Secure Digital Communication based on Hybrid Dynamical Systems

Hamid Hamiche, Malek Ghanes, Jean-Pierre Barbot, Said Djennoune

▶ To cite this version:

HAL Id: inria-00531074
https://hal.inria.fr/inria-00531074

Submitted on 1 Nov 2010

Secure Digital Communication based on Hybrid Dynamical Systems

H. Hamiche[*,†], M. Ghanes[*], J.-P. Barbot[*,‡], S. Djennoune[†]

[*]Equipe Commande de Systèmes EA3649, ENSEA, 6 avenue du Ponceau, 95014 Cergy Cedex, France
[†] Laboratoire de Conception et Conduite des Systèmes de Production L2CSP, UMMTO, Tizi-Ouzou, Algérie
[‡] EPI-ALIEN, INRIA, France

hamid.hamiche@ensea.fr, ghanes@ensea.fr, barbot@ensea.fr, djennoune@mail.ummto.dz

Abstract—In this work, a transmission scheme based on the hybrid and chaotic dynamics for private communications is proposed. The transmitter is composed of a continuous-time system and a discrete-time system in which the message is inserted by inclusion. The states of the continuous system are also included, after sampling, in the discrete system. The receiver is composed of a discrete-time delay observer and a continuous-time observer. The principle of the proposed hybrid method is to show that the reconstruction of discrete states of the receiver and the message passes at first by a synchronization of the two continuous-time chaotic systems. This new strategy makes the system of transmission robust, in particular against an attack known plaintext. Simulation results are presented to highlight the performances of the proposed method.

I. INTRODUCTION

In recent years, the theory of complex nonlinear systems and especially chaotic systems has been applied to cryptography in order to propose other methods of encryption. In 1990, T. Pecorra and L. Carroll [17] have shown the possibility of synchronizing chaotic systems. So, many encryption schemes based on chaos have been proposed in the literature [11]. However, very little work has really made the link between encryption algorithms standard and those based on the generation of chaotic sequences. In normal cryptography, from a variety of mechanisms encryption, there are symmetric encryption and public key encryption. The link between the standard symmetric encryption and the encryption by inclusion based on the chaos has been proposed by F. Anstett [1]. Many methods of encryption using chaotic systems has been proposed in the literature, we can cite the addition method [19], the parametric modulation [16], modulation chaotic [5], etc. These methods are all based on synchronization receiver with the transmitter in order to extract the message originally embedded in the chaotic carrier. In 1997, H. Nijmeijer and I. Mareels [14],[15] showed that the unidirectional synchronization of the chaotic systems can be considered as an observer design problem. Different observers has been proposed for chaotic systems (observers used only to reconstruct the transmitter states), [8],[9] and for chaotic systems with unknown inputs (observers for reconstructing the states of the transmitter and to recover the information) [2]. The right work of these observers depends on several conditions: the observability condition for reconstruct the system states, the observability matching condition to recover the system states and information embedded in the system (left invertibility of system), the condition of identifiability of parameters which represents the encryption keys. In this work, we are interested to study a transmission scheme composed of a hybrid dynamical system. The transmitter is composed of a continuous-time chaotic system called Colpitts and a discrete-time chaotic system called Henon. The receiver is composed from continuous and discrete observers. On the level of the receiver, the states of the continuous-time system are introduced in the dynamic of the discrete-time system to make its structure more complex. Thus, the new obtained hybrid system makes the system hardly observable since it gives more unknown parameters than the equations, and this is valid also for attacks with a known-plaintext. The transmitted output to the receiver is composed of a synchronization signal that comes from the continuous-time system and of a useful signal that contain the message (added by the inclusion method) that comes from the discrete-time system. To have a good transmission, it is necessary to have the ration of the useful signal to the transmitted signal as close to one as possible. The reconstruction of the states and the message of the observer discrete passes through the synchronization of two continuous-time chaotic systems (transmitter and receiver) before the synchronization of the two discrete-time chaotic systems. This approach present the advantage that the synchronization of the two systems can be obtained even in the case where the synchronization is lost. The work is organized as follow: in the section 2, the principle of the proposed method is presented by studying the transmitter and the receiver of the transmission system. The section 3 gives the simulation results. Finally, we conclude with a conclusion.

II. PRESENTATION OF THE METHOD

In this work a communication system based on the synchronization of two chaotic hybrid systems is realized. The global scheme of the proposed system for private communications is given by the Figure 1. In order to simplify the analysis, the added delays between the continuous and the discrete parts are removed. These delays ensure the robustness against an attack to a known clearly text.
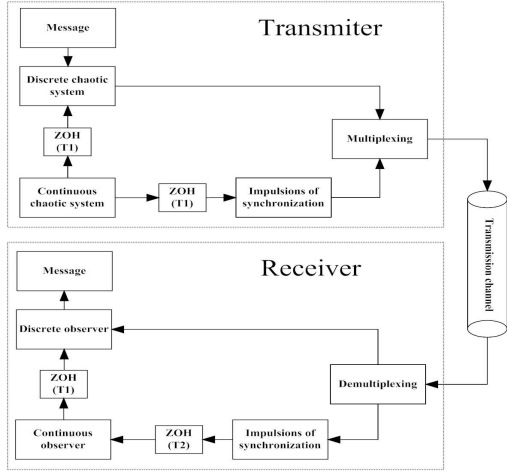
Fig. 1. Transmission chain based on a hybrid dynamical system

The developed method is presented as follow:

A. Study of the transmitter

The transmitter is composed of three blocks: a continuous-time chaotic system, a discrete-time chaotic system and a multiplexing block. These blocks are detailed as follows:

1) Continuous-time chaotic system: This system has been widely studied in the literature [12] and [13]. The state equations of the normalized Colpitts's oscillator in a continuous time is given as:

$$\Sigma_C : \begin{cases} \dot{z}_1 = a_1(-exp(-z_2) + 1 + z_3) \\ \dot{z}_2 = a_2 z_3 \\ \dot{z}_3 = -a_3(z_1 + z_2) - a_4 z_3 \end{cases} \quad (1)$$

with $a_1 = \frac{g}{q(1-k)}$, $a_2 = \frac{g}{qk}$, $a_3 = \frac{qk(1-k)}{g}$, $a_4 = \frac{1}{q}$.

To have a chaotic behavior, the parameters of system (1) are given as follows: $g = 4.46$; $q = 1.38$ and $k = 0.5$ with the initial conditions $z_1(0) = 1.6$; $z_2(0) = 8$ and $z_3(0) = 0.1$.

First, we begin by the study of the observability system with output $y_1 = z_1$. Using the results given in [10], it is easy to show that the rank observability matrix of system (1) is equal to 3, so, the system is locally weakly observable. Consequently, it is possible to obtain all the state from the output $y_1 = z_1$ and its derivatives.

2) Discrete-time chaotic system: The discrete-time chaotic system used in this work is the modified Henon's system. This system has been widely studied in the literature; one can site for instance the work by Vesely [18]. The system is given by the following equations :

$$\Sigma_D : \begin{cases} x_1(n+1) = a - x_2^2(n) - bx_3(n) \\ x_2(n+1) = x_1(n) \\ x_3(n+1) = x_2(n) \end{cases} \quad (2)$$

To have a chaotic behavior, the parameters of the system (2) are given as follows: $a = 1.76$ and $b = 0.1$ with initial conditions $x_1 = 0.1$, $x_2(0) = 0.1$ and $x_3(0) = 0.1$. At the emission level, our aim is to make the structure of the discrete system more complex. To do this, we introduce (without delay) in the dynamics of discrete-time system, the states z_1, z_2 and z_3 of the continuous-time system. It is noted that the states of the continuous-time system are first sampled with a rate $T1$ before their introduction into the discrete-time system. The period T1 (the value is given in simulation) is chosen in order to ensure the synchronization between the transmitter and the receiver of the two continuous-time systems (this is argued in the section (II-B.1)). Despite the fact that the system is a discrete time pure Henon's system, unconnected with the time here each iteration will be made after a fixed period of time $T1$. This fixed choice of the frequency was done to simplify the implementation of the receiver.

In this part, the system (2) will be used as the transmitter with $y_2(n) = x_2(n)$ as its output.

In our work, the two states (z_2, z_3) and the message m are added to the third dynamic of the system (2) in order to make the letter observable and not left invertible. The details of the reconstruction of the states and the message m are given in Section (II-B.2). The new obtained hybrid system is given as follows:

$$\Sigma_H : \begin{cases} x_1(n+1) & = & a - x_2^2(n) - bx_3(n) \\ x_2(n+1) & = & x_1(n) \\ x_3(n+1) & = & x_2(n) + Az_2(n) \\ & + & Bz_3(n) + Cm(n) \end{cases} \quad (3)$$

with: A, B and C, the new coefficients of the discrete-time system and m the message to send. To preserve the chaotic behavior of the system defined by (3), these parameters are chosen with precaution. In our case, we must respect the following values: $A \leq 0.04$, $B \leq 0.1$ and $C \leq 1$.

Based on the works of [4],[6], it is easy to show that the rank of the observability matrix of the system (3) is 3, so the system is locally observable. Moreover, the recovery condition of observability is guaranteed here, the message appears after 3 iterations. Consequently, it is possible to reconstruct all states and the message from the output and its delayed output.

By using the method input-output relationship approach detailed in the work of [1], it is easy to show that the system (3) is identifiable from the output and sufficient of these iterations and from the message and sufficient of these iterations if the continuous variables change frequently.

3) Multiplexing block: The output signal $y_1 = z_1$ comes from the continuous-time system will be first sampled with a period $T2$ but only blocked during $T1$. The signal $y_1 = z_1$ plays the role synchronization signal, it is sent into the channel during a time equal to $T1$. The signal y_2, is sent during $9T1$. The discrete-time system is not iterated for the tenth cycle (T1) which corresponds to the sending of the signal synchronization. Thus, the cycle is composed of 10 periods $T1$ illustrated by the figure 2.
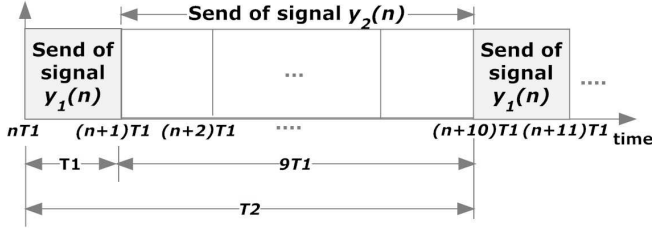
Fig. 2. Transmission cycles of y_1 and y_2

B. Study of the receiver

The receiver is composed of three blocks: a continuous-time chaotic observer, a discrete-time chaotic observer and a multiplexing block.

In the following, we will be interested to study the synchronization between the transmitter and the receiver in the proposed transmission scheme. We will present two observers (continuous and discrete) that allow to synchronize the systems (1) and (3) with their receivers, respectively.

1) Continuous-time chaotic observer: Consider the system (1) with the output $y_1 = z_1$. The aim is to design a reduced-order observer (see [16]) that allows to reconstruct the states $\hat{z}_1, \hat{z}_2$ and $\hat{z}_3$ of the system (1) from the output $y_1 = z_1$.

The equations of the observer are given by (4):

$$\Sigma_{OC} : \begin{cases} \dot{\hat{z}}_1 &= a_1(-\exp(\hat{z}_2) + 1 + \hat{z}_3) \\ & \quad + K(y_1 - \hat{z}_1) \\ \dot{\hat{z}}_2 &= a_2\hat{z}_3 \\ \dot{\hat{z}}_3 &= -a_3(\hat{z}_1 + \hat{z}_2) - a_4\hat{z}_3 \end{cases} \quad (4)$$

where $\hat{y}_1 = \hat{z}_1$ and K a real constant defined hereafter.
Define the observer errors:

$$e_1 = z_1 - \hat{z}_1, e_2 = z_2 - \hat{z}_2, e_3 = z_3 - \hat{z}_3 \quad (5)$$

The gain K is chosen so that the dynamic of the synchronization error $e_1 = z_1 - \hat{z}_1$ will be stable. This allows to ensure the convergence of the synchronization error $e_3 = z_3 - \hat{z}_3$ to zero, consequently the convergence of the synchronization error $e_2 = z_2 - \hat{z}_2$ to zero.
Subtracting equation (1) from equation (4) and using equation (5), we obtain the following errors system:

$$\begin{cases} \dot{e_1} = a_1(\exp(-z_2)\exp(e_2 - 1) + e_3) - Ke_1 \\ \dot{e_2} = a_2 e_3 \\ \dot{e_3} = -a_3(e_1 + e_2) - a_4 e_3 \end{cases} \quad (6)$$

Neglecting higher order terms in the Taylor series expression of $\exp(e_2)$, we obtain the simplified errors system:

$$\begin{cases} \dot{e_1} = a_1(\exp(-z_2)e_2 + e_3) - Ke_1 \\ \dot{e_2} = a_2 e_3 \\ \dot{e_3} = -a_3(e_1 + e_2) - a_4 e_3 \end{cases}$$

which can be rewritten as follows:

$$\dot{E} = AE \quad (7)$$

where

$$A = \begin{pmatrix} -K & \exp(-z_2)a_1 & a_1 \\ 0 & 0 & a_2 \\ -a_3 & -a_3 & -a_4 \end{pmatrix} \quad (8)$$

$$(9)$$

and $E = \begin{pmatrix} e_1 & e_2 & e_3 \end{pmatrix}^T$.

In order to ensure the convergence of the estimated variables $\hat{z}_1$, $\hat{z}_2$ and $\hat{z}_3$ to z_1, z_2 and z_3 respectively, we must guarantee the asymptotical stability of (7). Our main result is given by the following proposition.

Proposition
The errors system (7) is asymptotically stable if there exist a gain K which satisfy the following condition:

$$K > \frac{\sqrt{a_3^2 a_1^2 - 2a_3 a_1 a_4^2 + a_4^4 + 4a_4 a_3 a_1 a_2 M - 4a_4^2 a_3 a_2}}{2a_4}$$

$$- \frac{a_3 a_1 + a_4^2}{2a_4} \quad (10)$$

where M^1 is the bound of $\exp(-z_2)$ i.e.,

$$|\exp(-z_2)| \leq M. \quad (11)$$

Proof. We define a Lyapunov function for system (7) as follows:

$$V = E^T P E \quad (12)$$

where P is symmetric positive definite matrix, which is a solution of the following Lyapunov function

$$A^T P + PA = -Q \quad (13)$$

where Q is chosen semi-positive definite due to the zero eigenvalue of the matrix A (8), i.e.

$$Q = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 0 \end{pmatrix} \quad (14)$$

Taking account (11), the time derivative of V (12) along the trajectory of the system (7) leads to:

$$\begin{aligned} \dot{V} &= E^T A^T P E + E^T P A E \\ &= E^T(A^T P + PA)E \end{aligned}$$

which can be written, under the condition (11), in the following quadratic form:

$$\dot{V} \leq -E^T Q E.$$

According to the choice of Q (14), the system (7) is asymptotically stable if the matrix P defined by (13) is positive definite, which is guaranteed by the condition (10).
Now let's compare this direct Lyapunov method to the Azerman conjuncture one. The Azerman conjuncture consists to compute the eigenvalues of A (8) by using Routh criterium. The obtained result showed us that the eigenvalues of A are negative if the condition (10) is

---

[1]the numerical value of M is given in simulations

satisfied. So we get the same condition of K (10) with both methods, which is not true in a general case. This result represents a particular case and is justified by the eigenvectors of A which not change the direction.

This ends the proof.

2) Discrete-time chaotic observer: In this part, the system (3) with the output $y_2(n) = x_2(n)$ is considered. For the reception, based on the works of [4] and [6], we will design a delayed discrete observer, that works with a sampling time $T1$, as follows:
- Construction of the state $\hat{x}_1$:
From the system (3), we have:

$$\hat{x}_2(n+1) = \hat{x}_1(n)$$

By applying one delay on the output, we deduce the state $\hat{x}_1$ as following:

$$\hat{x}_1(n-1) = y_2(n) \quad (15)$$

- Construction of the state $\hat{x}_3$:
From the system (3), we have also:

$$\hat{x}_3(n) = \frac{a - \hat{x}_1(n+1) - \hat{x}_2^2(n)}{b}$$

Now, let us apply two delays on the output and using equation (15), we obtain the state $\hat{x}_3$ as following:

$$\hat{x}_3(n-2) = \frac{a - y_2(n) - y_2^2(n-2)}{b} \quad (16)$$

- Construction of message $\hat{m}$:
From system (3), we have:

$$\hat{m}(n) = \frac{\hat{x}_3(n+1) - \hat{x}_2(n) - A\hat{z}_2(n) - B\hat{z}_3(n))}{C}$$

Using three delays on the output and equation (16), we get:

$$\hat{m}(n-3) = \frac{a - y_2(n) - y_2^2(n-2)}{b}$$
$$- \frac{y_2(n-3) + A\hat{z}_2(n-3) + B\hat{z}_3(n-3)}{C} \quad (17)$$

Equation (17) allows constructing the message but only after the synchronization of the two continuous-time systems (1) and (4).

3) Demultiplexing block: At the reception, the received signal is first demultiplexed on two signals y_1 and y_2. The signal y_1 witch is accessible during the period $T1$ is now memorized during a period $T2 = 10T1$ (see figure 2). Then, the signal is introduced in the continuous observer. It should be noted that the sampling time $T2 = 10T1$ is chosen according to the Shannon's theorem. Another signal y_2 is accessible during 9 cycles and changes all cycles. This signal is introduced in the discrete observer (see figure 2).

III. SIMULATION RESULTS

In this section, the performances of the proposed method are evaluated using the Mtlab/Simulink software. First we will present the simulation results concerning the synchronization of the two continuous-time systems. The numerical value of M is equal to 23.16 and the gain K is equal to 10 and is chosen to ensure the stability of the observer (condition 10 given in section II-B.1). The initial conditions of the observer (4) are: $z_1(0) = 1.8$, $z_2(0) = 3$ and $z_3(0) = 0$. The initial conditions of the transmitter system are given in section II-A.1.

A. Synchronization results of the two continuous-time systems

Figures (3, 5 and 7) and (4, 6 and 8) give the states and their synchronization errors, respectively. From $t = 15s$, we can note that the amount percentage for errors e_1, e_2 and e_3 (Figures (4, 6 et 8)) are about 4.2%, 0.8% et 0.08%. This report allows us to assert that the errors are negligible, and all the states are perfectly estimated by the continuous observer.
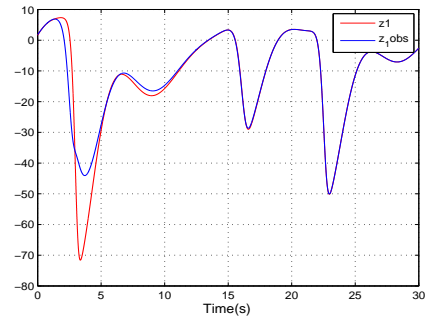

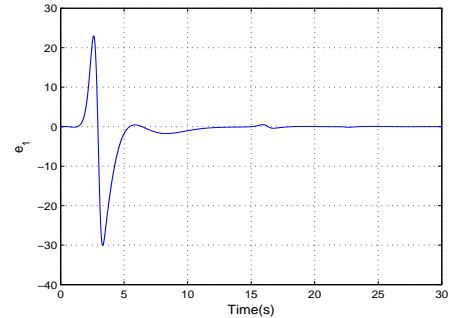Fig. 3. z_1 and $\hat{z}_1$

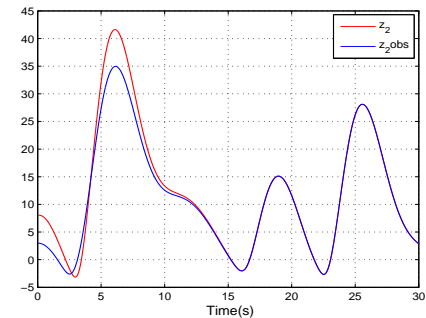Fig. 4. Synchronization error on the state z_1
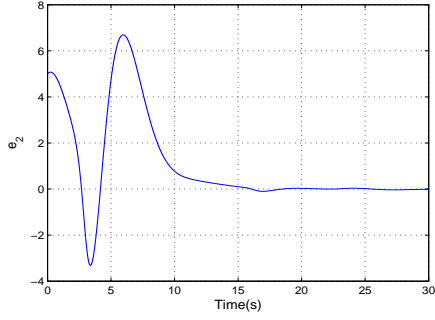

Fig. 5. z_2 and $\hat{z}_2$

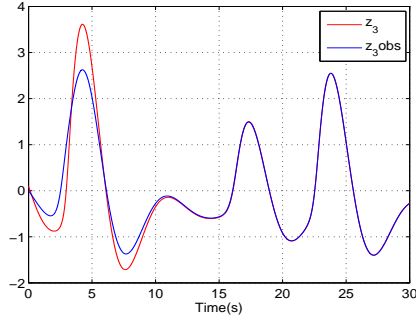Fig. 6. Synchronization error on the state z_2
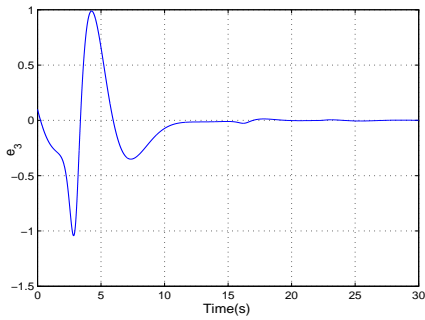

Fig. 7. z_3 and $\hat{z}_3$

Fig. 8. Synchronization error on the state z_3

.

B. Synchronization results of the two hybrid systems

In the following, we will present the simulation results concerning the synchronization of the two hybrid systems, i.e. the system (3) and the observer given in section (II-B.2). The new parameters A, B, C of the observer are: $A = 0.04$, $B = 0.1$ and $C = 1$ and the message to sent is a square signal with amplitude equal to C (the choice of theses amplitudes are justified just after the observer (3)). In our case, the continuous-time system (1) and its observer (4) still operate with the period $T1 = 0.001s$. The same period is used by discrete-time system (3) and its observer (15-16-17). The outputs (y_1 and y_2) are transmitted in the transmission channel at each period $T2 = 10T1$.

The Figures (9, 11) and (10, 12) give the states and the synchronization errors of the hybrid system with its corresponding observer, respectively. Note that the states x_1 et x_3 don't depend on the states z_1, z_2 and z_3 of the continuous-time system. This allows to establish that the

error $e_1 = x_1 - \hat{x}_1$ vanishes after the period $T1 = 0.001s$ which corresponds to the delay of one step on the output. (agree with equation (15)), and the error e_3 vanishes after a period $T = 2T1 = 0.002s$ which correspond to a delay of two steps on the output (agree with equation (16). On other hand, the reconstitution of the message m (see equation (17)) depends on the synchronization of the states z_1, z_2 and z_3 of the continuous-time transmitter (1) and the continuous receiver(4). From the previous figures (3, 5 and 7) and (4, 6 and 8)), we can notice that the time of the synchronization of the two systems (1) et (4) is obtained at $t = 15s$, and from this time the message is reconstituted (see figures 13 and 14).
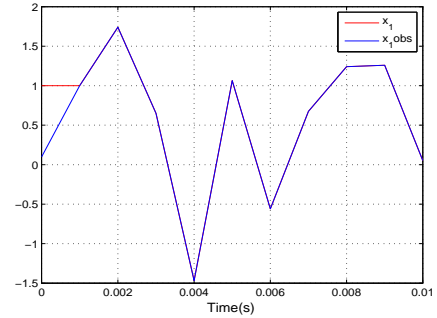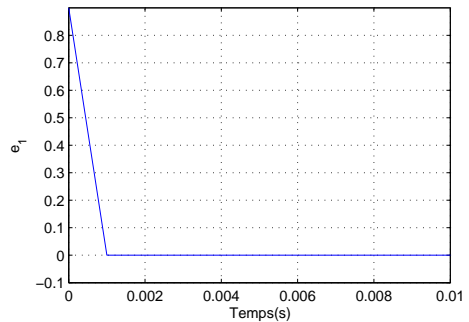

Fig. 9. x_1 and $\hat{x}_1$

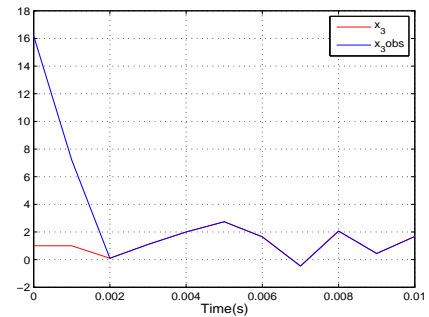Fig. 10. Synchronization error on the state x_1
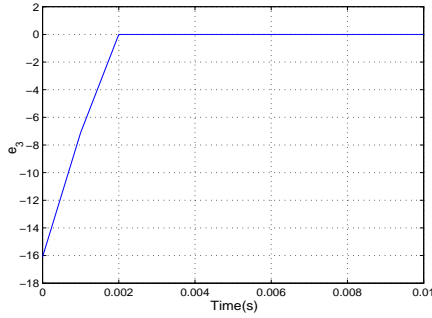

Fig. 11. x_3 and $\hat{x}_3$

Fig. 12. Synchronization error on the state x_3

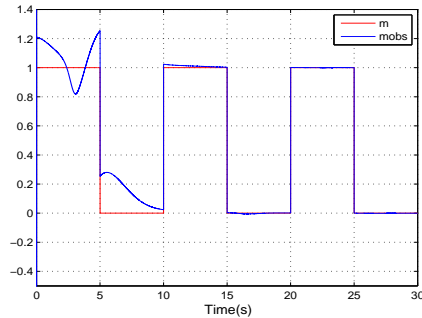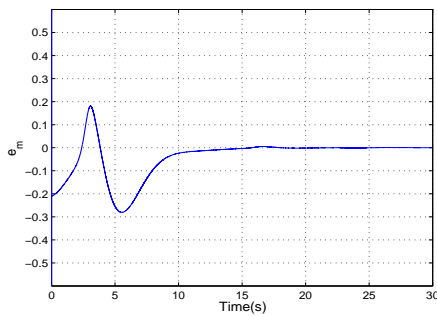

Fig. 13. Messages : m and $\hat{m}$

Fig. 14. Synchronization error on the message m

IV. CONCLUSION

In this paper, a transmission scheme based on dynamic hybrid systems is designed for private communications. In the transmitter part, the continuous chaotic system of type Colpitts is combined with a discrete chaotic system of type Henon in order to materialize a complex structure of the transmitter that is robust especially to a known-plaintext attacks. Also, the system is made robust by introducing delays [20] and continuous states, that don't ensure the observability recovery condition (this will be developed in our future works). In the transmission channel, the sent outputs are chosen with agreement with the rank of observability condition of the continuous-time system (Colpitts) and with the rank observability condition of the continuous-time system and the observability recovery condition of the discrete-time system (Henon). The strategy adopted to send the output signal consists

with composition of the two outputs $y_1 = z_1$ (Colpitts) and $y_2 = z_2$ (Henon) in the heterogeneous output signal which is transmitted in the channel transmission. In our study, we have demonstrated that the reconstruction of the discrete-time transmitter message depends on the synchronization of the transmitter and the receiver (continuous-time observer) and the exchange of the information is performed in discrete form. The choice of the sampling time of the continuous-time system must be done with more attention but this make the identification of its parameters complex. The study is validated in simulation, since the obtained results show that the message is reconstructed succefully on the level of the receiver (discrete observer) if and only if the two continuous systems (Colpitts and its observer) are synchronized.

REFERENCES

[1] F. Anstett, G. Millerioux and G. Bloch, "Chaotic Cryptosystems: Cryptanalysis and Identifiability," *IEEE Transactions on Circuits and Systems: Fundamantal Theory and Applications*,vol. 53, December 2006.

[2] J.P. Barbot, I. Belmouhoub and L.Boutat-Baddas, "Observability Bifurcations: Application to Cryptography," *In Chaos in Automatic Control, Taylor and Francis*, 2005.

[3] A. Basiliauskas, A.Tamasevicius, S. Bumeliene and E. Lindberg, "Synchronization of Chaotic Colpitts Oscillator," *Scientific proceeding of Riga Technical university*, pp. 55–58, 2001.

[4] I. Belmouhoub, M. Djemaï and J.P. Barbot, " Observability quadtatic Normal Form for Discrete-Time systems," *IEEE Transactions on Automatic Control*,vol. 50, July 2005.

[5] H. Dedieu H, M.P. Kennedy and M. Hasler, "Newblock Chaos shift keying: modulation and demodulation of a chaoticcarrier using self-synchronizing Chua's circuits," *IEEE Transactions on Circuits and Systems, Circuits and Systems II: Analog and Digital Signal Processing*, vol. 40, pp. 634–642, 1993.

[6] M. Djemaï, J-P. Barbot and I. Belmouhoub, "Discrete-Time Normal Form for Left Invertibility Problem,"*European Journal of Control*, vol. 15, pp. 194–204, 2009.

[7] A.S Dmitriev, G.A Kassian and A.D Khilinsky, "Chaotic synchronization of henon mappings: The information approach," *Technical Physics Letters*, vol. 28, May 2002.

[8] G.C Freeland and T.S Durrani, "Nonlinear state observers for chaotic systems and their application to communications signal process," *Exploiting Chaos in Signal Processing, IEE Colloquium on*, 1994.

[9] M.Ghanes, G. Zheng and J. De Leon, "On simultaneous parameter identification and state estimation for cascade state affine systems," American Control Conference (ACC), Seattle, Washington, USA,11-13 June, 2008.

[10] M. L'Hernault, J-P. Barbot and A. Ouslimani, "Feasability of Analogue Realization of Sliding Mode Observer: Application to Data Transmission," *IEEE Transactions on Circuits and Systems: Fundamantal Theory and Applications*, vol. 55, March 2008.

[11] L. Koracev, "Chaos-based cryptography : a brief overview," *IEEE Transactions on Circuits and Systems*, pp. 6–21, July 2001.

[12] G.M. Maggio and O.D. Feo, "Nonlinear Analysis of the Colpitts Oscillator and Application to Design," *IEEE Transactions on Circuits and Systems: Fundamantal Theory and Applications*, vol. 49, September 1999.

[13] G.M Maggio and M.P. Kennedy, "Experimental manifestations of chaos in the Colpitts oscillator," [Proc. of ICECS, Seville, spain, p. 194–204, 1997].

[14] H. Nijmeijer, "On Synchronization of Chaotic Systems," [Proc. 36th Conference on Decision and Control, San Diego, California USA, December 1997].

[15] H. Nijmeijer and Iven M.Y Mareels, "An observer Looks at Synchronization," *IEEE Transactions on Circuits and Systems: Fundamantal Theory and Applications*, vol. 44, October 1997.

[16] U. Parlitz, L.O. Chua, L. Kocarev, K.S. Halle and A. Shang, "Transmission of digital signals by chaotic synchronization," *International Journal of Bifurcations and Chaos*, vol. 3, pp. 973–977, 1993.

[17] L.M. Pecora and T.L. Carroll, "Synchronization in Chaotic Systems," *Physicals Review and Letters*, pp. 821–824, 1990.

[18] K. Veselyand J. Podolsky, "Chaos in a modified Henon- Heiles system describing geodesics in gravitational waves," *Technical Physics Letters A*, vol. 271, pp 368–371, July 2000.

[19] C.W. Wu and L.O. Chua, "Simple way to synchronize chaotic systems with applications to secure communications systems," *International Journal of Bifurcations and Chaos*, vol. 3, pp. 1619–1627, 1993.

[20] G. Zheng, D. Boutat, T. Floquet and J.P Barbot, "Secure data transmission based on multi-input multi-output delayed chaotic system," International Journal of Bifurcations and Chaos, vol. 18, 2007.