INVESTIGATION ON ORTHOGONAL SIGNALS FOR SECURE TRANSMISSION IN MULTIUSER COMMUNICATION SYSTEMS

Gobindar S. Sandhu and Stevan M. Berber
Department of Electrical and Computer Engineering, School of Engineering, University of Auckland
38 Princes Street, Auckland City, Auckland, New Zealand.
Email: gsan020@ec.auckland.ac.nz, s.berber@auckland.ac.nz

Abstract

In this paper the results of investigating various orthogonal signals that can be used as the carriers of users' information in a multiuser communication system are presented, primarily chaotic signals, wavelets, human body signals generated and classical orthogonal sequences like Walsh functions. In particular, the system that uses a combination of these investigated signals is analyzed in the presence of noise, fading and jamming. It was shown that a secure system can be designed that is based on the investigated signals and their combinations. For this purpose a theoretical model of communication systems is developed and then simulated and the results of simulation are presented and discussed. The aim of the research, to investigate possibility of development a secure multiuser system that is resistant to interception, interference and jamming, has been achieved.

1. Introduction

Multiuser communication systems are traditionally based on exploitation of the orthogonal characteristics of pseudorandom sequences like Walsh functions and variable-length orthogonal codes that are used in the 2nd and 3rd generation code division multiple access (CDMA) systems, respectively [1]. The number of these sequences is limited that in turn limits the network's capacity. It is a quite simple task to take out the users' information by dispreading the transmitted sequence. For these reasons there is on-going research that is focused on inventing new types of signals that have good orthogonality characteristics and are not limited in numbers.

The application of chaotic signals in communications was possible from the time when it was discovered that the electronic circuits exhibit chaotic behavior [2]. This discovery was supported by Pecora's and Carroll's discovery that two chaotic signals can be synchronized under appropriate driving conditions [2, 3]. Also, it was shown that the chaotic signals have extremely good autocorrelation and crosscorrelation characteristics and have a noise like spectral density that may be used to increase the security of the systems they are implemented in [2, 4-7]. A detailed analysis of such systems is presented in [8]. The importance of analyzing these systems is in their ability to be used in cryptography. Extensive work has been done in this field as can be seen from [9, 10].

Searching for the signals that can be used as carriers like chaotic signals or wavelets [11], led us to investigate some signals generated in human's body. Preliminary results for the possible use of these signals are presented .

The research presented in this paper goes beyond a simple application of chaotic signals generated from a single generator. Complex systems, that use a mixture of chaotic signals from different generators or a mixture of these signals and classical orthogonal sequences, like Walsh functions, are investigated and compared. It was shown that the combination of different chaotic signals or the combination of these signals and classical spreading sequences can be used as the carriers in the same multiuser system. This property may lead to the development of secure and jamming resistant systems.

The paper is organized as follows. In Section 2, a general model of a multiuser chaos-based communication system is analyzed. The BER characteristics of a chaotic phase shift keying (CPSK) scheme are investigated. Various generators, based on different mapping algorithms, are implemented in the simulator. Using a mixture of these generators and initial conditions, various modulation schemes are investigated with the aim to enhance the security of the communication system.

In Section 3 the characteristics of chaotic systems are investigated as a function of the number of users, level of the noise and fading. The interleaving technique is used to reduce the fading influence and enhance the security of the communication system. In Section 4 the characteristics of chaotic systems are investigated when jamming signals are present. The effect of interleaving techniques on BER characteristics of the system was investigated.

In Section 5, the implementation of convolutional codes, for reducing the BER, in considered. In Section 6 the characteristics of signals obtained by measurements on human's body, primarily brain signals, are investigated in order to estimate their applicability as the carriers of information in multiuser systems. It is shown that these signals may be used as the carriers of users' information.

2. Probability of error in the presence of white Gaussian noise in the system

The basic structure of the investigated multiuser system is shown in Figure 1. The transmitter generates a multiuser signal that is obtained by modulating the users' information bits $\gamma_j^{(g)}$ by orthogonal signals $x_t^{(g)}$, g = 1, 2, …, N. After transmission through a channel that is generally characterized by the presence of noise, fading and jamming signals, the received signal is processed by a bank of correlators that produce the estimates of user's information at their outputs $\tilde{\gamma}_j^{(g)}$, g = 1, 2, …, N. In the case when only the additive white Gaussian noise is present in the channel, the output of the g^{th} correlator is given by

$$z_1^{(g)} = \sum_{t=1}^{2\beta} s_t^{(g)} \cdot x_t^{(g)} + \sum_{n=1, n\neq g}^{N} \sum_{t=1}^{2\beta} s_t^{(n)} \cdot x_t^{(g)} + \sum_{t=1}^{2\beta} \xi_t \cdot x_t^{(g)}, \quad (1)$$

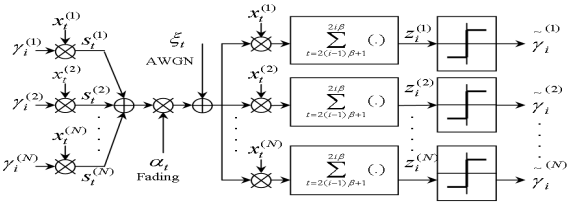

Figure 1. Basic structure of a chaotic communication system.

where the first term is the g^{th} user's transmitted signal, the second term is the inter-user interference, and the third term is the white noise. Using (1) and the fact that the chaotic sequences generated by different initial conditions are mutually independent to each other, the mean and variance of the correlator's output $z_1^{(g)}$, given that the g$^{\text{th}}$ user's transmitted bit is +1 and users have equal average transmit power P_s, is

$$E[z^{(g)} \mid \gamma^{(g)} = +1] = 2\beta P_s \quad (2)$$

$$\text{var}[z_1^{(g)} \mid (\gamma_1^{(g)} = +1)] = 2\beta \,\text{var}[(x_t^{(g)})^2] + \beta N_o P_s + 2\beta \cdot (N-1) P_s^2 \quad (3)$$

The bit error rate (BER), denoted by $p^{(g)}$, can be calculated as [3]

$$p^{(g)} = \frac{1}{2} p\left(z^{(g)} \le 0 \mid \gamma^{(g)} = +1\right) + \frac{1}{2} p\left(z^{(g)} > 0 \mid \gamma^{(g)} = -1\right) = \frac{1}{2}\text{erfc} \frac{E[z^{(g)} \mid \gamma^{(g)} = +1]}{\sqrt{2 \cdot \text{var}[z^{(g)} \mid \gamma^{(g)} = +1]}} \quad (4)$$

where the *error complimentary function,* erfc(.), is defined as in [3].

Substituting (2) and (3) into (4), and the fact that $E_b = 2\beta P_s$ gives

$$p^{(g)} = \frac{1}{2} erfc\left(\left[\frac{\Psi}{\beta} + \frac{(N-1)}{\beta} + \left(\frac{E_b}{N_o}\right)^{-1}\right]^{-\frac{1}{2}}\right), \quad (5)$$

where $\Psi = \text{var}[(x_t^{(g)})^2] / E^2[(x_t^{(g)})^2]$ represents time domain characteristics of the chaotic signal. The results of the CPSK scheme using the cubic map for 1, 2 and 4 users and the spreading factor of 2β = 100, are shown in Figure 2. The BER curve for chaos shift keying (CSK) [7] is also plotted for comparison. The number of errors is controlled in such way to achieve the confidence of probability of error estimation to be 99% for each measurement.

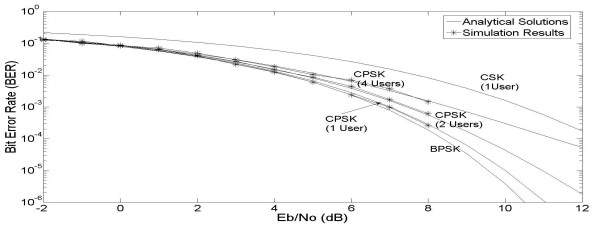

Figure 2. BER for 1, 2 and 4 user CPSK system.

As we expected the BER deteriorates when the number of users increases. However, for the proposed CPSK scheme, the BER is better than for the CSK scheme. In particular we investigated two cases with mixed carriers. Firstly we investigated a case when two chaotic generators, based on cubic and logistic maps [7] are used to transmit messages for 4 users (i.e. two users for each map). The theoretical curve of the probability of error for the 4 users, same map case and the BER curves for the mixed map case are plotted in Figure 3. The curves overlap each other, which means it is possible for the system to accommodate users with different generators. Thus, the security will be enhanced.

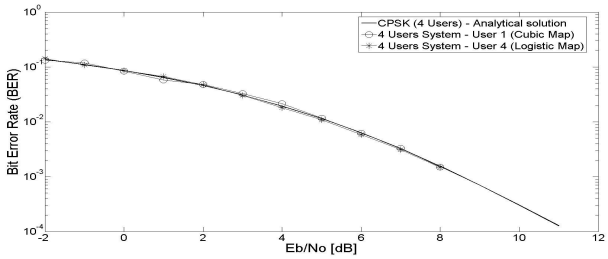

Figure 3. BER for system with mixture of cubic and logistic signals.

Secondly we investigated a case when one chaotic generator, based on cubic map, is used to transmit messages of 2 users, and the Walsh signals were used to transmit messages of the remaining 2 users. Similar to Figure 3, the theoretical curve of the probability of error for the 4 users, same map case and the BER curves for the mixed map case (i.e. Walsh and cubic signals) are plotted in Figure 4.

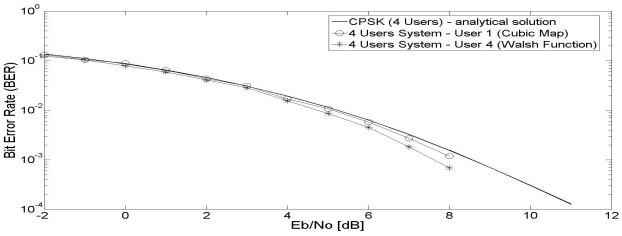

Figure 4. BER for system with mixture of cubic and Walsh signals

The curves show that the user's separation in the case when we use mixture of signals is better than in the case of only one chaotic generator. This is due to the use of Walsh signals that cross-correlate nicely with the chaotic sequences. Thus, in the existing systems based on application of Walsh signals we can incorporate some channels that will use chaotic signals that will enhance the security in message transmission.

3. Probability of error in the presence of fading

In the previous section, the performance of CPSK in the presence of the white Gaussian noise is investigated. However, in reality, there is another kind of impairment, called *Rayleigh* fading [12]. The fading has the effect of replacing the received symbol energy E_b with a^2E_b [12]. Thus the probability of error, in expression (5) can now be expressed as

$$p^{(g)}(a)=\frac{1}{2}erfc\left(\left[\frac{\Psi+N-1}{\beta}+\left(\frac{a^2E_b}{N_o}\right)^{-1}\right]^{-\frac{1}{2}}\right) \qquad (6)$$

This is a function of a new variable 'a' that has a Rayleigh distributed density function defined as [12]

$$p(a)=\frac{2a}{b}e^{-a^2/b}\ ,\ a\geq 0, \qquad (7)$$

where b is the mean square value of the Rayleigh random variable **a**, i.e., $b = E\{\mathbf{a}^2\}$. Since expression (6) is a function of variable a, the error probability in Rayleigh channel $P^{(g)}$ should be obtained by averaging this function, i.e.,

$$P^{(g)}=\int_0^\infty p^{(g)}(a)\cdot p(a)da=\int_0^\infty\frac{a}{b}erfc\left(\left[\frac{\Psi+N-1}{\beta}+\left(\frac{a^2E_b}{N_o}\right)^{-1}\right]^{-\frac{1}{2}}\right)\cdot e^{-a^2/b}da \qquad (8)$$

For our simulation we generated a Rayleigh fade by passing two independent white Gaussian noise samples with a power density of $N_0/2$ through low-pass filters [13] having the following frequency response $H(f)$. The in-phase and quadrature components $S_{rI}(t)$ and $S_{rQ}(t)$ are the PSDs for $r_I(t)$ and $r_Q(t)$, respectively, expressed as

$$S_{r_I}(f)=S_{r_Q}(f)=\frac{N_0}{2}|H(f)|^2 \qquad (9)$$

For our model, the spectral density of the complex envelope of the received signal is chosen to be [14]

$$S(f)=\begin{cases}\dfrac{b}{4\pi f_D}\dfrac{1}{\sqrt{1-(f/f_D)^2}} & |f|\leq f_D\\ 0 & else\end{cases} \qquad (10)$$

where $f_D = v/\lambda_c$ is the ratio of velocity to signal wavelength and also called the Doppler frequency, and b the average power of the fade. In this simulator, 100 errors are required instead of 35 due to the expected increase in bit error rate and bursty nature of the error sequence (i.e., fewer bits will need to transmit for the occurrences of same number of errors). Additional parameters are firstly, the Doppler frequency, which is set to 45.8 *Hz*. This corresponds to a mobile vehicle in motion at a speed of 55 *km/h*, with the carrier frequency set to 900 *MHz*.

Simulations conducted for three different average fade power (b) 0.1, 0.5 and 1, showed that as the average power of the received signal's envelope decreases, the BER increases quite rapidly, as was reported in [15]. To achieve a BER of 10^{-2}, the CPSK system operating in Rayleigh fading channel, with average fade power of 1, requires a E_b/N_o ratio of approximately 13.5 dB [15]. This is a huge degradation compared to the 5 dB required for the white Gaussian noise case.

The curve from [15] for the fade power of 1 is repeated in Figure 5 alongside with the theoretical curve obtained according to the expression (8). The result is obviously disappointing showing significant influence of fading on BER degradation. In order to improve these characteristics we investigated the case when an interleaver is used to "spread" and "outspread" the chip sequence in time domain. In that way the burst of degraded chips were spread before the demodulation and significant improvements, being enormous, are achieved. The results for simple block interleavers are shown in Figure 5 for the following interleaver sizes: 20x20, 50x50, 100x100 and 1000x1000.

This interleaving technique improves BER characteristics and, also, can be used as additional measure to enhance security of the communication system. Namely, the interleaving law can introduce a new randomness in the message signal transmitted that is known only to the system designer and system user.

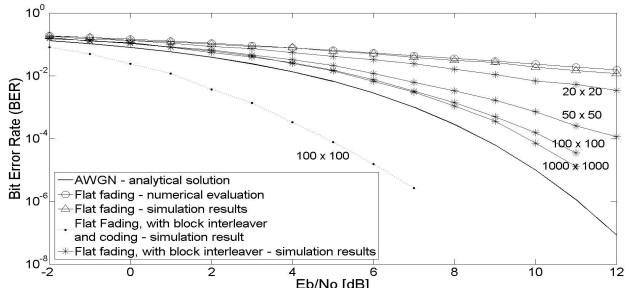

Figure 5. BER curves in the presence of fading for various interleaver sizes

However, the drawback is that these interleavers introduce delays due to the additional signal processing. Thus, future research will include further search for a simpler and more efficient interleaving scheme to be used with the clear intention to achieve the BER curve as close as possible to the curve obtained in AWGN channel.

4. Probability of error in the presence of jamming signals

The expression for the probability of error in the presence of slowly and fast switching jammers are derived and presented in [15] for the case when only AWGN is present in the channel. In the case when fading is present in the channel the expression for a slowly switching wideband jammer is given by

$$BER_{ss}=\frac{\varphi}{2}erfc\left(\left[\frac{\Psi+N-1}{\beta}+\frac{P_{jam}}{\varphi\beta P_s}+\frac{N_o}{a^2E_b}\right]^{\frac{1}{2}}\right)+\frac{1-\varphi}{2}erfc\left(\left[\frac{\Psi+N-1}{\beta}+\frac{N_o}{a^2E_b}\right]^{\frac{1}{2}}\right) \tag{11}$$

and for fast switching wideband jammer by

$$BER_{fs}=\frac{1}{2}erfc\left(\left[\frac{\Psi}{\beta}+\frac{(N-1)}{\beta}+\frac{P_{jam}}{\beta P_s}+\frac{N_o}{a^2E_b}\right]^{\frac{1}{2}}\right) \tag{12}$$

where P_{jam} denotes the average power of the jamming signal and φ is the duty cycle of the jammer. In the case of fading the probability of error $P^{(g)}$ for a slowly switching wideband jammer may be expressed as

$$P^{(g)}=\int_0^\infty p^{(g)}(a)\cdot p(a)da=\int_0^\infty\frac{\varphi a}{b}erfc\left(\left[\frac{\Psi+N-1}{\beta}+\frac{P_{jam}}{\varphi\beta P_s}+\frac{N_o}{a^2E_b}\right]^{\frac{1}{2}}\right)\cdot e^{-a^2/b}da$$
$$+\int_0^\infty\frac{(1-\varphi)a}{b}erfc\left(\left[\frac{\Psi+N-1}{\beta}+\frac{N_o}{a^2E_b}\right]^{\frac{1}{2}}\right)\cdot e^{-a^2/b}da \tag{13}$$

and for a fast switching jammer is

$$P^{(g)}=\int_0^\infty p^{(g)}(a)\cdot p(a)da$$
$$=\int_0^\infty\frac{\varphi a}{b}erfc\left(\left[\frac{\Psi}{\beta}+\frac{(N-1)}{\beta}+\frac{P_{jam}}{\beta P_s}+\frac{N_o}{a^2E_b}\right]^{\frac{1}{2}}\right)\cdot e^{-a^2/b}da \tag{14}$$

We tried to investigate possibilities to reduce the influence of jammers by interleaving/deinterleaving procedure. The results, for interleaver size of 100x100 and spreading factor of 100, are shown in Figure 6 and 7 for the fast and slow switching jammers, respectively.

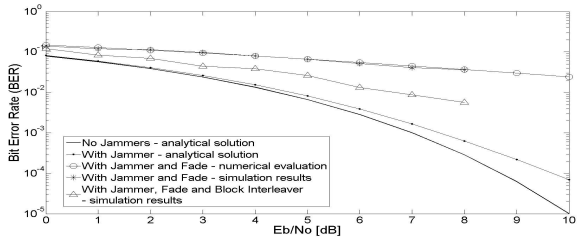

Figure 6. BER for slow-switching jammer, fading, and interleaving (duty factor σ=0.5).

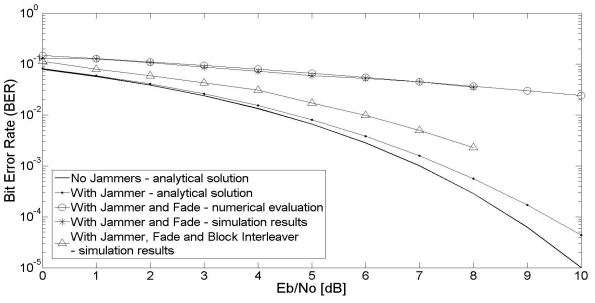

Figure 7. BER plot for fast-switching jammer, fading, and interleaving (duty factor σ=0.5).

By observing these 2 figures, it is clear that the interleaving procedure can reduce the BER. In order to further improve BER characteristics, error control coding schemes can be used. Our results related to the use of the Viterbi algorithm are shown in the following section.

5. Error Control Coding implementations

The BER characteristics of a CPSK signal are deteriorated in the case when fading or jamming signal exists in the communication channel. This effect is reduced by the interleaving procedure applied and explained in the previous section.

In order to further improve the BER, error correcting schemes, which are based on convolutinal codes and the soft decision Viterbi algorithm, were incorporated into the communication system and investigated. The encoder was inserted at the input of the transmitter and the decoder at the position of the decision circuit at the output of the receiver that is shown in Figure 1. It was assumed that the channel is memoryless. Therefore, the noise affecting a given bit is independent of the noise affecting any proceeding or succeeding bit. Let us assume that the message sequence **c** is transmitted in the time interval from $t = 0$ to $t = \tau$. The word error probability, having in mind the Bayes' rule [16], may have these forms

$$P = 1 - \int_{\mathbf{r}} p(\mathbf{c},\mathbf{z})d\mathbf{z} = 1 - \int_{\mathbf{r}} p(\mathbf{c}\mid\mathbf{z})p(\mathbf{z})d\mathbf{z} = 1 - \int_{\mathbf{r}} p(\mathbf{z}\mid\mathbf{c})p(\mathbf{c})d\mathbf{z} \tag{15}$$

where the received codeword, $\mathbf{z} = \mathbf{z}_1^{\tau}$ for an encoded sequence $\boldsymbol{\gamma}$, is processed and transmitted through the channel, where τ is the number of sets containing n bits generated at the output of a convolutional encoder having one input. The probability $p(\mathbf{z})$ is positive and independent of the message sequence **c**, or of the encoded sequence $\boldsymbol{\gamma}$, thus, the minimization of the word error probability is equivalent to maximizing the a posteriori probability $P(\mathbf{c}|\mathbf{z})$ or the conditional probability $P(\mathbf{z}|\mathbf{c})$, or the conditional probability $P(\mathbf{z}|\boldsymbol{\gamma})$ due to one-one correspondence between **c** and $\boldsymbol{\gamma}$. The Viterbi algorithm is based on the maximum likelihood algorithm (ML) that is further based on the maximization of the likelihood function, expressed in a logarithmic form as [16]

$$\begin{aligned}\log p(\mathbf{z}\mid\mathbf{c}) &= \log p\left(\mathbf{z}_1^{\tau}\mid\boldsymbol{\gamma}_1^{\tau}\right)\\ &= -\sum_{t=1}^{\tau}\sum_{i=0}^{n-1}\frac{\left(z_{t,i}-\gamma_{t,i}\right)^2}{2\sigma^2} - \frac{\tau n}{2}\log 2\pi - \tau n\log\sigma\end{aligned} \tag{16}$$

The results of simulations based on the soft output VA are shown in Figure 8. Obviously, we can improve the characteristics of the system enormously including this ECC scheme. An achieved coding gain for BER = 10^{-3} is 7 dB. We expect this improvement to be achieved in the case when the fading is present in the channel for the case when an interleaver is incorporated into the communication system. Also, further improvement can be achieved if one of turbo coding schemes is applied.

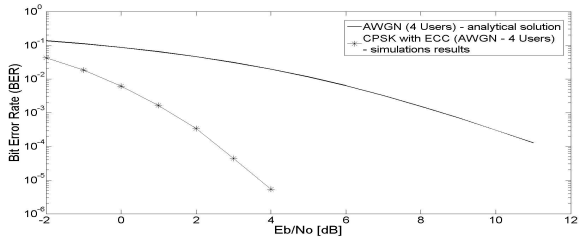

Figure 8. BER for the ECC scheme.

Error control scheme can be also applied in the case when fading is present in the channel as shown in Figure 3. In this case a coding gain of 5 dB for BER = 10^{-4} is achieved in the case when we use an 1000x1000 block interleave of the chaotic signal.

6. Brain signals investigations

In our search for signals having good autocorrelation and crosscorrelation characteristics, we preliminary investigated some signals obtained from human body. One sample of a brain signal is presented in Figure 9.

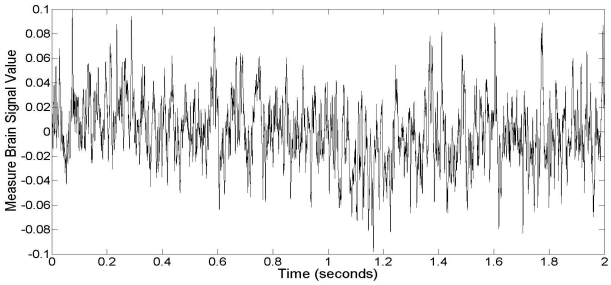

Figure 9. A sample of brain signal in time domain

For this signal the correlation and distribution characteristics are investigated. The autocorrelation function, shown in Figure 10, has a pronounced peak. From this point of view this signal could be used as carrier of information in a multiuser system.

A simulator of a multiuser system, that uses brain signals alongside with a chaotic signal generated by the cubic map, was created It was shown that the user's information transmitted using the brain signal as the carrier can be detected and separated from the user's information transmitted using the cubic map. However, the BER of the user using the brain signal carrier, shown in Figure 11, is significantly worse than for the user that uses the cubic

map. This rather disappointing result can not be taken so seriously and further research is suggested related to the ways of taking the signals from the human body as well as the way of their use in communications systems.

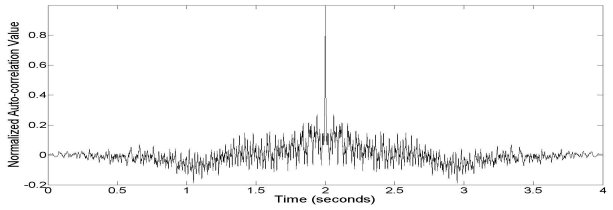

Figure 10. Autocorrelation function of a brain signal sample.

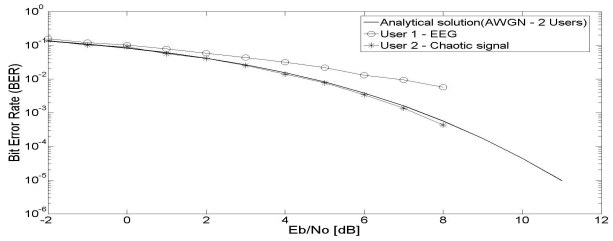

Figure 11. BER curves for a 2-user system

7. Conclusions

A multiuser system can be implemented using chaotic signals as the carriers of users' information. This system, when corrupted by the white noise, performs slightly better than the system with white noise and jamming signals, and substantially better than the system operating in Rayleigh fading channel. The BER of the CPSK system with fading can be improved by applying block interleaving technique on the chip sequence generated at the transmitter, which results in a BER curve close to the non-fading case. This improvement increases with the block interleaver sizes. For the interleaver size of 1000/1000 this improvement is enormous and the BER curve comes close to the BER curve for the AWGN case. For BER of 10^{-4} their difference is less than 1 dB. Further improvement can be achieved, as could be expected, by applying ECC scheme. For BER of 10^{-4} this improvement is 5 dB for the soft output Viterbi algorithm. Inside a particular multiuser system it is possible to use a mixture of different chaotic generators or the same generator with different initial conditions. In this way the security in signal transmission can be enhanced. Also, the chaotic signals investigated can be used in the classical systems alongside with the orthogonal sequences, like Walsh functions, due to good autocorrelation and crosscorrelation characteristics between them. The applications of signals taken from human's body are the subject of further research in this field because the results obtained and presented in this paper are promising, but preliminary.

REFERENCES

[1] E. H. Dinan & B. Jabbari, Spreading codes for direct sequence CDMA and wideband CDMA cellular networks, *IEEE Commun. Mag.,* Sept 1998, 48-54.

[2] J. Feng, Signal Reconstruction with Applications to Chaos-Based Communications, *PhD Thesis*, Department of Electronic and Information Engineering, The Hong Kong Polytechnic University, Hong Kong SAR, China, April 2002.

[3] T. L. Carroll & L. M. Pecora, Synchronization in Chaotic Systems, *Physical Review Letters*, *64*(8), February 1990, 821-825.

[4] J. P. Eckmann & D. Ruelle, Ergodic theory of chaos and strange attractors," *Rev. Modern Phys., 57,* 1985, 617–656.

[5] L. O. Chua & T. S. Parker, Chaos: A tutorial for engineers, *Proceedings of IEEE*, *75*, 1987, 982–1008.

[6] K. M. Cuomo, S. W. Isabelle, A. V. Oppenheim & G. W. Wornell, Signal processing in context of chaotic signals, *Proceeding of IEEE ICCASP, 4*, 1992, 117–120.

[7] F. C. M. Lau & C. K. Tse, *Chaos-Based Digital Communication Systems: Operating Principles, Analysis Methods, and Performance Evaluation* (Springer-Verlag, Berlin, 2003).

[8] W. M. Tam, F.C.M. Lau, C. K. Tse & A. Lawrence, Exact Analytical Bit Error Rates for Multiple Access Chaos-Based Communication Systems, *IEEE Transactions on Circuits and Systems – II, Express Briefs, 51*(9), September 2004, 473-481.

[9] S. Bu & B.-H. Wang, Improving the security of chaotic encryption by using a simple modulation method, *Chaos, Solitons & Fractals, 19*(4), 2004 919-24.

[10] L. Shujun, G. Alvares & G. Chen, Breaking a chaos-based communication scheme by an improved modulation method", *Chaos, Solitons & Fractals, 25,* 2005, 109-120.

[11] B. A. Liew, S. M. Berber & G. S. Sandhu, Performance of a Multiple Access Orthogonal Wavelet Division Multiplexing System, *Proc. 3rd International Conference on Information Technology and Applications*, *2,* Sydney, NSW, 2005, 350-353.

[12] J. S. Lee & L. E. Miller., *CDMA Systems Engineering Handbook, 1st edition*. (Artech House Publishers, Boston and London, 1998).

[13] G. Arredondo, W. Chriss & E. Walker, A Multipath Fading Simulator for Mobile Radio, *IEEE Transactions on Communications, 21*(11), Nov 1973, 1325–1328.

[14] T. S. Rappaport, *Wireless Communications: Principles and Practice, 2nd edition* (Prentice Hall PTR, Upper Saddle River, NJ, 2002).

[15] G. S. Sandhu & S. M. Berber, Investigation on Chaos-Based Multiuser Communication System in the presence of White Noise, Rayleigh Fading and Jamming Signals, *IEEE Transactions on Circuits and Systems*, Submitted for publications, 2005.

[16] B. Vucetic & J. Yuan, *Turbo Codes: Principles and Applications* (Kluwer Academic Publishers, AH Dordrecht, The Netherlands, 2002).