Masked Symmetric Chaos Shift Keying : Modulation and demodulation of Chua's circuits using PI control estimated from LMI criterion

F.Launay, R.Burghelea, P.Combeau, P.Coirault

Laboratiore d'Automatique et d'Informatique Industrielle
LAII-ESIP 40 av. du Recteur Pineau, Poitiers, 86022, France
frederic.launay@univ-poiters.fr
http://laii.univ-poitiers.fr/

Abstract

This paper deals with a new modulation technique based on Symmetric Chaos Shift Keying (SCSK) and its receiver structure is described for optimal synchronization. The Masked Symmetric Chaos Shift Keying (MSCSK) improves both security of information signal compared to SCSK and demodulation procedure. Optimal synchronization of two identical chaotic systems is performed in the paper. By using dissipativity theory, a PI control system is proposed according to Linear Matrix Inegality (LMI). The coefficients of PI are resolved using the MATLAB LMI Toolbox. The proposed controller is simple and can be easily implemented in the demodulator. Simulation results are presented for the Chua circuit and show the effectiveness of the proposed scheme.

I. Introduction

Mobile communication research undertakes significant efforts to promise security of mobile broadband access and faster information rate. Spread spectrum techniques for multiple access and interference suppression have been recently implemented to communication system, such like DSSS or FSSS (Direct Sequence/Hopping frequency Spread Spectrum : UMTS, Wi-Fi), and Ultra-Wideband Technology. Till now, PseudoNoise (PN) sequences are widely used and implemented as spreading factor for direct sequence and as hopping pattern in frequency hopping, but also as time pattern in pulse transmission (UWB). In the last decade, chaotic encryption for security and chaotic sequence to DSSS systems have been reported. Due to the aperiodic nature of the chaotics signals, chaos based digital communications schemes have been proposed to improve channel capacity compared to the conventionnal spread-spectrum system. The last are based on PN sequence and consequently are limited, whereas an infinite number of chaotic signals with good correlation properties can be ideally generated. Nevertheless, increasing the number of simultaneaous communication leads to reduce the SNR ratio to each communication. As a result, it is more difficult to ensure a correct detection since synchronization of a chaotic signal in noisy environment is the weak link of the receiver structure. Since the work of Pecora and Carroll [1] which have demonstrated that a drive signal could be used to synchronize a chaotic system, a number of chaotic synchronization with modulation schemes have been proposed. Typically, the response system is a duplicate of the drive system. The synchronization error, which is the difference between the transmitted signal and a similar reconstructed signal generated by the response system is injected through a controller in order to achieve synchronization.

In this paper, we propose a new modulation and demodulation scheme and a design procedure of a PI controller based on LMI approach. The modulation scheme is based on SCSK modulation : User's data sequence is first modulated using BPSK modulation. The transmitted signal is spreading thanks to a simple multiplication of BPSK modulated signal and a chaotic sequence. This involves discontinuities of the chaotic transmitted signal and leads to a more complex synchronization procedure since chaotic generator signal is modified by user's sequence. Our approach consist in masking SCSK signal by an other state of chaotic generator in order to simplify chaotic synchronization (bsince synchronization procedure is based on non modulated chaotic signal) and in order to hide the SCSK signal for security purpose.Chaos synchronization is studied by using an output feedback PI controller. A PI controller has been choosen since such controller is relatively simple and easy to implement for pratical applications. In the recent years, several approaches have been proposed to give efficient numerical procedures to find a stabilizating static output feedback [2], [3]. The basic idea is to use a stabilizating static state feedback and to introduce additional variables to give an equivalent problem involving Linear Matrix Inequality (LMI). The new concepts proposed in this paper are first a new modulation/demodulation scheme where the synchronisation procedure is demonstrated and not assumed and second we use dissipativity theory to formulate the problem of synchronization for a class of chatoic systems in terms of LMI framework.

This paper is organized as follow : in section 2, we focus on the coherent MSCSK system. Section 3, we present the control strategy. Section 4 is devoted to the controller design using LMI framework. Section 5, numerical results are provided to illustrate the effectiveness and efficiency of the proposed control methodology.

II. Modulation and demodulation of chaotic signals using Chua circuit : System description

Chaotic generator is based on Chua Circuit. This circuit has been widely studied ([4], [5] ...) and it consist of a linear parallel RLC circuit and a non linearity resistive part as shown in Figure 1.

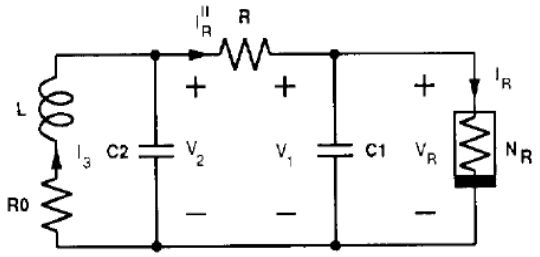

Fig. 1. Chua's Circuit

Usually, nonlinear resistance is represented by a three segment piecewise linear function as shown in figure 2.

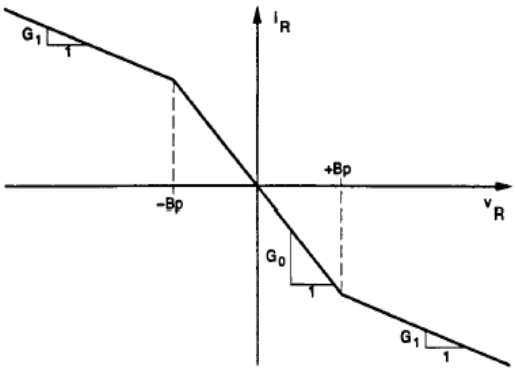

Fig. 2. Non Linear resistance characteristic

The inner region has slope G_0, the outer regions have slopes G_1. We note f: $Ir \rightarrow Vr = f(Ir)$ the nonlinear function. This circuit is completely described by a system of three differentiel equations.

$$\begin{cases} \frac{dI_3}{dt} = \frac{1}{L}V_2 \\ \frac{dV_2}{dt} = \frac{1}{C_2}I_3 - \frac{1}{RC_2}(V_2 - V_1) \\ \frac{dV_1}{dt} = \frac{1}{RC_1}(V_2 - V_1) - \frac{1}{C_1}f(V1) \end{cases} \quad (1)$$

V_1, V_2,I_3 are the vector state of Chua Circuit.

The procedure of MSCSK modulator is illustrated in figure 3. It consists in modulating $R_0 I_3$ with BPSK user's sequence and masking the resultant signal with V_1

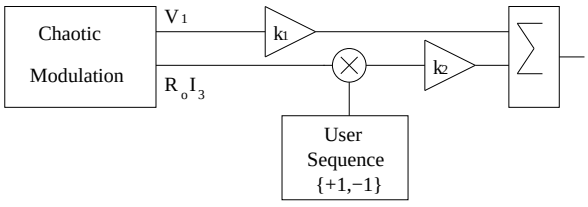

Fig. 3. MSCSK

The transmitted signal is $x_r(t) = k_1 V_1 + k_2 m(t) R_0 I_3$, where $m(t)$ is the BPSK user's sequence, k_1 and k_2 are two gains to mask the modulated signal with non modulated chaotic sequence ($k_1 > k_2$).

In the receiver, a synchronous chaotic system is coupled with a demodulator designed specifically to extract the information signal from the synchronization error as illustrated in figure 4.

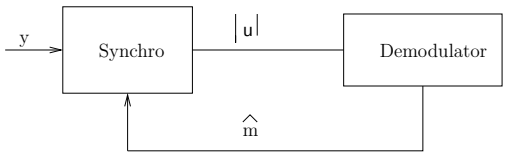

Fig. 4. receiver scheme

Let y(t) be the receive signal. In the sequel, we use the subscripts T and R to assigne transmitter, respectively the receiver signals. Assuming a noiseless channel, we have $y(t) = x_r(t)$. The synchronization system is based on a similar transmitter circuit. Assuming that demodulation procedure is able to extract $\hat{m} = m$ with a demodulation time constant, the synchronization error is $e = y - \hat{y}$:

$$e = k_1 V_{R1} + k_2 m(t) R_0 I_{R3} - k_1 V_{T1} + k_2 \hat{m}(t) R_0 I_{T3} \tag{2}$$

Due to time demodulation procedure and time synchronization, we add a PI controller to stabilize the system in order to tend e(t) assymptotycally towards 0. The estimation of PI controller is derived from LMI procedure which is defined in section 3 and 4. To sum up, the synchronization system is composed by a feedback function (2) composed by a Chua's circuit, two gains, a multiplier and a sommator in order to reconstruct the received signal as close as the transmitted signal and a PI that provides a dynamic estimate of the error. This error is injected to the Chua's receiver circuit as illustrated in figure 5

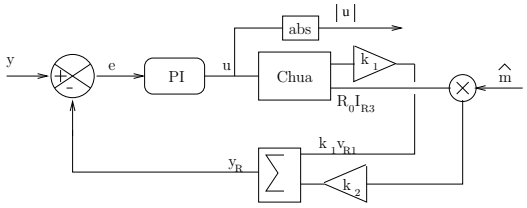

Fig. 5. Synchronization

Assuming stabilization of the receiver system, the error tends exponentially to 0 when $\hat{m} = m$. Nevertheless, as m is the user's information, the absolute synchronization error $|u|$ increase when a change of user's information occurs. The demodulation procedure is based on detecting the absolute synchronization error. The absolut eerror is injected to the clock of a JK latch. The J and K inputs of the latch remain on high state. Consequently, when a change of $|u|$ occurs (clock signal), the output of the lacht change its state. But, during this delay ($\hat{m}$ is not equal to m), the synchronization system is trying to minimize synchronization error by delivering V_{T1} and I_{T3} different to V_{R1} and I_{R3} which best satisfy (2). Once $\hat{m} = m$, the error synchronization rapidly growths to decrease according to (2). In order to not detect the new change of absolute synchronization error who leads to a change of $\hat{m}$, we add a debouncing system composed by a monostable and a RS latch, whose delay is theoritically defined according to the Lyapunov exponent of the synchronization system.

The demodulation scheme is shown in figure 6.

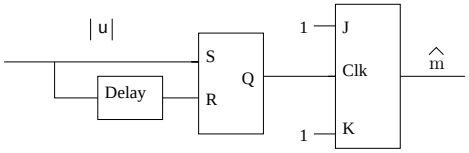

Fig. 6. demodulation

The performance of receiver system depend on the threhold detection and delay of the debouncing system. Improvement can be easy made when knowledge of the user rate is implemented on the receiver scheme. Indeed, a clock regenerator will replace debouncing system to hold a potentially change of state.

III. System definition and problem formulation to assess PI parameters

Let us consider a class of chaotic systems given by

$$\begin{cases} \dot{x} = Ax + B_1\omega \\ y = C(m)x \\ \omega = f(x, y) \end{cases} \tag{3}$$

where $x \in \mathbb{R}^n$ is the state vector, $y \in \mathbb{R}^{n_y}$ is the output vector, $m(t) \in \mathbb{R}$ is the information signal and $f(x, y) \in \mathbb{R}^{n_\omega}$ denotes the nonlinear function on the state x and the output y.

Assumption 1: The pair (A, B_2) is controllable

In this paper, we consider the problem of the synchronization of system (3) and the recovery of the information message vector m. The master (or drive) system (3) drives the slave (or response) system having identical equations defined as follows.

$$\begin{cases} \dot{\hat{x}} = A\hat{x} + B_1\hat{\omega} + B_2\hat{u} \\ \hat{y} = C(\hat{m})\hat{x} \\ \hat{\omega} = f(\hat{x}, y) \end{cases} \tag{4}$$

where $u \in \mathbb{R}^{n_u}$ is an additional control vector. The synchronization signal y is sent to the response system. B_2 is chosen in order to keep the system within its chaotic response.

Assume that the information signal $m(t) = 1$ is transmitted to achieve synchronization, i.e $C(m) = C$ Let the error signals be $e = x - \hat{x}$ and $\tilde{y} = y - \hat{y}$. In this case

$$\dot{e} = Ae + B_1(\omega - \hat{\omega}) - B_2 u \tag{5}$$

Assumption 2: $(f(x,y) - f(\hat{x},y))^\top (f(x,y) - f(\hat{x},y)) \leq k_1 e^\top C^\top C e$ where k_1 is a real positive number

Consider the following PI controller ([6]):

$$u(t) = F_1\tilde{y} + F_2 \int_0^t \tilde{y}(\tau)d\tau \tag{6}$$

F_1, $F_2 \in \mathbb{R}^{n_u \times n_y}$ are matrices to be designed.

Let

$$z = \begin{pmatrix} e \\ \int_0^t \tilde{y}(\tau)d\tau \end{pmatrix}$$

the state vector of the new system, and

$$\bar{\omega} = f(x,y) - f(\hat{x},y)$$

the perturbation vector.

$$\dot{z} = \bar{A}z + \bar{B}_1\bar{\omega} - \bar{B}_2 u \tag{7}$$

The matrices $\bar{A}$, $\bar{B}_1$ and $\bar{B}_2$ are defined as follows

$$\bar{A} = \begin{pmatrix} A & 0 \\ C & 0 \end{pmatrix} \quad \bar{B}_1 = \begin{pmatrix} B_1 \\ 0 \end{pmatrix} \quad \bar{B}_2 = \begin{pmatrix} B_2 \\ 0 \end{pmatrix}$$

Let $\bar{y} = \begin{pmatrix} \bar{y}_1 \\ \bar{y}_2 \end{pmatrix}$ with:

$$\begin{array}{l} \bar{y}_1 = \begin{pmatrix} C & 0 \end{pmatrix} z \\ \bar{y}_2 = \begin{pmatrix} 0 & I \end{pmatrix} z \end{array} \tag{8}$$

In this case, u becomes

$$u = \begin{pmatrix} F_1 & F_2 \end{pmatrix} \bar{y} = \bar{F}\bar{y} \tag{9}$$

The problem of PI controller design is reduced to that of static output feedback controller design for the system:

$$\begin{cases} \dot{z} = \bar{A}z + \bar{B}_1\bar{\omega} - \bar{B}_2 u \\ \bar{y} = \bar{C}z \\ u = \bar{F}\bar{y} \end{cases} \tag{10}$$

where

$$\bar{C} = \begin{pmatrix} C & 0 \\ 0 & I \end{pmatrix}$$

IV. PI controller design

In this section, the design problem of PI controller is investigated. The control objective is to stabilize non-linear system (10).

A. Problem statement

Consider the system (10) where z takes its values in a state space $\mathbb{Z}$, the output $\bar{y}$ taking its values in an output state $\mathbb{Y}$, $\bar{\omega}$ takes its values in a perturbation space Ω and u takes its values in a control space $\mathbb{U}$. Let

$$s : \mathbb{Z} \times \mathbb{Y} \times \Omega \times \mathbb{U} \to \mathbb{R} \tag{11}$$

be a mapping and assume that for all t_0, $t_1 \in \mathbb{R}$ and for all z, $\bar{y}$, $\bar{\omega}$, u satisfying the function

$$s(t) = s(z, \bar{y}, \bar{\omega}, u) \tag{12}$$

is such that

$$\int_{t_0}^{t_1} |s(t)dt| < \infty \tag{13}$$

Moreover, assume that

$$s(z, \bar{y}, \bar{\omega}, u) = \begin{pmatrix} z \\ \bar{y} \\ \bar{\omega} \\ u \end{pmatrix}^{\top} \mathbb{G} \begin{pmatrix} z \\ \bar{y} \\ \bar{\omega} \\ u \end{pmatrix} \leq 0 \tag{14}$$

In this case, $\mathbb{G}$ is a real symmetric definite negative matrix

$$\mathbb{G} = \begin{pmatrix} \bar{a} & \bar{b} & \bar{c} & \bar{d} \\ \bar{b}^{\top} & \alpha & \beta & \varphi \\ \bar{c}^{\top} & \beta^{\top} & \delta & \theta \\ \bar{d}^{\top} & \varphi^{\top} & \theta^{\top} & \psi \end{pmatrix} \tag{15}$$

where $\bar{a}$, $\bar{b}$, $\bar{c}$, $\bar{d}$, α, β, φ, δ, θ, ψ are matrices of appropriate dimensions. $s(t)$ is a supply function for system (10).

Substituting the output equation $\bar{y} = \bar{C}z$ in $s(z, \bar{y}, \bar{\omega}, u)$ shows that (14) can equivalently be viewed as a quadratic function in the variables z, $\bar{\omega}$ and u:

$$s(z, \bar{\omega}, \tilde{u}) = \begin{pmatrix} z \\ \bar{\omega} \\ u \end{pmatrix}^{\top} \Theta \begin{pmatrix} z \\ \bar{\omega} \\ u \end{pmatrix} \leq 0 \tag{16}$$

where Θ is a real symmetric definite negative matrix

$$\Theta = \begin{pmatrix} \bar{a} + \bar{C}^{\top}\bar{b}^{\top} + \bar{b}\bar{C} + \bar{C}^{\top}\alpha\bar{C} & \bar{c} + \bar{C}^{\top}\beta & \bar{d} + \bar{C}^{\top}\varphi \\ * & \delta & \theta \\ * & * & \psi \end{pmatrix}$$

Consider the following Lyapunov function

$$V = z^{\top} P z \tag{17}$$

P is a symmetric strictly positive definite matrix. System (10) is dissipative if

$$\dot{V} - s < 0 \tag{18}$$

There are several ways to choose the quadratic function $s(z, \bar{y}, \bar{\omega}, u)$. The control objective is to design a static output feedback controller such that z tends exponentially to zero as $t \to \infty$ despite of the nonlinearity difference $f(x, y) - f(\hat{x}, y)$. By considering $\bar{\omega}$ as a perturbation vector, the problem of design a controller for system (10) can be solved by choosing the following supply function

$$s(z, \bar{y}, \bar{\omega}, u) = \gamma^2 \bar{\omega}^{\top}\bar{\omega} - \bar{y}^{\top}\bar{y} \tag{19}$$

where γ is a strictly positive real number. The supply function (19) can be interpreted as follows. From (8), the inequality (16) is equivalent to

$$X_1 + X_2 \leq 0 \tag{20}$$

where

$$X_1 = \begin{pmatrix} e \\ f-\hat{f} \end{pmatrix}^\top \begin{pmatrix} -C^\top C & 0 \\ 0 & \gamma^2 \end{pmatrix} \begin{pmatrix} e \\ f-\hat{f} \end{pmatrix}$$

$$X_2 = -\int_0^t e^\top(\tau) C^\top C e(\tau) d\tau$$

A sufficient condition for (20) is $X_1 \leq 0$. From assumption 2, this means that there exists a positive real number γ, such that

$$k_1 \leq \frac{1}{\gamma^2} \tag{21}$$

The smallest possible value of γ corresponds to the largest upperbound of the sector condition described in assumption 2. From (18), system (10) is dissipative if there is a symmetric positive definite matrix P such that

$$\mathbb{M} = \begin{pmatrix} A_{cl}^\top P + P A_{cl} + \bar{C}^\top \bar{C} & P\bar{B}_1 \\ \bar{B}_1^\top P & -\gamma^2 I \end{pmatrix} \lessdot 0 \tag{22}$$

is feasible. The matrix A_{cl} has the following definition

$$A_{cl} = \bar{A} - \bar{B}_2 \bar{F} \bar{C}$$

Theorem 1: Assuming a driving system (3), a response system (4) and a quadratic function (19). The closed loop non linear system (10) is stable if the following conditions are satisfied:
1. The control vector u is choosen to be

$$u(t) = F_1 \tilde{y} + F_2 \int_0^t \tilde{y}(\tau) d\tau$$

$$\bar{F} = \begin{pmatrix} \bar{F}_1 & \bar{F}_2 \end{pmatrix}$$

2. Minimize $\gamma > 0$ over all variables of the following LMI's

$$\begin{aligned} & P = P^\top > 0 \\ & \begin{pmatrix} P A_0 + A_0^\top P + \bar{C}^\top \bar{C} & P\bar{B}_1 \\ \bar{B}_1^\top P & -\gamma^2 I \end{pmatrix} < 0 \end{aligned} \tag{23}$$

where

$$A_O = \bar{A} - \bar{B}_2 \bar{F}_0$$

3. With $\bar{F}_0$, P and γ, find $\bar{F}$ solution of the following LMI

$$\begin{pmatrix} \bar{C}^\top \bar{C} & 0 & P & 0 \\ 0 & -\gamma^2 I & 0 & 0 \\ P & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix}$$

$$+\mathsf{Sym}\left\{ \begin{pmatrix} f_1 \\ f_2 \\ f_3 \\ 0 \end{pmatrix} \begin{pmatrix} A_0 & \bar{B}_1 & -I & 0 \end{pmatrix} \right\}$$

$$+\mathsf{Sym}\left\{ \begin{pmatrix} f_1\bar{B}_2 \\ f_2\bar{B}_2 \\ f_3\bar{B}_2 \\ 0 \end{pmatrix} \begin{pmatrix} 0 & 0 & 0 & I \end{pmatrix} \right\}$$

$$+\mathsf{Sym}\left\{ \begin{pmatrix} 0 \\ 0 \\ 0 \\ I \end{pmatrix} \begin{pmatrix} G\bar{F}_0 - L\bar{C} & 0 & 0 & -G \end{pmatrix} \right\}$$

$$< 0$$

where f_1, f_2, f_3 are non null matrices and matrices G and L are such that $\bar{F} = G^{-1}L$.

See [7] for the complete proof of theorem 1

V. Numerical Results

In this section, to verify and demonstrate the effectiveness of the proposed method, simulation results are presented for a communication system built using Chua's Circuit ([8]).

The Chua's circuit is a simple electronic circuit. Its dynamic is described by system (3), where

$$A = \begin{pmatrix} -\frac{18}{7} & 9 & 0 \\ 1 & -1 & 1 \\ 0 & -14.286 & 0 \end{pmatrix} \qquad B_1 = \begin{pmatrix} \frac{27}{14} \\ 0 \\ 0 \end{pmatrix}$$

$$B_2 = \begin{pmatrix} \frac{1}{4} \\ 0 \\ 0 \end{pmatrix} \qquad C = \begin{pmatrix} 0 & 0 & 1 \end{pmatrix}$$

The non-linear characteristic is

$$f(x,y) = -\frac{3}{14}\left(|x_1+1| - |x_1-1|\right) \tag{24}$$

This equation means that the outer regions slopes of the non linear function is $G_1 = 0$. Notice moreover that non-linearity of Chua's circuit does not depend on the transmitted signal $y(t)$

Fig.7 presents the (x_1, x_2)-phase plane, that shows the chaotic nature of the system.

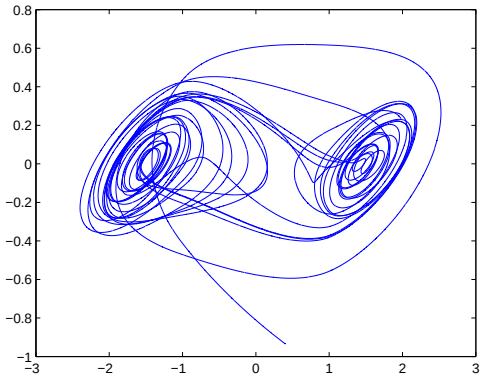

Fig. 7. Chaotic behavior of the Chua's circuit in the x_1-x_2 plane

Assuming that the user information is m=1, the numerical values that are obtained for the controller are $F_1 = 247.9$, $F_2 = 75.43$ with $\gamma = 0.0463$.

In Fig. 8 the detected signal (represented with cross point) can not be stabilize toward a state because of a too small time of debouncing and of a too low threshold detector.

To be optimized, our system needs to wait at least 50 ms before modifying the state of detected signal ($\hat{m}$).

Adjusting the delay to 50 ms, an error at the 7th bit (70 s) is shown in figure 9. This error occurs from a bad choice of threshold detector.

In this simulation, a noisy channel is added to empathize the role of detector threshold. The first transition of $\hat{m}$ takes place when magnitude of error is closed to 130 at time 50 s. A second transition occurs at time 60s when magnitude of error is close to 180, whereas an error appears at time 70 s because of a two small error synchronization (whose magnitude is 30).

Fig. 10 shows the transmitted and recovered binary signal for optimal detector parameters. The user's information is a random binary sequence defined at a bite rate of Tb=10s. The cross representing the received signal and the transmitted signal is shown by the solid line. We note no error in the following binary sequence.

The dash line presents the normalize state errors between transmitter and receiver. The errors quickly tend to zero. This means that the driving and response systems can be globally synchronized.

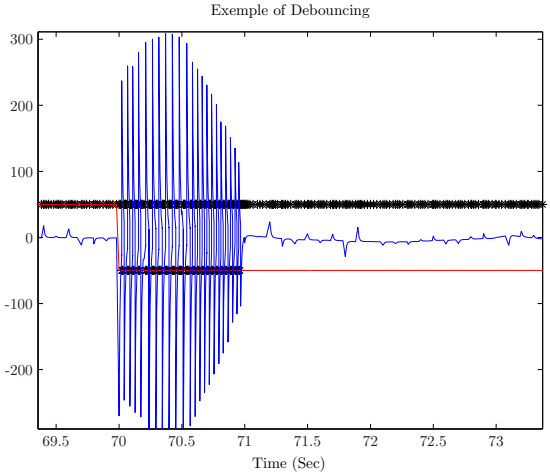

Fig. 8. Lack of debouncing

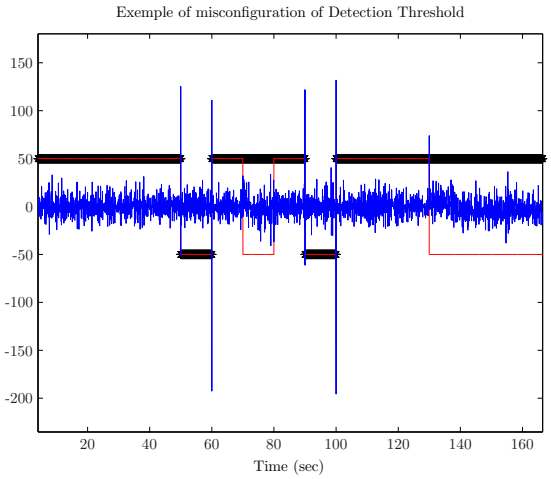

Fig. 9. bad threshold detector

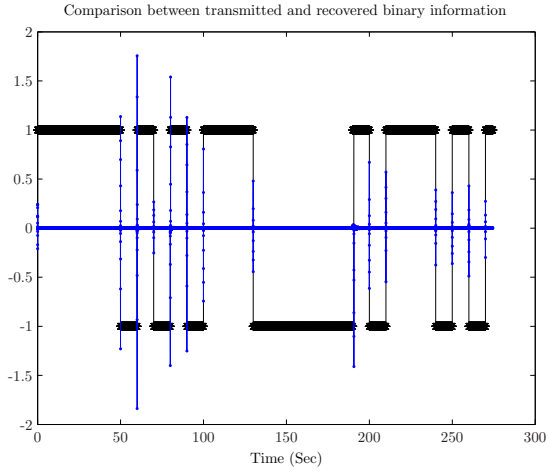

Fig. 10. Comparison of transmitted and received user's sequence

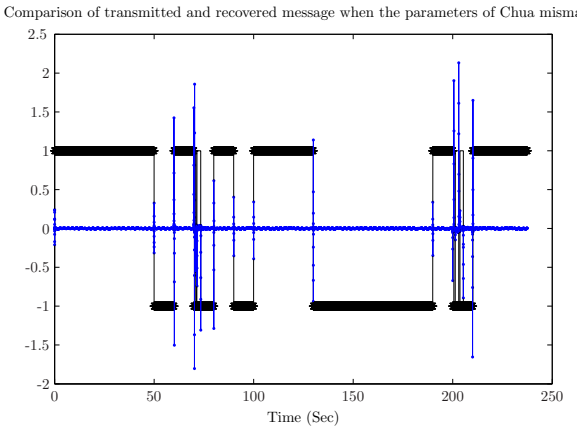

Fig. 11. Comparison of transmitted and received user's sequence with mismatch chua's parameters

In Fig. 11, 10 percent of parameters mismatch of Chua circuits lead to some errors (time T= 70 s and time T= 200s) in detection if we keep the same detection threshold . These errors occur because the magnitude of synchronization errors increase when the drive and the slave parameters differ.

Nevertheless, by modifying the detection threshold, we can solve such errors and we retrieve same result as Fig. 10. Consequently, the system is also robust against parameters mismatch between Chua's Circuit in emission and in reception.

VI. Conclusion

This paper proposes a new secure communication scheme of chaotic modulation and the reception circuit is defined by using the concept of dissipativity. For a class of chaotic systems, it is possible to design a PI controller to synchronize the drive system. The synthesis of the PI gains is converted into a static output feedback controller synthesis. The resulting bilinear matrix inequality can be then converted into a linear matrix inequality using a fictitious static state feedback. This approach is different from iterative LMI algorithms. It remains the problem of how to choose the stabilizing static state feedback among all the admissible candidates. Nevertheless, numerical simulation verifies the effectiveness of the proposed algorithm even if the parameters between the two chua's circuit don't match.

References

[1] L. Pecora and T. Carroll, "Synchronization in chaotic systems," *Physical Review Letters*, vol. 64, pp. 821–824, 1990.
[2] D. Peaucelle and D. Arzelier, "An efficient numerical soution for h_2 static output feedback synthesys," in *Europeen Control Conference*, (Porto, Portugal), 2001.
[3] D. Mehdi, E. Boukas, and O. Bachelier, "Static output feedback design for uncertain linear discrete time system," *IMA Journal of Mathematical Control and Information*, 2003.
[4] K. M. P., "Three steps to chaos - part i : Evolution and part ii : A chua's circuit primer," in *IEEE Transactions on Circuits and Systems-I: Fundamentals Theory and Applications*, no. 10, pp. 640 – 674, 1993.
[5] H. M.. Dedieu H., Kennedy M.P., "Chaos shift keying modulation and demodulation of a chaotic carrier using self synchronizing chua's circuit," in *IEEE Transaction on Circuit and System Part I: Fundamental Theory and Application*, no. 11, pp. 634 – 642, 1993.
[6] F. Zheng, Q. Wang, and T. Lee, "On the design of multivariable pid controllers via lmi approach," *Automatica*, vol. 38, pp. 517–526, 2002.
[7] F. Launay, P. Coirault, S. Cauet, and F.Hutu, "Synchronization of two chaotic systems using pid control," *Chaos 06*, 2006.
[8] H. Puebla and J. Alvarez-Ramirez, "More secure communication using chained chaotic oscillators," *Physical Letters A*, vol. 283, pp. 96–108, 2001.