Modeling and Analysis of Chaos-based Spread Spectrum Scheme using Irregular LDPC Code and Non-Coherent 16-DCSK under Fading and Jamming

Wei Wei
Electrical Engineering and Computer Science Department
College of Engineering, University of Toledo
Toledo, Ohio, U.S.A.

Junghwan Kim
Electrical Engineering and Computer Science Department
College of Engineering, University of Toledo
Toledo, Ohio, U.S.A.

Abstract—**In chaos-based spread spectrum systems, the use of spreading code and chaotic binary sequence expands the bandwidth of the information-bearing signal but this expansion results in SNR degradation under the constraint of constant channel capacity according to Hartley-Shannon law. To compensate for this drawback, our proposed model employs an irregular low-density parity-check (LDPC) code with its iterative decoding algorithm. Coupled with this forward error correction (FEC) coding, we used non-coherent (NC) 16-ary differential chaos shift keying (16-DCSK) that additionally provides the ability of data encryption due to its use of chaotic signals compared with the conventional modulation schemes. Analytical expressions of bit error probability (BEP) are derived under the assumption of the three-ray model along with partial band noise jamming (PBNJ) over a Rayleigh fading channel. Simulation results assert that the proposed system can mitigate the effect of PBNJ via lowering BEP by coding gain and processing gain under identical transmission power. It is also confirmed that a higher level of security can be provided by the use of proposed two iteration functions of Duffing Map-based chaotic binary sequence than the security level of one iteration function of Logistic Map, based on the balance and autocorrelation analysis.**

Keywords-BEP; chaos-based spread spectrum; chaotic binary sequence; irregular LDPC code; non-coherent 16-DCSK; PBNJ

I. INTRODUCTION

A typical chaos-based spread spectrum system utilizes chaotic binary sequences [1] as candidate spreading code to camouflage the information-bearing signal by expanding its bandwidth. This spreading code includes a state of chaotic properties of unpredictability, regularity and topology transition from its iterative chaotic map [2]. Due to these properties and the operation of the iterative chaotic map, one long sequence length of the spreading code is easy to generate with a less number of periodic repetitions along with wideband characterization. Additionally, it is proven to be more effective to reduce the peak-to-average power ratio (PAPR) than Gold code or other independent and identically distributed sequences (IID) [3]. In addition, the chaotic binary sequence is easy to generate to any sequence length without the limitation of sequence generator. As a result, the chaotic waveform-based spread spectrum system can transmit concealable information-bearing signal with properties of the counteraction of fading effects and jamming. To minimize channel effects, the idea of using a chaos-based spread spectrum scheme has been considered for decades. For example, [4] showed the simple circuitry of one chaos-based asynchronous direct-sequence code-division multiple access (DS-CDMA) that can reduce multiple-access interference over non-selective channels and improve 60% of error probability (or BEP performance) by transmission of un-correlated rectangular pulses along with mapping into $\{-1, +1\}$ to the matched filter type receiver. On the other hand, the synchronization-based DS-CDMA [5] was also utilized according to coherent chaos-shift keying (CSK). This modulation scheme can generate an exact replica of the transmission signal at the receiver from the transmitter without any depraved data. However, both systems have difficulty to estimate the bandwidth of chaotic binary sequence due to its sequence generator. Also, the chaotic binary sequence leads to a loss of chaotic signal properties and decreases the security of the chaos-based spread spectrum. Finally, the co-operation between the real value sequence and chaotic binary sequence must take into account the hardware implementation problem.

In order to optimize BEP performance and security of our proposed system, irregular LDPC code employing iterative decoding which provide outstanding BEP performance [6] can be utilized. Moreover, a simple circuitry [7] asynchronous and spectral efficiency [8] 16-DCSK is used as carrier along with the properties of the unpredictability, regularity and topology transition. Last but not least, Duffing Map-based chaotic binary sequence is utilized for data encryption. The contribution of this work can be summarized as follows:

- The analytical BEP expressions of the proposed scheme over additive white Gaussian noise (AWGN), three-ray model of Rayleigh fading and PBNJ are derived and analyzed.
- It is proven that the proposed spreading code using two iterative functions of Duffing Map can encrypt data with higher security than data encrypted by the code from the single iterative function of Logistic Map, based on the balance and autocorrelation analysis.

Corresponding author: Wei Wei (wei.wei@rockets.utoledo.edu)

- The results of BEP demonstrate that the coding gain and processing gain of the proposed scheme can effectively mitigate the effect of PBNJ.

II. PROPOSED CHAOS-BASED SPREAD SPECTRUM SCHEME

Figure 1 shows the block diagram of the proposed chaos-based spread spectrum scheme. In the transmitter, the input data are encoded by an irregular LDPC encoder and modulated by the non-coherent 16-DCSK modulator. Then, the candidate spreading code, Duffing Map-based chaotic binary sequence is used to hide the input data against Rayleigh fading and/or PBNJ to the receiver. Rayleigh fading channel is modeled as a three-ray model for a practical communication system. Under PBNJ, a part of the total spreading bandwidth can be affected and its effect will be further compared with the case of AWGN. In the receiver, this wideband signal is recovered to the original bandwidth again by Duffing Map-based chaotic binary sequence. Then, it is demodulated and decoded by a non-coherent 16-DCSK demodulator and irregular LDPC code decoder as the final output data. By using the Duffing Map-based chaotic binary sequence, the proposed spread spectrum system provides a higher level of data encryption due to the use of two iterative functions instead of one. As a result, users are not easy to identify chaotic binary sequence of two iterative functions which is compared with a chaotic binary sequence of a single iterative function.

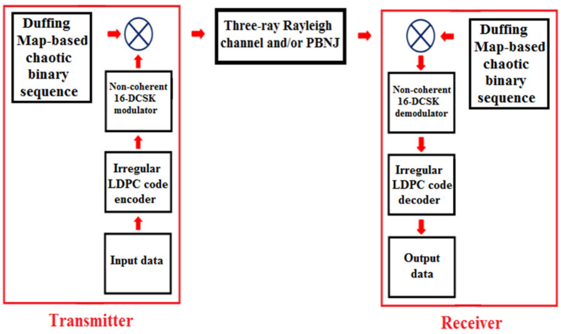
Duffing Map-based chaotic binary sequence
Non-coherent 16-DCSK modulator
Irregular LDPC code encoder
Input data
Three-ray Rayleigh channel and/or PBNJ
Duffing Map-based chaotic binary sequence
Non-coherent 16-DCSK demodulator
Irregular LDPC code decoder
Output data
Transmitter
Receiver

Fig. 1. Proposed chaos-based spread spectrum scheme

III. DUFFING MAP-BASED CHAOTIC BINARY SEQUENCE

In Figure 1, the input data are in digital format and the real-valued sequence of Duffing Map is often generated directly from an iterative chaotic map without digital format. As a result, the Duffing Map-based chaotic binary sequence of the proposed system should be converted to a digital signal. Accordingly, the Duffing Map [9] depicted in Figure 2 is intended to use two iterative functions $x(n)$ and $y(n)$ in this work and (1) denotes the relationship. It should be noted here that $x(0)$ and $y(0)$ are equal to 0.5. Figure 3 shows the waveform as the final output $y(n+1)$ in one period of 127s for simplicity.

$$x(n+1) = y(n)$$

$$y(n+1) = [-0.2 \times x(n)] + [2.75 \times y(n)] + [-y^3(n)] \quad (1)$$

To produce the typical chaotic behavior of Duffing Map, four values of the gain factor of Figure 2 are set as -1, 2.75, 1, and -0.2. In path 1, the triple of $y(n)$ passes through the block of gain factor -1. In path 2, $y(n)$ goes through the block of gain factor 2.75. In path 3, $y(n)$ passes through the gain factor 1 and is equal to $x(n+1)$. Then it generates $x(n)$ due to memory 1. Moreover it is input to the block of gain factor -0.2. Finally, the final output $y(n+1)$ is derived from the addition of these three paths. It is manifest that the final output $y(n+1)$ of the real-valued sequence of Duffing Map is not a digital signal yet in Figure 3. Hence, this work utilizes instantaneous sampling, quantization (two-level uniform quantizer of mid-riser type), and binary encoding to yield the proposed spreading code. Note that the decision threshold of the quantizer is set to be 0.5. If the real-valued of Duffing Map is larger than 0.5, the output is assigned to level +1. Otherwise, the output will be level -1. Finally yet importantly, level +1 and level -1 are denoted as bit 1 and 0 for the digital format of the proposed spreading code in Figure 4.

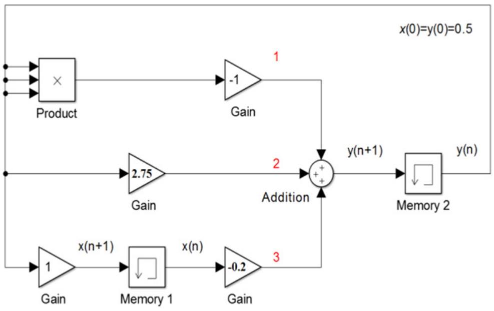

Fig. 2. Proposed model of Duffing Map

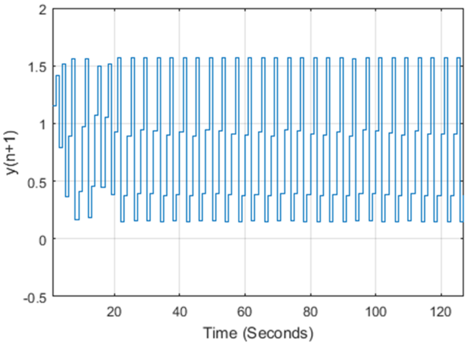

Fig. 3. Final output $y(n+1)$ of the real-valued sequence of Duffing Map

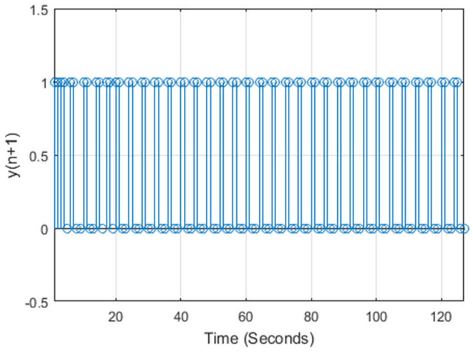

Fig. 4. Output waveform of Duffing Map-based chaotic binary sequence

IV. NON-COHERENT 16-DCSK

The most significant advantage of the non-coherent 16-DCSK which utilizes the chaotic sequence, is the generation of the chaotic signal with unpredictability, regularity, and topology transition for stronger data encryption according to its modem structures. Figure 5 presents the modulator of the non-coherent 16-DCSK. In the first time slot $(1 \leq k \leq \beta)$, one signal stemmed from the chaotic generator, the generator of chaotic signal, is split into two identical signals: One is X_k, the reference signal, which is directly transmitted to the considered channel. The same reference signal, X_k, is used to generate the β time-delayed one. In the second time slot $(\beta < k \leq 2\beta)$, the delayed reference signal X_k is modulated further by phase and amplitude of binary data sequence S as the information-bearing signal $X_{k-\beta}\left(S_x cos\theta + S_y sin\theta\right)$ for 16-ary signal schemes.

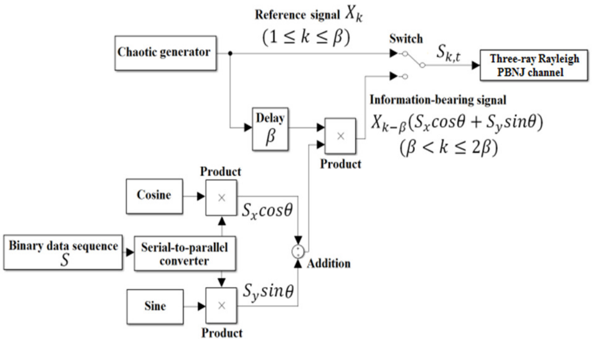

Fig. 5. Modulator of non-coherent 16-DCSK

Usually, the smaller value of β is taken for the proposed non-coherent 16-DCSK scheme to yield better BEP performance because the shorter time delay between the reference signal and the information-bearing signal can decrease the time to be affected by the adverse effect from the channel. Hence, the design of β is 1. At the demodulator, in the first time slot, the received reference signal X_k is split into two identical signals as shown in Figure 6(a). One is the input of β time delayed circuit for producing the delayed version of the received reference signal. Subsequently, in the second time slot, the received information-bearing signal $X_{k-\beta}(S_x cos\theta + S_y sin\theta)$ (or A of Figure 6(b)) is split into two identical signals. The upper path of the received information-bearing signal $X_{k-\beta}(S_x cos\theta + S_y sin\theta)$ (or A of Figure 6(b)) is then correlated with the β time-delayed reference signal $X_{k-\beta}$ (or B of Figure 6(b)). Being further demodulated with cosine and sine terms of the output of the correlator, the final output is obtained. Finally, the correlator is symbol-to-symbol operated so that the value of β is discrete under the summation. On the other hand, the value of β is continuous while doing time-delay operation. Based on Figures 5 and 6, the waveform of the non-coherent 16-DCSK can be generated from the modulator to the demodulator. For symbol mapping and symbol transmission, we use the two circular-ring based non-coherent 16-DCSK as shown in Figure 7. Note that each symbol is assigned to one specific region by a dotted circle and lines as their decision regions. According to the thresholds of decision regions, the BEP of the proposed modulation scheme can be evaluated.

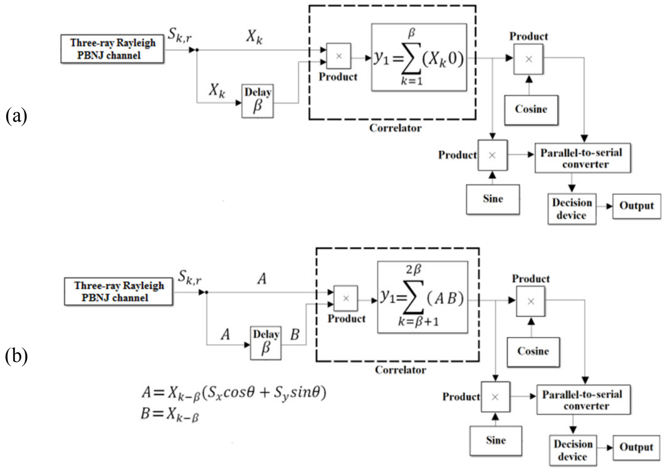
(a)
Three-ray Rayleigh PBNJ channel
$S_{k,r}$
X_k
X_k
Delay β
Product
$y_1 = \sum_{k=1}^{\beta} (X_k 0)$
Correlator
Product
Cosine
Product
Parallel-to-serial converter
Sine
Decision device
Output
(b)
Three-ray Rayleigh PBNJ channel
$S_{k,r}$
A
A
Delay β
B
Product
$y_1 = \sum_{k=\beta+1}^{2\beta} (AB)$
Correlator
Product
Cosine
Product
Parallel-to-serial converter
Sine
Decision device
Output
$A = X_{k-\beta}(S_x cos\theta + S_y sin\theta)$
$B = X_{k-\beta}$

Fig. 6. Demodulator of non-coherent 16-DCSK at two different time slots (a) in the 1st time slot $(1 \leq k \leq \beta)$ and (b) in the 2nd time slot $(\beta < k \leq 2\beta)$

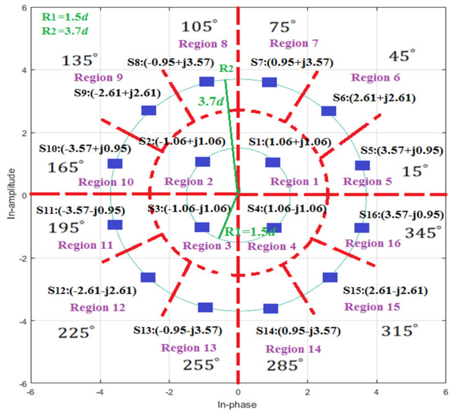

Fig. 7. Proposed signal constellation of non-coherent 16-DCSK

As a result, the first step of BEP evaluation of non-coherent 16-DCSK is to define all Euclidean distances between two successive symbols as a factor of d, hence, radii R_1 and R_2 are $1.5d$ and $3.7d$ respectively. As a result, all Euclidean distances of non-coherent 16-DCSK can be defined as (2). For example, $d_{1,2}$ denotes the Euclidean distance between symbol S_1 and symbol S_2.

$$d_{1,2} = d_{2,3} = d_{3,4} = d_{4,1} = 2.12d;$$

$$d_{1,6} = d_{2,9} = d_{3,12} = d_{4,15} = 2.2d;$$

$$d_{1,7} = d_{1,5} = d_{4,14} = d_{2,10} = d_{2,8} = d_{3,13} = d_{3,11}$$

$$= d_{4,16} = 2.51d;$$

$$d_{5,6} = d_{6,7} = d_{7,8} = d_{8,9} = d_{9,10} = d_{10,11} = d_{11,12} = d_{12,13} = d_{13,14} = d_{14,15} = d_{15,16} = d_{16,5} = 1.91d \quad (2)$$

By using the union bound of M-ary modulation [10], its symbol error probability (SEP) P_s can be shown in (3):

$$P_s = \frac{1}{M}\sum_{w=1}^{M}\sum_{j\neq 1; j\neq w}^{M} P\left(S_w \rightarrow S_j\right); M = 16 \quad (3)$$

where $P(S_w \rightarrow S_j)$ is the pairwise symbol error probability which means that symbol S_w is erroneously detected as symbol

S_j . Note that $P(S_w \rightarrow S_j)$ can be expressed using the complementary error function in (4), where $d_{w,j}$ is the Euclidean distance between symbol S_w and symbol S_j and it can be selected from (2).

$$P\left(S_w \rightarrow S_j\right) = 0.5erfc\left(\frac{d_{w,j}}{\sqrt{\frac{4N_0}{E_S}+\frac{2\beta N_0^2}{E_S^2}}}\right) \qquad (4)$$

In (4), β and N_0/E_s are time-delay unit and the ratio of noise power spectral density to the energy-per-symbol respectively, and N_0 is the two-side Gaussian noise power spectral density. Furthermore, the relationship [11] between the average symbol energy E_s and the Euclidean distance $d_{w,j}$ can be shown as $(1/M)\,[(N_1 \times R_1^2) + (N_2 \times R_2^2)]$ with $N_1 = 4, N_2 = 12$ and $M = 16$ according to Figure 7. N_1 is the number of symbols in the inner ring and N_2 is the number of symbols in the outer ring. Hence, E_s is equal to $10.83d^2$. By using (3), the overall symbol error probability of symbol S_1 can be calculated as:

$$S_1\!: P(S_1 \rightarrow S_2) + P(S_1 \rightarrow S_4) + P(S_1 \rightarrow S_5) + P(S_1 \rightarrow S_6) + P(S_1 \rightarrow S_7) \qquad (5)$$

Likewise, all other symbol error probabilities of the remainder symbols can be derived by (2), (3) and (4) according to Figure 7. Finally, the overall average SEP P_s is:

$$P_s = \frac{1}{16}(S_1 + S_2 + S_3 + S_4 + S_5 + S_6 + S_7 + S_8 + S_9 + S_{10} + S_{11} + S_{12} + S_{13} + S_{14} + S_{15} + S_{16}) \qquad (6)$$

In addition, assuming all symbol errors are equally probable, the relationship between SEP P_s and BEP $P_{b,16-DCSK}$ is given by (7), where $M = 2^k = 16$ and $k = 4$ is the number of bits per symbol of non-coherent 16-DCSK. Note that (7) is analyzed under AWGN and E_b/N_0 is the ratio of the energy-per-bit to noise power spectral density with $\beta = 1$. Figure 8 is the BEP evaluation of the proposed non-coherent 16-DCSK over AWGN according to (7).

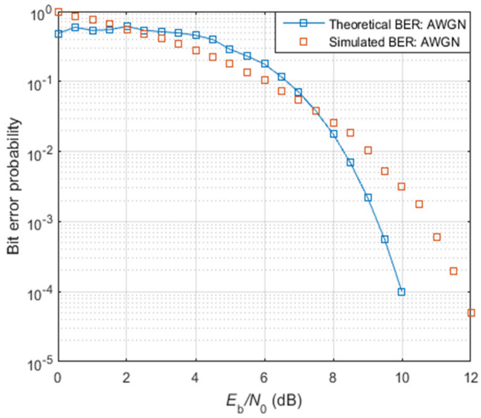

Fig. 8. BEP performances of the proposed non-coherent 16-DCSK over AWGN

We can see that the proposed system needs about 10-12dB to achieve a BEP of 10^{-4}. Furthermore, the difference between the simulated and theoretical curves of BEP is about 2dB in the high E_b/N_0 region under channel conditions due to the inter-symbol interference (ISI) [12].

$$P_{b,16-DCSK} = \left(\frac{\frac{M}{2}}{M-1}\right)P_s = \frac{8}{15}\{\frac{1}{16}[8erfc(\frac{E_b}{N_0}\frac{0.760\sqrt{E_b}}{\sqrt{\frac{4E_b}{N_0}+2\beta}}) + 4erfc(\frac{E_b}{N_0}\frac{0.642\sqrt{E_b}}{\sqrt{\frac{4E_b}{N_0}+2\beta}}) + 4erfc(\frac{E_b}{N_0}\frac{0.666\sqrt{E_b}}{\sqrt{\frac{4E_b}{N_0}+2\beta}}) + 12erfc(\frac{E_b}{N_0}\frac{0.578\sqrt{E_b}}{\sqrt{\frac{4E_b}{N_0}+2\beta}})]\} \qquad (7)$$

In contrast, to evaluate the practical communication systems under Rayleigh fading, we use a widely accepted three-ray multi-path fading model depicted in Figure 9. Based on [13], the corresponding PDF of the Rayleigh distribution of a three-ray model is written in (8), with notations of independent signal paths r_1,r_2, and r_3 along with the respective standard deviation σ_1, σ_2,and σ_3. Note that the average power of each signal path is in terms of $2\sigma^2$ [14]:

$$f(r_1, r_2, r_3) = \frac{r_1 r_2 r_3}{\sigma_1^2\sigma_2^2\sigma_3^2}e^{-\left(\frac{r_1^2 r_2^2 r_3^2}{8\sigma_1^2\sigma_2^2\sigma_3^2}\right)}; r_1, r_2, r_3 > 0 \qquad (8)$$

In general, the received signal at the receiver can be considered as the sum of multipath propagation, hence, the reflected ray of r_1 , r_2 and r_3 can be represented as: $\rho_1\cos(\omega t - \varphi_1)$, $\rho_2\cos(\omega t - \varphi_2)$ and $\rho_3\cos(\omega t - \varphi_3)$ where ρ_1 , ρ_2 ρ_3 and φ_1 ,φ_2 , φ_3 are the respective amplitudes and phases. According to Lambert's cosine law [15], the range of ρ_1 , ρ_2 , ρ_3 is between 0 and 1. When the reflected angle approaches 0°, ρ_1, ρ_2, ρ_3 approach 1. As a result, ρ_1 , ρ_2, ρ_3 of the reflected ray r_1, r_2, r_3 can be selected as 0.33, 0.66 and 0.85. Finally, φ_1 , φ_2 , φ_3 are related to the effect of delay spread [16], which usually has an extremely small value, thus φ_1, φ_2, φ_3 can be assumed to be 0° for simplicity.

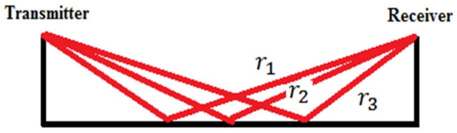

Fig. 9. Proposed of three-ray model

Finally, the BEP [17] of the un-coded non-coherent 16-DCSK using three-ray fading model is given in (9). Note that $P_{b,16-DCSK}$ should be in terms of r with $\beta = 1$. Figure 10 shows the BEP analysis of the proposed non-coherent 16-DCSK over the three-ray model by calculation of (9).

$$P_{b,16-DCSK,Three-ray\ model} = \int_0^\infty [(P_{b,16-DCSK})] \times [Eq.(8)]dr \quad (9)$$

If a BEP of 10^{-4} is desirable, note that the required power of the proposed system is only 5.5-7dB, which is about 5dB less than that in AWGN (see Figure 8), due to the fact that a constructive received signal is expected because the central-limit theorem [18] is applied to the deployed model.

In case of Partial Band Noise Jamming (PBNJ), the bandwidth of PBNJ, W_{PBNJ}, is the fraction of total spreading bandwidth W, hence, its fractional ratio ρ can be defined as W_{PBNJ}/W. If we consider the three-ray model under the effect of PBNJ for our proposed non-coherent 16-DCSK, the uncoded BEP equation (10) is derived. Note that $P_{b,16-DCSK}$ is in terms of r and ρ simultaneously with β=1. Figure 11 shows the BEP analysis of the proposed non-coherent 16-DCSK over the three-ray model along with PBNJ ($\rho = 0.4$) by (10). With additional PBNJ ($\rho = 0.4$), both simulated and theoretical BEP are commonly degraded due to the effect of non-uniform AWGN noise:

$$P_{b,16-DCSK,Three-ray\ model,PBNJ} = \int_0^\infty [(P_{b,16-DCSK})] \times [Eq.(8)]dr \quad (10)$$

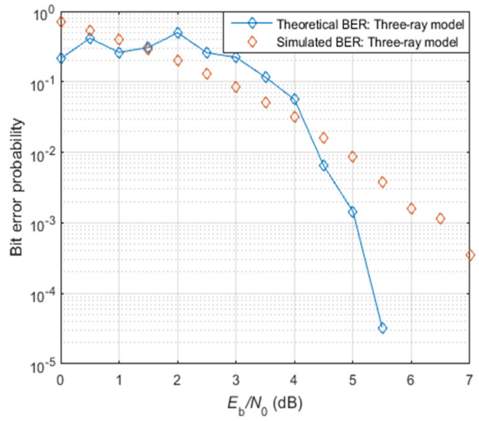

Fig. 10. BEP performances of the proposed non-coherent 16-DCSK over a three-ray model

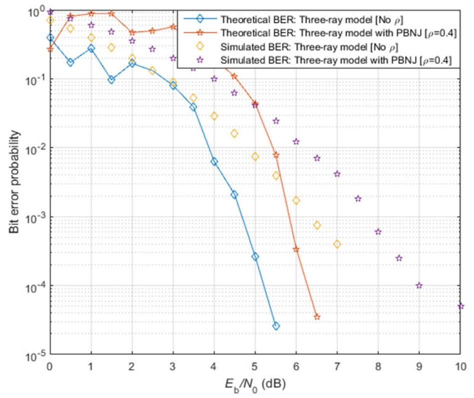

Fig. 11. BEP performance of the proposed non-coherent 16-DCSK over a three-ray model together with PBNJ ($\rho = 0.4$)

In summary, due to the design of $\beta = 1$, all simulation results of Figures 8, 10, and 11 show better power efficiency than those of [12]. For example, the single ring of non-coherent 16-DCSK needs at least 22dB to achieve a BEP of 10^{-4} at β of 60. In contrast, in our case, the two rings of non-coherent 16-DCSK, only require less than or equal to 12dB at β of 1. There are two main reasons: (a) The Euclidean distances of the two rings in circular signal constellation can be larger than that of one ring circular constellation, hence it is easier to correctly identify the symbol, (b) the smaller value of β yields better BEP performance because the shorter time delay between the reference signal and the information-bearing signal might decrease the time duration of channel effect at the demodulator. Note that the simulated BEP is obtained by using Monte Carlo simulation [19] and the processing gain is 1 while considering PBNJ ($\rho = 0.4$) for Figure 11.

V. IRREGULAR LDPC CODE

Due to the use of spreading code employing the Duffing Map-based chaotic binary sequence, the broadband signal usually suffers from the SNR degradation in the chaos-based spread spectrum system under constant channel capacity according to Hartley-Shannon law. To overcome this shortcoming, the use of an irregular LDPC code was proposed [20] to maintain the desirable SNR by coding gain. The advantages of irregular LDPC code can be summarized as: (a) it is suitable for parallel implementation, (b) it is more amenable to high coding rate, (c) has lower error floor, and (d) has superior error correcting capability. In this paper, the proposed irregular LDPC code is one kind of linear block code (LBC) in which each code-word U is equal to the product of the transmitted message m and the generator matrix G in the encoder as:

$$U = [m_1 m_2 m_3 \dots m_k] \begin{bmatrix} g_{1,1} & \cdots & g_{1,n} \\ \vdots & \ddots & \vdots \\ g_{k,1} & \cdots & g_{k,n} \end{bmatrix} = m \cdot G \quad (11)$$

The generator matrix G of the systematic is usually a $k \times n$ matrix (n is larger than k) as:

$$G = \begin{bmatrix} p_{1,1} & \cdots & p_{1,n-k} & 1 & \cdots & 0 \\ \vdots & \ddots & \vdots & \vdots & \ddots & \vdots \\ p_{k,1} & \cdots & p_{k,n-k} & 0 & \cdots & 1 \end{bmatrix} = [P_{k\times(n-k)}|I_{k\times k}]_{k\times n} \quad (12)$$

By (12), the parity check matrix H can be shown as

$$H = [I_{(n-k)\times(n-k)}|P^T_{k\times(n-k)}]$$
$$= [I_{(n-k)\times(n-k)}|P_{(n-k)\times k}]_{(n-k)\times n} \quad (13)$$

As a result, we can get the parity check matrix $H_{(n-k)\times n}$ as the decoder of the irregular LDPC code. This decoder can decode each bit simultaneously, differently from the widely used Meggitt decoder [21] of conventional decoding. Note that n and k are 12 and 6 respectively. As an irregular LDPC code, in which columns and rows have different numbers of "1" independently.

$$H_{(n-k)\times n} = \begin{bmatrix} 1&0&0&0&1&0&0&0&1&0&0&0 \\ 0&1&0&1&0&1&0&1&0&1&0&1 \\ 1&0&1&0&1&0&1&0&1&0&1&0 \\ 0&1&0&1&0&1&0&1&0&1&0&1 \\ 1&0&1&0&1&0&1&0&1&0&1&0 \\ 0&1&0&1&0&1&0&1&0&1&0&1 \end{bmatrix}_{6\times12} \quad (14)$$

The parity check matrix $H_{6\times12}$ has six rows and twelve columns so we have six parity check nodes for error correction and twelve information bit nodes for storage information (or code-word U) in the decoder of the irregular LDPC code. It should be noticed that the parity check node connects with the information bit node by the number of "1"s. Otherwise, they do not connect with each other by the number of "0"s. To decode the message m by (14), each information bit node transmits each code-word U to all adjacent parity check nodes for equally decoding. Next, each parity check node transmits the decoded code-word U back to all adjacent information bit nodes equally.

Finally, the previous two steps are repeated to construct each iterative decoding until having the perfect received message m. Mathematically, this received message m can be expressed by the log-likelihood ratio (LLR) assuming AWGN by (15). $P(y|m)$ is the conditional pdf of the received signal, y, conditioned on the transmitted message m (bit 1 or bit 0). If $L(y)$ is larger than the decision threshold of LLR calculation, the received message m is decoded as bit 1. Otherwise, bit 0 is assumed. Note that $q = 2$ is the number of iterations and it means that each code-word U completes two round trips between information bit nodes and parity check nodes for decoding.

$$L(y)_{coded\ 16-DCSK,AWGN} = \sum_{i=0}^{q} (log \frac{P(y|m=1)}{P(y|m=0)})_i. \quad (15)$$

The coded BEP of the proposed scheme under the effects of three-ray model and PBNJ is expressed in (16). $L(y)_{coded\ 16-DCSK,AWGN}$ is also represented in terms of r and ρ at the same time. Note that the processing gain is 1.

$$P_{b,coded\ 16-DCSK,Three-ray\ model,PBNJ} = \int_0^\infty [L(y)_{coded\ 16-DCSK,AWGN}] \times [Eq.(8)]\, dr \quad (16)$$

Accordingly, the theoretical BEP of the proposed irregular LDPC coded non-coherent 16-DCSK over the three-ray model along with PBNJ ($\rho = 0.4$) is illustrated in Figure 12 and is calculated by (16).

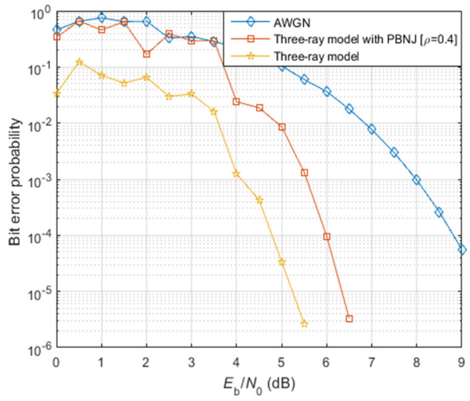

Fig. 12. Theoretical BEP performance of the proposed irregular LDPC coded non-coherent 16-DCSK over AWGN and three-ray model with and without PBNJ ($\rho = 0.4$).

The theoretical BEP curves show that the proposed system requires 6dB to achieve a BEP of 10^{-4} when the three-ray model is used over PBNJ ($\rho = 0.4$). It is obvious that the proposed system is BEP degraded under the effect of PBNJ. Moreover, due to the lack of constructive received power, the proposed system requires 3dB more power to achieve the identical BEP requirement over AWGN. Because of the design of $\beta = 1$, all theoretical BEP curves show better power efficiency than [19]. The system in [19] needs large transmission power to approach the expected BEP requirement due to its larger β. This causes an LDPC code of longer length that results in decoding complexity using iterative circuitry to compensate the effect of larger β for power efficiency. Our proposed model can reserve the transmission power by simple iterative circuitry with smaller β due to the use of shorter code-word length. Finally, this paper does not show the simulated BEP curve for the irregular LDPC coded cases because the irregular LDPC code has higher difficulty in circuit design, from which it is found that the irregular LDPC code still has a large room for optimization (as future work). However, the theoretical BEP is often referred to as the upper bound performance [12].

VI. Computer Simulations

A. The Effect of Coding Gain

In most three-ray models, the transmitted signals may be scattered by surrounding objects that can lead to fading and this can cause both constructive and destructive interference which may affect the BEP performance and waste transmission power. Hence, the coding gain of a coded system is often used to denote the effective reduction of power requirement when it is compared with the un-coded system at the same BEP. Theoretical BEP curves show that the un-coded system needs about 0.5dB more power than the coded while approaching the BEP of 10^{-4} under PBNJ (Figure 13). In other words, the effect of fading has been considerably minimized with the aid of irregular LDPC code. Note that the processing gain is set to be 1 in order to show the effect of coding gain in this case.

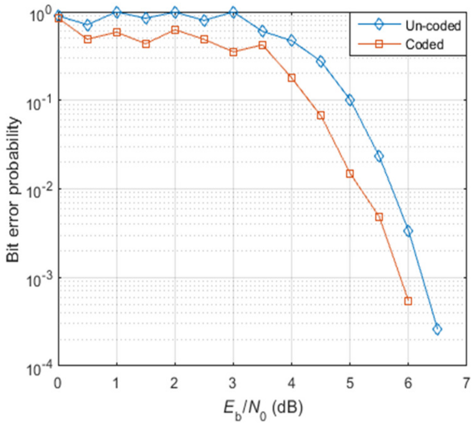

Fig. 13. Theoretical BEP performance of the coded and un-coded system in three-ray model together with PBNJ ($\rho = 0.4$)

B. The Effect of PBNJ

Partial spreading bandwidth is affected by AWGN in PBNJ, hence, the ratio of the bandwidth of PBNJ to the whole spreading bandwidth is not independent on the BEP performance. Figure 14 shows the comparison of theoretical BEPs of irregular LDPC coded non-coherent 16-DCSK over the three-ray model under different ρ. When ρ is decreased, the BEP of the proposed system is degraded due to the non-uniform AWGN effect. Furthermore, BEP curves may be overlapped at $\rho = 0.2$ and $\rho = 0.4$ in lower E_b/N_0 because of the effect of reduced transmission power at the receiver. This increases the difficulty for correct data detection. Note that the processing gain is 1 in order to show the effect of PBNJ in this case.

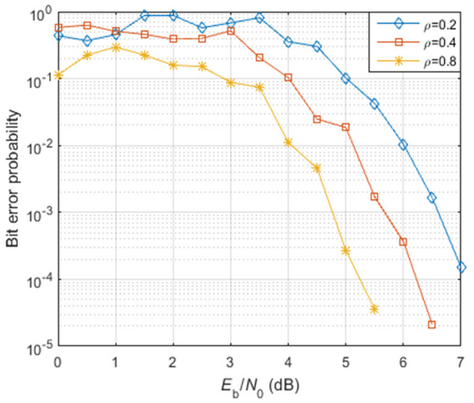

Fig. 14. Theoretical BEPsperformance of the irregular LDPC coded non-coherent 16-DCSK in three-ray model along with PBNJ ($\rho = 0.2; 0.4; 0.8$)

C. The Effect of Processing Gain (PG)

In section VI-A and VI-B, we did not considered different PGs for the BEP performances of our proposed system. Normally, the most important factor of chaos-based spread spectrum system is processing gain (PG) that is used to denote a suppression ratio of an interfering signal. To analyze the theoretical BEP performance, let PG be 1 and 5. When the proposed system lacks the spreading effect i.e. when PG = 1, the system is weak to resist the interfering signal and it results in BEP degradation. In contrast, larger PG increases higher correct signal detection via lower BEP with stronger resistance interfering signal. For example, the proposed system needs 6dB to achieve the BEP of 10^{-4} without the effect of PG but it can save 2dB under the effect of PG (Figure 15).

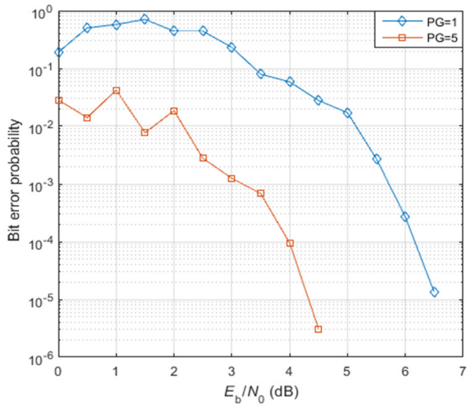

Fig. 15. Theoretical BEP performance of the irregular LDPC coded non-coherent 16-DCSK over three-ray model along with PBNJ ($\rho = 0.4$) under different PGs

D. Chaotic Binary Sequence Generated by Duffing Map and Logistic Map Comparison

To see which chaotic map provides higher level of data encryption, two iteration functions of Duffing Map-based chaotic binary sequence are compared with the sequence generated by the one iteration function of Logistic Map [22].

1) Balance Analysis

For a typical random binary data sequence, the number of 1s should be roughly the same as the number 0s in each period. Hence, we define that our proposed chaotic binary sequence and Logistic Map has 127 bits in one period for comparison. The value of 127 is one of the popular sequence periods in spread spectrum modulations. Both maps are processed by the same process of section III to get the digital format of spreading sequence along with the initial value of 0.5. As a result, Figure 16 shows the sequences from Logistic Map and Duffing Map with identical length of 127 bits.

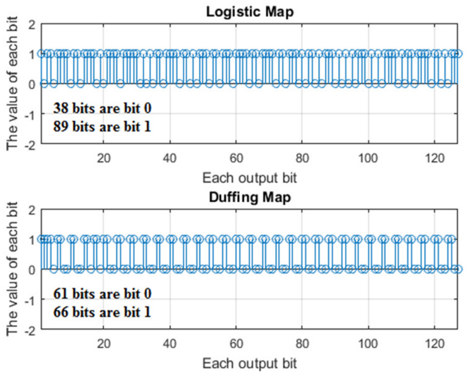

Fig. 16. Balance analysis of Logistic Map and Duffing Map

It can be seen that the numbers of bit 1 and bit 0 in the chaotic binary sequence by Duffing Map tend to be well balanced, and the balance is better than that generated by Logistic Map. In summary, our proposed chaotic binary sequence is easier to approach a truly random binary data sequence than that of Logistic Map for high level of data security.

2) Autocorrelation Analysis

The purpose of autocorrelation analysis is to identify the period of spreading code in spread spectrum modulations. We assume that both maps have a period of 127 [sec] with the waveform of Figure 16, while 127s is the time delay between two chaotic binary sequences. In Figure 17, the period identification of Duffing Map is more difficult than of Logistic Map because, around its period at 127s, there are multiple comparable values of autocorrelation in a noise-like form.

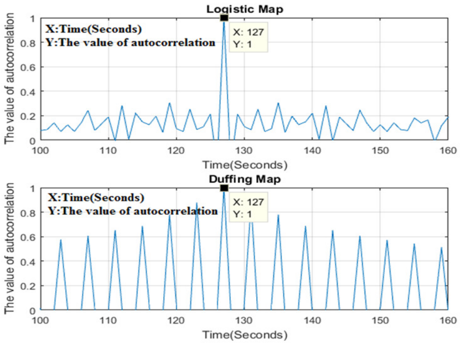

Fig. 17. Autocorrelation analysis of Logistic Map and Duffing Map

Hence, by using Duffing Map-based chaotic binary sequence, it is possible to enhance the required level of transmission security since it gets more difficult for the unauthorized user to identify the sequence period from autocorrelation analysis.

VII. Conclusion

This paper presents a chaotic spreading sequence-based 16-DCSK scheme in which the level of transmission security can be greatly enhanced by simply using efficient Duffing Map. Additional coding gain from the LDPC code with iterative decoding applied to the proposed scheme can easily compensate the loss of effective power due to bandwidth expansion from spreading sequence as well as the adverse effect of multipath Rayleigh fading. The effect of PBNJ is also evaluated with the fading effect on the BEP performance of the proposed scheme. It is found that, the coding and processing gain obtained from the use of spreading sequence can collectively compensate the degradation of BEP under the assumption of constant transmission power.

References

[1] A. Chengquan, Z. Tingxian, "Design of chaotic spread-spectrum sequences with good correlation properties for DS/CDMA", International Symposium on Circuits and Systems, Bangkok, Thailand, May 25-28, 2003

[2] A. Elsharkawi, R. M. El-Sagheer, H. Akah, H. Taha, "A novel image stream cipher based on dynamic substitution", Engineering, Technology & Applied Science Research, Vol. 6, No. 5, pp. 1195-1199, 2016

[3] G. Mazzini, G. Setti, R. Rovatti, "Chaotic complex spreading sequences for asynchronous DS-CDMA-part I: system modeling and results", IEEE Transactions on Circuits Systems I: Fundamental Theory and Applications, Vol. 44, No. 10, pp. 937-947, 1997

[4] G. Mazzini, R. Rovatti, G. Setti, "Chaos-based asynchronous DS-CDMA systems and enhanced Rake receivers: measuring the improvements", IEEE Transactions on Circuits and Systems-I: Fundamental Theory and Applications, Vol. 48, No. 12, pp. 1445-1453, 2001

[5] G. Kaddoum, "Wireless chaos-based communication systems: a comprehensive survey", IEEE Access, Vol. 4, pp. 2621-2648, 2016

[6] S. Y. Chung, G. D. Forney Jr, T. J. Richardson, R. Urbanke, "On the design of low-density parity-check codes within 0.0045 dB of the Shannon limit", IEEE Communications Letters, Vol. 5, No. 2, pp. 58-60, 2001

[7] G. Kaddoum, J. Olivain, G. B. Samson, P. Giard, F. Gagnon, "Implementation of a differential chaos shift keying communication system in GNU radio", International Symposium on Wireless Communication Systems, Paris, France, August 28-31, 2012

[8] S. Wang, X. Wang, "M-DCSK-based chaotic communications in MIMO multipath channels with no channel state information", IEEE Transactions on Circuits and Systems-II: Express Briefs, Vol. 57, No. 12, pp. 1001-1005, 2010

[9] M. M. Hasan, T. M. Faruqi, M. Tazrean, T. H. Chowdhury, "Biometric encryption using Duffing map", 4th International Conference on Advances in Electrical Engineering, Dhaka, Bangladesh, September 28-30, 2017

[10] W. Sung, S. Kang, P. Kim, D. I. Chang, D. J. Shin, "Performance analysis of APSK modulation for DVB-S2 transmission over nonlinear channels", International Journal of Satellite Communications, Vol. 27, pp. 295-311, 2009

[11] S. Lin, D. Costello, Error control coding, Pearson-Prentice Hall, 2004

[12] L. Wang, G. Cai, G. Chen, "Design and performance analysis of a new multiresolution M-ary differential chaos shift keying communication system", IEEE Transactions on Wireless Communications, Vol. 14, No. 9, pp. 5197-5208, 2015

[13] A. Elsanousi, S. Ozturk,"Performance analysis of OFDM and OFDM-MIMO systems under fading channels", Engineering, Technology & Applied Science Research, Vol. 8, No. 4, pp. 3249-3254, 2018

[14] D. P. Agrawal, Q. A. Zeng, Introduction to wireless and mobile systems. Cengage Learning, 2016

[15] F. L. Pedrotti, L. M. Pedrotti, L. S. Pedrotti, Introduction to optics, Cambridge University Press, 2017

[16] S. Buzzi, L. Venturino, A. Zappone, "Multipath delay acquisition in asynchronous doubly-selective DS/CDMA fading channels", IEEE Communications Letters, Vol. 14, No. 4, pp. 276-278, 2010

[17] Y. Xia, C. K. Tse, F. C. M. Lau, "Performance of differential chaos-shift-keying digital communication systems over a multipath fading channel with delay spread", IEEE Transactions on Circuits and Systems-II: Express Briefs, Vol. 51, No. 12, pp.680-684, 2004

[18] H. Taub, D. L. Schilling, Principles of communication systems, McGraw-Hill, 1971

[19] J. Zhan, L. Wang, M. Katz, G. Chen, "A differential chaotic bit-interleaved coded modulation system over multipath Rayleigh channels", IEEE Transactions on Communications, Vol. 65, No. 12, pp. 5257-5265, 2017

[20] L. Jordanova, L. Laskov, D. Dobrev, "Influence of BCH and LDPC code parameters on the BER characteristic of satellite DVB channels", Engineering, Technology & Applied Science Research, Vol. 4, No. 1, pp. 591-595, 2014

[21] J. Meggitt, "Error correcting codes and their implementation for data transmission systems", IRE Transactions on Information Theory, Vol. 7, No. 4, pp. 234-244,1961

[22] W. Wei, J. Kim, "Modeling and analysis of the anti-jamming (AJ) spread spectrum system using quantized chaotic sequence with LDPC for reliable data link", VII International Conference on Network, Communication and Computing, Taipei, Taiwan, December 14-16, 2018