Enhancement of Differential Chaos Shift Keying Communication System Based on LDPC Codes

Mahmood F. Mosleh[1], Fadhil S. Hasan [2], Aya H. Abdulhameed[3]
{ drmahfa@yahoo.com[1], fadel_sahib@uomustansiriyah.edu.iq [2], ayaaloosy@gmail.com [3]}

Department of Computer Engineering Techniques, Middle Technical University
Baghdad, Iraq.[1,3],
Department of Electrical Engineering, Al Mustansiriyah University
Baghdad, Iraq.[2]

Abstract. LDPC code is a preferred channel code used in modern communication because of its robustness to mitigate the huge noise. In this paper, LDPC with four decoder types is combined with Differential Chaos Shift Keying (DCSK) communication system under AWGN channel. The system is simulated using MATLAB program version 2019a with various amounts of half spreading factor, $\beta \in \{8, 16, \text{and } 32\}$. The results show that a coding gain is achieved in a range of (1.3 – 4.6) dB between the coded and uncoded DCSK system. Also, log domain decoder is the best decoder among all types, while hard decision bit flipping decoder appears the worst case in contrast with its simplicity.

Keywords: Differential chaos shift keying **(**DCSK), LDPC codes, Bit-Flipping, Log Domain, Prop Domain, Min-Sum, Iterative receiver.

1 Introduction

Chaos signal is spread along wideband which is suitable for spread-spectrum communication [1]. It is considered aperiodic with random features for a long time duration and considered unpredictable. Also, it has an advantage of that spectrum in case of inter-user interference, secure communication, multipath mitigation and got the immunity against anti-jamming [2]. A chaos signals can be employed for digital communication such as Chaos Shift Keying (CSK) and Differential Chaos Shift Keying (DCSK) [1] which has spatial advantages like non-coherent detection, no threshold-shift problem, less sensitive to channel distortion, and does not ask for any Channel State Information (CSI) [3] etc. Two methods of chaos modulation namely coherent and non-coherent. However, synchronization is an important issue for the first one of modulation at the receiver end, taking into account that it can be generated a large number of chaos signals easily due to changing the initial condition [4].

On the other hand, the non-coherent scheme like DCSK modulation represents a suitable solution to address the synchronization problem. Also, the Channel State Information (CSI) is not required with such a scheme [5]. In DCSK modulation two-time slots are used in the transmitted sequence, one for the reference sequence and the other for carrying information sequence. At the receiver, the information is detected by correlating the information and reference sequence. However, due to the large length of non-periodic chaos signal, DCSK is suffering from non-constant energy per bit which leads to data losses. To address this problem, an advanced technique was proposed by applying frequency modulation (FM) modulation to the chaotic sequence in DCSK system and named FM-DCSK [6].

IMDC-SDSP 2020, June 28-30, Cyberspace

DOI 10.4108/eai.28-6-2020.2297915

Recently, due to higher mobility and huge interference of the communication system, a large number of errors are accusing which reduces device accuracy. To improve the performance, Foreword Error Correction (FEC) is employed to detect and correct an error without feedback. One of the most important types of FEC is Low-Density Parity Check (LDPC). It is a kind of binary linear block code with a sparse parity check matrix included fewer ones, simple algorithms of decoding algorithms as well as low-complexity decoder designs [7]. LDPC codes are one of the famous communication art adopted by satellite broadcasting, Ethernet system, conduct to use in wireless LAN system, especially (IEEE 802.3an), and latest 5G of wireless communication [8]. Many types of research are concerned with a digital communication system included LDPC code and DCSK, like [6] where FM-DCSK system is proposed enhanced by LDPC codes. In [9] the authors utilized chaotic Walsh transform codes combined integrated with LDPC code and a convolutional code. Thus, the code group is supported by MIMO wireless communication system. Also, in [10] a design of alternative receivers based on M- Array DCSK is presented.

In this paper, a communication system is constructed by using DCSK modulator to show its performance. It is expected that such a system needs more Signal to Noise Ratio (SNR) to match new communication systems that need low power consumption. To address this problem LDPC code will be added to the system in order to improve such performance. Various types of decoders like Bit Flipping (BF), Log Domain, Prob Domain and min-sum are investigated and compared their performance in terms of BER and complexity.

2 DCSK

The generating of the chaotic sequence becomes simpler by using one of the most common polynomial maps as chaotic logistic maps [11]. The logistic map Chebyshev polynomial function (CPF) of order 2 will be used to generate the chaotic signal by using (1).

$$x_{k+1} = 1 - 2x_k^2 . \tag{1}$$

where x is a variable with range $(-1 \leq x \leq 1)$. This logistic map is well suited for chaotic communication [2].

In modulation, the carrier signal of DCSK is represented by the chaotic sequences, with differential shift keying modulator. Every single transmitted bit, the duration is divided into two equal time slots or segments. The reference segment related to the chaotic sequence x_k has been represented by the first slot period and data segment in the second. For transmitted bit '1', the reference segment x_k must be as equal as the Segment. In contrast, the data segment will be equal to the negative value of the reference segment x_k with a bit of '0' [12]. So, the output sequence S_k in the transmitter for *l*-the transmitted bit is given by:

$$S_k = \begin{cases} x_k & for\ k = 2(l-1)\beta + 1, \ldots, (2l-1)\beta \\ b_l\, x_{k-\beta} & for\ k = (2l-1)\beta + 1, \ldots, 2l\beta \end{cases} \tag{2}$$

where β is half spreading factor, x_k and therefore 2β represent spreading factor, i.e., number of chaotic sequences needed for transmitting information bit. Figures 1 and 2 are representing the block diagram regarding binary DCSK modulation and demodulation respectively. DCSK

demodulation uses simple Autocorrelation Receiver (AcR) which does not ask for any Channel State Information (CSI). The reference segments of the received sequence $r_k, k = 2(l-1)\beta + 1, \ldots., (2l-1)\beta, (2l-1)\beta + 1, \ldots.,2l\beta,$ has been correlated with corresponding data segments. Output related to correlator over the first-bit duration might be provided as:

$$y_l = \sum_{k=(2l-1)\beta+1}^{2\beta l} r_k \; r_{k-\beta} \tag{3}$$

As a result, the final output value b_l' will be decided by the threshold detector, which its value set to zero and check if y_l is greater or less than zero [13].

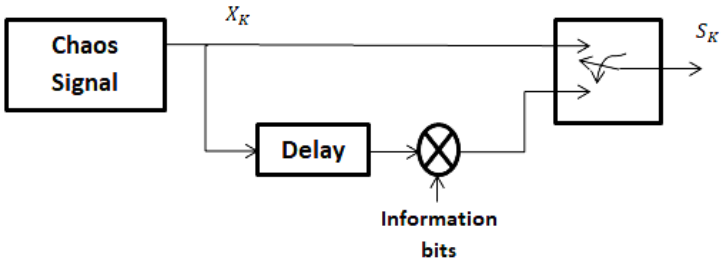

Fig. 1. Block doigram of DCSK modulation.

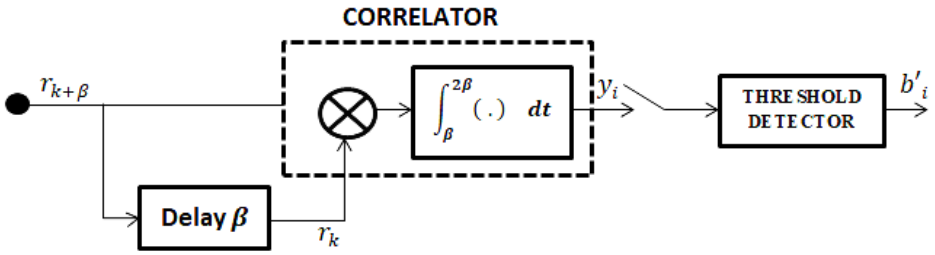

Fig. 2. Block diagram of DCSK demodulation.

3 LDPC

LDPC codes are defined by $M \times N$ binary matrix which is referred to as parity check matrix (H), in which M represents the number of rows defining parity check length constraint for code, and N represents the number of columns that is equal to the code length. Information length K is $K = M - N$ for full-rank matrices. With regards to H matrix, the number of nonzero entries in all columns and rows is collectively referred to as the degree distribution. It is regular in the case when distribution degree related to columns and rows are uniform, or else it will be defined as irregular. The regular parity-check matrix with 8-bit code length is represented by:

$$H = \begin{matrix} v_1 v_2 \cdots \cdots \cdots v_i \\ \begin{bmatrix} 0\,1\,0\,1\,1\,0\,0\,1 \\ 1\,1\,1\,0\,0\,1\,0\,0 \\ 0\,0\,1\,0\,0\,1\,1\,1 \\ 1\,0\,0\,1\,1\,0\,1\,0 \end{bmatrix} \end{matrix} \begin{matrix} c_1 \\ c_2 \\ \vdots \\ c_j \end{matrix}$$,where i = 1, 2, 3 …N and j = 1, 2, 3 ...M

Another representation of H matrix can be shown as Tanner graph consists of check node and variable nodes sets which are corresponding to each row and column of H matrix respectively as shown in Figure 3 [14].

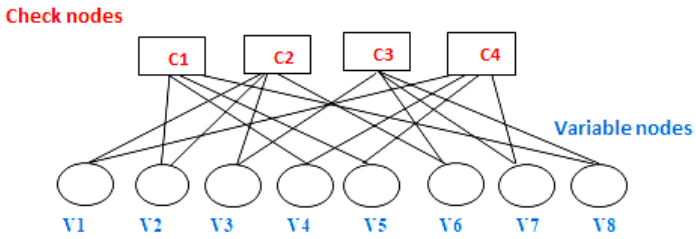

Fig. 3. LDPC codes graphical representation.

3.1 Encoder

Encoder utilizes the generator matrix for encoding information bits for producing code-word. Parity check matrix and generator are considered to be inter-related. With regards to the standard form, the parity check matrix will be provided as follows:

$$H = [A|I_{n-k}]. \tag{4}$$

and the generator matrix is:

$$G = [I_k|A^T] \tag{5}$$

A codeword C will be generated as follows:

$$C = UG. \tag{6}$$

In which U represent block related to the information bits and G represent the generator matrix. Valid codeword should be verified as follows:

$$HC^T = 0. \tag{7}$$

where $(.)^T$ represents the transpose matrix. In the case when the result in (7) is non-zero, then C will be invalid, also the error correction procedure will be utilized in such condition [15].

3.2 Decoder

The decoder of parity check is iterative included two main categories, hard decision and soft decision. The first one is simply applied but suffers from high error in a multipath

environment. One of the most important types of hard diction is Bit Flipping algorithm. The soft decision part is subdivided into many other types which will be explained in the following.

Bit Flipping Algorithm (BFA). It is sometimes called a message-passing technique. The idea is to send the information of any bit from i^{th} variable node to j^{th} check node through *H* matrix. A parity check procedure is applied on any received bit from the variable node and then reply a message included primary information about the bit value (8). It sends the message back to the respective variable nodes with a suggestion of the expected bit value for the parity check to be satisfied. BFA check node operation:

$$\mathrm{C}_j = \mathrm{V}_1 \oplus V_2 \oplus \ldots\ldots \oplus V_i \qquad \forall \mathrm{i} \neq \mathrm{j}. \tag{8}$$

where i, j = 1,2,….degree of check node
Such operation will be repeated till the parity check is achieved or the maximum number of iterations will be reached [16]. BFA variable node operation:

$$V_n = \begin{cases} 0 & if, majority(C_k) = 0 \\ 1 & if, majority(C_k) = 1. \\ V_n & otherwise, \end{cases} \tag{9}$$

where, n = 1,2,….number of variable nodes
k = 1,2,….degree of variable node

Sum-Product Algorithm (SPA). SPA is a soft decision message-passing algorithm where the input of each received bit is represented by the probability of prior information received from the channel. Depending on the message structure between variable nodes and check nodes, SPA algorithm can be classified into: Probability Domain, Log Domain and Min-Sum SPA. The details parameters of these types will be described in Table 1.

Table 1. Described of parameters.

Parameters	Descriptions
y_i	The received data with AWGN.
σ	The noise variance.
$p_i^0 \; and \; p_i^1$	The probabilities of the codeword from the AWGN channel.
$r_{i,j}$	The gathering of all incoming messages from variable nodes to each check node.
$q_{i,j}$	Gathering of information from check nodes to corresponding variable node.
Q_i	Represent the values for each decoder output bit.

*Prob Domain***.** This algorithm applies real probability values in iterative preparation regarding the messages between check nodes and variable nodes. Its process has described by the following steps.

Step 1: Messages from the variable nodes for checking nodes indicated as $q_{i,j}$ will be initialized to probability ($p_i^0 \; and \; p_i^1$) values with the use of (10) and (11). This is achieved once for the decoding of each received codeword.

$$q_{i,j}^0 = 1 - p_i^1 = \; p_i^0 = \frac{1}{1 + e^{-2y_i/\sigma^2}} \tag{10}$$

$$q_{i,j}^1 = p_i^1 = \; p_i^0 = \frac{1}{1 + e^{2y_i/\sigma^2}} \tag{11}$$

Step 2: Messages from the check nodes to variable nodes will be determined (variable node process).

$$r_{j,i}^0 = \frac{1}{2}\left[1 + \prod_{i' \in row[j]/\{i\}} (q_{i,j}^0 - q_{i,j}^1)\right] \tag{12}$$

$$r_{j,i}^1 = \frac{1}{2}\left[1 - \prod_{i' \in row[j]/\{i\}} (q_{i,j}^0 - q_{i,j}^1)\right] \tag{13}$$

where $i' \in row[j]/\{i\}$ indicates indices i' ($1 \leq i \; \leq n$) regarding all bits in j ($1 \leq j \leq m$) that have value one.

Step 3: Messages from the bit nodes for checking nodes will be determined (check node process).

$$q_{j,i}^0 = \alpha_{i,j} \, p_i^0 \prod_{j^i \in col[i]/\{j\}} r_{j,i}^0 \tag{14}$$

$$q_{j,i}^1 = \alpha_{i,j} \, p_i^1 \prod_{j^i \in col[i]/\{j\}} r_{j,i}^1 \tag{15}$$

Step 4: Extrinsic probabilities of decoder output bits are calculated and the hard decision is made according to Q_i value.

$$Q_i^0 = \alpha_i \prod_{j^i \in col[i]} r_{j,i}^0 \tag{16}$$

$$Q_i^1 = \alpha_i \prod_{j^i \in col[i]} r_{j,i}^1 \tag{17}$$

$$\widehat{c_i} = \begin{cases} 1 & if\ Q_i^1 > 0.5 \\ 0 & Otherwice \end{cases}$$

Step 5: Syndrome check.

$$\widehat{c_i} \times H^T = \hat{S} \tag{18}$$

If $\hat{S}$ is a zero vector this indicates received code word will be correctly decoded. Or else, the decoding will continue through repeating the algorithm starting from Step 2 until it arrived at the maximum number of iterations [17].

*Log Domain***.** This algorithm is similar to the probability domain in its calculation except using log-likelihood ratios (LLR) instead of real probability. Thus, instead of $q_{i,j}$ values $L(q_{i,j})$ values are used which are calculated as $\triangleq\ log\frac{q_{i,j}^0}{q_{i,j}^1}$. As same as $r_{i,j}$ values replaced with $L(r_{i,j}) \triangleq log\frac{r_{i,j}^0}{r_{i,j}^1}$. Its process has described by the following steps.

Step 1: Messages from the variable nodes for checking nodes indicated as $L(q_{i,j})$ will be initialized to LLR $L(p_i)$ values with the use of (10) and (11). This is achieved once for the decoding of each received codeword.

$$L(p_i) = log\frac{p_i^0}{p_i^1} = \frac{2}{\sigma^2}y_i \tag{19}$$

$$L(p_i) = L(q_{i,j}) \tag{20}$$

Step 2: Messages from the check nodes to variable nodes will be estimated as LLR (variable node process).

$$L(r_{j,i}) = 2.tan^{-1}\left(\prod_{i' \in \frac{row[j]}{\{i\}}} \tanh\left(\frac{L(q_{i',j})}{2}\right)\right) \tag{21}$$

Where $i' \in \frac{row[j]}{\{i\}}$ indicates indices i' $(1 \le i' \le n)$ of all bits in j $(1 \le j \le m)$ that have value one.

Step 3: Messages from bit nodes for checking nodes will be estimated as LLR (check node process).

$$L(q_{i,j}) = L(p_i) + \sum_{j' \in col[i]/\{j\}} L(r_{j,i}) \tag{22}$$

Step 4: Extrinsic LLR values regarding decoder output bits are estimated and the hard diction is made according to Q_i value.

$$L(Q_I) = L(p_i) + \sum_{j' \in col[i]/\{j\}} L(r_{j,i}) \tag{23}$$

$$\widehat{c_i} = \begin{cases} 1 & if\ Q_i^1 > 0.5 \\ 0 & Otherwice \end{cases}$$

Step 5: Syndrome check.

$$\widehat{c_i} \times H^T = \hat{S} \tag{24}$$

If $\hat{S}$ is a zero vector this indicates received codeword is correctly decoded. Or else, decoding will continue through algorithm starting from Step 2 until it arrived at the maximum number of iterations [18].

SPA in Min-Sum. It is the most simplified decoding algorithms. To reduce the computational complexity in (21) of Log Domain step.2 it will modify as followed:

$$L(r_{j,i}) = \prod_{i' \in \frac{row[j]}{\{i\}}} \text{sign}\left(L(q_{i',j})\right) \min(|L(q_{i',j})|) \tag{25}$$

However, comparing to SPA decoder, the Min-Sum decoder achieves higher BER. Thus, there is a trade-off between performance and complexity in terms of different LDPC decoding [19].

4 System model

In this paper, a communication system that included DCSK combine with LDPC is simulated using Matlab version 2019a, as shown in Figure 4.

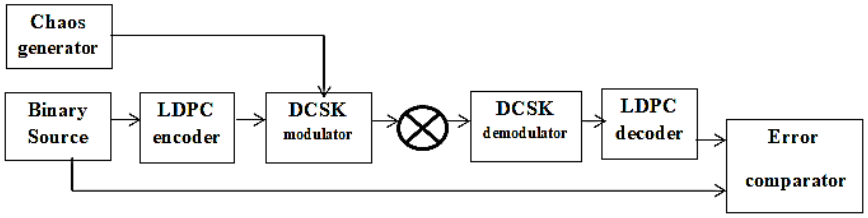

Fig. 4. The block diagram of system module.

Firstly, the binary bits generated by the source are encoded by LDPC code which is to be transmitted with a length of 100 bits per frame. The produced code-word will be 200 bits/frame because of coder rate is set to $1/2$. The DCSK modulates each bit using the chaotic sequence which is generated by the logistic map as a carrier. The number of the chaotic samples that send

for every bit is called as separating factor which will be used in this module as 2β. The channel will be adding noise depending on the environment of the communication system. In this research, it has been considered as the Additive White Gaussian Noise (AWGN) channel with zero mean and power spectral density equals $N_0/2$. The received signal r_k will be represented by:

$$r_k = S_k + n_k \tag{26}$$

where S_k is transmitted signal and n_k is AWGN channel.
The most important parameter of the system module is listed in Table 2.

Table 2. The parameter of the system module.

System parameters	Value
Decoded methods of LDPC	Bit Flipping, Log Domain, Prob Domain and Min-Sum product
Channel	AWGN with $N_0/2$
Modulation	DCSK
Number of bit per Column (Wc)	3
Number of iteration	6
Block length(No. of bit in frame)	100
Number of information bit	504
Chip tare (beta)	8, 16, 32

The simulation model can be represented by the flow chart of Figure 5.

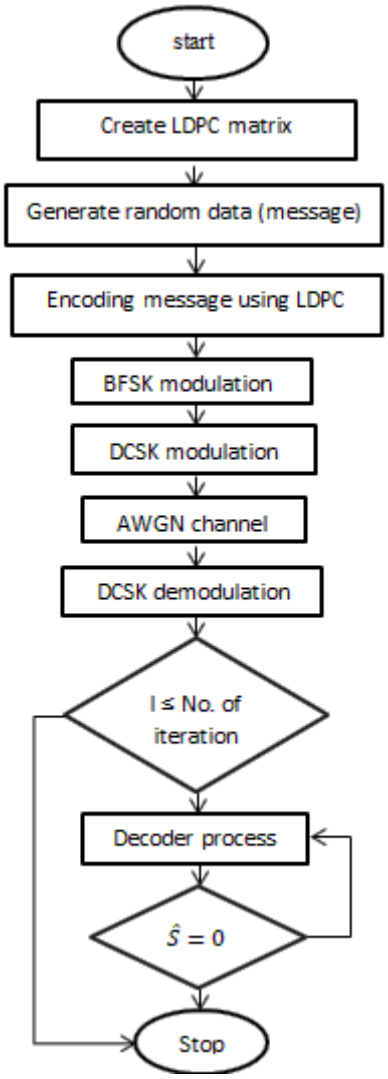

Fig. 5. The simulation flow chart of the model.

5 Results

The simulation is utilized using Matlab version 2019a. In order to show the enhancement of adding LDPC to the system model. The results is given in term of Bit Error Rate (BER) as a function of SNR. In this paper, four LDPC decoding algorithms are used to investigate with DCSK system and compared under AWGN channel. Figures 6, 7, 8 and 9 illustrate the decoding performance of BF, Prob Domain, Log Domain and Min-Sum respectively while all results are summarized in Table 3.

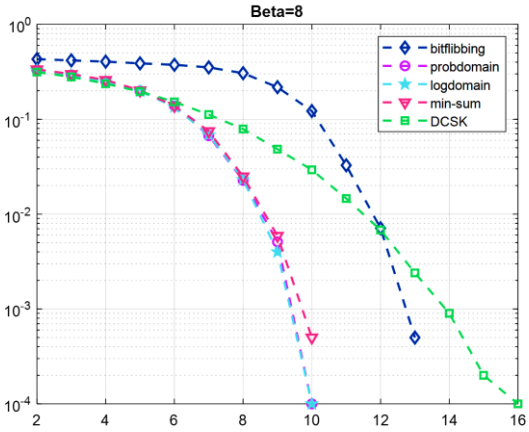

Fig. 6. Performance comparison, with β=8.

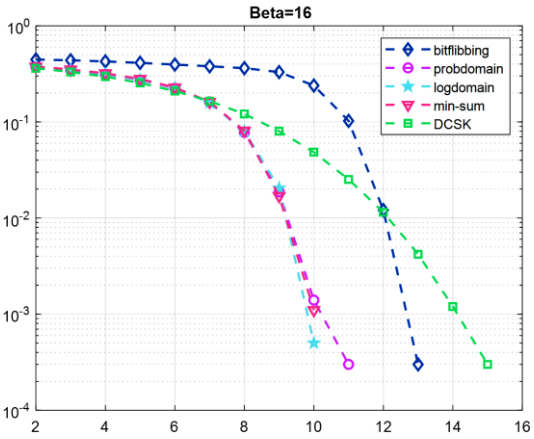

Fig. 7. Performance comparison, with β=16.

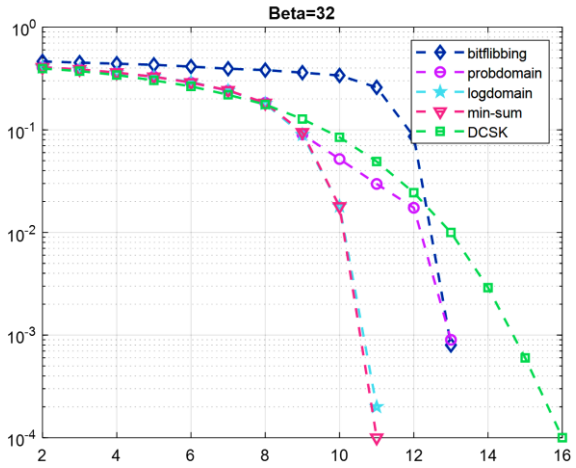

Fig. 8. Performance comparison, with β=32.

Table 3. The summarized results of simulation at BER of 10^{-3}.

Algorithms	SNR (dB)		
Beta	8	16	32
DCSK without LDPC	14	14.2	14.7
DCSK with BF decoder	12.7	12.7	13
DCSK with Prob Domain decoder	9.4	10.2	13
DCSK with Log Domain decoder	9.4	9.8	10.6
DCSK with Min-Sum decoder	9.7	10	10.5

From previous results, it is clear that the worst case is the BF decoder because of the hard decision method used in these algorithms. On the other hand, the improvement added by BF to the DCSK transceiver is 1.3, 1.5 and 1.7 dB as again for β=8,16 and 32 respectively.

Also, the results show that a close performance is illustrated when using Prob Domain, Log Domain and Min-Sum, but all share the same amount of gain when varying β from 8,16 and 32. It is clear that better performance accrues in β=8. The coding gain for each three soft-decision decoders (Prob Domain, Log Domain and Min-Sum) is about 1.7 to 4.6 dB. It is worth mentioning that this performance of such a system may be inverted when using a selective fading channel instead of AWGN channel which used in such simulation for simplicity.

6 Conclusion

In this paper, an evolution of DCSK performance is applied with and without the LDPC code to show its performance within the AWGN channel and clear out the effect of code presenting. The results show that the system needs more than 14 dB SNR to approach 10^{-3} BER without code. On the other hand, by inserting LDPC code, the performance of such a system is improved by the various amount of SNR depending on the type of decoders. The proposed

system results show that the range of code gain is about 1.7 to 4.6 is achieved by using soft decision decoders. While (1.3 – 1.7) dB can be achieved when using hard decision decoder, taking into account the complexity for each decoder. From all results, we can say that using LDPC code can improve the performance of DCSK for various numbers of β.

References

[1] Xia, Y., Tse, C. K., & Lau, F. C. M.: 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. pp. 680-684 (2004).

[2] Khieu, H. T., Le, D. K., & Van Nguyen, B.: On the performance analysis of a DCSK system under the pulse jamming environment. PloS one. pp. 1-11 (2018)

[3] Majeed, M.: Implementation of Differential Chaos Shift Keying Communication System Using Matlab-Simulink. Journal of American Science. pp. 240-244 (2014)

[4] Wang, L., Cai, G., & Chen, G. R.: Design and performance analysis of a new multiresolution M -ary differential chaos shift keying communication system. IEEE Transactions on Wireless Communications. pp. 5197-5208 (2015).

[5] Mohammed, R. A., Hassan, F. S., & Zaiter, M. J.: Design and implementation of Haar wavelet packet modulation based differential chaos shift keying communication system using FPGA. International Journal of Advanced Computer Research. pp. 268-284 (2018)

[6] Wang, L., & Chen, G.: Using LDPC codes to enhance the performance of FM-DCSK. In The 2004 47th Midwest Symposium on Circuits and Systems. pp. I-401 (2004)

[7] Mosleh, M. F.: Evaluation of Low Density Parity Check Codes Over Various Channel Types. Engineering and Technology Journal. pp. 961-971 (2011)

[8] Ullah, W., & Yahya, A.: Comprehensive algorithmic review and analysis of ldpc codes. Indonesian Journal of Electrical Engineering and Computer Science. pp. 111-130 (2015)

[9] Faruk, M. O., & Ullah, S. E.: Performance Evaluation of Orthogonal Multi-level Chaos Shift Keying Modulation Scheme Aided MIMO Wireless Communication System. International Journal of Networks and Communications. pp. 10-17 (2018)

[10] Chen, Q., Wang, L., Lyu, Y., & Chen, G.: Designing protograph-based LDPC codes for iterative receivers on M-ary DCSK systems. IEEE Transactions on Circuits and Systems II: Express Briefs. pp. 466-470 (2017)

[11] Liu, Z., Zhang, J., & Liu, H.: Design of the differential chaos shift keying communication system based on DSP builder. Computer Modelling & New Technologies. pp. 138-43 (2014)

[12] Kumar, A.: Differential Chaos Shift Keying Modulation for Cooperative and Spatial Diversity Communication Systems. PhD Thesis. Indian Institute of Technology Guwahati (2015)

[13] Mohammed, R. A.: Design of Haar Wavelet Packet Modulation Based Differential Chaos Shift Keying and Implemented by Xilinx System Generator. Msc. Thesis. Middle Technical University (2018)

[14] Mosleh, M. F., & Hasan, F. S.: Comparison between Different Decoding Algorithms for Low-Density Parity Check. 4th Scientific International Conference-Najaf (4th SICN-2019). pp. 1-6 (2019)

[15] Johnson, S. J.: Introducing low-density parity-check codes. MSc. Thesis. University of Newcastle Australia (2006)

[16] Chandrasetty, V. A., & Aziz, S. M.: FPGA implementation of a LDPC decoder using a reduced complexity message passing algorithm. Journal of Networks. pp. 36-45 (2011)

[17] Kumar, A.: FPGE implementation of LDPC codes. PhD Thesis. National Institute of Technology, Rourkela (2013)

[18] Nurellari, E.: LDPC coded OFDM and it's application to DVB-T2, DVB-S2 and IEEE 802.16 e. PhD Thesis. Eastern Mediterranean University (EMU) (2012)

[19] Liu, J.: Novel LDPC coding and decoding strategies: design, analysis, and algorithms. PhD Thesis. University of York (2012)