ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 6, June 2015

CDSK Based Security of Chaos Communication Using MIMO

Hegde Pooja Vijay, Susmitha Alamuru

M.Tech, Dept. of E&C, NHCE, VTU, Bengaluru India

Assistant Professor, Dept. of E&C, NHCE, VTU, Bengaluru, India

ABSTRACT: The privacy or security provided by chaos communication system is far greater than other digital communication system due to its distinct features such as broad band or wide-band, easy to implement, non-predictability and its sensitivity to initial condition. In chaos communication the number of transmitted symbols is increased as the chaos communication system spreads and transmits the symbols or information bits according to the chaos maps characteristic. So, research is done in this field to improve transmission speed of data in chaos communication system. However, if more number of antennas is applied to this chaos communication system, capacity can be increased; as capacity of data is directly proportional to the antenna numbers. Therefore, MIMO application to chaos communication is good option. In this paper, (CDSK) correlation delay shift keying scheme is proposed using 2x2 MIMO and BER performance is evaluated over Rayleigh fading channel using detection algorithm of MIMO such as MMSE and Zero forcing for two chaotic map such as boss map and tent map, to analyze which detection algorithm of MIMO gives better result and also to analyze which chaotic map gives better BER performance. Lastly BER performance is evaluated for 2x2MIMO, 4x4 MIMO and 8x8MIMO by applying both chaotic map and using both detection algorithms for detection.

KEYWORDS: chaos communication, CDSK, MIMO, MMSE, Zero forcing

I. INTRODUCTION

In mathematics a portion of study is chaos theory. It is having application in area of physics, biology, sociology, engineering, philosophy and meteorology. Initial conditions are most sensitive part that is assumed in chaos theory. Observing the behavioral changes of dynamical systems which are very sensitive to initial condition is the study of chaos theory. Even a smallest difference in initial condition will give very diverging outputs, which is highly impossible to predict. Even though they are deterministic in nature, predicting outcome is difficult; as future behavior of dynamic system is based on their initial condition.

The security of chaos communication system is lot better than other digital communication system, due to its characteristics such as easy implementation, aperiodic, not easy to predict, broad band and sensitive to initial conditions. It shows sensitive behavior to initial condition, since chaos signal is changed to a complete different signal when initial condition is changed. If initial conditions are unknown, then it is impossible to predict the chaos signal. Chaotic signals have broadband spectrum, because of these characteristics they are used as carriers in spread spectrum communication. The chaotic sequence make the transmitted signal seems to be like noise; thus; it does not any unfriendly receiver towards it. This advantage makes the security of chaos communication a lot better than digital communication systems. Chaos communication system maximizes the number of the transmitted symbols by spreading it according to the characteristic of chaos maps. Capacity of data is directly proportional to the antenna number.so, application of multiple inputs and multiple outputs (MIMO) to the chaos communication system will improve the communication system. Chaos communication system gives bad BER performance than digital communication system, and it is very bad when used in fading channel. For improving the BER performance, chaos communication system calculates the BER performance using different chaos maps to get better BER performance with suitable chaos map. So, that user of chaos communication system can selectively choose chaos map that gives the best BER performance. Chaos communication systems BER performance can be improved by applying the MIMO system in fading channel .Presently, especially in mobile communication; multipath fading is the biggest factor effecting high-speed data

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 6, June 2015

communication. If MIMO system is used along with the chaos communication system, performance of system can be improved. Diversity gain and array gain can be achieved. These gains have a good effect on the BER performance.MIMO communication system sends or transmits data by different paths using several antennas. In receiver side, interference is reduced by detecting received signal at each path, providing the better data rate, bandwidth efficiency and link reliability. Capacity of data communication increases in MIMO directly in proportion to number of antenna, with provision of high data processing speed. Error can be minimized while using CDSK because MIMO method yields spatial diversity and it gives orthogonality between the symbols and its conjugates.

In this paper, correlation delay shift keying (CDSK) is used with 2×2 MIMO technique and is used for evaluation of BER performance over Rayleigh MIMO fading channel applying the boss map and tent map using MIMO detection algorithm such as minimum mean square error (MMSE) and zero forcing (ZF). We will evaluate the performance of different chaotic maps in the CDSK chaotic modulation system such as tent map and boss map and will find out which chaotic map shows superior BER. As the numbers of antennas are increased, BER performance also increases, so in this paper 4x4 and 8x8 antennas BER performance will be evaluated.

I. RELATED WORK

In Dec.2000"Performance analysis of correlation- based communication schemes utilizing chaos,"chaotic signal was used in spread-spectrum communications as it has a few clear advantages over traditional approaches.Two communication schemes were suggested that provide a processing gain. The performance of these and of the earlier proposed differential chaos shift keying is studied analytically and numerically for discrete time implementations. It is shown that, when performance is characterized by the dependence of bit error rate on E_b/N_0, the increase of the spreading sequence length beyond a certain point degrades the performance. For a given E_b/N_0, there is a length of the spreading sequence that minimizes the bit error rate.

In June 2007“Non-coherent correlation-based communication systems choosing different chaotic maps”
This paper proposes a new non-coherent detection system improved based on the differential chaos shift keying (DCSK) and the correlation delay shift keying (CDSK). In this scheme, a transmitter changes chaotic maps for generating a chaotic sequence efficiently depending on an initial value. Also, the proposed method can choose the chaotic map by a very simple algorithm. In order to investigate the proposed method, computer simulations were carried out and observe the performance.

In May 2010"Performance of differential chaos-shift-keying digital communication systems over several common channels,"
In this paper, based on the fundamental theories and with some recent researches of others, the DCSK performance is analysed and the expressions of the bit error rates are derived for DCSK under AWGN channel, Rayleigh fading channel and Rician fading channel. In the end, the Logistic mapping with zero mean is used for chaos generation in simulation and compared with simulation results.

In May 2011”Design of frequency-modulated correlation delay shift keying chaotic communication system,"
Considering the shortcomings of differential chaos shift keying (DCSK) with bad secrecy and low data transfer rate, this study designs and researches a new chaos shift keying digital modulation scheme- frequency-modulated correlation delay shift keying (FM-CDSK). The scheme has both the merits of CDSK and FM-DCSK. This study provides the particular theoretical derivation of the principle of modulation and demodulation. The simulation analysis of data transmission rate and confidentiality verify that this new scheme has more superior performance than DCSK and CDSK, and the transmission rate is twice as much as original shift keying schemes.

In Jan 2013"Performance evaluation of DCSK system with chaotic maps"
In this paper, the performance in differential chaos shift keying (DCSK) schemes using different chaotic maps such as Gauss map, Tent map, Gingerbread man map, and Henon map is analyzed. As technologies of communications develop, the need for data security is also significantly improved. DCSK modulation technique has advantages of traditional spread spectrum system and also provides enhanced data security. The performance with Henon map is better than the other chaotic maps with typical spreading factors and at reasonable SNR levels.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 6, June 2015

Existing methods used linear modulation systems, which posed limitation on data rate as well as imposed security risk on transmitted data as the number of users increased rapidly and linear technologies reached their limits, research on nonlinear modulation systems techniques made their way into front line.

II.PROPOSED METHOD

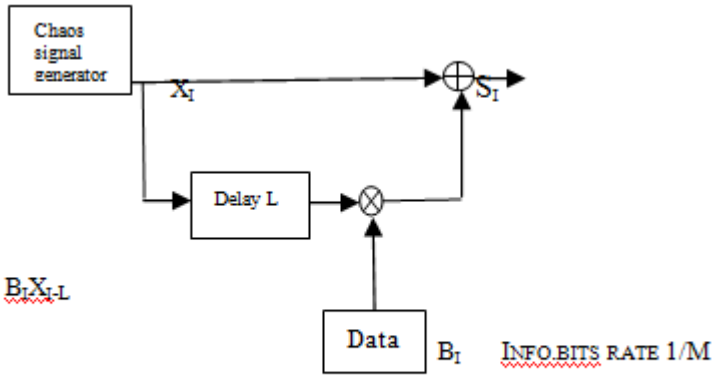

FIG.1 CDSK MODULATION

A.Correlation delay shift keying system(CDSK):

The disadvantage of DCSK is the requirement to transmit same chaotic sequence twice, which makes system prone to interference and even wastage of power and eavesdropper occur due to twice transmission. Even transmitter needs a switch and a delay element, or a generator which can reproduce same chaotic sequence. This all makes technical implementation difficult. The correlation delay-shift-keying (CDSK) technique is also non-coherent detection technique, similar to or can say derivative of DCSK technique. In this CDSK technique, the chaotic signal and the information bearing signal with some time delay are added together in transmitted signal. Therefore, each transmitted signal sample contains one reference sample and the information bearing sample, which is why transmitted signal sample is never reoccurred or repeated. Since, individual reference signal is not sent, efficiency of bandwidth is enhanced. By removing the switch needed to work as a switch between the reference chaotic signal and information containing signal in the DCSK system, CDSK allows continuous operation to be performed by transmitter. The switch is now replaced by an adder; as a result transmitted signal is repeated. Therefore the transmitted signal is less susceptible to interception and more correlative.

$$S_i = x_i + b_i x_{i-L} \qquad (1)$$

Equation (1) is sum of added delay chaos signal multiplied by information bit and generated chaos signal which forms the transmitted signal of a transmitter. L is delay time.

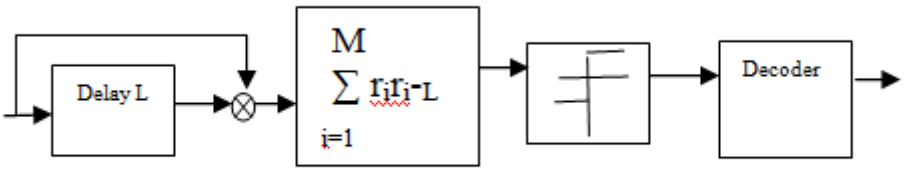

Fig.2 Receiver of CDSK system

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 6, June 2015

Figure 2 exhibits receiver of CDSK demodulation. To recover the symbol, CDSK receiver works as correlator. The received and delay of received signal are multiplied and this signal is passed through threshold and decoder to decode the information signal.

$$S = \sum_{i=1}^{M} r_i r_{i-L} \qquad (2)$$

Equation.2 shows output of correlator of CDSK demodulation. Here, $\sum r_i r_{i-L}$ is performed. Exact information bit transmitted can be decoded if delay time L is known.

B.Chaos map:

In this paper, two types of chaos map are used Tent map and Boss map. Researchers found Boss map means a novel chaos that improves the BER performance.

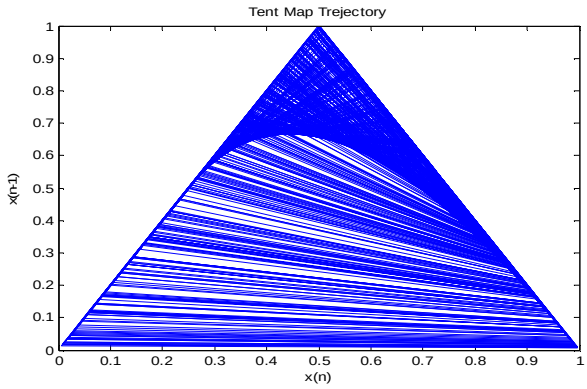

Fig.3 Trajectory of Tent map

Figure.3 shows trajectory of Tent map. The x-axis and the y-axis of figure.3 is x(n) and x(n-1) respectively. Tent map has trajectory of triangular shape.

$$X_{n+1} = \begin{cases} \alpha x_n & \text{for } x_n < 0.5 \\ \alpha(1-x_n) & \text{for } 0.5 < x_n \end{cases} \qquad (3)$$

Equation(3) expresses tent map. The output of previous value is considered as input to current value. To obtain fig.14 initial condition is considered as 0.1 and α as 1.99999.

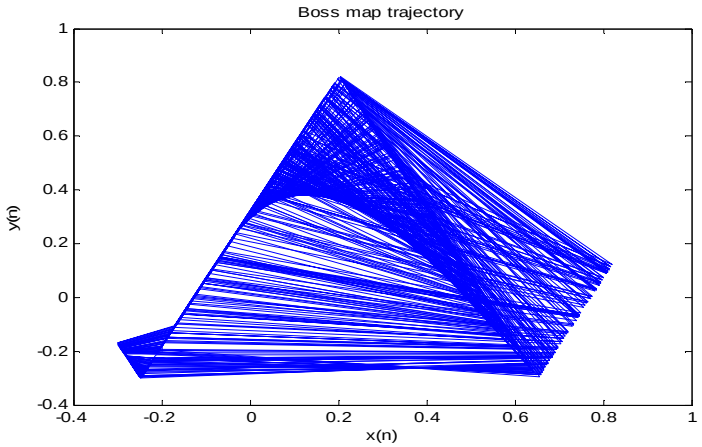

Fig.4 Trajectory of Boss map.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 6, June 2015

Figure 4 shows trajectory of Boss map that proposed anovel chaos map in order to improve the BER performance shows trajectory of boss map where x-axis as x(n) and y-axis as y(n) respectively. Pyramid shape trajectory is shown in Boss map.

$$X_{n+1} = \alpha \mid 0.45 - \mid 0.53 - X_n \mid \mid \qquad (4)$$
$$Y_{n+1} = X_n - 0.3$$

Equation (4) is expressed for Boss map. Boss map is formed from transformation of tent map, so trajectory of Boss is similar to tent map little. Initial condition is considered as 0.1 and α =2.5.

C. CDSK system applied to MIMO technique with detection algorithms:
For MIMO is necessary. Many types of MIMO detection algorithm are present but we apply MMSE and Zero Forcing in this paper. The BER performance evaluation for each algorithm is needed because performance changes rendering to the types of MIMO detection algorithm.

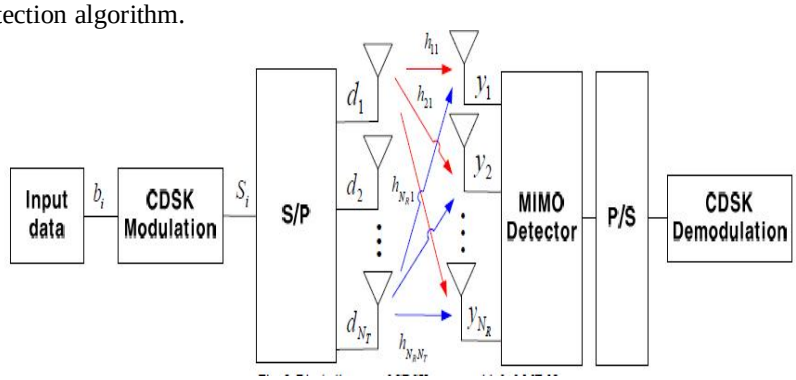

Fig.5. Block diagram of CDSK system with 2x2 MIMO

Figure 5 shows the block diagram of CDSK system that is applied to 2x2 MIMO systems. In 2x2 MIMO 2 transmitter and 2 receiver antennas are present to transmit and receive the signal. In MIMO due to multipath fading, the received signal has transmitted signal as well as signals from other antennas that are undesired signals. So, MIMO detection algorithms are used to separate the transmitted signal; and then the information symbols are recovered by the use of CDSK receiver.At receiver antennas the signal received is in the form of

$$Y = Hd + n$$
$$Y_1 = h_{11}d_1 + h_{12}d_2 + n_1 \qquad (5)$$
$$Y_2 = h_{21}d_1 + h_{22}d_2 + n_2$$

$$\begin{pmatrix} Y_1 \\ Y_2 \end{pmatrix} = \begin{pmatrix} h_{11} & h_{12} \\ h_{21} & h_{22} \end{pmatrix} \begin{pmatrix} d_1 \\ d_2 \end{pmatrix} + \begin{pmatrix} n_1 \\ n_2 \end{pmatrix}$$

Equation (5) shows that signal Y_1 and Y_2 are received signals to first and second antenna. The transmitted signals from first transmitted antenna have to be received by first received antenna; but it is able to identify that transmitted signal from other antenna was summed up to preferred signal. So, MIMO detection algorithm are used in receiver part.

$$y = Hd + n \qquad (6)$$
$$W = (H H^H)^{-1} H^H$$

$$Wy = (H H^H)^{-1} H^H (Hd + n) \qquad (7)$$
$$= d + (H H^H)^{-1} H^H n$$

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 6, June 2015

In equation (6), it indicates that transmitted symbol d is multiplies by channel H and is added to noiseSo, to recover the transmitted symbol, pseudo Inverse (W) is multiplied to receive symbol Y. Equation.7 shows for Zero forcing method.

$E\{[Wy - d][Wy - d]H\}]$ (8)

$W = (H H^H + N0I)^{-1} H^H$

Equation (8) is expressed the pseudo inverse of MMSE. Pseudo inverse of MMSE is similar to Zero Forcing, but *N0I* term exists in MMSE. In the case of the Zero Forcing, Pseudo Inverse is found by using estimation matrix equation. However, pseudo Inverse of MMSE is found by considering not only estimation matrix equation but also noise. Therefore, performance of MMSE is superior to Zero Forcing.

II. PERFORMANCE EVALUATION

1)Comparison of performance analysis of CDSK with 2x2 MIMO in Rayleigh channel using tent map and boss map for MMSE detection algorithm and Zero forcing algorithm

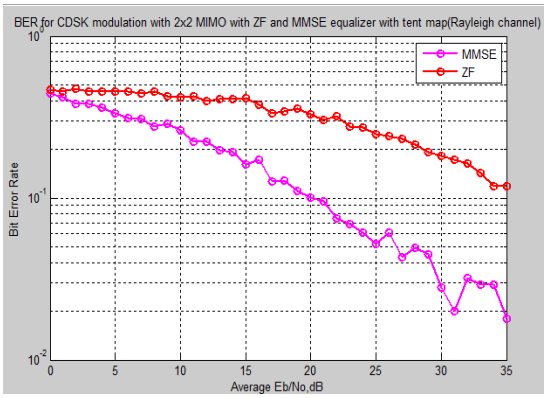

Fig.6. Using Tent map

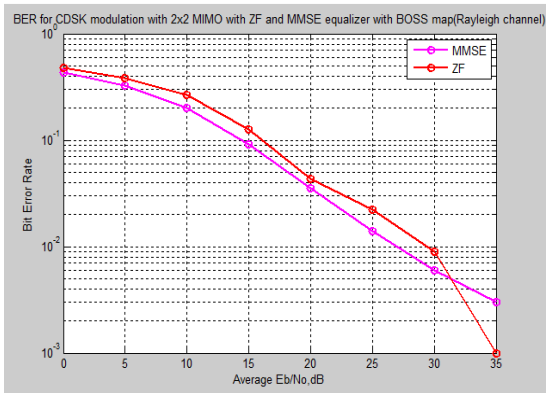

Fig.7 Using Boss map

Figure.6 and figure.7shows BER performance for CDSK applied to 2x2 MIMO using tent map and Boss map respectively; and is detected using both detection algorithms MMSE and Zero forcing in Rayleigh fading channel. For both chaotic map MMSE Shows better result than Zero forcing since pseudo inverse of MMSE considers both estimation matrix and noise term, minimizing the errors as seen in equation.8

2) BER performance of Tent and Boss map using both MMSE and Zero forcing detection algorithms for 2x2 MIMO

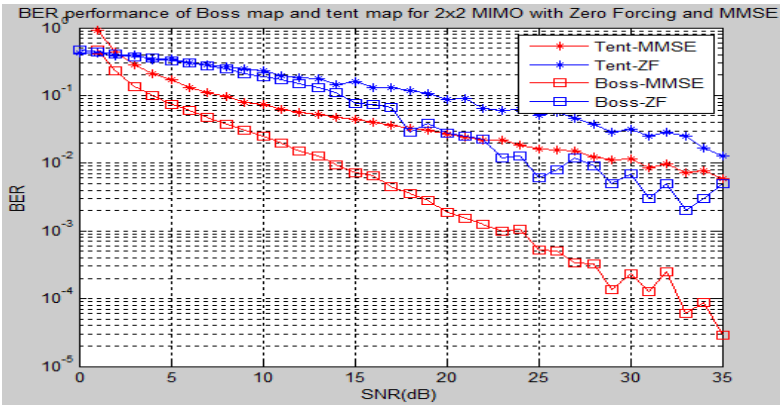

Fig.8 BER analysis of tent map and boss map for 2x2 MIMO with CDSK.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 6, June 2015

In figure.8 BER performance is evaluated using tent map and boss map for 2x2 MIMO with the use of CDSK for both MMSE and Zero forcing detection in Rayleigh fading channel. The graph shows that BER performance of Boss map gives better result than tent map. In this graph Boss-MMSE shows the best result and Tent ZF shows the worst result.

3) 2x2MIMO, 4x4 MIMO and 8x8 MIMO performance analysis for both maps and both detection algorithms

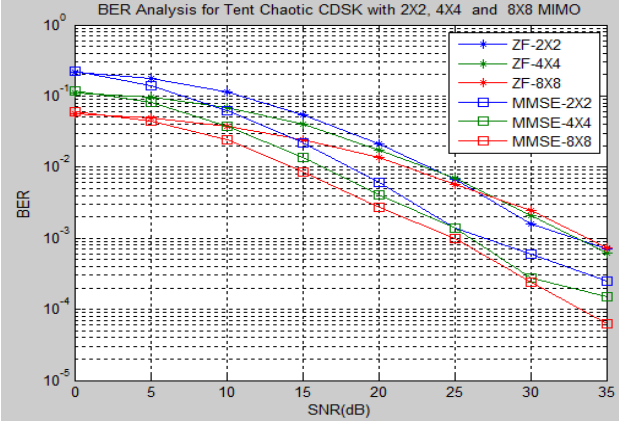

Fig.9 For tent chaotic map using CDSK

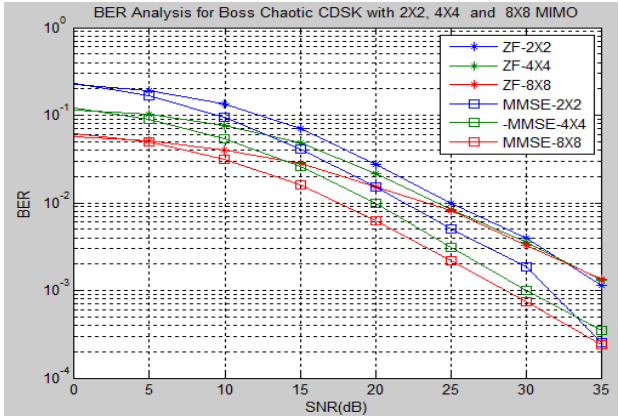

Fig.10 For Boss chaotic map using CDSK

Figure.9 and 10 shows that as the number of antennas increases, capacity of data transmission increases proportionally. Here, in this graph MMSE – 8x8 MIMO shows the best BER performance and ZF – 2x2 MIMO shows the worst performance. Overall 8x8 MIMO shows better performance than 4x4 MIMO and 4x4 MIMO shows better result than 2x2 MIMO.In MIMO capacity increases as number of antennas increases, in the same way as MIMO is prone to multipath fading if number of antennas increases at both transmitter and receiver side BER performance improves. So, from figure 9 and 10 conclusions can be drawn that 8x8 MIMO show better result than 4x4 MIMO for both tent and boss maps and 4x4 MIMO shows better result than 2x2 MIMO for both tent and boss chaotic maps with CDSK in Rayleigh channel.

III. CONCLUSION AND FUTURE WORK

In this paper, BER performances is evaluated in Rayleigh fading channel using 2x2 MIMO and CDSK system modulation by applying or using MIMO detection algorithm like MMSE and Zero forcing with different chaotic maps like Tent map and Boss map are compared. In chaos communication system information is spread according to the characteristic of chaos map, so the number of transmitted symbols increases. Here, 2x2 MIMO is used, so to extract transmitted symbol at receivers side, MMSE and Zero forcing detection methods are used for various types of chaotic maps like tent map and Boss map; So, in conclusion out of both MMSE and Zero forcing detection method, BER performance of MMSE detection method shows superior result than Zero forcing method for all three chaotic map in chaos communication system. In MMSE detection method pseudo Inverse considers estimation matrix as well as noise unless like Zero forcing whose pseudo inverse considers only estimation matrix.

In this paper BER performance for 2x2 MIMO for both MMSE and Zero forcing is evaluated using CDSK modulation for tent map and boss map in which boss map shows better result than the tent map in Rayleigh fading channel.
In this paper 2x2 MIMO, 4x4 MIMO and 8x8 MIMO BER performance is compared for each chaos map with both detection showing result as 8x8 MIMO shows better result than 4x4 MIMO and 4x4 MIMO shows better result than 2x2 MIMO for MMSE detection with Boss map in Rayleigh fading channel.
For future scope, work can be further carried out for various chaos maps in different channel models for betterment of system's performance.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 6, June 2015

REFERENCES

1. L.S.Tsimring ,M.Suschik and A.R Volkovskii 'Analysis on performance of correlation-based communication schemes using chaos and 'circuits and.Fundamental theory and applications, in IEEE transactions in vol.47 and number 12 and pp.1684-1691, on dec.2000.
2. Sung II Hong and Eun young Jang 'Chaotic signal in implementation of FPGA in digital transceiver' in Korea institute of information technology review in volume 8, number 8 and pp.9-15 in august.2010'.
3. Q. Ding and J.N Wang 'Frequency-modulated correlation delay shift keying (FM-CDSK) design in chaotic communication system' in Communications, IET, Volume 5 and number 7 and pp.901-905, in May 2011.
4. Zhang Dianlun, Cheng YiPing and Shi Ying and,'Differential chaos shift keying (DCSK) performance over common channels' in (ICFCC) Future computer and communication, in 2010's 2nd International Conference on volume 2 and pp.755-759, in May 2010.
5. Junyeong Bok, Suwa Kim and Heung-GyoonRyu,'Evaluation of DCSK system performance using chaotic maps' in(ICOIN) Information Networking, International conference ,2013 in pp.556-559, in Jan.2013.
6. Nishio and S. Arai Y, 'Choosing different chaotic maps for Non coherent correlation based communication systems' in Proc. IEEE International Symposium on Circuits and systems in New Orleans in USA and pp.1433-1436 on June 2007.
7.Junyeong Bok and Heung-GyoonRyu,'CDSK modulation based digital chaotic communication system' in the Journal of the Korean Institute of communications and Information Sciences in volume 38A, number 6 and pp.479-485, on June 2013.
8. Jun-Hyun Lee and Heung-GyoonRyu in Yeosu ,'CDSK based chaotic communication system using new chaos maps' on 'The 28th International Technical Conference on Circuits and system, computers and communication (ITC-CSCC in 2013) in Korea, in pp.775-778, on July 2013.
9. M.A. Ben Farah and A. Kachouri ,M. Samet,'DCSK chaotic modulation used for designing secure digital communication system' in Design and test of Integrated systems in nanoscale technology in DTIS 2006, International Conference on , in pp.200-204, on sept.2006.
10. Jun-Hyun Lee and Heung-GyoonRyu,'DCSK and CDSK modulation method used in chaos communications system for Anti jamming performance' in the journal of Korean Institute of Electromagnetic Engineering and Science in volume 24,number 4 and pp.417-425, on April 2013.
11. G.Kaddoum and F.Gagnon,Mai Vu,' analyzing performance of (CSK) chaos shift keying in MIMO communications systems' in Wireless Communications and networking Conference (WCNC), IEEE in pp. 1432-1437, on March.
12. Dian-Wu Yue and K.Q.T Zhang,'Transmission method by using Wireless MIMO systems in fading environments' in Wireless Communications, Networking and Mobile Computing (WiCOM) in 8th International Conference on pp.1-8, on September 2012.

BIOGRAPHY

Hegde Pooja V., 4th Semester, M.Tech, Communication system, Department of Electronics and Communication, New Horizon College of Engineering, Outer Ring Road, Marathalli, Bengaluru, India.

SusmithaAlamuru, Assistant Professor , Project Guide, Department of Electronics and Communication, , New Horizon College of Engineering, Outer Ring Road, Marathalli, Bengaluru, India.