2012 International Conference on Radar, Communication and Computing (ICRCC), SKP Engineering College, Tiruvannamalai, TN., India. 21 - 22 December, 2012. pp.1-5.

BER Performance Improvement for Secure Wireless Communication Systems based on CSK- STBC Techniques

Lwaa Faisal Abdulameer[1], D. Jokhakar Jignesh[2], U. Sripati[3] and Murlidhar Kulkarni[4]

Abstract— **There has been a growing interest in the use of chaotic techniques for enabling secure communication in recent years. This need has been motivated by the emergence of a number of wireless services which require the channel to provide very low bit error rates (BER) along with information security. This paper investigates the feasibility of using chaotic communications over Multiple-Input Multiple-Output (MIMO) channels by combining chaos modulation with a suitable Space Time Block Code (STBC). It is well known that the use of Chaotic Modulation techniques can enhance communication security. However, the performance of systems using Chaos modulation has been observed to be inferior in BER performance as compared to conventional communication schemes. In order to overcome this limitation, we have proposed the use of a combination of Chaotic modulation and Alamouti Space Time Block Code. We have studied the performance of Chaos Shift Keying (CSK) with 2×1 Alamouti scheme for different chaotic maps over Additive White Gaussian Noise (AWGN) and Rayleigh fading channels. Our simulations indicate that the use of the Alamouti schemes can allow service providers to enhance security without degrading the BER performance while communicating over these channels.**

Keywords— **CSK, chaotic techniques, MIMO.**

I. INTRODUCTION

Recently, there has been growing interest in the use of chaotic techniques for enabling secure communication [1,2]. It has been demonstrated that even one dimensional discrete chaotic system is able to provide a high level of security [3]. It is well known that maintaining information security on wireless channels is a challenging task. This is because with suitable receivers, anybody can intercept information from wireless transmission in the local area. In addition, it is difficult to discover such interceptions. So, security of wireless transmission is very important. Chaotic signals can be used in secure communications due to their wideband property and sensitive dependence on initial conditions. The use of CSK provides strong resistance against interception and capture for longer period of time. So, it is said that wireless communication method based on chaotic system is robust and secure [4,5]. Various methods for chaos-based secure transmission of private information signals have been proposed by several authors; see [6], [7], [8], [9]. In these schemes, a chaos generator is used to generate chaos shift keying (CSK) sequences, where different sequences can be generated using the same generator but with different initial conditions [10]. Over the past decade, the problem of synchronization of chaotic systems and their potential application in securing communication has received a lot of attention. In [11] Carroll and Pecora have proposed a method to synchronize two identical chaotic systems. In this paper, we assume that our systems can correctly achieve the synchronization proposed in [12]. We have studied the performance of the CSK scheme over channels perturbed by Rayleigh distribution because Rayleigh fading channel is widely accepted as a realistic model for understanding the behavior of for RF wireless links. Highly secure communication links with an optimum bit-error rate (BER) performance are required to protect information integrity against channel induced impairments and criminal activity directed at wireless communication systems and [10]. Many researchers have studied the BER performance of the chaos based communication system for the Single Input Single Output (SISO) channels [13]. It is now well established that exploitation of channel diversity via the use of Multi-Input-Multi-Output (MIMO) techniques channel utilizing multiple antennas is an optimum method to combat fading in wireless communications [14]. Motivated by these considerations, we have investigated the feasibility of employing chaotic techniques to enhance information security in MIMO channels by implementing space-time coding schemes combined with CSK modulation. Because of the non periodic nature of chaotic signals, it is certainly the case that after passing through the chaotic modulator, the transmitted bit energy varies from one bit to another. However, most papers compute the BER performance by considering the bit energy as constant. This approximation, which is widely known as the Gaussian approximation (GA), suffers from a low

[1] Ph.D Research Scholar, E&C dept., NITK., Mangalore, India. Email: lwaa@kecbu.uobaghdad.edu.iq
[2] M. Tech (Research), E&C dept., NITK., Mangalore, India., jokhakarjignesh@gmail.com
[3] Associate Prof., E&C dept., NITK, Mangalore, India. Email: sripati_acharya@yahoo.co.in
[4] Prof., E&C dept., NITK., Mangalore, India. Email: mkulkarni@nitk.ac.in

978-1-4673-2758-9/12/$31.00 ©2012 IEEE

precision when the spreading factor is low. Another approach integrates the BER expression for a given chaotic map over all possible spreading sequences of a given spreading factor. This latter method when compared with the BER computation under the Gaussian assumption, gives more accurate results, but suffers from high computation complexity. Another accurate computation is the exact BER performance for coherent and non coherent chaos based communication systems. The idea of this approach, is to first compute the probability density function (PDF) of the bit energy, and then use use the computed PDF to compute the BER expression [15, 16, 17]. Recently, a MIMO system has been proposed for CSK system. In their paper, they show the design of the CSK-MIMO system for 2×2 Alamouti scheme for Chebyshev map under additive white Gaussian noise (AWGN).

II. CHAOTIC GENERATORS

These maps are chosen because of the simplicity in terms of generating chaotic sequences. Here we will illustrate the dynamics of these maps.

A. Tent map

The mapping has a constant coefficient p, referred to as the peak value. This is the point at which the mapping reaches its maximum output value, shown at $x_n = p = 0.5$ in fig. (1). Above and below this value the fraction decreases linearly to reach to zero at $x_n = 0$ and $x_n = 1$.[19]

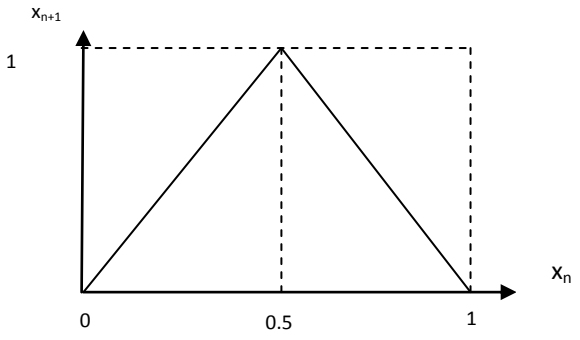

Fig. 1. Piecewise linear one-dimensional chaotic tent map

The dynamic of the tent map is obtained as shown in equation (1).

$$x_{n+1} = \begin{cases} \frac{x_n}{p} \ mod1 \ \ if \ \ x_n \le p \\ \frac{1-x_n}{1-p} \ \ mod1 \ \ if \ \ x_n > p \end{cases} \quad (1)$$

B. Logistic map

It is defined as follows

$$x_{n+1} = F\{x_n\} = p x_n[1 - x_n] \quad (2)$$

C. Bernoulli map

$$x_{n+1} = 2x_n mod1 \quad (3)$$

D. Chebyshev map

Its dynamic described as [13],

$$x_{n+1} = 1 - 2x_n^2 \quad (4)$$

In equations (1, 2, 3 and 4) x_n and x_{n+1} represent the current and next symbols of the chaotic sequence respectively. In equations (1 and 2) p represents the control parameter.

III. CHAOS SHIFT KEYING (CSK)

In CSK communication system the signal $\mathbf{x(t)}$ is first generated by one of the chaotic maps defined in section (II). If a $"+1"$ is transmitted, the chaotic signal will be sent. If $"-1"$ is transmitted, an inverted copy of the chaotic signal is used as the transmitted signal. Hence the transmitted signal can be expressed as,

$$s(t) = \begin{cases} x_k, & \text{when symbol "-1"is transmitted} \\ -x_k, & \text{when symbol "-1"is transmitted} \end{cases} \quad (5)$$

Consider the data information symbols $(s_l = \pm 1)$ with period $\mathbf{T_s}$ are separated by a chaotic sample (or chip) is generated at every time interval equal to $\mathbf{T_c}(x_k = x(kT_C))$. The emitted signal at the output of the transmitter is:

$$u(t) = \sum_{l=0}^{\infty} \sum_{k=0}^{\beta-1} s_l x_{l\beta+k} \quad (6)$$

Where the spreading factor β is equal to the number of chaotic samples in symbol duration $(\beta = \frac{T_s}{T_c})$; for the AWGN channel, the received signal is,

$$r(t) = u(t) + n(t) \quad (7)$$

Where $\mathbf{n(t)}$ is the AWGN with zero mean and power spectral density equal to $N_0/2$. In order to demodulate the transmitted bits, the received signal is first despreaded by the local chaotic sequence, and then integrated on a symbol duration $\mathbf{T_s}$. Finally, the transmitted bits are estimated by computing the sign of the decision variable at the output of correlator.

$$Ds_l = sign\ (s_l T_c \sum_{k=0}^{\beta-1} (x_{l\beta+k})^2 + w_l)$$
$$= sign(s_l E_b^{(l)} + w_l \quad (8)$$

Where $\mathbf{sign(.)}$ is the sign operator, $E_b^{(l)}$ is the bit energy of the l^{th} bit and w_l is the noise after despreading and integration.

IV. CSK-2×1 ALAMOUTI SCHEME USING ALAMOUTI SPACE TIME CODE

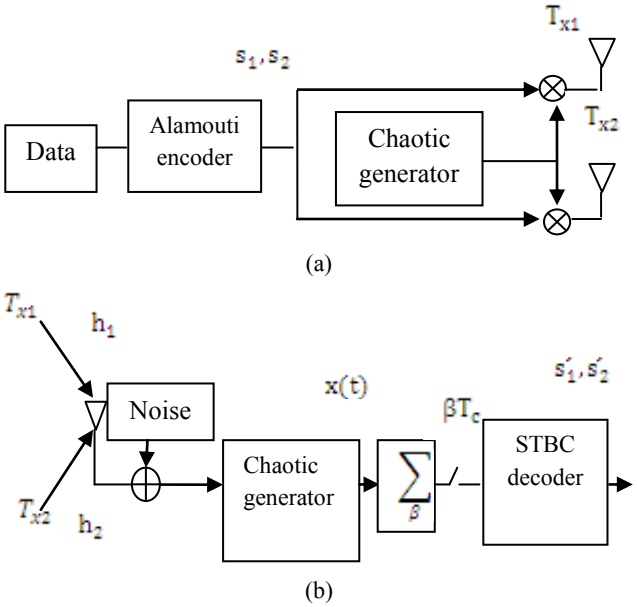

Fig. 2. CSK-MIMO transmitter with two antennas, b- receiver with one antennas

The Alamouti matrix for symbol s_1 and s_2 is

$$\begin{pmatrix} s_1 & -s_2^* \\ s_2 & s_1^* \end{pmatrix} \tag{9}$$

Table I. The design of the transmitted signal

Time	$s_1(t)$ from T_{x1}	$s_2(t)$ from T_{x2}
$[0, \beta T_c]$	$s_1 x_k$	$s_2 x_k$
$[\beta T_c, 2\beta T_c]$	$-s_2^* x_{k+\beta}$	$s_1^* x_{k+\beta}$

The energy of a given bit l is $E_b^{(l)} = \sum_{k=1}^{\delta} x_k^{(l)2}$.

Table II. The received signal of the 2×1 Alamouti

Time	*Received signal*
$[0, \beta T_c]$	$h_1 s_1 x_k + h_2 s_2 x_k + n_k^1$
$[\beta T_c, 2\beta T_c]$	$-h_1 s_2^* x_{k+\beta} + h_2 s_1^* x_{k+\beta} + n_k^2$

Table III. The equivalent baseband model of the received symbol

Time	*The equivalent baseband model of the received symbol*
$[0, \beta T_c]$	$Y_1 = E_b(h_1 s_1 + h_2 s_2) + N_1$
$[\beta T_c, 2\beta T_c]$	$Y_2 = E_b(-h_1 s_2^* + h_2 s_1^*) + N_2$

Where N_1 and N_2 represent noise components while h_1 and h_2 represent the channel gains.

Where h_{11}, h_{21}, h_{12} and h_{22} are the channel gains. These equations are derived in [13].

The channel model can be written as

$$Y = E_b HS + N \tag{10}$$

The transmitted bits are estimated by multiplying the signal Y by the conjugate transpose of the channel H:

$$\begin{pmatrix} D_{s1} \\ D_{s2} \end{pmatrix} = H^* Y \tag{11}$$

Again, justification of this equation is provided in [13].

The estimated bits are computed from the sign of the decision variables,

$$s_1' = \text{sign}\, D_{s1}; \quad \acute{s}_2 = \text{sign}\, D_{s2} \tag{12}$$

V. PERFORMANCE ANALYSIS

The main objective of this paper is to study the performance of the CSK-MIMO system under channels perturbed by AWGN and Rayleigh fading channels. The channel gains for 2×1 Alamouti is constant under the AWGN assumption. The overall BER expression of the CSK-MIMO system for 2×1 Alamouti is given in (13) [15, 16, 17].

For 2×1 Alamouti, the BER expression is given by

$$BER = \int_0^{\infty} \frac{1}{2} \text{erfc}\left(\sqrt{\frac{(h_1^2 + h_2^2)E_b^{(l)}}{N_0}}\right) p\left(E_b^{(l)}\right) dE_b^{(l)} \tag{13}$$

Where $p\left(E_b^{(l)}\right)$ is the probability density function of the energy $E_b^{(l)}$. The BER expression is the result of the integral given in equations (13). To compute the integral in (13) , we must first have the bit energy distribution. Since the PDF seems to be intractable, the only way to evaluate the BER is to compute the histogram of the bit energy followed by a numerical integration. Fig. (3) shows the histogram of the bit energy, for spreading factor β=4 and 50000 samples.

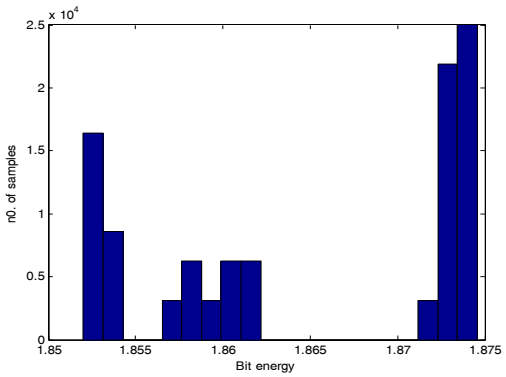

Fig. 3. Histogram of the bit energy

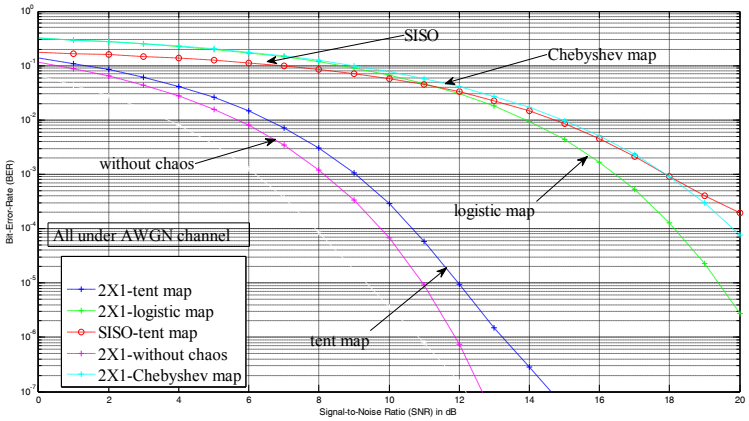

Fig. 4. BER of 2×1 Alamouti for various types of chaotic maps under AWGN channel

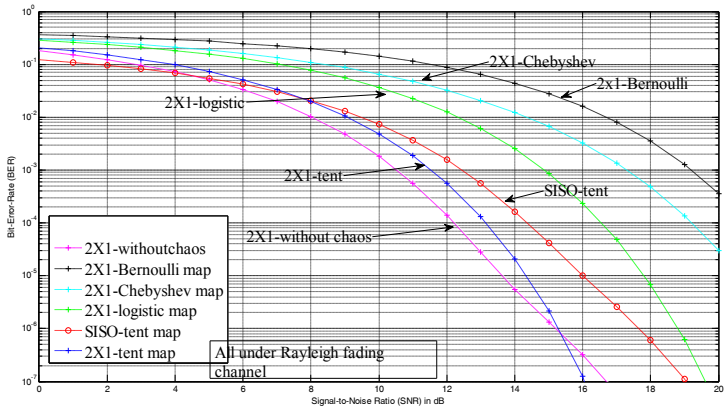

Fig. 5. BER of 2×1 Alamouti for various types of chaotic maps under Rayleigh fading channel

The equations (8 and 9) have been explained in [13,15,16,17].

After numerical integration the BER expression for 2×1 Alamouti is given by,

$$BER = \sum_{l=1}^{m} \frac{1}{2} \operatorname{erfc}\left(\sqrt{\frac{(h_1^2+h_2^2)E_b^{(l)}}{N_0}}\right) p\left(E_b^{(l)}\right) \qquad (9)$$

Where m is the number of histogram classes and $p\left(E_b^{(l)}\right)$ is the probability of having the energy in interval centered on $E_b^{(l)}$.

VI. Simulations

In fig. (4) we have compared the performance of different chaotic maps described in section (II) under AWGN. The channel gain is constant and equal to 1, β=4 and $T_c = 1$. Our simulations indicate that the tent map gives best performance when compared to other chaotic maps. Hence, the use of tent map is preferred over other maps because it offers superior BER performance in addition to security. Additionally, our simulation results indicate that the use of 2×1 Alamouti scheme provides a gain of 8 dB as compared to SISO when both schemes employ chaotic techniques up to a BER of 10^{-3}. From fig 4 it can be seen that up to a BER of 10^{-5}, chaos systems maintain nearly the same BER performance as BPSK without using chaos. (A difference of 0.75 dB at difference at a of 10^{-5} is observed) Additionally they provide security against eavesdroppers. Therefore, this technique provides additional security while maintaining a BER of 10^{-5}. It is observed in fig. (5) that under Rayleigh fading conditions, tent map gives the best BER performance as compared to other maps. An 2×1 Alamouti scheme gives 2 dB gain in BER performance as compared to SISO with CSK. This improvement is realized with only a marginal increase in computational complexity at the transmitter and receiver.

VII. Conclusion

The BER performance of 2×2 Alamouti and 2×1 Alamouti schemes combined with CSK for different chaotic maps under different fading channel conditions have been computed and plotted. These schemes give the benefit of providing additional security while maintaining

BER performance at levels similar to that obtained by the use of simple BPSK alone.

REFERENCES

[1] D. Frey, "Chaotic digital encoding: an approach to secure communication", IEEE Transaction of Circuits and Systems: Analog and Digital Signal Processing, Vol. 40, No. 10, pp. 660-666,1993.

[2] M. Itoh, H.Murakami and L. O. Chua, "Secure communication systems via Yamakawa's chaotic chips and Chua's circuits", Proceedings of Third IEEE Conference on Computational Intelligence, 1293-1296. , June 1994, pp.

[3] H. Zhou, x. Ting and J. Yu, "Secure communication via one-SD-dimensional chaotic inverse systems", IEEE International Symposium on Circuits and Systems, Hong Kong., pp. 1029-1032 , 1997.

[4] L. Jie, C. Tao, H. Jinghua, Z. Yinghai and W. Yuexin, , "Chaos-shift-keying secure signal communications using feedback to synchronize Chua's circuit :simulation and realization", IEEE, p.p. 552-554, 1996.

[5] Z. Dai, B. Wang and P. Li, "Wireless secure communication systems design based on chaotic synchronization", IEEE, International Conference on Communication Technology, 2006.

[6] Y. Seng and Z. M. Hussain, , "A New approach in chaos shift keying for secure communication", IEEE Proceedings of the Third International Conference on Information Technology and Applications (ICITA'05), 2005.

[7] J. Lee, C. Lee and D. B. Williams, "Secure communication using chaos", IEEE, Global Telecommunication Conference, pp. 1183-`1187, 1995.

[8] Z. Li, K. Li, C. Wen and Y. Soh, "A new chaotic communication system", IEEE Transaction on Communication, Vol. 51, No.8, 2003.

[9] G. Tang et al, , "A secure communication scheme based on symbolic dynamics", IEEE, International Conference on Communication, Circuits and Systems, p.p. 13-17, 2004.

[10] Y. Lau, K. H. Lin and Z. M. Hussain, "Space-time encoded secure chaos communications with transmit beamforming", IEEE, TENCON, 2005.

[11] L. Pecora and T. Carroll, "Synchronization in chaotic systems", Physical Review Letters Vol. 64, No. 8. 1990.

[12] G. Kaddoum, D. Roviras, P. Charg´e, and D. Fournier Prunaret, "Robust synchronization for asynchronous multi-user chaos-based DS-CDMA," Elsevier Signal Process, vol. 89, pp. 807–818, 2009.

[13] G. Kaddoum, M. Vu and F. Gagnon, "On the performance of chaos shift keying in MIMO communications systems", IEEE WCNC-PHY, pp. 1432-1437, 2011.

[14] H. Ma and H. Kan, "Space-time coding and processing with differential chaos shift keying scheme", IEEE, Communication Society, 2009.

[15] G. Kaddoum, P. Charge and D. Roviras, "A generalized methodology for bit-Error-rate rrediction in correlation-based communication schemes using chaos", IEEE Communication Letters, Vol. 13, No. 8. , 2009.

[16] G. Kaddoum, P. Charge, D. Roviras and D. Pruntaret, "A methodology for bit error rate prediction in chaos-based communication systems", Circuits System Signal Process, 2009.

[17] W. M. Wai, F. C. Lau, C. K. Tse and A. J. Lawrance, "Exact analytical bit error rates for multiple access chaos-based communication systems", IEEE Transactions on Circuits and Systems, Vol. 51, No. 9. 2004.

[18] A. Mozsary, L. Azzinari, K. Krol and V. Porra, "Theoretical connection between PN-sequences and chaos makes simple FPGA pseudo-chaos sources possible", IEEE International Conference on Electronics, Circuits and Systems, 2001.

[19] A. Awad, S. El-Assad, W. QianxueC. Vladeanu and B. Bakhachi , "Comparative study of 1-D chaotic generator for digital data encryption", IAENG International Journal of Computer Science, 2008.