Global Journals LaTeX JournalKaleidoscope™

Artificial Intelligence formulated this projection for compatibility purposes from the original article published at Global Journals. However, this technology is currently in beta. *Therefore, kindly ignore odd layouts, missed formulae, text, tables, or figures.*

Performance Evaluation of Encrypted Text Message Transmission in 5G Compatible Orthogonal Multi-level Chaos Shift Keying Modulation Scheme Aided MIMO Wireless Communication System

Md. Omor Faruk[1] and Shaikh Enayet Ullah[2]

[1] University of Rajshahi

Received: 10 December 2017 Accepted: 31 December 2017 Published: 15 January 2018

Abstract

- In this paper, a comprehensive performance evaluative study has been made on encrypted text message transmission in 5G compatible orthogonal multi-level chaos shift keying modulation scheme aided MIMO wireless communication system. The 4 X 4 multi-antenna supported simulated system incorporates four channel coding (1/2-rated Convolutional, (3, 2) SPC, LDP Cand Repeat and Accumulate (RA)), different signal detection (MMSE, ZF, Cholesky decomposition and Group Detection (GD) approach aided Efficient ZeroForcing (ZF)), and Chaotic Walsh-Hadamard encoding schemes.

Index terms— OM-DCSK modulation, scambing, Hilbert transform and walsh-hadamard codes, signal to noise ratio (SNR),

(MC-CSK) modulation system based on multi-carrier transmission and multi-level chaos shift keying modulation. In their works, both analytical and simulation results confirmed that the MC-CSK system outperformed differential CSK (DCSK) and MC-DCSK systems in BER performance [3]. At [4] in 2017, Kaddoum and et al. proposed an SR-DCSK system that performed simultaneous wireless information and power transfer (SWIPT) with an exploitation of the saved time gained from the fact that reference signal duration of SR-DCSK scheme occupied less than half of the bit duration to transmit a signal. The authors demanded that with their simplified designed system, the results showed that the proposed solution saved energy without sacrificing the non-coherent fashion of the system or reducing the rate as compared to conventional DCSK. In 2018, Dai and et al. proposed a novel carrier index DCSK modulation system for increased energy and spectral efficiencies based on splitting all data bits into two groups carried by the chaotic signals and their Hilbert transforms. With their derived analytical bit error rate expressions over additive white Gaussian noise and multipath Rayleigh fading channels, the advantages of their proposed system emphasized the improvement of security in Free Space Optical (FSO) communication system with the utilization of the Gamma-Gamma turbulence model and DCSK scheme. In their work, the performance of the proposed chaotic FSO system was studied with consideration of different turbulence conditions and derived an analytical expression of the probability of error.

In this present study, we have implemented a novel non-coherent multi-level DCSK modulation technique on secured text message transmission. Such technique and multi-level orthogonal modulation, where each data-bearing signal is chosen from a set of orthogonal chaotic wavelets which is constructed by a reference signal [7].

1 II. Signal Processing Techniques

In this section, an overview of different implemented signal detection and channel coding schemes is given.

2 a) MMSE and ZF Signal Detection

In T R N N × MIMO system, the signal model can be represented by y=Hx+n (1) Where, H is a channel matrix with its (j,i) th entry ?? ???? for the channel gain between the i th transmit antenna and the j th receive antenna, j=1,2,??.NR and i=1,2,??.NT, ? . Following the signal model presented in equation 1, the minimum mean square error (MMSE) weight matrix can be described as:H 1 2 n H MMSE H) I H H (W ? ? + = (2)

And the transmitted signal is given byy W x ~MMSE MMSE =**(3)**

In the ZF scheme, the ZF weight matrix has been given byH 1 H ZF H) H H (W ? = (4)

And the transmitted signal is given by [8] y W x ~ZF ZF = (5)

3 b) Cholesky Decomposition (CD) based ZF detection

In Cholesky Decomposition (CD) based ZF detection scheme, the matched filtering (MF) based detected signals using equation (1), can be written as:n H Hx H y H x ?H H H MF + = = (6)

Where, H H is the Hermitian conjugate of the estimated channel. In interference constraint scenarios, the more forwarded ZF detector has been required which operates on the MF data by,MF 1 H ZF x) H H (x ?? = (7)

Equation (7) has been written in modified form as:MF 1 H MF 1 H ZF x) LL (x) H H (x ?? ? = = (8)

With onward and backward substitution, the identified signal in CD-based ZF detection could be [9]:MF 1 H ZF x L L x ?? ? =**(9)**

c) Group Detection (GD) approach aided Efficient Zero-Forcing (ZF) In Group Detection (GD) approach aided Efficient Zero-Forcing (ZF) signal detection scheme, Equation(1) can be reworded as:[ ] n s H s H n s s H H y 2 2 1 1 2 1 2 1 + + = + ? ? ? ? ? ? ? = (10)

Where, L N 1 R C H × ? and) L N (N 2 R C H ? × ? are composed+ + = (11)

Or equivalently, we can writen W s H W y W s 1 2 2 1 1 1 ? ? = (12)

Substituting equation (12) into equation (11) and after some small manipulation, we get2 2 2 2 n s H ? + = (13)

Where,, 1 N 2 R C y × ? ,) L N (N 2 R C H ~? × ? and 1 N 2 R C n × ? . The 2 y , 2 H ~and 2

n can be reworded as:y) W H I (y 1 1 2 ? = (14) 2 1 1 2 H) W H I (H ~? = (15) n) W H I (n 1 1 2 ? = (16)

Where I is the identity matrix. On the basis of) y W (Q s ?1 1 2 =

, where the symbol Q is indicative of quantization. The effect of 2 s is canceled out from y to get2 2 1 s ? y y ? = . The sub-symbol vector 1 s is estimated using) y W (Q s ?1 1 1 =

. The transmitted signal vector x has been approximated as [10]:[ ] T T 2 T 1 s ? x ?= (18)

4 d) Convolutional Channel Coding

Convolutional codes have been commonly specified by three parameters (n,p, q), where, n = number of output bits; p = number of input bits; q = the code rate, and it is a measure of the efficiency of the code. In this present study, ½ rated convolutional encoders are designed so that the decoding can be functioned in some structured and simplified way based on Viterbi decoding algorithm. The constraint length, L= (p(q-1)) represents the number of bits in the encoder memory that affect the generation of the n output bits. The currently deliberated convolutional channel encoder 7and code generator polynomials of 171 and 133 in the octal numbering system. The code generator polynomials G1 and G2 can be expressed as [11] G1=x0+x2+x3+x5+x6=10 1 1 0 1 1=133 (19) G2= x0+x1+ x2+x3+ x6=1 1 1 1 0 0 1 =171 (20)

5 e) LDPC Channel Coding

The low-density parity-check (LDPC) code was discovered by Gallager as early as 1962. An LDPC code is linear block code, and the parity-check matrix H of it contains only a few 1's in comparison to 0's (i.e., sparse matrix).Such LDPC codes have been graphically depicted by the bilateral Tanner graph. Its nodes have been combined into one set of n bit nodes (or variable nodes) and the other set of m check nodes (or parity nodes). Check node i has been connected to bit node j in the event of any elemental value of the parity matrix unity. The decoding operates alternatively on the bit nodes and the check nodes to find the most likely codeword c that satisfies the condition cHT = 0. In iterative Log Domain Sum-Product LDPC decoding under discretion of AWGN noise channel of variance ?2 and received signal vector r, log-likelihood ratios (LLRs) instead of probability have been defined as:)] r 1 c (P /) r 0 c (P [ln) c (L i i i i i i = = ?) P / P [ln) P (L 1 ij 0 ij ij ? (21)) Q / Q [ln) Q (L 1 ij 0 ij ij ?) Pj / Pj [ln) P (L 1 0 j ? Wherein (.

) represents the natural logarithm operation. The bit node j is initially set with an edge to check node i:2 i i ij / r 2) c (L) P (L ? = = (22) In message

passing from check nodes to bit nodes for each check node i with an edge tobit node j; L(Q ij) has been updated as:) j j and n .... 2 , 1 j ( )] ([ ) Qij (L j j i j j i ? ? = ? ? ? ? ? = ? ? ? ? ? ? (23) .)] P (L [and)] P (L [sign , where ij ij ij ij ? ? ? ?

The ?function is expressed as:)] 1 e /( ) 1 e ln[( )] 2 / x ln[tanh( ) x (x x ? + = ? = ? (24)

L (Pj) is updated from bit nodes to check nodes for every bit node j with an edge to check node ias:) i i and m .... 2 , 1 i ( ) Qij (L) c (L) Pij (L i i ? ? = ? + = ? ? (25)

Decoding and soft outturns: for j=1, 2, 3?,n; L (Pj) has been updated as:) m .... 2 , 1 i ( ) Pij (L) c (L) Pj (L i i = + = ? (26) ? ? ? < = else 0 0) P (L if 1 c j i (27)

If cH T =0 or the number of iterations reaches the maximum limit [12] f). **??**

6 3, 2) SPC Channel Coding

In SPC channel coding, the transmitted binary bits have been rearranged into very short code words consisting of merely two consecutive bits. In such coding, (3, 2) SPC code has been used with addition of a single parity bit to the message u = [u0, u1] so that the elements of the resulting codeword x = [x0, x1, x2] are given by x0 = u0, x1 = u1 and x2 = u0 ?u1 Where the symbol ?has been considered here to denote the sum over GF (2)

7 g). Repeat and Accumulate (RA) Channel Coding

The RA is a powerful modern error-correcting channel coding scheme. In such channel coding technique, all the extracted binary bits from the audio is arranged into a single block, and the binary bits of such block is repeated two times and rearranged into a single block containing binary data which is double of the number of input binary data [13].

8 III. System and Signal Models

The block diagram of the 5G compatible orthogonal multi-level chaos shift keying modulation scheme aided simulated MIMO wireless communication system has been depicted in Figure 1. In such a simulated technique, a text message has been converted into binary bit form and the extracted binary signal vector m?(0,1) afterward it is channel encoded, interleaved and Till the end of two consecutive bit duration, this sequence is then delayed and repeatedly outputted for one more time.

The originated chaotic sequence undergoes pulse shaping and can be described under consideration of chip time ð ?"ð ?" ?? and for a length of time?-1 slot ð ?"ð ?" ?? = ??ð ?"ð ?" ?? . ? ? ? + ? = 1 - 0 - i) c iT t (T ih N n x) t (x**(28)**

In case of considering ?? ð ?"ð ?" (t) as the impulse response of a pulse shaping filter with time duration of T c , the reference signals in the n-th symbol duration can then be described as( ) ? ? + = ? = 1 N) 1 n (nN k s r) kT t (x t y (29)

And the data-bearing signal in the n th symbol duration is computed by? ? ? ? ? = ? + = + ? = ? + = ? + ? = 1 N 0 m 1 N) 1 n (nN k s k , m N m , n 1 N 0 m 1 N) 1 n (nN k s k , m m , n t , d) kT t (x ? a) kT t (x w a y (30) Where) iT t (h i N x) t (x ?c T 1 0 i n ? + ? = ? ? ? = (31)

Finally, the transmitted signal in the n th symbol duration has been obtained as:s s 0 d 0 r n NT) 1 n (t nNT), t f 2 sin( ) t (y) t f 2 cos( ) t (y) t (s + < ? ? ? ? = (32)

Where ?? ?? is the frequency of the sinusoidal?? ?? ? ?? ð ?"ð ?" ?? ?

In an AWGN and Rayleigh fading channel H, the obtained signal has been corrupted by stationary Gaussian noise with zero mean and power spectral density of ?? ?? /??.

The received signal can be described byr n (t) = H × s n (t) + n(t)**(33)**

The obtained signal has been passed through a signal detection technique and fed into a spatial multiplexing decoder and for producing a signal channel data vector,r ? n (t) = s ? n (t) + n(t)**(34)**

and quadrature components of RF signal and filtered with properly designed matched filters. The outputs of the matched filters can be defined as;i k i k i , r

x y+ ? + ? ? + =) N) 1 n (i k nN ? + < + ? ? ? (35) ,) x â x a (W y i k 1 N 0 m i k N m , n i k m , n k , m i , d + ? ? = + ? + + ? ? + + = ? (36)

Where ? k?+i and ? k?+1 are two independent Gaussian random variables and both with zero mean From the format of the signal in OM-DCSK, it can be simply inferred that in (**??**5) and (36) as follow;, x x i i k = + ? ? < ? i 0 N) 1 n (k nN + < ? (37) , x x ?i i k = + ? ? < ? i 0 N) 1 n (k nN + < ? (38) ? ? ? ? ? ? ? ? ? = ? + = ? ? = ? + = ? ? = ? 1 N) 1 n (nN k 1 0 i i , d i , r k , m 1 N) 1 n (nN k 1 0 i i , d i , r k , N m y y W y y ? m Z (39)

By comparing all the correlator outputs, the outturns will be laid to one, while the remaining are zero.

Finally, the data bits can be recaptured based on the reversed version of the mapping rule (Table 1 of [14]). The estimated coefficient values have been converted into binary form, de-interleaved, channel decoded, binary to integer converted and the text message has been retrieved after decryption. The output of the m th correlator (presented figure number 2 of [14]) has been obtained then as: coefficient a m,n associated with the greatest correlator This r ? n (t) signal is multiplied with both in-phase And ?? ? ??????+?? is the Hilbert transform of ?? ??????+?? and ?? ??,?? are the four orthogonal Walsh Hadamard codes used for proper identification of individual signal. The reference signal in (29) and the data-bearing signal in (30) have been modulated onto a cosine and a sine carrier, respectively, so that they could be delivered via the in-phase and quadrature channels.? + < + ? ? ? N) 1 n (i k nN 2 m 0 < ? 4 m 2 < ? Global Journal of

9 IV. Result and Discussion

Hereafter, a series of simulation results have been depicted in terms of BER to illustrate the impact of the system performance in Orthogonal Multi-level Chaos Shift Keying Modulation Scheme aided MIMO Wireless Communication System.

The performance of the system is illustrated by using MATLAB Ra2017a based on the simulation parameters are demonstrated in the following Table -1 It is critically noticed that the result of the system provides comparatively better performance under the implementation of MMSE signal detection technique from the graphical illustration presented in Figure **??** to Figure 5.

In Figure **??**, the performance of the system is highly well defined under various implemented signal detection and ½-rated convolutional channel coding techniques. For a typically presumed SNR value of -4 dB, in the aspect of ZF, MMSE and Cholesky Decomposition and Group Detection (GD) approach aided Efficient ZF signal detection techniques, the ZF and 1.90 dB in MMSE as compared to Cholesky decomposition.

Under the identical consideration of SNR value (-4 dB), it is noticeable from the Figure-3 that the estimated BER values are 0.1613, 0.2014, 0.2027 and 0.2246 in case of MMSE, Cholesky decomposition, ZF and GD approach aided Efficient ZF signal detection technique respectively. In such cases, the system performance improvement of 0.96 dB and 0.99 dB have been achieved in MMSE as compared to Cholesky decomposition and ZF signal detection techniques. At 10% BER, SNR gain of 0.65 dB and 0.72 dB have been obtained in MMSE as compared to Cholesky Decomposition and GD approach aided Efficient ZF signal detection.

In Figure 4, it has been observed that the system performance is well segregated in the different scenario at low SNR region (-5dB to -2dB). For a typically presumed SNR value of -4 dB, the It is keenly noticeable from Figure 5 that the system performance is not well segregated in all signal detection techniques excepting MMSE. For a typically considered SNR value of -4 dB, the approximated BERs are found to have values of 0.0301 and 0.0861 in case of MMSE and ZF which is indicative a system performance of 4.56dB. At 2% BER, a low SNR (-3dB) is required for MMSE. On the other hand, comparatively, a high SNR (-1.5dB) is required for the GD approach aided Efficient ZF signal detection technique. 0.1880, 0.0315, 0.1412 and 0.1458 respectively which [1] [2] [3]

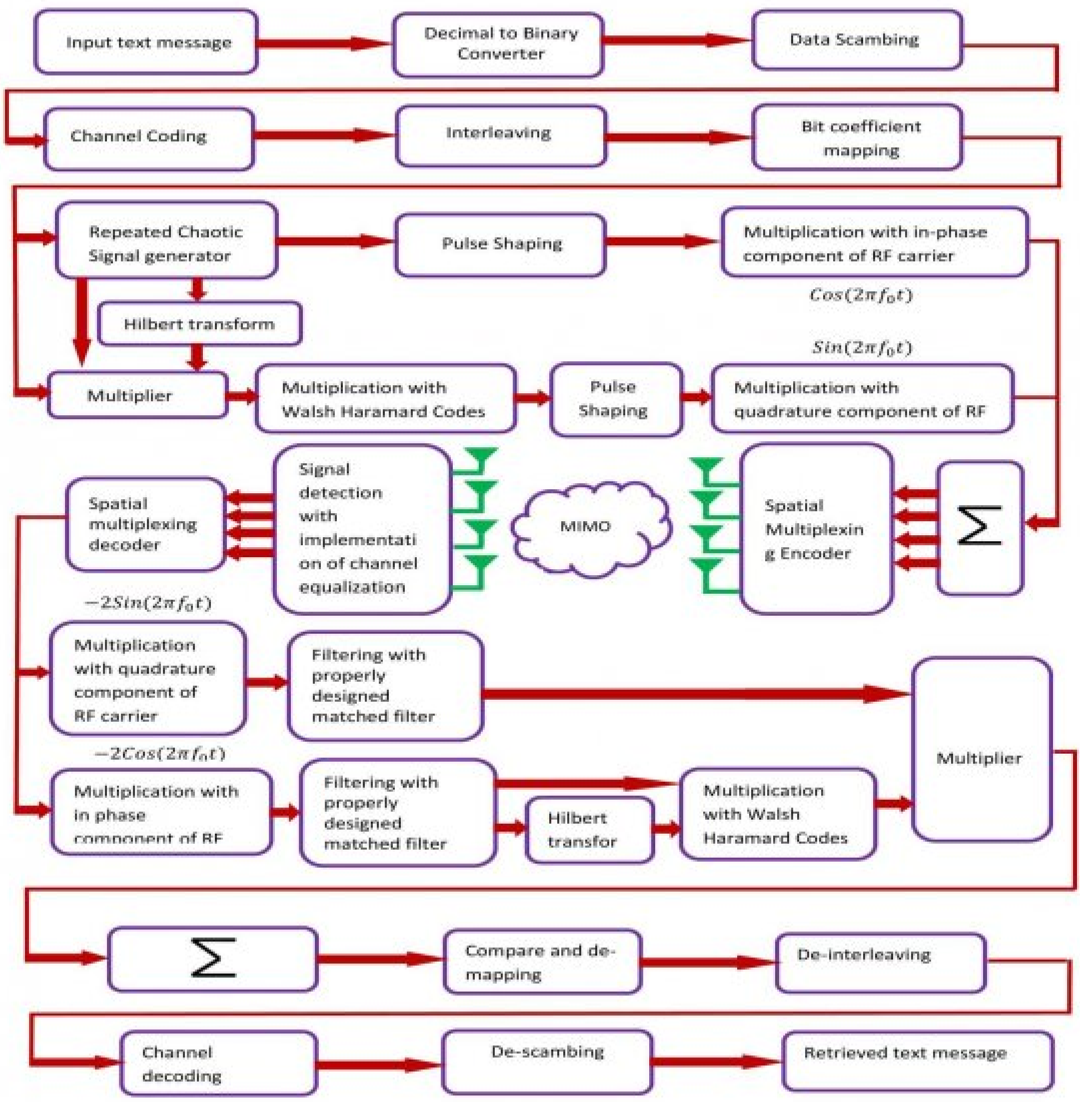
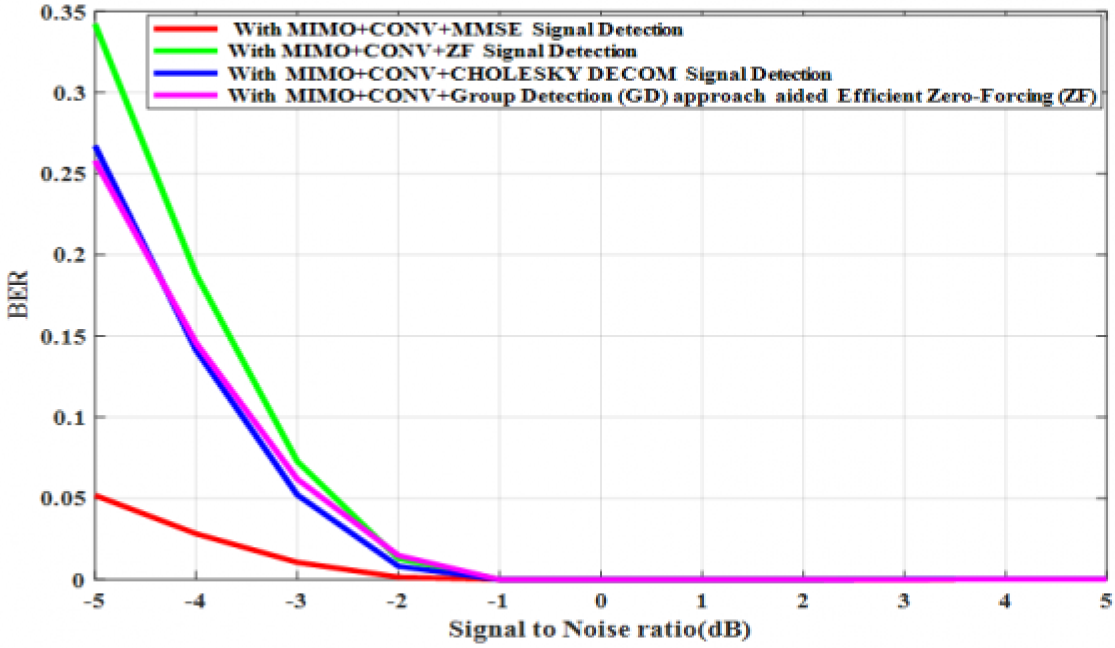

Input text message
Decimal to Binary Converter
Data Scambing
Channel Coding
Interleaving
Bit coefficient mapping
Repeated Chaotic Signal generator
Pulse Shaping
Multiplication with in-phase component of RF carrier
$Cos(2\pi f_0 t)$
Hilbert transform
$Sin(2\pi f_0 t)$
Multiplier
Multiplication with Walsh Haramard Codes
Pulse Shaping
Multiplication with quadrature component of RF
Spatial multiplexing decoder
Signal detection with implementati on of channel equalization
MIMO
Spatial Multiplexin g Encoder
$-2Sin(2\pi f_0 t)$
Multiplication with quadrature component of RF carrier
Filtering with properly designed matched filter
Multiplier
$-2Cos(2\pi f_0 t)$
Multiplication with in phase component of RF
Filtering with properly designed matched filter
Hilbert transfor
Multiplication with Walsh Haramard Codes
Compare and de-mapping
De-interleaving
Channel decoding
De-scambing
Retrieved text message

Figure 1:



1

Figure 2: Fig. 1 :

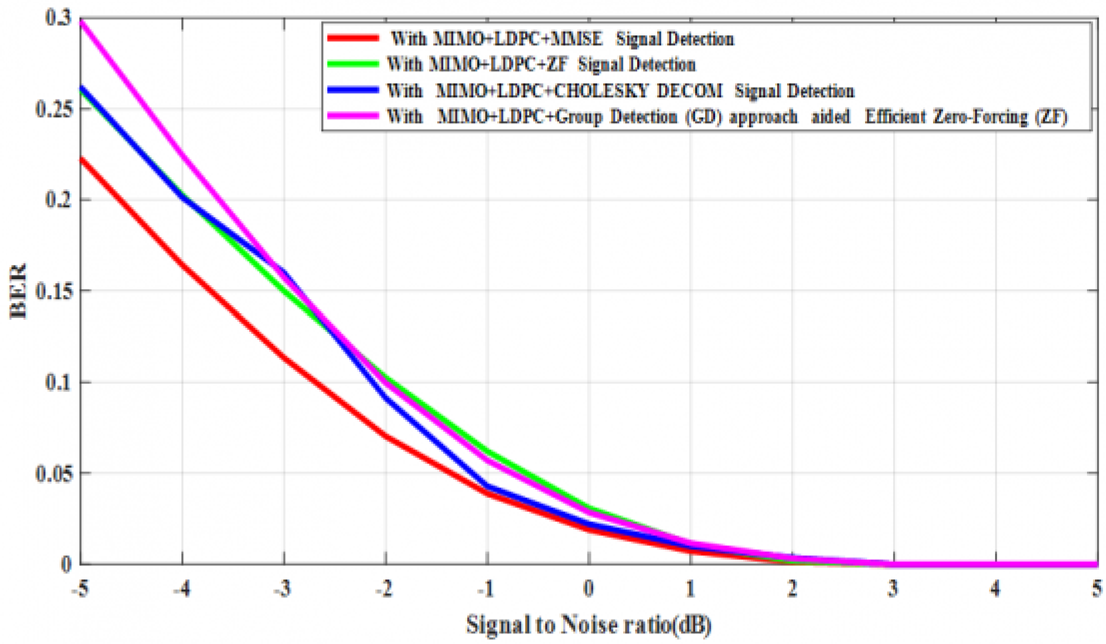


Figure 3:

32

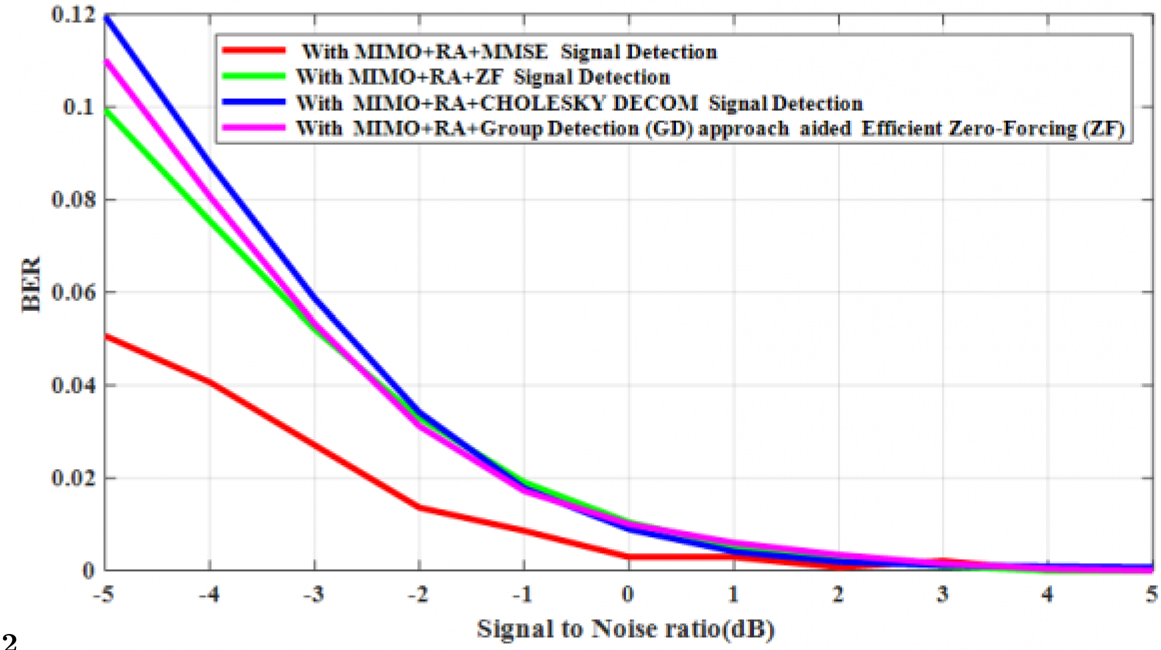


Figure 4: Fig. 3 :Fig. 2 :

4

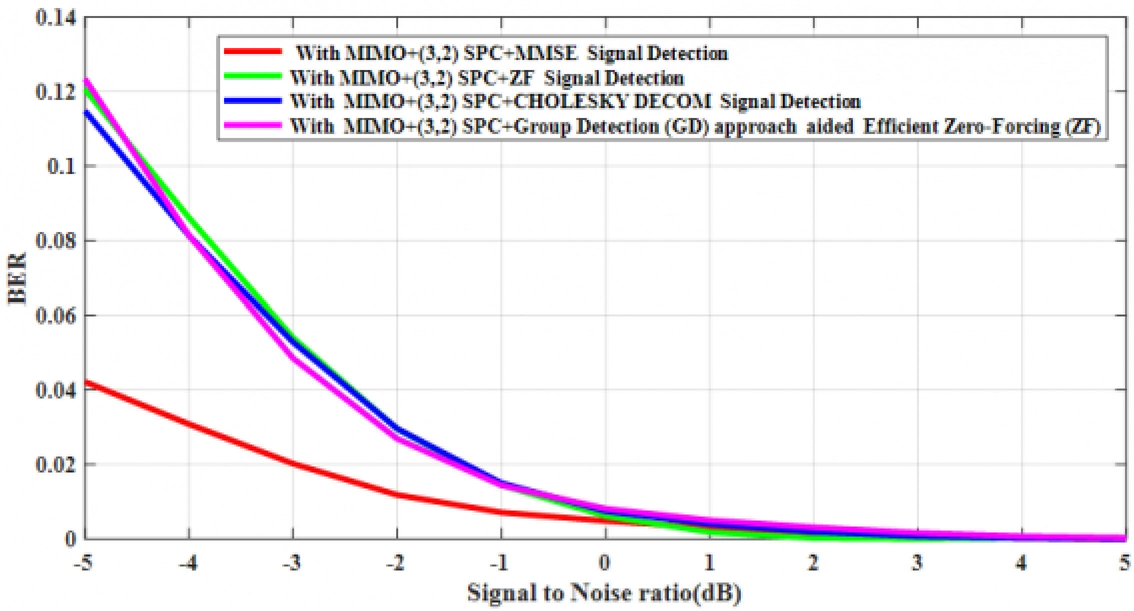


Figure 5: Fig. 4 :

1

Text message with number of binary bits	1400
Signal detection techniques	MMSE, ZF, Cholesky Decomposition and Group Detection (GD) approach aided Efficient Zero-Forcing (ZF)
Channel coding	Half rated Convolutional, (3,2) SPC, LDPC, and Repeat and accumulate (RA)
Length of orthogonal Walsh Hadamard code	64
Pulse shaping filter with Rolloff factor	Raised cosine with 0.25
Bit rate	1Gbps
No of samples generated in Chaotic signal, ? value	64
No. of transmitting/ Receiving antennas	4/4
Channel	MIMO fading channel
Signal to noise ratio (SNR)	-5 to 5 dB

Figure 6: Table 1 :

Year 2018
18
Volume XVIII Issue IV Version I
)
E
(
Global Journal of Computer Science and Technology

approximated BER values are found to have values of

effectively ratifies system performance improvement of 7.76 dB, 6.52 dB and 6.65 dB in the aspect of MMSE in comparison with to ZF, Cholesky decomposition and Group Detection (GD) approach aided Efficient Zero-Forcing (ZF) signal detection techniques respectively. At 5% BER,

Figure 7:

.1 ?

Original transmitted text message: The large available bandwidth and high spectrum efficiency certainly makes mmWave massive MIMO a promising choice to significantly improve overall system throughput for future 5G cellular networks.

.2 (a)

Retrieved text message at -1dB:

The large available bandwidth and high spectrum enfmciency$certainly makes mmWave massive M MO a promising choice0vo significantly imprnve overall syst%mthroughput for future 5G cellular network{.

.3 (b)

Retrieved text message at 1dB:

The0large available bandwidth and high spectrum efficiency certaInly makes mmWavemarsive MIMO a promising"choice to significantly kmprove overall system throughput for future 5G cellular networks.

.4 (c) Retrieved text message at 2dB:

The large available bandwidth and high spectrum efficiency certainly makes mmWave-assiveMIMO a promising choice to significantly improvu overall system throughpwt for future 5G cellular networks*

.5 (d) Retrieved text message at 3dB:

The large available bandwidth and high spectrum efficiency certainly makes mmWave massive MIMG a prolisingchoice to significantly improve overall system throughput for future 5G cEllularnetworks.

.6 (e) Retrieved text message at 4dB:

The large available bandwidth and high spectrum efficiency certainly makes mmWave massive MIMO a promising choice to significantly improve overall system throughput for future 5G cellular networks.

.7 V. Conclusions

In this present work, we have tried to accomplish various signal detection and channel coding techniques for making a fruitful investigation on the performance of orthogonal multi-level CSK modulation scheme aided MIMO wireless communication system. From the simulative study, it has been observed that the system provides robust performance in retrieving data at negligible SNR value region with proper utilization of MMSE signal detection technique under execution of (3, 2) SPC channel coding scheme.

However, based on the simulative study, it can be concluded that the orthogonal multi-level chaos shift keying modulation scheme is suitable in IoT applications or 5G/B5G wireless communication networks.

[Gangarajaiah et al. ()] 'A Cholesky Decomposition based Massive MIMO Uplink Detector with Adaptive Interpolation'. Rakesh Gangarajaiah , Hemanth Prabhu , Ove Edfors , Liang Liu . *proceeding of IEEE International Symposium on Circuits and Systems (ISCAS)*, (eeding of IEEE International Symposium on Circuits and Systems (ISCAS)) 2017. p. .

[Jiang ()] *A Practical Guide to Error-Control Coding Using MATLAB*, Yuan Jiang . 2010. Norwood, MA, USA: Artech House.

[Weikaixu et al. ()] 'Code-Shifted differential chaos shift keying with code index modulation for High Data Rate Transmission'. Tingting Weikaixu , Lin Huang , Wang . *IEEE Transactions on Communications* 2017. 65 p. .

[Tran and Kong ()] 'Design of simultaneous wireless information and power transfer scheme for short reference DCSK communication systems'. Georges Kaddoum Ha-Vu Tran , Long Kong , Michealatallah . *IEEE Transactions on Communications* 2017. 65 (1) p. .

[Nguyen et al. ()] 'Efficiency Zero-Forcing Detectors based on Group Detection for Massive MIMO systems'. Thanh-Binh Nguyen , Tien-Dong Nguyen , Minh-Tuan Le , Vu-Duc Ngo . *proceeding of International Conference on Advanced Technologies for Communications (ATC)*, (eeding of International Conference on Advanced Technologies for Communications (ATC)) 2017. p. .

[Narang et al.] *Error probability analysis of FSO Communication System using Differential Chaos Shift Keying*, Ghanishtha Narang , Mona Aggarwal , Hemani Kaushal , Swaran Ahuja . (In proceeding of 5th)

[Yang et al. ()] 'Multi-Carrier chaos shift keying: System Design and Performance Analysis'. Hua Yang , K S Wallace , Guanrong Tang , Guo-Ping Chen , Jiang . *IEEE Transactions on Circuits and Systems-I* 2017. 64 p. .

[Huang et al. ()] 'Multilevel code-shifted differential-chaos shift-keying system'. Tingting Huang , Lin Wang , C M Weikai Xuand Francis , Lau . *IET Communications* 2016. 10 p. .

[Md et al. ()] 'Performance Evaluation of Orthogonal Multi-level Chaos Shift Keying Modulation Scheme Aided MIMO Wireless Communication System'. Omor Md , Shaikh Enayet Faruk , Ullah . *International Journal of Networks and Communications* 2018. 8 (1) p. .

[Bawane and Gohokar ()] 'Simulation of Convolutional Encoder'. Sneha Bawane , V V Gohokar . *International Journal of Research in Engineering and Technology(IJRET)* 2014. 3 (3) p. .

[Soo Cho et al. ()] Yong Soo Cho , Jaekwon Kim , Won Young Yang , Chung G Kang . *MIMO-OFDM Wireless Communications with MATLAB*, (Singapore) 2010. John Wiley and Sons.

[Yang et al. ()] 'System design and performance analysis of orthogonal multi-level differential chaos shift keying modulation scheme'. Hua Yang , K S Wallace , Guanrong Tang , Guo-Ping Chen , Jiang . *IEEE Transactions on Circuits and systems* 2016. 63 (1) p. .

[Dai et al. ()] 'Two-Layer Carrier Index Modulation Scheme Based on Differential Chaos Shift Keying'. Wenhao Dai , Hua Yang; Yurong Son , Guoping Jiang . *IEEE Access* 2018. 6 p. .

[Vitetta et al. ()] Giorgio M Vitetta , Desmond P Taylor , Giulio Colavolpe , Fabrizio Pancaldi , Philippa A Martin . *Wireless Communications Algorithmic Techniques*, (United Kingdom) 2013. John Wiley and Sons Ltd.