the chaotic signal is simple to produce and has the same important characteristics as a non-periodic, wideband spectrum. Its values have low cross-correlation properties and impulse-same auto-correlation [10]. These characteristics are significant for supporting the security of transmission, better performance of multiple access, greater resistance to interference or jamming, and many multipath immunity effects. There are numerous proposed types of research on chaos-based coherent and non-coherent communication systems. The synchronization of chaotic signals at the receiver side is considered the main disadvantage of coherent-based chaos communication schemes, the same as chaos shift-keying (CSK) [11], because it forms a challenging work in channels that are noisy described. Fortunately, the non-coherent-based chaos communication scheme can accomplish well at the receiver side without needing the synchronization of the sent chaotic signal and also demonstrates resistance that is robust to properties of multipath fading [12]. Therefore, it is studied increasingly via the community scientific.

The initial non-coherent chaotic structure is the differential chaos shift keying (DCSK) scheme [13]. In DCSK, there are two slots for each transmitted bit duration. In the 1st time slot, the reference sample of chaotic is transmitted, but, in the 2nd time slot, modulated bit is sent by multiplying the bit with the delayed version of the chaotic sample. On the receiver side, to recover the sent bit, the chaotic reference (CR) is correlated with the modulated sample. The advantages of this system are easy to implement, multipath interferences resistance, recovery of the chaotic sequence is eschewed and the state estimator of the channel at the receiver is inexistent. Nevertheless, the main disadvantages of this system are the low rate of data, high energy utilisation, and the use of delay lines, which are wideband RF, which are hard to carry out in CMOS knowledge [14]. It ought to likewise be referenced that the delay line in RF is a problem in analogue employments only, whereas in digital employments, same as system-on-chip (SoC) or field programmable gate arrays (FPGA), is presently not a problem, and lack of security of this system as compared to communications systems based on coherent chaos. As a matter of fact, in digital communication, security is the significant motivation behind the use of chaotic signals [15]. Therefore, the crucial point in this paper is that the security of the DCSK scheme will be enhanced.

Therefore, in this paper, we focus only on PLS techniques from the information-theoretic perspective by suggesting a new transmission system by using DCSK system that depends on the permutation index modulation orthogonal frequency division multiplexing (PIM-OFDM-DCSK) to accomplish high data rate, high security of transmission, high physical layer data security and high-reliability performances by random permutation of the CR for each data symbol. The contributions of this paper are outlined as:

a) Permutation index modulations aided OFDM-DCSK systems is suggested named PIM-OFDM-DCSK system. The proposed PIM-OFDM-DCSK system modulates M data symbols, where each symbol is consisting of $n + 1$ bits, where n bits are mapped to a unique permutation of reference chaotic signal, then the choice of the permuted sequence is utilized to spread the single bit named modulating bit, which is physically sent. Then the produced signal for each frame consists of a single reference signal slot, and M slots, for each M slot, the modulating bit is sent after spread by the particular choice permuted chaotic sequence, which is modulated by an OFDM technology in which the signal is sending over different carrier frequencies by using inverse fast fourier transform (IFFT). After adding the guard interval, the serial sequence will be transmitted over a multipath Rayleigh fading channel (MRFC) and additive white gaussian noise (AWGN) channel. At the receiver after eliminating the guard interval from the parallel received sequence, then the sequence pass to OFDM demodulation by FFT, and then the correlation is done between all possible 2^n versions of the permuted reference chaotic signal and the received sequence for each M slot. Then summated over the symbol duration. Then the received bits are assessed by determining the maximum correlator outputs that point to the correct index of permutation by which the n bits are transmitted, then the sign of the maximum output correlator is utilized to detect the modulating bit. When the design of the proposed system is accomplished, the performance is determined by computing the performance of bit error rate (BER) over an MRF and AWGN channels.

b) The BER theory of the PIM-OFDM-DCSK scheme is derived over AWGN and MFRC. As well, the simulated of BER is compared with the analytical BER to confirm the accuracy of the analysis. Additionally, the proposed systems are compared with recent works on the DCSK systems. Notation: the complex conjugate, transpose and the real part are denoted by $(\,.\,)^{*}$,$(\,.\,)^{T}$, and $\Re\,(.)$, respectively.

The rest of this paper is organized as follows: section 2 gives the proposed scheme of a PIM-OFDM-DCSK system. Section 3 and section 4 give system analysis and theoretical performance analysis. Simulation results and discussions are provided in section 5. Finally, the conclusion of the paper is given in section 6.

2. PROPOSED PIM-OFDM-DCSK SYSTEM MODEL

This section presents the procedure designed in detail for the proposed PIM-OFDM-DCSK system. The transmitter scheme construction is shown in Figure 1. The receiver scheme construction is shown in Figure 2. The details of transmitter and receiver scheme construction are explained as follows:

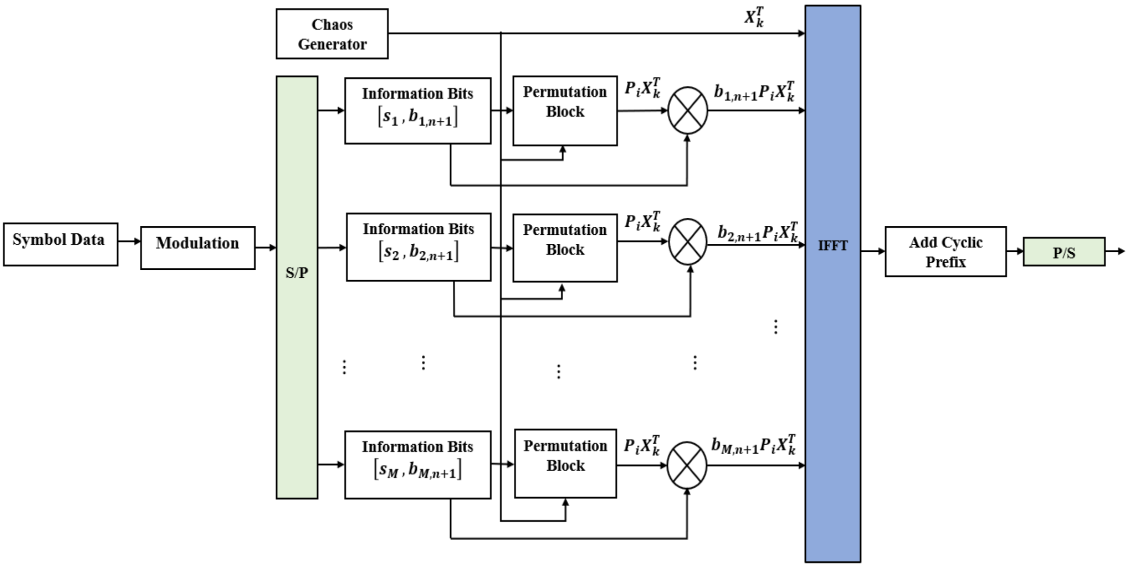

Figure 1. PIM-OFDM-DCSK transmitter diagram

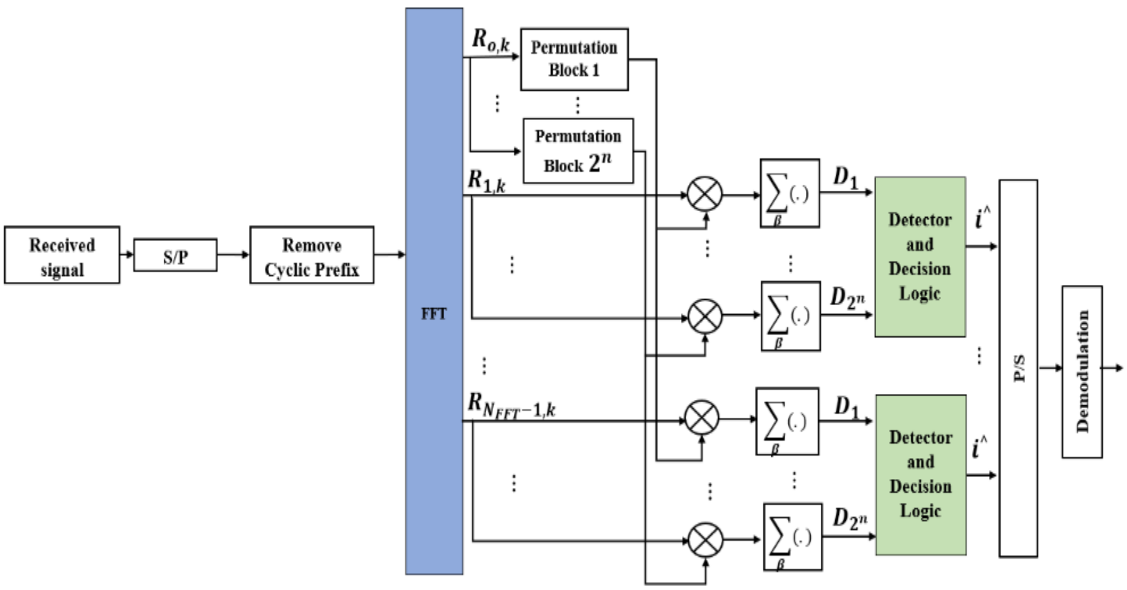

Figure 2. PIM-OFDM-DCSK receiver diagram

2.1. The proposed PIM-OFDM-DCSK transmitter scheme

At the transmitter, the 1st time slot is occupied by a CR sequence with β samples length produced by the source of chaotic, which is used as a CR signal. In PIM-OFDM-DCSK, the number of modulated symbols is M symbols in each frame, where each symbol is consisting of $n+1$ bits. The m^{th} block of symbol in each frame can be described as: $b_m = \left[s_m , b_{m,n+1}\right]$ where $s_m = \left[b_{m,1}\ b_{m,2}\ \dots\dots\dots\ b_{m,n}\right]$, $m = 1,..,M$ is the vector of n mapping bits. Each mapping bits s_m is overloaded in to block of permutation. The permutation block is permutated the reference signal to $(\beta! - 1)$ perms. In the PIM-OFDM-DCSK the permutations are selected in a manner such that, for different selected perms, there is quasi-orthogonality (QO) between them. Moreover, for large spreading factor, it is demonstrated that there is a QO between different selected perms of the chaotic signal [16], such that:

$$P_i(X_k)P_z(X_k^T)^T \approx 0, i \neq z , k = 1,..,\beta \tag{1}$$

$$X_k P_i(X_k^T)^T \approx 0 \tag{2}$$

Where X_k is a vector that encompasses β length CR samples, $P_i(X_k)$ denotes the i^{th} permutation operator and $(\cdot)^T$represents to transpose. Because the mapping bits number is n bits, there are 2^n distinct permutations of the reference signal that will be selected out of $(\beta! - 1)$ at each transmitter. Therefore, the mapping bits s_m choice one of the 2^n predefined permutations of chaotic sequence, i.e., $s_m \to P_i$ where $P_i \in \{P_1\ P_2\ \dots\dots\dots\ P_{2^n}\}$. Then the selected permuted sequence is utilized to spread the modulated bit $b_{m,n+1}$. Therefore, the total number of transmitted bits for each fram is $M(n+1)$. Nevertheless, it should be noted that the selected permutations out from the group of $(\beta! - 1)$ permutations must be chosen such that the property of low cross-correlation is satisfied. If permutations are not correctly selected, the system's performance may reduce. For each frame, the signal after permutation can be represented by the baseband matrix $S_{m,k} \in \mathbb{R}^{(M+1)\times\beta}, m = 0,1,..,M, k = 0,1,..,\beta - 1$, given as (3):

$$S_{m,k} = \begin{bmatrix} X_k \\ b_{1,n+1}P_iX_k^T \\ b_{2,n+1}P_iX_k^T \\ \vdots \\ b_{M,n+1}P_iX_k^T \end{bmatrix}, where \begin{matrix} i \in [1, 2^n], k = 1, \dots, \beta \\ m = 0,1,..,M \end{matrix} \tag{3}$$

Where, $X_k = \left[x_1 x_2\ \dots\dots\dots\ x_\beta\right]$ is the CR segment, $0 < k \leq \beta$, $P_iX_k^T$ with a length of β represents the selected permutated form of the CR signal mapped from the m^{th} information vector b_m, and i is the PI of the m^{th} subcarrier. Then, the signal $S_{m,k}$ is applied to IFFT function for transmission over multiple subcarriers to produce the k^{th} OFDM modulated sequence given by [17]:

$$s_{v,k} = \frac{1}{\sqrt{N_{FFT}}}\sum_{m=0}^{N_{FFT}-1} S_{m,k}\, e^{j2\pi\frac{mv}{N_{FFT}}}, 0 \leq v < N_{FFT} , 0 \leq k < \beta \tag{4}$$

Where N_{FFT} is the FFT size ($N_{FFT} = M + 1$). Then, the resulting symbols of OFDM are applied to P/S conversion and a cyclic prefix (CP) is added to avoid the ISI, and then sent over the channel. Then the k^{th} transmitted sequence is transmitted through L path RFC and AWGN, according to [17]:

$$r_{v,k} = \sum_{\rho=1}^{L} \alpha_\rho s_{v,k-\tau_\rho} + \eta_{v,k} \tag{5}$$

Where $\eta_{v,k}$ is the complex AWGN sequence with a mean value equal to zero and variance N_o. α_ρ and τ_ρ are the channel coefficient and time delay for the ρ^{th} path, respectively, and the number of paths is L, and the variables α_ρ, $\rho = 1,..,L$ are random variables Rayleigh distributed that are considered to be flat and quasi-static over the one transmitted frame with the following probability density function (PDF) [18]:

$$f_\alpha(z) = \frac{z}{\sigma^2} exp(-z^2/2\sigma^2) \tag{6}$$

Where σ is root mean square (RMS) value of the receipted sequence before the envelope detector.

2.2. The proposed PIM-OFDM-DCSK received scheme

The received symbols at the receiver side are applied to the FFT function for OFDM demodulation after S/P conversion and CP is eliminated to generate the k^{th} OFDM demodulation sequence given by [19]:

$$R_{m,k} = \frac{1}{\sqrt{N_{FFT}}} \sum_{v=0}^{N_{FFT}-1} r_{v,k}\, e^{-j2\pi \frac{mv}{N_{FFT}}}, 0 \le m < N_{FFT}, 0 \le k < \beta \quad (7)$$

Then OFDM demodulated samples of the reference sequence are sent to the bank of permutation to generate 2^n different permutations. Then, the correlation process will be done between all generated permutations of the reference sequence and the OFDM demodulated information samples during the m^{th} time slot of duration, $m = 1, .., M$. Therefore, for each m^{th} time slot of duration, there are 2^n decision variables. Therefore, for the m^{th} time slot and the z^{th} correlator output of the decision variable $D_{m,z}$ is expressed as (8):

$$D_{m,z} = \Re \left\{ P_z \left(\sum_{\rho=1}^{L} \alpha_\rho X_k + N_{R,k} \right) \times \left[\left(\sum_{\rho=1}^{L} \alpha_\rho\, b_{m,n+1} P_i X_k + N_{m,k} \right)^* \right]^T \right\} \quad (8)$$

Where $N_{R,k}$ and $N_{m,k}$ is the AWGN sequence of the reference and m^{th} time slot, respectively. The correlator output can be expanded to:

$$D_{m,z} = \Re \left\{ \sum_{k=0}^{\beta-1} P_z \left(\sum_{\rho=1}^{L} \alpha_\rho x_k \right) \times \left(\sum_{\rho=1}^{L} \alpha_\rho b_{m,n+1} P_i x_k \right)^T \right\} + \Re \left\{ \sum_{k=0}^{\beta-1} P_z \left(\sum_{\rho=1}^{L} \alpha_\rho x_k \right) \times [\eta_k{}^*]^T + P_z \eta_k \times \left(\sum_{\rho=1}^{L} \alpha_\rho b_{m,n+1} P_i x_k \right)^T \right\} + \Re \left\{ \sum_{k=0}^{\beta-1} P_z \eta_k \times [\eta_k{}^*]^T \right\} \quad (9)$$

Since,

$$\Re \left\{ \sum_{k=0}^{\beta-1} P_z \left(\sum_{\rho=1}^{L} \alpha_\rho x_k \right) \times \left(\sum_{\rho=1}^{L} \alpha_\rho b_{m,n+1} P_i x_k \right)^T \right\} = SS \text{ or } SI \quad (10)$$

$$\Re \left\{ \sum_{k=0}^{\beta-1} P_z \left(\sum_{\rho=1}^{L} \alpha_\rho x_k \right) \times [\eta_k{}^*]^T + P_z \eta_k \times \left(\sum_{\rho=1}^{L} \alpha_\rho b_{m,n+1} P_i x_k \right)^T \right\} = SN \quad (11)$$

$$\Re \left\{ \sum_{k=0}^{\beta-1} P_z \eta_k \times [\eta_k{}^*]^T \right\} = NN \quad (12)$$

Where SS represents the favourite signal component at $z = i$, the correlation process between the CR signal and its permutation form produced the inter-signal-interference, which SI represents at $z \neq i$. In contrast, SN and NN represent the cross-correlation between the CR signal and the noise and the noise-to-noise correlation, respectively, which seriously affects the system's performance, especially at a high value of spreading factor β. Then, for each m^{th} time slot of duration, the largest output of the correlator compared with other correlator outputs, which is represented the correct permutation index $i^\wedge$ is determined by:

$$i^\wedge = arg\ max \left\{ \left| D_{m,z} \right| \right\} z \in \{1,2,3 \ldots \ldots \ldots\ 2^n\} \quad (13)$$

By using the estimated index $i^\wedge$, the m^{th} bits s_m can be detected.

Then to detect the modulating bit $\hat{b}_{m,n+1}$, computed the sign of the maximum output correlator that was used in the previous step, by which the correct permutation index $i^\wedge$ is determined, i.e.,

$$\hat{b}_{m,n+1} = sgn(D_{m,i^\wedge}) \quad (14)$$

In our analysis, we suppose that the reference signal duration βT_C is much greater than the maximum value of delay τ_{max} for all combination paths, i.e., $0 < \tau_{max} << \beta T_C$ under this assumption, the inter-symbol interference (ISI) may be ignored.

3. ANALYSIS OF THE PROPOSED SYSTEM

This section explains the system analysis of PIM-OFDM-DCSK concerning energy efficiency. Energy efficiency enhancement of the PIM-OFDM-DCSK scheme is analyzed using the data energy to bit energy ratio (DBR) measure, as it's defined in [18]. This measurement is employed to assess the energy efficiency economizing to the number of sent data bits, and it is calculated as [12], [20]:

$$DBR = E_{data}/E_b \quad (15)$$

Where E_{data} is the conveying data signal energy, whereas the overall energy of bit is represented by E_b, which is required to convey every data bit. As such, it is the ratio between the number of sent sequences of chaotic to the number of sent data bits. Under the assumption that all systems with equal chip rate T_c. In the suggested system, to transmit M symbols, a single reference chaotic signal is used in each frame. Each symbol has n bits that are used to select one of a 2^n permutation versions of the CR signal. Therefore, the average symbol energy E_s can be represented by:

$$E_s = E_{data} + \frac{E_{ref}}{M} \tag{16}$$

$$E_{data} = \beta E(x_k^2) \tag{17}$$

$$\frac{E_{ref}}{M} = \frac{\beta E(x_k^2)}{M} \tag{18}$$

Then, the whole average E_s can be express as (19) and (20):

$$E_s = \beta E(x_k^2) + \frac{\beta E(x_k^2)}{M} \tag{19}$$

$$E_s = \beta E(x_k^2)(1 + \frac{1}{M}) \tag{20}$$

Since, each M symbol is used to transmit $\log_2 N = (n + 1)$ bits:

$$(n + 1)E_b = \beta E(x_k^2)(1 + \frac{1}{M}) \tag{21}$$

$$E_b = \frac{(M+1)\beta}{M\, log_2 N} E(x_k^2) \tag{22}$$

$$\frac{E_{data}}{E_b} = \frac{\beta E(x_k^2)}{\frac{(M+1)\beta}{M\, log_2 N} E(x_k^2)} = \frac{M\, log_2 N}{(M+1)} \tag{23}$$

4. THEORETICAL PERFORMANCE ANALYSIS

The theoretical performance for the PIM-OFDM-DCSK scheme is obtained, and BER analytical expressions are derived over AWGN and MRF channels. The equation $x_{k+1} = 1 - 2x_k$ describes the Chebyshev polynomial function (CPF). It will be employed in this effort due to its simplicity and excellent statistical properties [21] to produce the chaotic signal with a mean value equal to zero and variance unity, i.e., $E(x_k) = 0$, and $E({x_k}^2) = 1$, where $E(.)$ is the expectation operator. Also, for a simple process, assume that the chip rate T_C is unity. The Gaussian approximation (GA) process will also be utilized to determine the system performance analysis. For a high value of β, the GA method gives an accurate performance, while a smaller value of β displays some inaccuracy performance [22]. However, the property of the large value of β makes GA appropriate for investigation in communication schemes based-chaos.

4.1. BER analysis of PIM-OFDM-DCSK

The number of the total sent bits in every frame of PIM-OFDM-DCSK system are $M(n + 1)$ bits, where Mn bits are the mapping bits utilised to distinguish the permutation indices and M are the modulating bits. Hence, the overall BER of the PIM-OFDM-DCSK scheme consists of the mapping bits BER ($P_{r_{map}}$) and the modulating bits BER ($P_{r_{mod}}$). Hence, the overall BER P_{r_M} would be expressed as (24) [23]:

$$P_{r_M} = \frac{n*M}{M*log_2 N} P_{r_{map}} + \frac{M}{M*log_2 N} P_{mod} \tag{24}$$

For each m^{th} time slot of duration, the probability of $P_{r_{map}}$ is reliant on n mapping bits and on the $P_{r_{ed}}$, which is the erroneous detection probability of the permutation index. Moreover, if the index of permutation is wrongly detected, then an erroneous grouping of mapping bits will be assessed. The individually erroneous grouping may comprise a different number of erroneous bits as compared to the exact transmitted group. Consequently, the $P_{r_{ed}}$ probability can be transformed into an equivalent $P_{r_{map}}$ using [24].

$$P_{r_{map}} = \frac{2^{n-1}}{2^{n}-1} P_{r_{ed}} \tag{25}$$

The correct detection of the modulating bit $b_{m,n+1}$, for each m^{th} time slot of duration relies on the correct detection of the PI and the correct de-spreading process. Hence, there are two various cases that reason an error to happen. In the 1st case, the detection of the permutation index is corrected, but an error occurs during the modulating bit de-spreading process. In PIM-OFDM-DCSK, the de-spreading process is accomplished in a similar way as in the conventional DCSK. While in the 2nd case, the PI is wrongly assessed, and, therefore, the de-spreading process of the modulating bit occurs at the output of the improper correlator. Therefore, the correct detection probability of the modulating bit $b_{m,n+1}$ will be simply equivalent to 0.5. Subsequently, the total BER of modulating bits can be given as (26) [23]:

$$P_{mod} = P_{rDCSK}(1 - P_{red}) + 0.5P_{red} \tag{26}$$

Where P_{rDCSK} is the BER of the DCSK system.

4.2. Erroneous permutation detection probability, $P_{r_{ed}}$

For the proposed PIM-OFDM-DCSK scheme, after the OFDM demodulation, the correct estimation of the permutation index of each sent symbol is accomplished by choosing the maximum absolute value from the result of the correlator outputs. The correlator output results equal the correlation between the 2^n different permutations of the CR signal and the received sequence. Hence, for each m^{th} time slot of duration, there are 2^n correlator outputs.

The output of every correlator can be demonstrated as a Gaussian random variable, $D_{m,z}$. For equiprobable sent permuted sequences, assessment conditioned of the error probability of the PI, P_i is expressed as (27):

$$P_{r_{ed}} = \left(P_r\left|D_{m,i}\right| < \max P_r\left|D_{m,z}\right|\right), 1 \leq z \leq 2^n, z \neq i \tag{27}$$

Where $D_{m,i}$ and $D_{m,z}$ are the variables of decision at z^{th} and i^{th} correlator outputs, respectively. The $P_{r_{ed}}$ will occur if the maximum value of $\left|D_{m,z}\right|$ is greater than $\left|D_{m,i}\right|$, where $z \neq i$.

To detect the first symbol, the z^{th} outputs of the correlator can have two different expressions; the first expression is when the correlator output index at the receiver (z) is equivalent to the sent permutation index (i), while the second expression is when the correlator output index at the receiver (z) is not equal to the permutation index used at the transmitter (i), then the decision variable $D_{m,z}$ can be rewritten as (28):

$$D_{m,z} = \begin{cases} SS_{m,i} + SN_{m,i} + NN_{m,i} \; for \; z = i \\ SI_{m,z} + SN_{m,z} + NN_{m,z} \; for \; z \neq i \end{cases} \tag{28}$$

The correlation components for $z = i$ can be calculated as (29):

$$D_{m,i} = SS + SN + NN \tag{29}$$

$$SS_{m,i} = \Re\left\{\sum_{k=0}^{\beta-1} P_i \left(\sum_{\rho=1}^{L} \alpha_\rho \, x_k\right) \times \left(\sum_{\rho=1}^{L} \alpha_\rho b_{m,n+1} P_i x_k\right)^T\right\}$$

$$= \Re\{\sum_{k=0}^{\beta-1} \sum_{\rho=1}^{L} \alpha_\rho{}^2 \; b_{m,n+1} \, P_i \, (x_k) P_i x_k^T\} \approx b_{m,n+1} \sum_{k=1}^{\beta} \sum_{\rho=1}^{L} \alpha_\rho{}^2 \; x_k^2 \tag{30}$$

$$SN_{m,i} = \Re\left\{\sum_{k=0}^{\beta-1} P_i \left(\sum_{\rho=1}^{L} \alpha_\rho \, x_k\right) \times [\eta_k{}^*]^T + P_i \eta_k \times \left(\sum_{\rho=1}^{L} \alpha_\rho b_{m,n+1} P_i x_k\right)^T\right\} \tag{31}$$

$$= \Re\left\{\sum_{k=0}^{\beta-1} \sum_{\rho=1}^{L} \alpha_\rho \, x_k' [\eta_k{}^*]^T + b_{m,n+1} \sum_{k=1}^{\beta} \sum_{\rho=1}^{L} \alpha_\rho \, \tilde{\eta_k} \, x_k^T\right\} \tag{32}$$

$$NN_{m,i} = \Re\left\{\sum_{k=0}^{\beta-1} P_i \eta_k \times [\, \eta_k{}^*]^T\right\} = \Re\left\{\sum_{k=1}^{\beta} \tilde{\eta_k} \, [\, \eta_k{}^*]^T\right\} \tag{33}$$

The last expression of $SS_{m,i}$ is approximated due to the property of the low autocorrelation between the different delayed of the chaotic sequences, i.e.,

$$X_{m,\tau_\rho,k}\left(X_{m,\tau_l,k}^T\right) \approx 0 \; for \; l \neq \rho \tag{34}$$

Supposing that the noise is complex AWGN has PSD equivalent to N_o, with a mean value equal to zero where $\eta_{\tilde{k}}$ is the noise sample that is permutated. Under the supposition that the correlation between noise sample and chaotic samples is negligible, for the sufficient value of β, and the maximum value of delay of MRFC is much less than the duration of the reference signal, i.e., $\tau_{max} << \beta T_C$, which means that ISI is negligible. Then the mean of $D_{m,i}$ for a given $b_{m,n+1}$, is:

$$E(D_{m,i}) = E(SS_{m,i}) + E(SN_{m,i}) + E(NN_{m,i}) = E\left(b_{m,n+1} \sum_{k=1}^{\beta} \sum_{\rho=1}^{L} \alpha_\rho{}^2\ x_k^2\right) + 0 + 0 \tag{35}$$

$$= b_{m,n+1}\, \beta \sum_{\rho=1}^{L} \alpha_\rho{}^2\ E(x_k^2) = b_{m,n+1} \frac{log_2 N * M E_b}{(M+1)} \sum_{\rho=1}^{L} \alpha_\rho{}^2 \tag{36}$$

All terms in $SN_{m,i}$ and $NN_{m,i}$ are uncorrelated, whereas coefficients of channel and samples of noise are independent. Therefore, the total variance of the i^{th} correlator decision variable $D_{m,i}$ can be written as (37) and (38):

$$V(D_{m,i}) = V(SN_{m,i}) + V(NN_{m,i}) = \mathrm{V}\left(\Re\left\{\sum_{k=0}^{\beta-1} \sum_{\rho=1}^{L} \alpha_\rho\, x'_k [\eta_k{}^*]^T + b_{m,n+1} \sum_{k=1}^{\beta} \sum_{\rho=1}^{L} \alpha_\rho\, \eta_{\tilde{k}}\, x_k^T\right\}\right) V\left(\Re\left\{\sum_{k=1}^{\beta} \eta_{\tilde{k}}\, [\eta_k{}^*]^T\right\}\right) \tag{37}$$

$$= N_O\ \frac{log_2(N)\ M\ E_b}{(M+1)} \sum_{\rho=1}^{L} \alpha_\rho{}^2 + \beta \frac{{N_O}^2}{2} \tag{38}$$

The correlation components for $z \neq i$ can be determined as (39)-(43):

$$D_{m,z} = SI_{m,z} + SN_{m,z} + NN_{m,z} \tag{39}$$

$$SI_{m,z} = \Re\left\{\sum_{k=0}^{\beta-1} \sum_{\rho=1}^{L} \alpha_\rho\, P_z(x_k) \times \sum_{\rho=1}^{L} \alpha_\rho b_{m,n+1}\ P_i x_k^T\right\} \approx 0 \tag{40}$$

$$SN_{m,z} = \Re\left\{\sum_{k=0}^{\beta-1} \sum_{\rho=1}^{L} \alpha_\rho\, P_z(x_k))\, \eta_k^T + P_z(\eta_k)(\sum_{\rho=1}^{L} \alpha_\rho b_{m,n+1}\, P_i x_k^T\right\} \tag{41}$$

$$= \Re\left\{\sum_{k=1}^{\beta} \sum_{\rho=1}^{L} \alpha_\rho\, x'_k \eta_k + b_{m,n+1} \sum_{k=1}^{\beta} \sum_{\rho=1}^{L} \alpha_\rho\, \eta_{\tilde{k}} x_k\right\} \tag{42}$$

$$NN_{m,z} = \Re\left\{\sum_{k=0}^{\beta-1} P_z \eta_k \times [\eta_k{}^*]^T\right\} = \sum_{k=1}^{\beta} \eta_{\tilde{k}}\, [\eta_k{}^*]^T \tag{43}$$

Consequently, the mean and variance for z^{th} correlator at m^{th} time slot of duration, where $z \neq i$, can be expressed as (44) and (45):

$$E(D_{m,z}) \approx 0 \tag{44}$$

$$V(D_{m,z}) = V(SN_{m,z}) + V(NN_{m,z}) = N_O\ \frac{log_2(N)\ M\ E_b}{(M+1)} \sum_{\rho=1}^{L} \alpha_\rho{}^2 + \beta \frac{{N_O}^2}{2} \tag{45}$$

It's clear that the variance values of $SN_{m,i}$ and $NN_{m,i}$ are equal to the variance values of $SN_{m,z}$ and $NN_{m,z}$, respectively. In the following derivations, the $|D_{m,i}|$ mean value is independent on the value of the modulating bit ($b_{m,n+1}$), because of the absolute operator value of decision variable $D_{m,i}$. Therefore, the $b_{m,n+1}$ will be absent. Because of the $D_{m,z}$ is a zero mean Gaussian random variable. Therefore, the other $2^n - 1$ absolute values of $|D_{m,z}|$ are independent and folded normal distribution [25]. By using their order statistics theory for calculating $P_{r_{ed}}$ as (46) [23].

$$P_{r_{ed}} = 1 - \int_0^{\infty} \left(F_{D_{m,z}}(y)\right)^{2^n-1}\ f_{D_{m,i}}(y)\, dy \tag{46}$$

Where $F_{D_{m,z}}(y)$ and $f_{D_{m,i}}(y)$ are cumulative distribution function (CDF) of the random variable $D_{m,z}$ and PDF of the random variable $D_{m,i}$, can be expressed as, respectively:

$$F_{D_{m,z}}(y) = \mathrm{erf}\left(\frac{y}{\sqrt{2V(D_{m,z})}}\right) \tag{47}$$

$$f_{D_{m,i}}(y) = \frac{1}{\sqrt{2\pi V(D_{m,i})}}\left[e^{-\frac{(y-E(D_{m,i}))^2}{2V(D_{m,i})}} + e^{-\frac{(y+E(D_{m,i}))^2}{2V(D_{m,i})}}\right] \tag{48}$$

Subsequently, $P_{r_{ed}}$ can be rewritten as (49):

$$P_{r_{ed}} = 1 - \frac{1}{\sqrt{2\pi V(D_{m,i})}}\int_0^\infty \left(erf\left(\frac{y}{\sqrt{2V(D_{m,z})}}\right)\right)^{2^n-1}\left[e^{-\frac{(y-E(D_{m,i}))^2}{2V(D_{m,i})}} + e^{-\frac{(y+E(D_{m,i}))^2}{2V(D_{m,i})}}\right] dy \tag{49}$$

By substituting $\gamma_D = \frac{E_b \sum_{\rho=1}^{L} \alpha_\rho{}^2}{N_O}$ and let $2V(D_{m,z}) = W = \frac{2M \log_2 N}{(M+1)}\gamma_D + \beta$. Then, $P_{r_{ed}}$ can express as (50):

$$P_{r_{ed}} = 1 - \frac{1}{\sqrt{\pi W}}\int_0^\infty \left(erf\left(\frac{y}{\sqrt{W}}\right)\right)^{2^n-1}\left[e^{-\frac{(y-\frac{M \log_2 N}{(M+1)}\gamma_D)^2}{W}} + e^{-\frac{(y+\frac{M \log_2 N}{(M+1)}\gamma_D)^2}{W}}\right] dy \tag{50}$$

4.3. The BER of modulating bits

The de-spreading process is executed in the same way as in the conventional DCSK, due to guessing the modulating bit $b_{m,n+1}$, by comparison the decision variable $D_{m,i}$ to the threshold of zero value. Hence, utilizing $E(D_{m,i})$ and $V(D_{m.i})$, subsequently, the P_{rDCSK} can be written as (51):

$$P_{rDCSK} = \frac{1}{2} erfc\left(\frac{E(D_{m,i})}{\sqrt{2V(D_{m.i})}}\right) = \frac{1}{2} erfc\left(\frac{M \log_2 N \gamma_D}{(M+1)\sqrt{W}}\right) \tag{51}$$

The E_b can be supposed as a constant value for a higher value of β. Consequently, for the L path that identically and independently RFC distributed, the PDF of instantaneous γ_D can be described as (52) [24]:

$$f(\gamma_D, \gamma_c, L) = \frac{\gamma_D^{L-1}}{(L-1)!\,\gamma_C^L}\exp\left(-\frac{\gamma_D}{\overline{\gamma_c}}\right) \tag{52}$$

Where $\overline{\gamma_c} = \frac{E_b}{N_O} E(\alpha_\rho{}^2) = \frac{E_b}{N_O} E(\alpha_l{}^2)\ for\ l \neq \rho$

The PDF of γ_D is described as (53):

$$f(\gamma_D) = \sum_{\rho=1}^{L} \frac{\mu_\rho}{\gamma_\rho}\exp\left(-\frac{\gamma_D}{\overline{\gamma_\rho}}\right) \tag{53}$$

Where $\mu_\rho = \prod_{\substack{l=1 \\ l\neq\rho}}^{L} \frac{\overline{\gamma_\rho}}{\overline{\gamma_\rho} - \overline{\gamma_l}}$.

The channel became AWGN if $L = 1$ and $\alpha_1 = 1$. Lastly, the averaged BER of the PIM-OFDM-DCSK scheme over MRFC can express as (54) [18]:

$$\overline{P_{r_M}}_{PIM-OFDM-DCSK} = \int_0^\infty P_{r_M} f_{\gamma_D}(\gamma_D) d\gamma_D \tag{54}$$

5. SIMULATION RESULT AND DISCUSSION

The simulation and analysis of the proposed PIM-OFDM-DCSK system performance are evaluated. For generating the chaotic samples, the CPF is used. Under the AWGN and MRF channels, the performance analysis is carried out. To carry out the performance in MRF channels by using two-ray RFC, these two paths are characterized by average power gain $E(\alpha^2) = 1/3$, $E(\alpha^2) = 2/3$ and the delays $\tau = 0$ and $\tau = 2\,T_c$, for each path, respectively. The parameters of simulations are set as the following, the data rate R for DCSK, PI-DCSK, and proposed PIM-OFDM-DCSK is 1, $(n + 1)$, and $(n + 1) \times M$, respectively. In the proposed PIM-OFDM-DCSK, the value of M is related to the number of FFT size ($NFFT = 128$), $M = N_{FFT} - 1 = 127$ and the guard interval $Ng = 0.25NFFT = 32$.

5.1. Performance evaluation

Figures 3(a) and 3(b), illustrate the performance of BER through the effect of different values of bits per symbol n on the proposed PIM-OFDM-DCSK over AWGN and the MRF channels. These figures observed that, as n increases, the number of bits mapped to a symbol would be increased for the identical sent energy. Therefore the E_b/N_o required to reach a certain BER will be reduced, and the BER performance of PIM-OFDM-DCSK will be enhanced. As indicated in Figure 4 clearly shows that to achieve the same BER of 10^{-3}, for $n = 6$, the E_b/N_0 required level is almost 3 dB lower than E_b/N_o required level for $n = 2$. In other words, as the number of bits per symbol increases, the bits number per transmitted frame increases for constantly sent energy; therefore, the desired E_b/N_o required to accomplish a specific performance of BER is reduced.

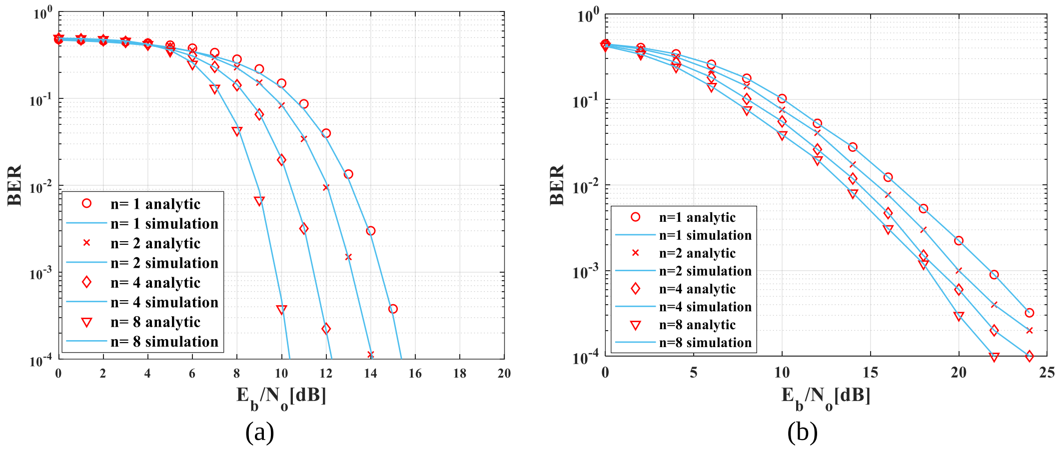

Figure 3. The effect of different bits per symbol n on PIM-OFDM-DCSK performance for $\beta = 200$ over; (a) AWGN and (b) MRFC channels

Figures 4(a) and 4(b), respectively, show the performance of PIM-OFDM-DCSK BER under the effect of β over AWGN and MRF channels. It is clear that when the value of β is increased, the performance of BER reduces. This is because of that the significance of the noise across correlation becomes large for a higher spreading factor, which influences the performance of BER and causes its degradation. Additionally, it can be realized that the performance of BER weakens as the β heightens, in spite of the rise of QO between two different permuted sequences of the CR signal for the high value of β. This is due to the significant noise across correlation becoming larger than the rise of QO between two different permuted sequences of the reference signal.

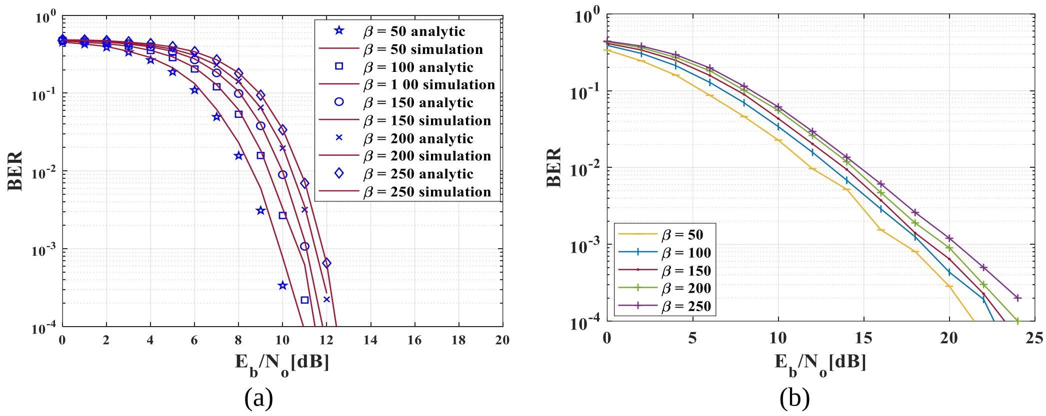

Figure 4. The effect of different spreading factors on PIM-OFDM-DCSK performance for $n = 4$ over; (a) AWGN channel and (b) MRF channel

5.2. Compared with other non-coherent chaotic modulations

Figures 5(a) and 5(b) show the performance of PIM-OFDM-DCSK BER in comparison with DCSK and PI-DCSK is assessed over AWGN and MRF channels. This comparison clearly shows that the BER performance of the proposed PIM-OFDM-DCSK outperforms the other performances of other DCSK systems. For instance, to reach a BER=10^{-3}, the PIM-OFDM-DCSK requires E_b/N_o level at the receiver almost 2,6 dB less than PI-DCSK and DCSK, respectively over an AWGN channel.

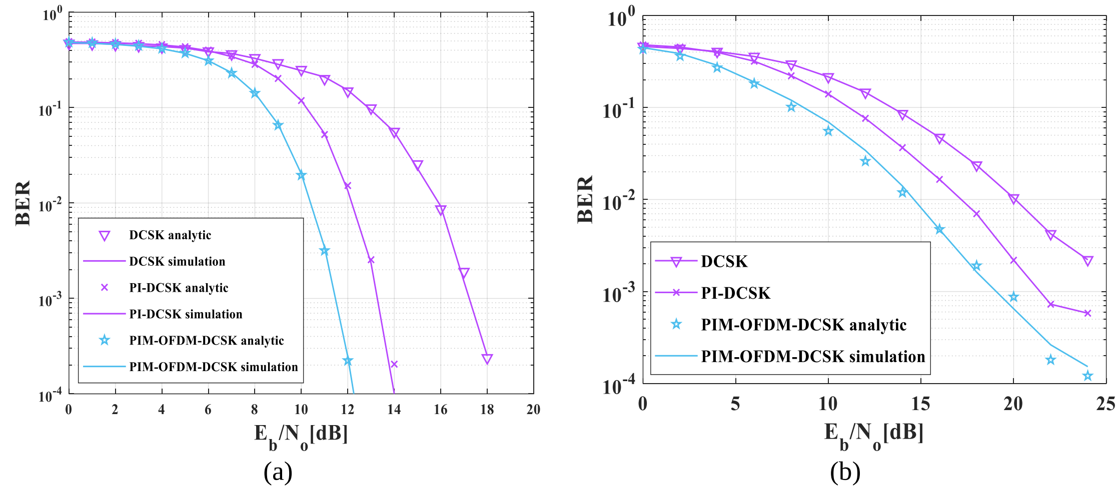

Figure 5. Compare the BER performance of PIM-OFDM-DCSK to PI-DCSK and DCSK for $n = 4$ and $\beta = 200$ in; (a) AWGN channel and (b) MRF channel

It is clear that there is a difference in the performance between the proposed PIM-OFDM-DCSK system and the other recent systems. The reason behind this difference is the transmission of multiple information-bearing signals with the modulating bits using only a single reference signal, leading to a higher data rate and saving in energy. While the DCSK system transmits a bit with a dedicated reference signal for each transmitted bit, PI-DCSK [18] system transmits a symbol with dedicated reference signals for each transmitted symbol. This explains the resulting performance behavior and verifies the proposed scheme's high energy and spectral efficiencies.

5.3. Secrecy performance

In this section, the proposed PIM-OFDM-DCSK scheme's secrecy performance is studied based on a wiretap system model using BER. Figures 6(a) and 6(b) show the comparison of the BER performances of the legitimate receiver (Bob) and eavesdropper (Eve) for the proposed PIM-OFDM-DCSK scheme based on the wiretap system model for AWGN and MRFC channels, respectively. It's clear that the BER performance at the legitimate receiver (Bob) is better compared with the BER performance at the eavesdropper (Eve). The Eve BER is still at 0.5 for any increased signal power to noise power ratio under the secret permutation index key.

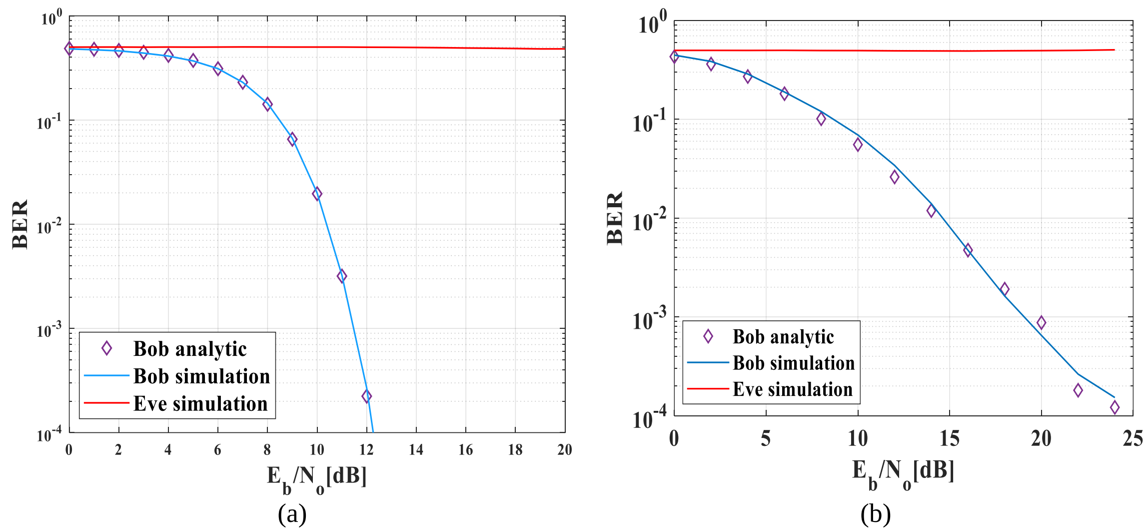

Figure 6. Compare the BER performance of the proposed PIM-OFDM-DCSK for Bob and Eve under secret permutation index key for $n = 4$ and $\beta = 200$; (a) AWGN channel and (b) MRF channel

6. CONCLUSION

In this paper, we focus only on PLS techniques from the information-theoretic perspective by suggesting a new transmission system using a DCSK system that is reliant on the PIM-OFDM to accomplish high data rate, high security of transmission, high physical layer data security and high-reliability performances by random permutation of the CR for each data symbol. The proposed PIM-OFDM-DCSK system modulates M information symbols, where every symbol is consisting of $n + 1$ bits, where n bits are mapped to a unique permutation of reference chaotic signal, then the choice of the permuted sequence is used to spread the single bit named a modulated bit, which is physically sent, each frame that consists of a single reference signal slot, and M slots, for each M slot, the modulated bit is sent after spread by the particular choice permuted chaotic sequence. Then the produced signal is modulated by an OFDM technology, and then the serial sequence will be sent over MRF and AWGN channels. At the receiver, the received sequence pass to OFDM demodulation and then the correlation is done between all 2^n permuted versions of the reference signal, out of possible permutations $(\beta! - 1)$, and the received sequence for each M slot. Then, summated over the symbol duration. Then, the received bits are assessed by determining the maximum of the correlator outputs that sign to the correct index of permutation by which the n bits are transmitted, and then the sign of the maximum output correlator is utilized to detect the modulated bit. Then, the performance of the proposed PIM-OFDM-DCSK is evaluated by computing and simulating the BER over a MRFC and AWGN channel. Moreover, the proposed system BER over AWGN and MRF channels are derived, and then the system's performance is tested under the effect of different parameters, same as the number of bits per symbol n and spreading factor β are analyzed. The test result shows that the best BER performance is as an increase in the value of n and a decrease in the value of β. Additionally, Results demonstrate that the proposed system gives the best BER performance compared with DCSK and PI-DCSK.

REFERENCES

[1] C. E. Shannon, "Communication Theory of Secrecy Systems," *Bell System Technical Journal*, vol. 28, no. 4, pp. 656–715, Oct. 1949, doi: 10.1002/j.1538-7305.1949.tb00928.x.

[2] A. D. Wyner, "The Wire-Tap Channel," *Bell System Technical Journal*, vol. 54, no. 8, pp. 1355–1387, Oct. 1975, doi: 10.1002/j.1538-7305.1975.tb02040.x.

[3] Y.-S. Shiu, S. Chang, H.-C. Wu, S. Huang, and H.-H. Chen, "Physical layer security in wireless networks: a tutorial," *IEEE Wireless Communications*, vol. 18, no. 2, pp. 66–74, Apr. 2011, doi: 10.1109/MWC.2011.5751298.

[4] A. Mukherjee, S. A. A. Fakoorian, J. Huang, and A. L. Swindlehurst, "Principles of Physical Layer Security in Multiuser Wireless Networks: A Survey," *IEEE Communications Surveys & Tutorials*, vol. 16, no. 3, pp. 1550–1573, 2014, doi: 10.1109/SURV.2014.012314.00178.

[5] Y. Liu, H.-H. Chen, and L. Wang, "Physical Layer Security for Next Generation Wireless Networks: Theories, Technologies, and Challenges," *IEEE Communications Surveys & Tutorials*, vol. 19, no. 1, pp. 347–376, 2017, doi: 10.1109/COMST.2016.2598968.

[6] Y. Zou, J. Zhu, X. Wang, and L. Hanzo, "A Survey on Wireless Security: Technical Challenges, Recent Advances, and Future Trends," *Proceedings of the IEEE*, vol. 104, no. 9, pp. 1727–1765, Sep. 2016, doi: 10.1109/JPROC.2016.2558521.

[7] M. Bloch and J. Barros, "Physical-layer security: from information theory to security engineering," in *Cambridge University Press*, 2011.

[8] A. Sanenga, G. Mapunda, T. Jacob, L. Marata, B. Basutli, and J. Chuma, "An Overview of Key Technologies in Physical Layer Security," *Entropy*, vol. 22, no. 11, p. 1261, Nov. 2020, doi: 10.3390/e22111261.

[9] L. Kong, G. Kaddoum, and M. 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)*, IEEE, Oct. 2015, pp. 283–288, doi: 10.1109/WiMOB.2015.7347973.

[10] F. C. M. Lau and C. K. Tse, "Chaos-Based Digital Communication Systems," in *Operating Principles, Analysis Methods and Performance Evaluation, Springer-Verlag,* in Signals and Communication Technology. , Berlin, Heidelberg: Springer Berlin Heidelberg, 2003, doi: 10.1007/978-3-662-05183-2.

[11] H. Dedieu, M. P. Kennedy, and M. 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*, vol. 40, no. 10, pp. 634–642, 1993, doi: 10.1109/82.246164.

[12] G. Kaddoum, F.-D. Richardson, and F. Gagnon, "Design and Analysis of a Multi-Carrier Differential Chaos Shift Keying Communication System," *IEEE Transactions on Communications*, vol. 61, no. 8, pp. 3281–3291, Aug. 2013, doi: 10.1109/TCOMM.2013.071013.130225.

[13] G. Kolumbán, B. Vizvári, W. Schwarz, and A. Abel, "Differential chaos shift keying: a robust coding for chaos communication," *Proc. NDES*, vol. 96, pp. 87–92, 1996.

[14] 14. W. Xu, L. Wang, and G. Kolumbán, "A novel differential chaos shift keying modulation scheme," *International Journal of Bifurcation and Chaos*, vol. 21, no. 03, pp. 799–814, Mar. 2011, doi: 10.1142/S0218127411028829.

[15] G. Kaddoum, F. Gagnon, and F.-D. Richardson, "Design of a secure Multi-Carrier DCSK system," in *2012 International Symposium on Wireless Communication Systems (ISWCS)*, IEEE, Aug. 2012, pp. 964–968, doi: 10.1109/ISWCS.2012.6328511.

[16] F. C. M. Lau, K. Y. Cheong, and C. K. Tse, "Permutation-based DCSK and multiple-access DCSK systems," *IEEE Transactions on Circuits and Systems I: Fundamental Theory and Applications*, vol. 50, no. 6, pp. 733–742, Jun. 2003, doi: 10.1109/TCSI.2003.812616.

[17] F. S. Hasan, "Design and Analysis of an OFDM-Based Short Reference Quadrature Chaos Shift Keying Communication System," *Wireless Personal Communications*, vol. 96, no. 2, pp. 2205–2222, Sep. 2017, doi: 10.1007/s11277-017-4293-1.

[18] M. Herceg, G. Kaddoum, D. Vranjes, and E. Soujeri, "Permutation Index DCSK Modulation Technique for Secure Multiuser High-Data-Rate Communication Systems," *IEEE Transactions on Vehicular Technology*, vol. 67, no. 4, pp. 2997–3011, Apr. 2018, doi: 10.1109/TVT.2017.2774108.

[19] F. S. Hasan and A. A. Valenzuela, "Design and Analysis of an OFDM-Based Orthogonal Chaotic Vector Shift Keying Communication System," *IEEE Access*, vol. 6, pp. 46322–46333, 2018, doi: 10.1109/ACCESS.2018.2862862.
[20] N. Al Bassam and O. Al-Jerew, "A new scheme to enhance the performance of permutation index–differential chaos shift keying communications system," *EURASIP Journal on Wireless Communications and Networking*, no. 1, pp. 1–18, Dec. 2021, doi: 10.1186/s13638-021-02060-9.
[21] G. Kaddoum, P. Chargé, D. Roviras, and D. Fournier-Prunaret, "A Methodology for Bit Error Rate Prediction in Chaos-based Communication Systems," *Circuits, Systems and Signal Processing*, vol. 28, no. 6, pp. 925–944, Dec. 2009, doi: 10.1007/s00034-009-9124-5.
[22] M. Sushchik, L. S. Tsimring, and A. R. Volkovskii, "Performance analysis of correlation-based communication schemes utilizing chaos," *IEEE Transactions on Circuits and Systems I: Fundamental Theory and Applications*, vol. 47, no. 12, pp. 1684–1691, 2000, doi: 10.1109/81.899920.
[23] G. Kaddoum, Y. Nijsure, and H. Tran, "Generalized Code Index Modulation Technique for High-Data-Rate Communication Systems," *IEEE Transactions on Vehicular Technology*, vol. 65, no. 9, pp. 7000–7009, Sep. 2016, doi: 10.1109/TVT.2015.2498040.
[24] J. G. Proakis, "Digital communications systems," in *McGraw-Hill*, New York, 2001.
[25] A. Papoulis, "Probability, Random Variables, and Stochastic Processes," in *McGraw-Hill*, 1991.

BIOGRAPHIES OF AUTHORS

Dhuha Hussein Hameed was born in Baghdad, Iraq in 1993. She received her B.Sc. degree in Electrical Engineering in 2015 and her M.Sc. degree in Electronics and Communication Engineering in 2018, both from the Mustansiriyah University, Iraq. She is currently pursuing an Ph.D. in Communication Engineering at the Department of Electrical Engineering, Al-Mustansiriyah University. Her research interests include wireless communication, spread spectrum, physical layer security, OFDM based DCSK, and chaotic theory. She can be contacted at email: eeph006@uomustansiriyah.edu.iq.

Fadhil S. Hasan was born in Baghdad, Iraq in 1978. He received his B.Sc. degree in Electrical Engineering in 2000 and his M.Sc. degree in Electronics and Communication Engineering in 2003, both from the Mustansiriyah University, Iraq. He received Ph.D. degree in 2013 in Electronics and Communication Engineering from the Basrah University, Iraq. In 2005, he joined the Faculty of Engineering at the Mustansiriyah University in Baghdad. His recent research activities are wireless communication systems, multicarrier system, wavelet based OFDM, MIMO system, speech and image signal processing, chaotic cryptography, chaotic modulation, FPGA, and xilinx system generator-based communication system. Now he has been an assist. prof. at the Mustansiriyah University, Iraq. He can be contacted at email: fadel_sahib@uomustansiriyah.edu.iq.