IMPROVING SECURITY IN CHAOTIC SPREAD SPECTRUM COMMUNICATION SYSTEMS WITH A NOVEL 'BIT POWER PARAMETER SPECTRUM' MEASURE

Branislav Jovic
Department of Electrical and Computer Engineering, University of Auckland, 38 Princes street, Auckland, New Zealand

Charles Unsworth
Department of Engineering Science, Univesity of Auckland, 70 Symonds street, Auckland, New Zealand

Keywords: Security, Spread Spectrum, Communications, Chaos, PC Synchronization, Bit Power Parameter Spectrum.

Abstract: Due to the broadband nature and the high sensitivity to parameter and initial conditions in chaotic signals, chaotic spread spectrum (SS) communication systems have been regarded as highly secure. However, it is often easier to decrypt chaotic parameter modulation (CPM) based SS systems than was originally thought. In this paper, a single user CPM based chaotic communication system implementing Pecora-Carroll (PC) synchronization is described. Following this, the CPM based communication system, employing the chaotic carrier generated by the Burger's map is proposed. To highlight the security aspect a new measure called 'Bit Power Parameter Spectrum' (BPPS) is introduced. The BPPS is then used to identify parameters that provide high secure and insecure regions for the chaotic map. Furthermore, it is demonstrated how a binary message can be decrypted easily if the parameters of the map exist in the insecure region of the BPPS and how security is optimised if the parameters exist in the secure region of the BPPS. The results are contrasted with those of the standard Lorenz CPM based system. The BPPS measure shows that the Lorenz CPM based system is easily decrypted for nearly all parameter values thus rendering the carrier insecure.

1 INTRODUCTION

In 1990 Pecora and Carroll (PC) discovered that chaotic systems can be synchronized. Along with the broadband nature and the high sensitivity of chaotic systems to parameter and initial condition perturbations, chaotic synchronization allowed researchers to design SS chaotic communication systems. These systems were primarily designed with the aim of the increased security over the existing SS systems. However, as will be discussed shortly, chaotic communications are often insecure.

A PC synchronization scheme can be viewed as a master-slave synchronization system (Jovic et al., 2006a). The master system provides at least one of its chaotic outputs to the slave system. The slave system uses the given master output (driving signal), to elegantly synchronize itself to the master system, regardless of its initial conditions. The master-slave system can also be viewed as the transmitter-receiver communication system. Since the introduction of the PC synchronization method a number of communication schemes based on this method have been proposed, (Wu and Chua, 1994; Oppenheim et al., 1992; Cuomo and Oppenheim, 1993; Jovic et al., 2006a). These include such methods as the chaotic masking (CS) (Oppenheim et al., 1992), the chaotic parameter modulation (CPM) (Cuomo and Oppenheim, 1993) and the initial condition modulation (ICM) (Jovic et al., 2006a). Other chaotic SS communication systems, such as those based on DS-CDMA synchronization also exist and have been studied in (Jovic et al. 2007a).

In contrast to PC synchronization where the master-slave system either synchronizes or does not, it is also possible to design controllers which enforce synchronization. Such design techniques have been investigated for both chaotic flows (Jovic and Unsworth, 2007b) and chaotic maps (Millerioux and Mira, 1998, 2001; Yan, 2005). In a number of cases it has been shown that these techniques can be

Jovic B. and Unsworth C. (2007).
IMPROVING SECURITY IN CHAOTIC SPREAD SPECTRUM COMMUNICATION SYSTEMS WITH A NOVEL 'BIT POWER PARAMETER SPECTRUM' MEASURE.
In *Proceedings of the Second International Conference on Security and Cryptography*, pages 273-280
DOI: 10.5220/0002125302730280

applied to chaotic communications (Millerioux, 1998; Nan, 2000). In (Millerioux and Mira, 1998, 2001) synchronization of piecewise linear chaotic maps in a master-slave configuration is investigated. In particular, finite time synchronization is considered and the conditions for it discussed. It is shown that finite time synchronization requires the eigenvalues of the error system matrix to be equal to zero. The significance of the results in relation to secure chaotic communications is also discussed.

A similar method to that of the master-slave map synchronization of (Millerioux and Mira, 2001) is proposed here. In our method the general approach to master-slave synchronization of chaotic maps is presented and the requirements for synchronization outlined. It is shown that the synchronization is achieved by keeping the eigenvalues of the error system matrix within the unit circle in the *z* domain. Furthermore, the method of implementing the synchronized master-slave system within a CPM based secure SS chaotic system is demonstrated.

With the development of secure communication techniques based on the concept of chaotic synchronization, eavesdropping techniques have also been developed in parallel, highlighting the lack of security in many of the proposed systems. The eavesdropping techniques include those based on the prediction attacks (Short, 1994), short-time zero-crossing rate (STZCR) attacks (Yang, 1995), generalized synchronization attacks (Álvarez et al., 2004c), return map attacks (Pérez and Cerdeira, 1995), spectral analysis attacks (Álvarez et al., 2004b), and parameter estimation attacks (Álvarez et al., 2004a), among other.

In perhaps the broadest of terms the chaotic communication eavesdropping techniques, in the literature today, can be divided into those which directly extract the transmitted message without the knowledge of the dynamics of the transmitter (Short, 1994; Yang, 1995; Álvarez et al., 2004b), and those which make certain assumptions about the dynamics of the transmitter before attempting the extraction of the message (Álvarez et al., 2004a, 2004c).

In this paper, it is demonstrated how one can decrypt a binary message from a CPM based SS communication system with no prior knowledge of the dynamics of the transmitter. The message extraction technique is based on the average power of the received signal which for a secure system must be equal for both bits 0 and 1. The carrier powers of bits 0 and 1 must be equal, or very nearly equal, to each other to eliminate the possibility of recognising the message from these (Álvarez et al., 2004c). It is shown that in terms of the bit power security, the Burgers' map CPM system can be optimized and outperforms the Lorenz CPM system.

2 SS CHAOTIC SYNCHRONIZATION BASED COMMUNICATION SYSTEMS

In this section, the chaotic communication system with the receiver based on the PC chaotic synchronization, namely chaotic parameter modulation (CPM) is briefly described. A block diagram of a SS chaotic communication system based on the CPM concept is shown in Figure 1. A requirement for the CPM scheme is for the master-slave system to synchronize for a given driving signal (Jovic and Unsworth, 2007b).

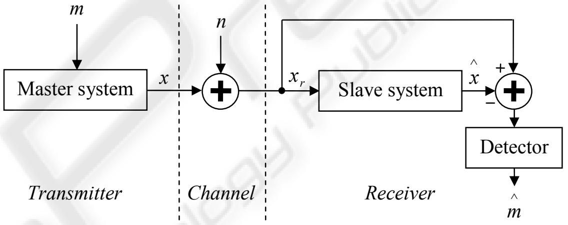


Figure 1: A block diagram of the chaotic communication system based on the parameter modulation concept.

In Figure 1, the message signal *m* varies between the two particular values, depending on whether a binary 0 or a binary 1 is to be transmitted. The message is incorporated into a certain modulating parameter of the master system causing it to change its value with the change in the message. The parameters of the slave system are fixed at all time. When the master-slave parameters are identical synchronization occurs. This forces the synchronization error to zero, indicating that bit 0 has been transmitted. Alternatively, with the master-slave parameter mismatch the system does not synchronize, indicating that bit 1 has been transmitted. Assuming that the additive white Gaussian noise (AWGN) component *n* is near zero, and that sufficient amount of time has passed for x_r and $\hat{x}$ to synchronize, the transmitted message *m* is recovered in the form of $\hat{m}$. The choice of the modulating parameter of the master chaotic system must be chosen with care to ensure chaotic properties of the system at all time. This ensures the increased security within the communication system.

3 GENERAL APPROACH TO THE DESIGN OF THE SS CHAOTIC SYNCHRONIZATION BASED COMMUNICATION SYSTEMS

In this section, the general approach to the design of the synchronized chaotic maps is proposed and applied to the design of the CPM based SS communication systems.

3.1 Synchronization of Chaotic Maps

In (Pecora and Carroll, 1990), the chaotic synchronization concept with a single signal of the master system supplied to the slave system is considered. The general result of this is that the master-slave system either synchronizes or does not (Pecora and Carroll, 1990; Jovic et al, 2006a). In this subsection, the design of nonlinear controllers for the chaotic map master-slave systems is proposed. In particular, the method is demonstrated on the two dimensional Burgers' chaotic map. These controllers then ensure the synchronization among the master-slave systems. The design of the nonlinear control laws is via the following theorem:

Theorem 1:

Suppose: $e_{n+1} = A_n e_n + U_n e_n, \forall\ n \geq 0,$

$$\left|eig(A_n + U_n)\right| = \left|eig(B)\right| < 1.$$

Then: $\|e_n\| \to 0$, *as* $n \to \infty, \forall\ e_0 \in R^n$.

The theorem states that the equilibrium **0,** *of the error system* e_{n+1}, *is globally asymptotically stable if and only if all eigenvalues of* $B = A_n + U_n$ *have magnitude less than one.*

Special case: If the matrix B is a function of n, then the condition that $\|B_{n+1} - B_n\|$ *remains bounded must also be satisfied.*

In the above theorem the brackets | | denote the magnitude of the eigenvalues of a matrix, and the brackets || || denote the Euclidian norm. In the following sections theorem 1 is used for the purpose of synchronizing one, two and three dimensional master-slave chaotic maps.

3.2 SS Communication System based on the Synchronization of Burgers' Map Master-Slave Chaotic System

In this subsection, the master-slave synchronization of the Burgers' map master-slave system is considered and the CPM based SS communication system proposed.

The Burgers' map (Whitehead and MacDonald, 1984) is given by equation 1:

$$\begin{aligned} X_{n+1} &= aX_n - Y_n^2 \\ Y_{n+1} &= bY_n + X_nY_n \end{aligned} \tag{1}$$

With the parameters a = 0.75 and b = 1.75 the system is chaotic.

The design procedure of the synchronizing nonlinear control laws of the Burgers' map CPM based SS chaotic communication system of Figure 2 is now explained. Let the error be defined by equation 2:

$$e_{1_n} = \hat{X}_n - X_n \tag{2a}$$

$$e_{2_n} = \hat{Y}_n - Y_n \tag{2b}$$

In order to demonstrate the design of the controller of Figure 2 assume no noise in the system. It follows then that: $Y_{rn} = Y_n$. The difference error, (the error system), can then be represented by equation 3:

$$\begin{aligned} e_{1_{n+1}} &= \hat{X}_{n+1} - X_{n+1} \\ &= a\hat{X}_n - aX_n - \hat{Y}_n^2 + Y_n^2 + u_{1_n} \\ e_{2_{n+1}} &= \hat{Y}_{n+1} - Y_{n+1} \\ &= b\hat{Y}_n - bY_n + \hat{X}_n\hat{Y}_n - X_nY_n + u_{2_n} \end{aligned} \tag{3}$$

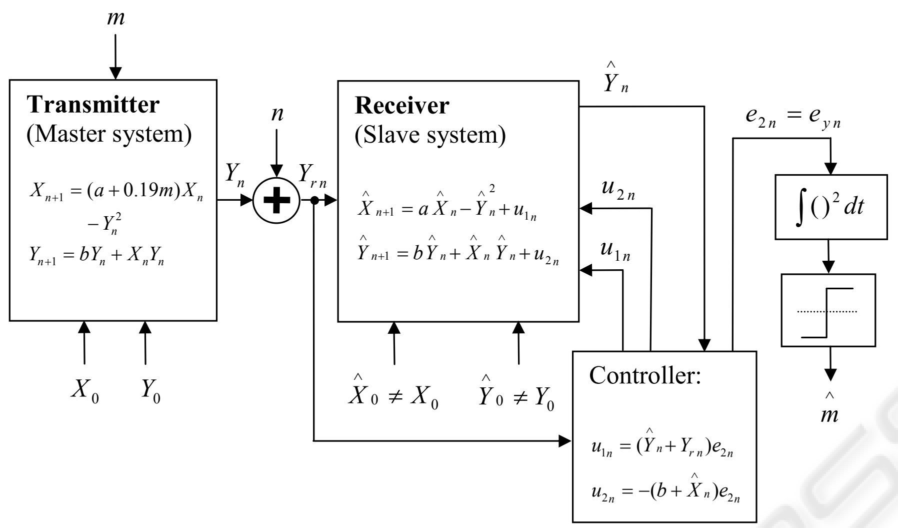
Equation 3 can also be represented by equation 5, keeping in mind the identities of equation 4:

$$\begin{aligned} -\hat{Y}_n^2 + Y_n^2 &= -\hat{Y}_n e_{2_n} - Y_n e_{2_n} \\ \hat{X}_n\hat{Y}_n - X_nY_n &= Y_n e_{1_n} + \hat{X}_n e_{2_n} \end{aligned} \tag{4}$$

$$\begin{aligned} e_{1_{n+1}} &= ae_{1_n} + e_{2_n}(-\hat{Y}_n - Y_n) + u_{1_n} \\ e_{2_{n+1}} &= Y_n e_{1_n} + e_{2_n}(b + \hat{X}_n) + u_{2_n} \end{aligned} \tag{5}$$

With theorem 1 in mind matrix equation 6 is formed:

$$e_{n+1} = A_n e_n + U_n e_n \tag{6}$$



m
Transmitter
(Master system)
$X_{n+1} = (a+0.19m)X_n - Y_n^2$
$Y_{n+1} = bY_n + X_nY_n$
X_0
Y_0
n
Y_n
Y_{rn}
Receiver
(Slave system)
$\hat{X}_{n+1} = a\hat{X}_n - \hat{Y}_n^2 + u_{1_n}$
$\hat{Y}_{n+1} = b\hat{Y}_n + \hat{X}_n\hat{Y}_n + u_{2_n}$
$\hat{X}_0 \neq X_0$
$\hat{Y}_0 \neq Y_0$
$\hat{Y}_n$
u_{2n}
u_{1n}
$e_{2n} = e_{yn}$
$\int ()^2 dt$
$\hat{m}$
Controller:
$u_{1_n} = (\hat{Y}_n + Y_{rn})e_{2_n}$
$u_{2_n} = -(b+\hat{X}_n)e_{2_n}$

Figure 2: The Burgers' map SS chaotic communication system based on the parameter modulation concept.

where:

$$A_n = \begin{bmatrix} a_{11n} & a_{12n} \\ a_{21n} & a_{22n} \end{bmatrix},\quad U_n = \begin{bmatrix} u_{11n} & u_{12n} \\ u_{21n} & u_{22n} \end{bmatrix},\quad e_n = \begin{bmatrix} e_{1n} \\ e_{2n} \end{bmatrix}.$$

Therefore:

$$e_{n+1} = \begin{bmatrix} a_{11n} & a_{12n} \\ a_{21n} & a_{22n} \end{bmatrix} e_n + \begin{bmatrix} u_{11n} & u_{12n} \\ u_{21n} & u_{22n} \end{bmatrix} e_n \qquad (7)$$

Modifying equation 5 to fit the matrix form of equation 7, equation 8 is obtained:

$$e_{n+1} = \begin{bmatrix} a & -\hat{Y}_n - Y_n \\ Y_n & b+\hat{X}_n \end{bmatrix} e_n + \begin{bmatrix} u_{\mathrm{i}\,n} & u_{\mathrm{ii}\,n} \\ u_{\mathrm{iii}\,n} & u_{\mathrm{iv}\,n} \end{bmatrix} e_n \qquad (8)$$

where:

$$u_{1n} = u_{\mathrm{i}\,n}e_{1n} + u_{\mathrm{ii}\,n}e_{2n},\quad u_{2n} = u_{\mathrm{iii}\,n}e_{1n} + u_{\mathrm{iv}\,n}e_{2n}.$$

Therefore:

$$B = A_n + U_n = \begin{bmatrix} a & -\hat{Y}_n - Y_n \\ Y_n & b+\hat{X}_n \end{bmatrix} + \begin{bmatrix} u_{\mathrm{i}\,n} & u_{\mathrm{ii}\,n} \\ u_{\mathrm{iii}\,n} & u_{\mathrm{iv}\,n} \end{bmatrix} \qquad (9)$$
$$= \begin{bmatrix} a + u_{\mathrm{i}\,n} & -\hat{Y}_n - Y_n + u_{\mathrm{ii}\,n} \\ Y_n + u_{\mathrm{iii}\,n} & b + \hat{X}_n + u_{\mathrm{iv}\,n} \end{bmatrix}$$

Following theorem 1 the control laws can be chosen in the following manner:

$$u_{\mathrm{i}_n} = 0,\ u_{\mathrm{ii}_n} = \hat{Y}_n + Y_n,\ u_{\mathrm{iii}_n} = 0,\ u_{\mathrm{iv}_n} = -(b+\hat{X}_n) \qquad (10)$$

With the control laws of equation 10, the matrix *B* of equation 9 takes the form of equation 11:

$$B_n = \begin{bmatrix} a & 0 \\ Y_n & 0 \end{bmatrix} \qquad (11)$$

It is then readily verifiable that the eigenvalues of matrix B_n of equation 11 are equal to 0 and *a*. Furthermore, the theorem 1 above requires matrix *B* to be constant. As the matrix *B* is a function of *n*, it must also be ensured that $\|B_{n+1} - B_n\|$ remains bounded to guarantee global asymptotic stability which is the requirement for synchronization. The fact that $\|B_{n+1} - B_n\|$ remains bounded is demonstrated by equation 12:

$$B_{n+i}B_{n+(i-1)}\ldots B_ne_n = \begin{bmatrix} a & 0 \\ Y_{n+i} & 0 \end{bmatrix}\begin{bmatrix} a & 0 \\ Y_{n+(i-1)} & 0 \end{bmatrix}\cdots\begin{bmatrix} a & 0 \\ Y_n & 0 \end{bmatrix}$$
$$= \begin{bmatrix} a^{i+1} & 0 \\ a^iY_n & 0 \end{bmatrix} \rightarrow 0$$

$$\forall\ |a| < 1, \text{ and as } i \rightarrow \infty. \qquad (12)$$

Therefore, as stated in equation 12, in order for the master and slave systems of Figure 2 to synchronize, the parameter *a* must be kept within the unit circle in *z* domain.

The control laws u_{1_n} and u_{2_n} are therefore given by equations 13 and 14, and incorporated into Figure 2.

$$u_{1n} = u_{\mathrm{i}\,n} e_{1n} + u_{\mathrm{ii}\,n} e_{2n} = (\hat{Y}_n + Y_n) e_{2n} \qquad (13)$$

$$u_{2n} = u_{\mathrm{iii}\,n} e_{1n} + u_{\mathrm{iv}\,n} e_{2n} = -(b + \hat{X}_n) e_{2n} \qquad (14)$$

The important feature of the master-slave system of Figure 2 is that it only requires the master signal Y_n to synchronize the master and slave systems. This fact is of particular importance for communications as only one signal needs to be transmitted thus reducing the required bandwidth (Jovic et al., 2006a,b).

In Figure 2, the master system parameter set of $a = 0.015$ and $b = 1.75$ has been chosen to represent a bit 0. The master system parameter set of $a = 0.205$ and $b = 1.75$ has been chosen to represent a bit 1. The reasoning behind such choice of parameters is clarified in the next section. Note that the message *m* of Figure 2 takes on the values of 0 and 1 depending on the polarity of a bit transmitted. The slave system parameters are set for all time at $a = 0.015$ and $b = 1.75$, so that synchronization at the receiver side signals a bit 0 and de-synchronization signals a bit 1. Both parameter sets, $a = 0.015$ and $b = 1.75$, and $a = 0.205$ and $b = 1.75$ generate chaotic behaviour within the system (Whitehead and MacDonald, 1984).

The transmitted signal Y_n is shown in Figure 3 when the series of 10 bits is transmitted, that is, when *m* = [0 0 1 0 1 1 0 1 0 1]. Figure 3 also shows the corresponding squared synchronization error, e_{yn}^2, under noiseless conditions.

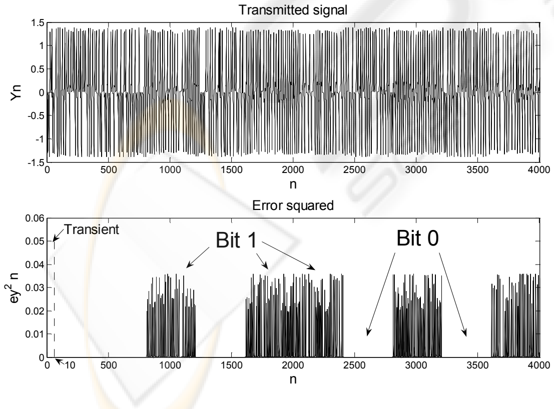


Figure 3: The transmitted signal Y_n and the squared synchronization error e_{yn}^2.

The received bits are detected by squaring and integrating the error e_{yn}. The output of the integrator is then compared to the predetermined threshold and the decision is made whether a bit 0 or a bit 1 was sent. Note that the spreading factor of 400 has been used to represent one bit. By definition, the spreading factor denotes the number of discrete points (chips) contained within one information bit. It is the ratio of a bit period to a chip period (Jovic and Unsworth, 2007b). A transient period of 10 chips has been allowed for the case of Figure 3. During the transient period there is no data transmission taking place.

4 BIT POWER SECURITY ISSUES OF THE SS CHAOTIC COMMUNICATION SYSTEMS

In this section, highly secure and insecure regions of the Burgers’ map CPM based SS communication system are identified using a new measure called the ‘Bit Power Parameter Spectrum’ (BPPS). The analysis is also performed on a standard Lorenz CPM based SS system. It is shown that an eavesdropper can readily decode the message, without any assumptions about the system, if the system is operated outside the secure regions of the BPPS.

4.1 Security Evaluation of the Burgers’ Map CPM based SS Chaotic Communication System

For any secure chaotic communication system it is imperative that the power of the chaotic carriers representing bits 0 and 1 be approximately equal to avoid the possibility of decoding information by a third party simply based on the average powers of the chaotic carriers (Álvarez et al., 2004c). In order to perform the security analysis on the Burger’s map communication system of Figure 2, and thus explain the choice of the modulating parameters, the average power of the chaotic carriers representing bits 0 and 1 is now analysed. To do so the average power of a number of bits (1024) is first calculated and the mean of those powers and the corresponding standard deviation found. A number of points are then obtained for a number of different sets of chaotic parameters and the average power graph, with the error bars, versus the varied parameter, plotted. A pseudo random binary sequence (PRBS) generator has been used to model the transmitted bits. The plots have been produced with the concept of security in mind. If the average power of the chaotic carriers of bits 0 and 1 are different during the same transmission, with the confidence intervals which do not overlap, then the security of the system based on those carriers is jeopardized.

Figure 4 shows the BPPS of the chaotic carriers representing the bits transmitted. For the bits 1 the parameter b is always kept constant at 1.75 with the parameter a varied in steps of 0.01 from a = 0 to a = 0.75. For the case of Figure 4 bits 0 are represented by the parameter values: a = 0.6 and b = 1.75 at all times. Bits 1 must then be represented by some other parameter values in order to achieve successful communication. From Figure 4 it can be observed that the average power of the chaotic carriers is approximately the same, (and the deviation of this power), when the parameter a is kept in the region: 0 < a < 0.22, whereas it differs drastically outside of this region. Therefore, choosing the parameter sets for bits 0 and 1 anywhere outside this region would jeopardize the security of the system. Thus, choosing the parameter values: a = 0.6 and b = 1.75 to represent bits 0 is not suitable for the security reasons. In order to remedy this let the parameter values representing bits 0 be: a = 0.015 and b = 1.75. In this case Figure 5 is obtained. From Figure 5 it is observed that the carrier powers of the bits 0 and 1 have approximately equal values thus offering increased security over the choice of parameters of Figure 4.

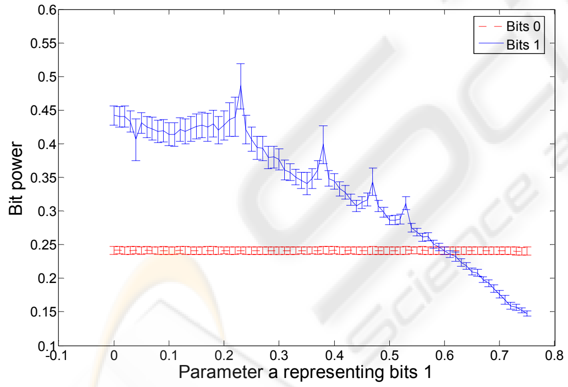


Figure 4: The BPPS within the Burgers' CPM based SS chaotic communication system when the bits 0 are represented by the parameter set: a = 0.6, b = 1.75.

Based on the findings of Figure 5, it is now shown that choosing the parameter set: a = 0.015 and b = 1.75, to represent bits 0, and the parameter set, a = 0.205 and b = 1.75, to represent bits 1, produces the best performance in terms of the bit error rate (BER). In Figure 6, the BER vs. the bit energy to noise power spectral density ratio (E_b/N_o) curves have been plotted. Figure 6 demonstrates the progressive improvement represented by the BER curves with the parameter a varied in the secure region of Figure 5 from a = 0.0625 up to a = 0.205 in steps of 0.0475. The parameter b has been set to 1.75 for both bits 0 and 1. The parameter a representing bit 0 has been set to: a = 0.015. Note that the best BER performance is achieved by choosing the parameter sets, representing bits 0 and 1, to be as far apart as possible from each other within the secure region of Figure 5. Also note further improvement in the BER curve, marked by the open circles, as one exits the secure region.

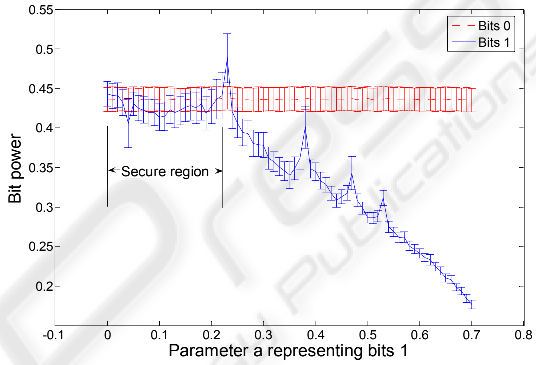


Figure 5: The BPPS within the Burgers' CPM based SS chaotic communication system when the bits 0 are represented by the parameter set: a = 0.015, b = 1.75.

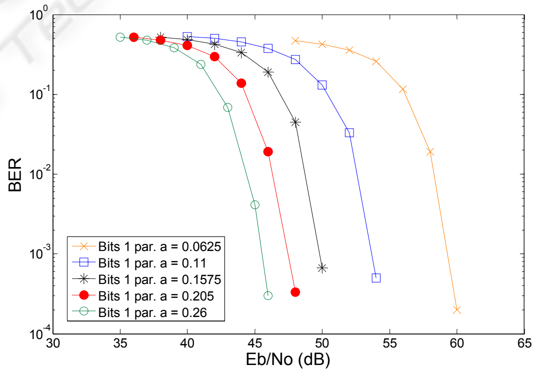


Figure 6: The secure region BER curves of the SS chaotic communication system based on the parameter modulation of the Burgers' chaotic map with the progressively increasing bits 1 parameter a.

Figure 7 illustrates the effect on security caused by choosing inappropriate parameter sets which produce chaotic carriers of different power. In case of Figure 7 bits 0 have been represented by the parameter set of a = 0.6 and b = 1.75, while bits 1 have been represented by the parameter set of a = 0.205 and b = 1.75. The average power of the transmitted signal of Figure 7 has been evaluated using the sliding window of 400 chips in length (the spreading factor of a single bit). The sliding window is then shifted one chip in time and the average power evaluated again. This process is repeated until the end of the transmitted signal. It can be observed from Figure 7 that the average power of the chaotic carriers of the transmitted bits oscillates periodically with the change of the binary message. In contrast to Figure 7, Figure 8 illustrates the effect on security caused by choosing the appropriate parameter sets which produce chaotic carriers of approximately equal power. In case of Figure 8 bits 0 have been represented by the parameter set of $a = 0.015$ and $b = 1.75$, while bits 1 have been represented by the parameter set of $a = 0.205$ and $b = 1.75$.

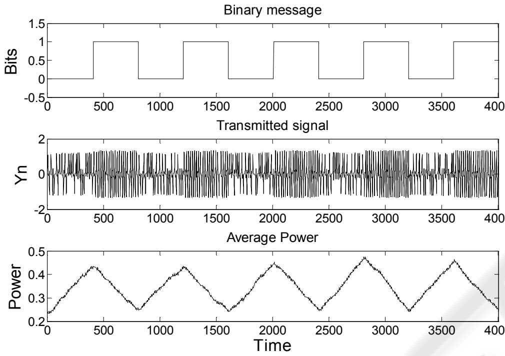


Figure 7: The binary message, the transmitted signal Y_n and the average power of the transmitted signal. Bits 0 parameter set: $a = 0.6$ and $b = 1.75$. Bits 1 parameter set: $a = 0.205$ and $b = 1.75$.

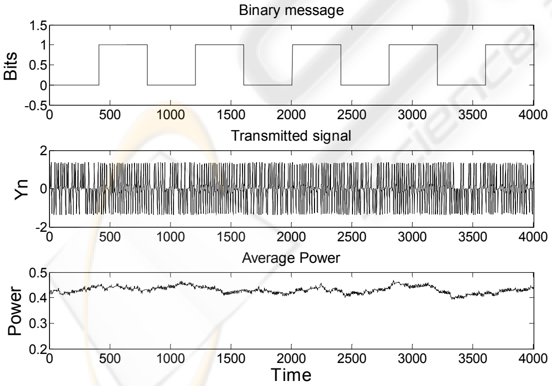


Figure 8: The binary message, the transmitted signal Y_n and the average power of the transmitted signal. Bits 0 parameter set: $a = 0.015$ and $b = 1.75$. Bits 1 parameter set: $a = 0.205$ and $b = 1.75$.

4.2 Security Evaluation of the Lorenz CPM based SS Chaotic Communication System

In (Cuomo and Oppenheim, 1993), the Lorenz CPM based SS chaotic communication system has been presented. In this scheme the binary message is used to alter the parameter b of the master (transmitter) between 4 and 4.4 depending on whether a bit 0 or bit 1 is to be transmitted. However, at the slave (receiver) side the parameter b is fixed at 4 for all time. Thus, the synchronization either occurs or does not, depending on the state of the parameter b at the transmitter (master) side. The other Lorenz parameters, namely σ and r, are fixed at 16 and 45.6, respectively. A BPPS as that of Figures 4 and 5 is plotted in Figure 9 but for the Lorenz CPM based chaotic communication system of (Cuomo and Oppenheim, 1993). In this case the parameter b of the bits 1 is varied from 0.1 to 10 in steps of 0.1 with the other parameters being fixed at the constant values specified above. From Figure 9 one can see that there are no secure regions where one can operate the system as the power of the bits 1 increases, almost linearly, with the parameter b. Therefore, to minimise the impact on the security, the parameters b representing bits 0 and 1, must be kept as close to each other as possible.

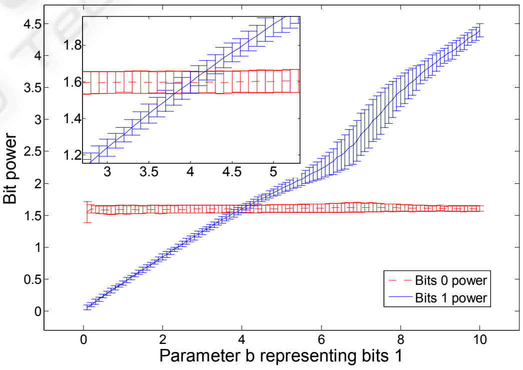


Figure 9: The BPPS within the Lorenz CPM based SS chaotic communication system. The close up is shown in the upper left hand corner.

5 CONCLUSIONS

In this paper, a method of synchronizing chaotic maps and its implementation within a CPM based SS chaotic communication system has been proposed. The security of the proposed, as well as of the existing SS chaotic communication systems, has then been evaluated in terms of the average power of the chaotic carriers of the bits transmitted. In order to do so, a novel analysis technique, termed the 'Bit Power Parameter Spectrum' (BPPS), has been proposed. Without any assumptions about the system architecture or its characteristics, the BPPS has been used to show that the CPM based SS systems are not as secure as often thought.

The design of the nonlinear control laws for the synchronization of the chaotic map master-slave systems has been proposed and demonstrated on the two dimensional Burgers' map master-slave system.

Following this, the method of implementing the synchronized master-slave system within a CPM based secure SS communication system has been demonstrated on the two dimensional Burgers' map. The nonlinear control laws were designed in such a way to force the synchronization among the master and slave systems using only one signal of the master system. This is of particular importance for communications as only one signal needs to be transmitted thus reducing the required bandwidth.

Finally, the Lorenz CPM based SS chaotic communication system has been presented. The security of the proposed and the existing CPM SS chaotic communication systems has been evaluated in terms of the average power of the chaotic carriers of the bits transmitted using the newly proposed technique of BPPS. It has then been shown that due to the largest BPPS overlap region, the Burgers' map CPM based SS chaotic communication system can be optimized and is thus more secure than the Lorenz CPM based SS system. As the BPPS relies on the evaluation of average power, the security optimization is thus achieved by assuming that an eavesdropper has no knowledge of the system architecture or its dynamics. Furthermore, it has been shown that the BER performance of the Burgers' map CPM based SS chaotic communication system can also be optimized. The optimization is achieved by choosing the parameter sets, representing bits 0 and 1, to be as far apart as possible within the secure operating region of the BPPS.

REFERENCES

Álvarez, G., Montoya, F., Pastor, G., Romera, M., 2004a. Breaking a secure communication scheme based on the phase synchronization of chaotic systems. Chaos, 14 (2), 274-278.

Álvarez, G., Montoya, F., Romera, M., Pastor, G., 2004b. Breaking Two Secure Communication Systems Based on Chaotic Masking. IEEE Trans. Circuits Systems: Express Briefs, 51 (10), 505-506.

Álvarez, G., Montoya, F., Romera, M., Pastor, G., 2004c. Breaking parameter modulated chaotic secure communication system. Chaos, Solit. Fract., 21 (4), 783-787.

Cuomo, K.M., Oppenheim, A.V., 1993. Circuit Implementation of Synchronized Chaos with Applications to Communications. Phys. Rev. Lett., 71 (1), 65-68.

Jovic, B., Berber, S., Unsworth, C.P., 2006a. A novel mathematical analysis for predicting master – slave synchronization for the simplest quadratic chaotic flow and Ueda chaotic system with application to communications, Physica D, 213 (1), 31-50.

Jovic, B., Unsworth, C.P., Berber S., 2006b. De-noising 'Initial Condition Modulation' Wideband Chaotic Communication Systems with Linear & Wavelet Filters. In *AUS Wireless'06, 1st IEEE Internat. Conf. on Wireless Broadband and Ultra Wideband Communications*.

Jovic, B., Unsworth, C.P., Sandhu, G.S., Berber, S.M., 2007a. A robust sequence synchronization unit for multi-user DS-CDMA chaos-based communication systems, Signal Processing, 87 (7), 1692-1708.

Jovic, B., Unsworth, C.P., 2007b. *Synchronization of Chaotic Communication Systems*. In C.W. Wang (Ed.), *Nonlinear Phenomena Research Perspectives*, Nova Publishers, New York, In Press.

Millerioux, G., Mira, C., 1998. Communicating via Chaos Synchronization Generated by Noninvertible Maps. In *ISCAS'98,Internat. Symp. Circuits and Systems*.

Millerioux, G., Mira, C., 2001. Finite-Time Global Chaos Synchronization for Piecewise Linear Maps, IEEE Trans. Circuits Systems, 48 (1), 111-116.

Nan, M., Wong, C-n., Tsang, K-f., Shi, X., 2000. Secure digital communication based on linearly synchronized chaotic maps, Phys. Lett. A, 268 (1-2), 61-68.

Oppenheim, A.V., Wornell, G.W., Isabelle, S.H., Cuomo, K.M., 1992. Signal processing in the context of chaotic signals. In Proc. *IEEE ICASSP'92*.

Pecora, L.M., Carroll, T.L., 1990. Synchronization in chaotic systems, Phys. Rev. Lett., 64 (8), 821-824.

Pérez, G., Cerdeira, H.A., 1995. Extracting Messages Masked by Chaos, Phys. Rev. Lett, 74 (11), 1970-1973.

Short, K.M., 1994. Steps Toward Unmasking Secure Communications, Internat. J. Bifur. Chaos, 4 (4), 959-977.

Whitehead, R.R., MacDonald, N., 1984. A chaotic mapping that displays its own homoclinic structure, Physica D, 13 (3), 401-407.

Wu, C.W., Chua, L.O., 1994. A unified framework for synchronization and control of dynamical systems, Internat. J. Bifur. Chaos, 4 (4), 979-998.

Yan, Z., 2005. Q-S synchronization in 3D Henon-like map and generalized Henon map via a scalar controller, Phys. Lett. A, 342 (4), 309-317.

Yang, T., 1995. Recovery of Digital Signals from Chaotic Switching, Internat. J. Circuit Theory Applic., 23 (6), 611-615.