HAL open science

Secure data transmission based on multi-input multi-output delayed chaotic system

Gang Zheng, Driss Boutat, Thierry Floquet, Jean-Pierre Barbot

To cite this version:

Gang Zheng, Driss Boutat, Thierry Floquet, Jean-Pierre Barbot. Secure data transmission based on multi-input multi-output delayed chaotic system. International journal of bifurcation and chaos in applied sciences and engineering , 2008, 18 (7), pp.2063-2072. 10.1142/S0218127408021567 . inria-00176896v2

HAL Id: inria-00176896

https://inria.hal.science/inria-00176896v2

Submitted on 23 Oct 2007

HAL is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L'archive ouverte pluridisciplinaire **HAL**, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d'enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.

Secure Data Transmission Based on Multi-input Multi-output Delayed Chaotic System

G. Zheng[1], D. Boutat[1], T. Floquet[3,5] and J.-P. Barbot[4,5]
[1]INRIA Rhône-Alpes,
655 avenue de l'Europe, 38334 St Ismier Cedex, France
[2]LVR, ENSI-Bourges/Université d'Orléans,
10, Bd. Lahitolle, 18020 Bourges, France
[3]LAGIS UMR CNRS 8146, Ecole Centrale de Lille,
BP 48, Cité Scientifique, 59651 Villeneuve-d'Ascq, France
[4]Equipe Commande des Systèmes (ECS), ENSEA,
6 Av. du Ponceau, 95014 Cergy, France
[5]Equipe Projet ALIEN INRIA-Futurs, France

Abstract

This paper deals with the problem of secure data transmission based on multi-input multi-output delayed chaotic systems. A new multi-input secure data transmission scheme is proposed. Moreover, in order to increase again the robustness of secure data transmission, delays are introduced as a second firewall against known plain-text attack. With this method, the parameters used as secret keys of the system are not identifiable and, as a result, the proposed scheme is robust to known plain-text attacks.

Keywords: Multi-input Multi-output system, Chaos, Observer, Left Invertibility Problem, Delays system.

1 Introduction

Over the past decade, synchronization of chaotic systems and its potential application to secure communications have received a lot of attention since Pecora and Carrol proposed a method to synchronize two identical chaotic systems (Pecora *et al.*, 1990). Many chaos-based secure data transmission systems have been proposed, which can be roughly classified at least into the following categories: chaotic masking (Kovarev *et al.*, 1992), chaotic masking with delays (Lee *et al.*, 2003), chaotic switching (Parlitz *et al.*, 1992), chaotic modulation (Wu *et al.*, 1993) and inverse system approach (Feldmann *et al.*, 1996)....

Since the work (Nijmeijer *et al.*, 1997), synchronization can be viewed as a special case of observer design problem, i.e the state reconstruction from measurements of an output variable under the assumption that the system structure

and parameters are known. For a synchronization chaos-based cryptosystem, a receiver (an observer from a control theory point of view) is designed in order to synchronize the transmitter (a chaotic system with unknown inputs from a control theory point of view) and to reconstruct the confidential messages (the unknown inputs of the chaotic system from a control theory point of view). Many techniques arising from observation theory have been applied to the problem of synchronization: observers with linearizable dynamics (Huijberts et al., 2001), adaptive (Fradkov et al., 2000) or sliding mode observers (Boutat et al., 2001), generalized hamiltonian form based observers (H. Sira Ramirez and C. Cruz Hernandez, 2001), etc ...

It is known that some of the designed secure data transmission systems based on chaos with single input have been broken (Pérez *et al.*, 1995), (Short, 1994), (Yang *et al.*, 1998), (Anstett *et al.*, 2006). Particularly, it has been recently shown in (Anstett *et al.*, 2006) that traditional methods of data transmission by synchronization of chaotic systems suffer from the serious drawback of not being robust with respect to known plain-text attacks. More precisely, according to the famous Kerkhoff assumption (Kerkhoff, 1883), it is assumed that hackers know all the details about the cryptosystem but the secret key. It is known that, for the chaos-based cryptosystem, the keys are usually the chaotic system parameters. So from a control theory point of view, the possibility to reconstruct the keys for chaos-based cryptosystem is equivalent to the possibility to identify the parameters of the chaotic system (Huijberts *et al.*, 1997). Consequently, a robust and reliable chaos-based cryptosystem should be designed such that its parameters are not identifiable.

Although chaotic synchronization using systems with a single input has been widely investigated in the last decade, it is not the case for the multi-input case. One of the main reasons is the possibility, for systems with several inputs, to use multiplexing techniques before ciphering the messages. Thus, the problem becomes similar to a single input one. Nevertheless, although multiplexing techniques appear to be a very convenient and economical means, the main drawback of this kind of scheme is that all the messages have the same risk to be broken.

In this paper, solutions are provided to improve the secure data transmission based on chaotic synchronization. First, a real multi-input secure data transmission is proposed. In this scheme, the inputs are not composed in order to obtain only one input which 'drives' the chaotic system but the totality of the inputs drive the chaotic system and only the outputs are multiplexed. This approach decreases the risk of known plain-text attacks, because the probability to know all plain-texts at the same time is less than to know only one message. Moreover, the multi-input scheme has the advantage to allow different priorities of secure data transmission. For example, every user can access to one input while only the administrator of the group can access to other inputs. Inspired by the above consideration, a new scheme is derived as follows: for the transmitter system, the composition is used to combine the outputs, instead of combining the inputs directly. This approach relies on the problem of designing an observer for chaotic system (Nijmeijer *et al.*, 1997) but with unknown inputs. Actually,

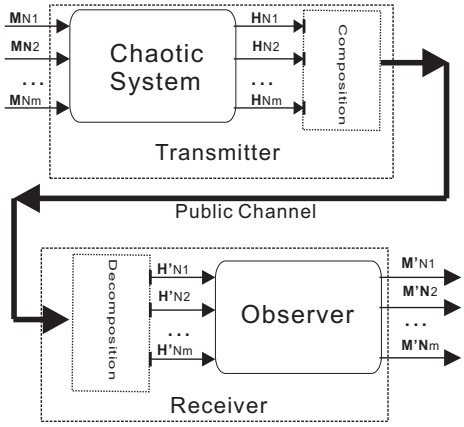

Figure 1: Scheme for multiple secure data transmission system

the problem of recovering the message is a left invertibility problem (Hirschorn R.M., 1979; Singh S.N., 1982; Respondek W., 1990). This scheme can also be seen as a version for multi-input multi-output systems of the traditional inverse system approach proposed in (Feldmann *et al.*, 1996). Fig. 1 illustrates the scheme of the considered approach. According to this scheme, the inputs can not always be recovered simultaneously, i.e., even if the message M_{N_1} in Fig. 1, for example, has been broken, the other ones still remain unbroken. Note that the users can be divided into several groups according to different requirements or emergent levels. In that case, different groups (M_{N1}, M_{N2},..., M_{Nm} in Fig. 1) have different degrees of security.

Even if it reduces the risk of the messages to be broken, it will be shown that this multi-input approach is not robust enough against an attack to known plain-texts if all the inputs are known at the same time. Indeed, in that case, the parameters used as secret keys are still identifiable. To solve this problem, we propose to introduce delays (that will also be considered as a part of the secret keys) in the outputs of the systems. As a result, the parameters are not identifiable anymore and classical attacks are inefficient.

The outline of the paper is as follows. The next section is devoted to the analysis of the observability and the identifiability of multi-input multi-output systems without delays. A left inversion algorithm for systems with unknown inputs, that was introduced in (Barbot *et al.*, 2005), is recalled. Then, cryptanalysis and identifiability problems are discussed in Section 3 and, in Section 4, a new scheme is given to design a multiple secure data transmission system with delays based on a given chaotic system, in which the risk for the keys to be broken by known plain-text attacks can be reduced. In Section 5, an example based on Qi's chaotic system (Qi *et al.*, 2005) illustrates the proposed method.

2 A left invertibility algorithm for systems without delays

In this section, the left invertibility algorithm given in (Barbot *et al.*, 2005) is recalled.

Consider first a chaotic system without delays in the following general form:

$$\dot{x} = f(x) \tag{1}$$

$x \in U$ is the state vector, U is an open set of $\Re^n$, and $f : \Re^n \to \Re^n$ is analytic.

The aim is to establish a multiple secure data transmission system which can be described by the following form:

$$\begin{cases} \dot{x} = f(x,k) + \sum_{i=1}^{m} g_i(x,k)\, u_i \\ y = [h_1(x), ..., h_p(x)]^T \end{cases} \tag{2}$$

where $k \in \Re^q$ is the key vector, $y \in \Re^p$ is the output vector and $u = [u_1, \ldots, u_m]^T \in \Re^m$ represents the confidential information to be transmitted. The vector fields $f = [f_1, \ldots, f_n]^T$, $g = [g_1, \ldots, g_m]$ and $h = [h_1, \ldots, h_p]^T$ are assumed to be sufficiently smooth on U, where f_i, $h_j \in R$ and $g_l \in R^n$, $i \in [1,n]$, $j \in [1,p]$, $l \in [1,m]$. Without loss of generality, it is assumed that, for all $x \in U$, the distribution $span\{g_1, \ldots, g_m\}$ and the codistribution $span\{dh_1, \ldots, dh_p\}$ are nonsingular. It is also assumed that $p \geq m$.

Let us define the following sets that will be used in the sequel:

- The vector relative degree ρ of the system (2) is defined by $\rho = \{\rho_1, ..., \rho_p\}$, where $\rho_i = \min\{s \text{ such that } L_{g_k} L_f^{s-1} h_i \neq 0 \text{ for } k = 1:m\}, \in [1,p]$.
- Φ is the codistribution spanned by the time derivatives of the measured outputs not affected by the inputs:

$$\Phi = span\{dh_1, ..., dL_f^{\rho_1 - 1} h_1, ..., dh_p, ..., dL_f^{\rho_p - 1} h_p\}$$

- Ω is a basis of Φ:

$$\Omega = \{dh_1, ..., dL_f^{r_1 - 1} h_1, ..., dh_p, ..., dL_f^{r_p - 1} h_p\}$$

  where $r = \dim \Omega = \sum_{i=1}^{p} r_i$.

  $\pounds$ is the commutative algebra linked to Ω:

$$\pounds = span\{h_1, ..., L_f^{r_1 - 1} h_1, ..., h_p, ..., L_f^{r_p - 1} h_p\} \tag{3}$$

- $\Omega_{\pounds}$ is the module spanned by Ω over $\pounds$, and $\Omega_{\pounds}^1$ is the submodule spanned by

$$\{dh_1, ..., dL_f^{r_1 - 2} h_1, ..., dh_p, ..., dL_f^{r_p - 2} h_p\}$$

  over $\pounds$ where by definition $L_f^{-1} h_j = 0$ and $L_f^0 h_j = h_j$.

- G is the smallest involutive distribution that contains $\{g_1(x), ..., g_m(x)\}$. Denote $k = dimG$, $m \leq k \leq n$.
- $G^{\perp}$ is the annihilator of G, i.e.

$$G^{\perp} = span\{\alpha_1, ..., \alpha_{n-k}\}$$

where the α_i are one-forms such that for all $\lambda \in G$, $l_\lambda \alpha_i = 0$ for $i = 1 : n-k$, where $l_\lambda \alpha = \alpha(\lambda)$ is the inner product of the vector field λ and α.

Using the set Ω, one can define a transformation $(\xi, \eta) = \phi(x)$ such that the system (2) is locally transformed into the following normal form:

$$\begin{cases} \dot{\xi}_1^i = \xi_2^i \\ \vdots \\ \dot{\xi}_{r_i-1}^i = \xi_{r_i}^i \\ \dot{\xi}_{r_i}^i = L_f^{r_i} h_i(x) + \sum_{j=1}^{m} L_{g_j} L_f^{r_i-1} h_i(x) u_j \\ \dot{\eta} = p(\xi, \eta) + q(\xi, \eta) u \\ y_i = \xi_1^i \end{cases} \tag{4}$$

where

$$\xi = \begin{bmatrix} (\xi^1)^T & \cdots & (\xi^p)^T \end{bmatrix}^T$$

and

$$\xi^i = \begin{bmatrix} \xi_1^i \\ \vdots \\ \xi_{r_i}^i \end{bmatrix} = \begin{bmatrix} h_i(x) \\ \vdots \\ L_f^{r_i-1} h_i(x) \end{bmatrix}, \text{ for } i \in [1, p].$$

Using classical observation algorithms, the unknown input u can be obtained (and thus the left invertibility problem can be solved) under some restrictive conditions: one should have $r = n$ or the distribution $span\{g_1, \ldots, g_m\}$ should be involutive. In order to increase the complexity of the unknown message recovery, it is proposed here to set the unknown input channel such that $r < n$ and such that $span\{g_1, \ldots, g_m\}$ is not involutive. In (Barbot *et al.*, 2005), the authors described an observation algorithm that solves the left invertibility problem for such systems. It is briefly recalled here. The main idea of this algorithm is to find extra information through functions of the outputs and their time derivatives. Let us define:

$$\begin{aligned} V &= \begin{bmatrix} L_f^{r_1} h_1(x) & \cdots & L_f^{r_p} h_p(x) \end{bmatrix}^T + \Gamma(x) u \\ &= \begin{bmatrix} y_1^{(r_1)} & \cdots & y_p^{(r_p)} \end{bmatrix}^T \end{aligned} \tag{5}$$

with

$$\Gamma(x) = \begin{bmatrix} L_{g_1} L_f^{r_1-1} h_1(x) & \cdots & L_{g_m} L_f^{r_1-1} h_1(x) \\ \vdots & \ddots & \vdots \\ L_{g_1} L_f^{r_m-1} h_p(x) & \cdots & L_{g_m} L_f^{r_m-1} h_p(x) \end{bmatrix}$$

that can be known using the normal form (4). Assume there exists a $1 \times p$ vector function $K(x) = [k_1(x), ..., k_p(x)] \neq 0$, with $k_i \in \pounds$, $i = 1, ...p$ such that

$$K\Gamma = 0 \tag{6}$$

and define a dummy output as follows:

$$\bar{y} = \bar{h}(x) = KV = \sum_{i=1}^{p} k_i(x) L_f^{r_i} h_i(x).$$

If $d\bar{y} \notin \Omega_{\pounds}$, it can be considered as a suitable fictitious output in order to estimate more states. The system has a new vector relative degree $\bar{r} = n$ with respect to the original outputs and the fictitious output $\bar{y}$. If $\bar{r} = n$, it has been shown in [Barbot, *et al.*, 2005] that both the state x and the unknown inputs u can be estimated in finite time.

The following proposition gives some equivalent conditions that guarantee the existence of a solution to Equation (6) and thus, the existence of a proper dummy output.

Proposition 1 *(Barbot et al., 2005) The following conditions are equivalent:*
i) Equation (6) has a non trivial solution K and $d\bar{y} \notin \Omega_{\pounds}$.
ii) the set of equivalence classes $E = \frac{G^{\perp} \cap \Omega_{\pounds}}{G^{\perp} \cap \Omega_{\pounds}^1}$ of elements of $G^{\perp} \cap \Omega_{\pounds}$ modulo $G^{\perp} \cap \Omega_{\pounds}^1$ is such that $E \neq \varnothing$,
iii) $\Xi = \{\alpha \in G^{\perp} \cap \Omega_{\pounds}$ such that $l_f \alpha \notin \pounds\} \neq \varnothing$.

The dummy outputs $\bar{y}$ are only function of the previously known outputs and their time derivatives. If the system is left invertible, the algorithm derived in (Barbot *et al.*, 2005) provides an expression of all the states and the unknown inputs as functions of the original outputs y, their time derivatives and the key vector[1]:

$$\begin{cases} x = \Xi\left(y, \dot{y}, ..., y^{(n-1)}, k\right) \\ u = \Psi\left(y, \dot{y}, ..., y^{(n-1)}, k\right) \end{cases} \tag{7}$$

Then, the states and the unknown inputs can be reconstructed in finite time via for instance sliding mode observers (see (Floquet and Barbot, 2006)).

Consequently, for this scheme, the security of the transmission is partially based on the difficulty to find all the dummy outputs $\bar{y}$. But, when all $\bar{y}$ are formally known it is possible to derive equations (7). Then, the main question is whether or not it is possible from (7) to identify the key k. This point is discussed in the next section.

[1]This algebraic point of view was also adopted in (Cannas *et al.*, 2005) and (Sira, 2006) for the finite time synchronization of some classes of chaotic systems.

3 Cryptanalysis and identifiability

Equation (7), and consequently the proposed scheme, can not resist to known plain-texts attack when all plain-texts are known at the same time. Indeed, consider the second equation of (7) at different instants $t_1, ..., t_l$. It is possible to obtain independent equations with respect to k:

$$\left\{\begin{array}{ccc} u(t_1) & = & \Psi\left(y(t_1), \dot{y}(t_1), ..., y^{(n-1)}(t_1), k\right) \\ u(t_2) & = & \Psi\left(y(t_2), \dot{y}(t_2), ..., y^{(n-1)}(t_2), k\right) \\ \vdots & \vdots & \vdots \\ u(t_l) & = & \Psi\left(y(t_l), \dot{y}(t_l), ..., y^{(n-1)}(t_l), k\right) \end{array}\right. \tag{8}$$

Then, two cases appear:

- there exist $q = l$ independent equations, which is equivalent to:

$$rank \begin{pmatrix} \frac{\partial \Psi\left(y(t_1), \dot{y}(t_1), ..., y^{(n-1)}(t_1), k\right)}{\partial k} \\ \frac{\partial \Psi\left(y(t_2), \dot{y}(t_2), ..., y^{(n-1)}(t_2), k\right)}{\partial k} \\ \vdots \\ \frac{\partial \Psi\left(y(t_q), \dot{y}(t_q), ..., y^{(n-1)}(t_q), k\right)}{\partial k} \end{pmatrix} = q$$

  From the implicit function theorem it is obvious that all parameters are identifiable. Consequently, such a data transmission scheme is not robust against known plain-text attacks.

- $l < q$, which means that $q - l$ parameters are not identifiable and can not play the role of the key. Thus, the knowledge of these parameters is not necessary for recovering the message and those parameters are of no interest in the transmitter design.

The question is how to obtain an input-output relation equation, sensitive to parameters, but that should be not identifiable even if all the inputs are known. To solve this problem, it is proposed here to introduce delays (that are also a part of the unknown parameters) in the secure data transmission system.

Assume for instance that at least one delay appears in (7). Then, (8) becomes:

$$\left\{\begin{array}{ccc} u(t_1) & = & \Psi(y(t_1), \dot{y}(t_1), ..., y^{(n-1)}(t_1), \\ & & y(t_1 - \tau), ..., y^{(j)}(t_1 - \tau), k) \\ u(t_2) & = & \Psi(y(t_2), \dot{y}(t_2), ..., y^{(n-1)}(t_2), \\ & & y(t_2 - \tau), ..., y^{(j)}(t_2 - \tau), k) \\ \vdots & \vdots & \vdots \\ u(t_l) & = & \Psi(y(t_l), \dot{y}(t_l), ..., y^{(n-1)}(t_l), \\ & & y(t_l - \tau), ..., y^{(j)}(t_l - \tau), k) \end{array}\right. \tag{9}$$

with $j \leq n - 1$. From (9), it can be seen that there are more unknown inputs, $y^{(s)}(t_z - \tau)$ and k, than the number of independent equations. Consequently,

the introduction of the delay operator into the input-output relation equation exhibits a robust characteristics with respect to known plain-text attacks.

In the following section, the robustness of the previously proposed scheme is improved by the introduction of delays.

4 Secure data transmission scheme based on systems with delays

Consider the system (2) with delays:

$$\begin{cases} \dot{x} = f(x,k) + \sum_{i=1}^{m} g_i(x, y(t-\tau_1), .., y(t-\tau_l), k)\, u_i \\ y = [h_1(x), ..., h_p(x)]^T \end{cases} \tag{10}$$

where the l delays are also a part of the secret key. Let us show that the algorithm given in (Barbot *et al.*, 2005) still allows to solve the left invertibility problem and thus to recover the messages u_i.

Since the delays only appear in the g_i vector fields, it is always possible to transform such system in the form (4) with delays:

$$\begin{cases} \dot{\xi}_1^i = \xi_2^i \\ \vdots \\ \dot{\xi}_{r_i-1}^i = \xi_{r_i}^i \\ \dot{\xi}_{r_i}^i = L_f^{r_i} h_i(x) + \sum_{j=1}^{m} L_{g_j} L_f^{r_i-1} h_i(x) u_j \\ \dot{\eta} = p(\xi,\eta) + q(\xi,\eta,y(t-\tau_1),..,y(t-\tau_l))u \\ y_i = \xi_1^i \end{cases} \tag{11}$$

where $L_{g_j} L_f^{r_i-1} h_i$ is given by:

$$L_{g_j} L_f^{r_i-1} h_i = \frac{\partial L_f^{r_i-1} h_i}{\partial x} g_j(x, y(t-\tau_1), .., y(t-\tau_l), k).$$

Then Equation (5) becomes

$$\begin{aligned} V &= \left[\begin{array}{ccc} L_f^{r_1} h_1(x) & \cdots & L_f^{r_p} h_p(x) \end{array}\right]^T \\ &+ \Gamma(x, y(t), y(t-\tau_1), .., y(t-\tau_l), k)u \\ &= \left[\begin{array}{ccc} y_1^{(r_1)} & \cdots & y_p^{(r_p)} \end{array}\right]^T. \end{aligned} \tag{12}$$

Assume it is possible to find $K(x) = [k_1(x), ..., k_p(x)] \neq 0$ with $k_i \in \pounds$ such that

$$K(x)\Gamma(x, y(t), y(t-\tau_1), ..., y(t-\tau_l), k) = 0.$$

Then, in a similar way to the case without delays, it is possible to recover the message u in finite time.

As a way of illustration, an example is given in the next section in order to illustrate all the key points of the proposed method. A sliding mode observer that provides the knowledge of the confidential information in finite time is also designed.

5 Illustrative example

Let us construct a multiple secure data transmission system based on Qi's Chaotic System in (Qi *et al.*, 2005), which is described as follows:

$$\begin{cases} \dot{x}_1 = a(x_2 - x_1) + x_2x_3x_4 \\ \dot{x}_2 = b(x_1 + x_2) - x_1x_3x_4 \\ \dot{x}_3 = -cx_3 + x_1x_2x_4 \\ \dot{x}_4 = -dx_4 + x_1x_2x_3 \end{cases} \tag{13}$$

where x_i $(i = 1, ..., 4)$ are the state variables, and $a,\ b,\ c,\ d$ are all positive real constant parameters. Consider the following transmitter which is based on the chaotic system (13):

$$\begin{cases} \dot{x}_1 = a(x_2 - x_1) + x_2x_3x_4 \\ \qquad +(1 + e\,(x_1(t-\tau))^2)m_1 \\ \dot{x}_2 = b(x_1 + x_2) - x_1x_3x_4 \\ \dot{x}_3 = -cx_3 + x_1x_2x_4 + x_3m_2 \\ \dot{x}_4 = -dx_4 + x_1x_2x_3 - x_4m_2 \end{cases} \tag{14}$$

where e is a positive real constant, τ is the introduced delay and, for sake of notation simplicity, x_i stands for $x_i(t)$.
Note that $g_1 = \begin{bmatrix} (1 + e\,(x_1(t-\tau))^2) & 0 & 0 & 0 \end{bmatrix}^T$ and $g_2 = \begin{bmatrix} 0 & 0 & x_3 & -x_4 \end{bmatrix}^T$.
It is assumed that m_1 and m_2 are small, that $0 < m_2 < \beta$ and that the following condition is satisfied:

$$d - c - \beta > 0. \tag{15}$$

The outputs are set as $y = \begin{bmatrix} x_1 & x_2 \end{bmatrix}^T$. The input channel vector fields g_1 and g_2 have been chosen such that the strong relative degree of the system is $r = 3$. So, following the lines of the algorithm proposed in (Barbot *et al.*, 2005), calculate

$$\begin{aligned} \Gamma &= \begin{pmatrix} L_{g_1}h_1 & L_{g_2}h_1 \\ L_{g_1}L_fh_2 & L_{g_2}L_fh_2 \end{pmatrix} \\ &= \begin{pmatrix} (1 + e\,(x_1(t-\tau))^2) & 0 \\ (1 + e\,(x_1(t-\tau))^2)(b - x_3x_4) & 0 \end{pmatrix}. \end{aligned}$$

Thus, one can choose

$$K = \begin{pmatrix} b - x_3x_4, & -1 \end{pmatrix}$$

such that $K\Gamma = 0$. Since K is not a function of the delayed output, it is possible to use again the algorithm proposed in (Barbot *et al.*, 2005). One has

$$\begin{aligned} \pounds &= span\{h_1, h_2, L_fh_2\} \\ &= span\{x_1, x_2, x_3x_4\} \end{aligned}$$

because

$$L_fh_2 = b(x_1 + x_2) - x_1x_3x_4 = x_3x_4 \mathrm{mod}\{x_1, x_2\}$$

Then, the following dummy output can be defined as:

$$\begin{aligned}\bar{y} &= K\begin{bmatrix} L_f h_1 \\ L_f^2 h_2 \end{bmatrix} = (b - x_3 x_4)\,\dot{y}_1 - \ddot{y}_2 \\ &= \left(x_3^2 + x_4^2\right) \bmod \pounds(x)\end{aligned}$$

and $d\bar{y} \notin \Omega_{\pounds}$. Thus, item $i)$ of Proposition 1 is satisfied. Then, let us set

$$y \triangleq \begin{bmatrix} x_1, & x_2, & x_3^2 + x_4^2 \end{bmatrix}^T.$$

With this new output y, the dimension of the set

$$\Phi = span\{dx_1, dx_2, dx_3x_4, d\left(x_3^2 + x_4^2\right)\}$$

is equal to 4. This means that one can recover all the state in finite time. A straightforward consequence of the fact that $span\{g_1, g_2\}$ is regular, is the possibility to reconstruct the unknown messages also in finite time. For this, let us design a sliding mode observer as follows:

$$\begin{cases} \dot{\hat{x}}_1 = a\,(x_2 - x_1) + x_2\tilde{x}_3\tilde{x}_4 + E_1\lambda_1 sign(x_1 - \hat{x}_1) \\ \dot{\hat{x}}_2 = b(x_1 + x_2) + \lambda_2 sign(x_2 - \hat{x}_2) \\ \frac{d(\hat{x}_3\hat{x}_4)}{dt} = -\,(c + d)\,\tilde{x}_3\tilde{x}_4 \\ \qquad +E_2\lambda_3 sign(\tilde{x}_3\tilde{x}_4 - \hat{x}_3\hat{x}_4) \\ \frac{d\left(\hat{x}_3^2+\hat{x}_4^2\right)}{dt} = -2c\tilde{x}_3^2 - 2d\tilde{x}_4^2 + 4x_1x_2\tilde{x}_3\tilde{x}_4 \\ \qquad +2E_3\lambda_4 sign\left(\left(\tilde{x}_3^2 + \tilde{x}_4^2\right) - \left(\hat{x}_3^2 + \hat{x}_4^2\right)\right) \end{cases} \tag{16}$$

with

$$\begin{aligned} &\lambda_i > 0,\ i = 1, ..., 4 \\ &E_1 = \begin{cases} 1 & x_2 = \hat{x}_2 \\ 0 & \text{otherwise} \end{cases} \\ &E_2 = \begin{cases} 1 & \text{if } E_1 = 1 \text{ and } x_1 = \hat{x}_1 \\ 0 & \text{otherwise} \end{cases} \\ &E_3 = \begin{cases} 1 & \text{if } E_2 = 1 \text{ and } \tilde{x}_3\tilde{x}_4 = \hat{x}_3\hat{x}_4 \\ 0 & \text{otherwise} \end{cases} \end{aligned}$$

and with the auxiliary states:

$$\tilde{x}_3\tilde{x}_4 = -\frac{\lambda_2 sign(x_2 - \hat{x}_2)}{x_1} \tag{17}$$

$$\tilde{x}_3^2 + \tilde{x}_4^2 = \frac{E_2\lambda_3 sign(\tilde{x}_3\tilde{x}_4 - \hat{x}_3\hat{x}_4)}{x_1x_2}. \tag{18}$$

Observability bifurcations can also introduced in order to improve the robustness of the transmission scheme. Here, the submanifold of observability singularity is given by

$$S = \{x_1 = 0\} \cup \{x_1x_2 = 0\}.$$

In order to overcome the singularity, one can use the same method as in (Barbot *et al.*, 2003).

The following quantities will be used to reconstruct the messages:

$$\tilde{m}_1 = \frac{E_2\lambda_1 sign(x_1-\hat{x}_1)}{(1+e\,(x_1(t-\tau))^2)} \tag{19}$$

$$\tilde{m}_2 = \frac{E_4\lambda_4 sign\left(\left(\tilde{x}_3^2+\tilde{x}_4^2\right)-\left(\hat{x}_3^2+\hat{x}_4^2\right)\right)}{\tilde{x}_3^2-\tilde{x}_4^2}. \tag{20}$$

where

$$E_4 = \begin{cases} 1 & \text{if } E_3 = 1 \text{ and } \tilde{x}_3^2+\tilde{x}_4^2 = \hat{x}_3^2+\hat{x}_4^2 \\ 0 & \text{otherwise} \end{cases}$$

The observation errors are defined by:

$$\begin{cases} e_1 = x_1-\hat{x}_1 \\ e_2 = x_2-\hat{x}_2 \\ e_{34} = x_3x_4-\hat{x}_3\hat{x}_4 \\ e_{3^2+4^2} = \left(x_3^2+x_4^2\right)-\left(\hat{x}_3^2+\hat{x}_4^2\right) \end{cases}$$

From system (14), it can be computed that:

$$\frac{d\,(x_3x_4)}{dt} = -\,(c+d)\,x_3x_4 + x_1x_2\left(x_3^2+x_4^2\right)$$

and

$$\begin{aligned} \frac{d\left(x_3^2+x_4^2\right)}{dt} &= -2cx_3^2+4x_1x_2x_3x_4 \\ &\quad -2dx_4^2+2\left(x_3^2-x_4^2\right)m_2. \end{aligned} \tag{21}$$

Thus, the dynamics of the observation error is given by:

$$\begin{cases} \dot{e}_1 = x_2\,(x_3x_4-\tilde{x}_3\tilde{x}_4)+(1+e\,(x_1(t-\tau))^2)m_1-E_1\lambda_1 sign(e_1) \\ \dot{e}_2 = -x_1x_3x_4-\lambda_2 sign(e_2) \\ \dot{e}_{34} = -\,(c+d)\,(x_3x_4-\tilde{x}_3\tilde{x}_4)+x_1x_2\left(x_3^2+x_4^2\right) \\ \qquad -E_2\lambda_3 sign(\tilde{x}_3\tilde{x}_4-\hat{x}_3\hat{x}_4) \\ \dot{e}_{3^2+4^2} = -2c\left(x_3^2-\tilde{x}_3^2\right)-2d\left(x_4^2-\tilde{x}_4^2\right) \\ \qquad +4x_1x_2\,(x_3x_4-\tilde{x}_3\tilde{x}_4)+2\left(x_3^2-x_4^2\right)m_2 \\ \qquad -2E_3\lambda_4 sign\left(\left(\tilde{x}_3^2+\tilde{x}_4^2\right)-\left(\hat{x}_3^2+\hat{x}_4^2\right)\right) \end{cases}$$

The convergence of the sliding mode observer relies on a step-by-step procedure.

First step: one has:

$$\dot{e}_2 = -x_1x_3x_4-\lambda_2 sign(e_2).$$

All the states are bounded. So, one can choose the gain $\lambda_2 > \sup_{\forall t>0}|-x_1x_3x_4|$ so that a sliding motion appears after a finite time t_1 on $e_2 = 0$. Writing that $\dot{e}_2 = 0$ gives :

$$-x_1x_3x_4 = \lambda_2 sign(e_2).$$

Then

$$\tilde{x}_3\tilde{x}_4 = -\frac{\lambda_2 sign(e_2)}{x_1} = x_3x_4 \tag{22}$$

and

$$E_1 = 1. \tag{23}$$

Second step: for $t > t_1$, using (22) and (23), the e_1 dynamics becomes:

$$\dot{e}_1 = (1 + e\left(x_1(t-\tau)\right)^2)m_1 - \lambda_1 sign(e_1).$$

Thus, if $\lambda_1 > \sup_{\forall t>0} |m_1|$, there exists t_2, such that, for $t > t_2 > t_1$, $e_1 = \dot{e}_1 = 0$. Then:

$$(1 + e\left(x_1(t-\tau)\right)^2)m_1 - \lambda_1 sign(e_1) = 0$$

and

$$E_2 = 1. \tag{24}$$

The relation (19) provides a finite time estimation of m_1.

$$\tilde{m}_1 = \frac{E_2\lambda_1 sign(e_1)}{(1 + e\left(x_1(t-\tau)\right)^2)} = m_1.$$

Third step: for $t > t_2$, using (22) and (24), one has:

$$\dot{e}_{34} = x_1x_2\left(x_3^2 + x_4^2\right) - \lambda_3 sign(e_{34}).$$

If λ_3 is chosen such that

$$\lambda_3 > \sup_{\forall t>0} \left|x_1x_2\left(x_3^2 + x_4^2\right)\right|,$$

one obtains after a finite time t_3, $e_{34} = \dot{e}_{34} = 0$. Thus,

$$x_1x_2\left(x_3^2 + x_4^2\right) - \lambda_3 sign(e_{34}) = 0$$

and $E_3 = 1$. From the definition of the auxiliary variable (18):

$$\tilde{x}_3^2 + \tilde{x}_4^2 = \frac{\lambda_3 sign(e_{34})}{x_1x_2} = x_3^2 + x_4^2.$$

The possibility to estimate m_2 requires the knowledge of $\tilde{x}_3^2$ and $\tilde{x}_4^2$. Define

$$\begin{array}{l} \tilde{x}_3\tilde{x}_4 = A \\ \tilde{x}_3^2 + \tilde{x}_4^2 = B \end{array}$$

There are two groups of solutions:

$$\begin{array}{c} S_1 : \left\{ \begin{array}{l} \tilde{x}_{3_1}^2 = \frac{B+\sqrt{B^2-4A^2}}{2} \\ \tilde{x}_{4_1}^2 = \frac{B-\sqrt{B^2-4A^2}}{2} \end{array} \right. \\ \text{and} \\ S_2 : \left\{ \begin{array}{l} \tilde{x}_{3_2}^2 = \frac{B-\sqrt{B^2-4A^2}}{2} \\ \tilde{x}_{4_2}^2 = \frac{B+\sqrt{B^2-4A^2}}{2} \end{array} \right. \end{array} \tag{25}$$

Suppose that S_1 is the correct solution. From (21), the confidential message can be recovered correctly as follows:

$$-c\tilde{x}_{3_1}^2 - d\tilde{x}_{4_1}^2 + \left(\tilde{x}_{3_1}^2 - \tilde{x}_{4_1}^2\right) m_{2_1} = -2x_1x_2\tilde{x}_3\tilde{x}_4 \triangleq C. \tag{26}$$

In this case, one has for S_2:

$$-c\tilde{x}_{3_2}^2 - d\tilde{x}_{4_2}^2 + \left(\tilde{x}_{3_2}^2 - \tilde{x}_{4_2}^2\right) m_{2_2} = C. \tag{27}$$

Using (26) and (27), one has:

$$m_{2_2} = \frac{\begin{bmatrix} -c\tilde{x}_{3_1}^2 - d\tilde{x}_{4_1}^2 + \left(\tilde{x}_{3_1}^2 - \tilde{x}_{4_1}^2\right) m_{2_1} \\ +c\tilde{x}_{3_2}^2 + d\tilde{x}_{4_2}^2 \end{bmatrix}}{\left(\tilde{x}_{3_2}^2 - \tilde{x}_{4_2}^2\right)}$$

Note that $\tilde{x}_{3_1}^2 = \tilde{x}_{4_2}^2$ and $\tilde{x}_{3_2}^2 = \tilde{x}_{4_1}^2$. So this equation becomes

$$\begin{aligned} m_{2_2} &= \frac{\begin{bmatrix} -c\tilde{x}_{3_1}^2 - d\tilde{x}_{4_1}^2 + \left(\tilde{x}_{3_1}^2 - \tilde{x}_{4_1}^2\right) m_{2_1} \\ +c\tilde{x}_{4_1}^2 + d\tilde{x}_{3_1}^2 \end{bmatrix}}{\left(\tilde{x}_{4_1}^2 - \tilde{x}_{3_1}^2\right)} \\ &= c - d - m_{2_1} \end{aligned}$$

If m_{2_1} is the correct solution, then $m_{2_2} < 0$ according to Eq. (15) and this excludes the solution m_{2_2}. Following this way, the correct solution corresponding to $\tilde{x}_3^2$ and $\tilde{x}_4^2$ can be found.

Fourth step: Since $\tilde{x}_3^2$ and $\tilde{x}_4^2$ have been estimated, one has:

$$\dot{e}_{3^2+4^2} = 2(x_3^2 - x_4^2)m_2 - 2E_3\lambda_4 sign\left(e_{3^2+4^2}\right).$$

Thus, tuning $\lambda_4 > \sup_{\forall t>0} \left|(x_3^2 + x_4^2)m_2\right|$ ensures that $e_{3^2+4} = \dot{e}_{3^2+4^2} = 0$, after a finite time t_4, and:

$$(x_3^2 - x_4^2)m_2 - \lambda_4 sign\left(e_{3^2+4^2}\right) = 0.$$

The relation (20) leads to the finite time estimation of the second confidential message:

$$\tilde{m}_2 = \frac{E_4\lambda_4 sign\left(e_{3^2+4^2}\right)}{\tilde{x}_3^2 - \tilde{x}_4^2} = m_2.$$

For the simulation, the following values were chosen:

$$\begin{cases} a = 35, b = 10, \\ c = 1, d = 10, \\ \tau = 3 \end{cases}$$

Figures 2, 3, 4 and 5 show the behaviour of the states of the transmitter and those of the receiver. Figures 6 and 7 illustrate the original messages (m_1 and m_2) and their estimations. Figures 2, 3, 4 and 5 show that the states of the receiver converge fast to those of the transmitter. It can be seen in Figures 6 and 7 that, once the state is estimated, the confidential messages are well reconstructed.

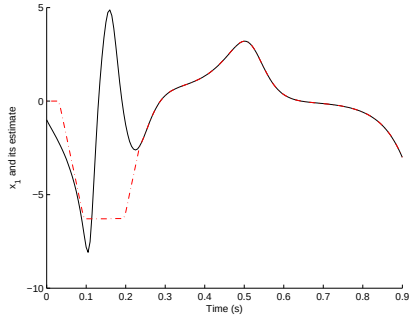

Figure 2: simulation of x_1 and its estimate

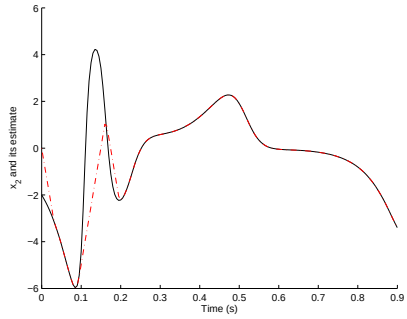

Figure 3: simulation of x_2 and its estimate

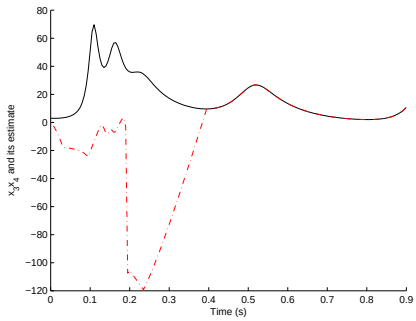

Figure 4: simulation of x_3x_4 and its estimate

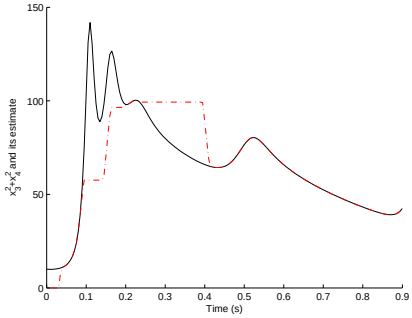

Figure 5: simulation of $x_3^2 + x_4^2$ and its estimate

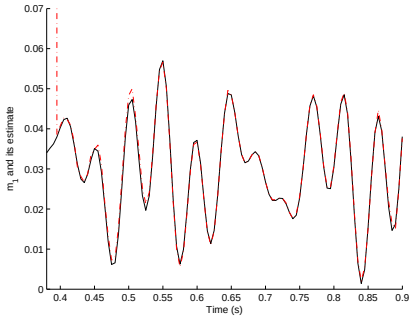

Figure 6: simulation of m_1 and its estimate

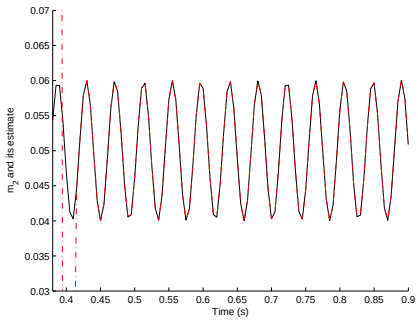

Figure 7: simulation of m_2 and its estimate

6 Conclusion

In this article, a new multiple secure data transmission system based on multi-input multi-output chaotic delayed systems was proposed. The multi-input multi-output scheme allows to reduce the risk for the messages to be broken because it is more difficult to know all the unknown inputs at the same time. Some delays were also introduced in order to improve the robustness of the secure data transmission with respect to known plain-text attacks.

References

Anstett F., Millerioux G. & Bloch G. [2006] "Chaotic Cryptosystems: Cryptanalysis and Identifiability," *IEEE Transactions on Circuits and Systems - Part I 53(12), 2673-2680.*

Barbot J. P., Belmouhoub I. & Boutat-Baddas L. [2003] "Observability Normal Form," *In W. Kang et al., editior, LNCIS 295, New trends in nonlinear dynamics and control, Springer Verlag.*

Barbot J.P, Boutat D. & Floquet T. [2005] "A new observation algorithm for nonlinear system with unknown inputs," In *IEEE CDC-ECC, Sevilla, Dec 2005.*

Boutat-Baddas L., Boutat D., Barbot J.- P., Tauleigne R. Quadratic observability normal form, in *IEEE Conf. on Decision and Control*, 2001.

Cannas B., Cincotti S. & Usai E. [2005] "A chaotic modulation scheme based on algebraic observability and sliding mode differentiators," *Chaos, Solitons and Fractals, 26, 363–377.*

Chua L.O. [1993] "Global unfolding of Chua's circuit," *IEICE Trans. Fundamentals, 704-734.*

Feldmann U., Hasler M. & Schwarz W. [1996] "Communication by chaotic signals: The inverse system approach," *Int. J. Circuit Theory and Applications 24, 551-576.*

Floquet T. & Barbot J.P., "A canonical form for the design of unknown input sliding mode observers", in *Advances in Variable Structure and Sliding Mode Control*, Lecture Notes in Control and Information Sciences, Vol. 334, C. Edwards, E. Fossas Colet, L. Fridman, (Eds.), Springer Edition, 2006.

Fradkov A, Nijmeijer H., Markov A. Adaptive observer-based synchronization for communication. *Int. J. Bifurcat. Chaos*, 10:2807–2813, 2000.

Huijberts N. H., Nijmeijer H. & Willems R. [2000] "System identification in communication with chaotic systems," *IEEE Trans. Circuits Syst. I, 47, 800–808.*

Huijberts H.J.C., Lilge T., Nijmeijer H. Nonlinear discrete-time synchronization via extended observers, *Int. J. Bifurcat. Chaos*, 11 (7):1997–2006, 2001.

Isidori A. [1989], *Nonlinear control systems*, *Springer-Verlag, 2nd edition.*

Lee M. W., Larger L. & Goedgebuer J.-P. [2003] "Transmission system using chaotic delays between lightwaves," *IEEE J. Quantum Electron 39, 931-935.*

Kerkhoff A. [1883] "La cryptographie militaire," *Journal des sciences militaires IX, 5–83.*

Kovarev L., Eckert K. S., Chua L. O. & Parlitz U. [1992] "Experimental demonstration of secure communications via chaotic synchrionization," *Int. J. Bifurcation and Chaos 2, 709-713.*

Nijmeijer H. & Mareels I. M. Y. [1997] "An observer looks at synchronization," *IEEE Trans. on Circuits and Systems-1: Fundamental theory and Applications 44(10), 882-891.*

Parlitz U., Chua L.O. *et al* [1992] "Transmission of digital signals by chaotic synchronization," *Int. J. Bifurcation and Chaos 2, 973-977.*

Pecora L.M. & Carroll T. L. [1990] "Synchronization in chaotic systems," *Physical Review Letters 64, 821-824.*

Pérez G. & Cerdeira H. A. [1995] "Extracting messages masked by chaos," *Physical Review Letters 74, 1970-1973.*

Perruquetti W. & Barbot J.P. [2002] *Sliding Mode Control in Engineering M. Dekker, 2002.*

Qi G. Y., Du S. Z., Chen G. R. *et al* [2005] "On a four-dimensional chaotic system," *Chaos, Solitons and Fractals, 23.*

Hirschorn R. M. [1979] "Invertibility of nonlinear control systems," *SIAM J. Contr. and Optim. 17(1979), 287-289.*

Respondek W. [1990] "Right and Left Invertibility of Nonlinear Control Systems," in *Nonlinear Controllability and Optimal Control*, ed., Sussmann H. J. (Marcel Dekker, New York,) pp. 133-176.

Short K. M. [1994] "Steps toward unmasking secure communication," *Int. J. Bifurcation and Chaos 4, 959-977.*

Singh S. N. [1982] "Invertibility of observable multivariable nonlinear system," *IEEE Trans Automat. Control 27, 487-489.*

Sira Ramirez H. and Cruz Hernandez C. Synchronization of chaotic systems: a generalized Hamiltonian approach, *Int. J. Bifurcat. Chaos* 11(5):1381–1395, 2001.

Sira-Ramirez & H. Fliess M [2006] "An algebraic state estimation approach for the recovery of chaotically encrypted messages", *Int. J. Bifurcation and Chaos 16, 295–309.*

Wu C. W. & Chua L. O. [1993] "A simple way to synchronize chaotic systems with applications to secure communication systems," *Int. J. Bifurcation and Chaos 3, 1619-1627.*

Yang T. & Chua L.O. [1997] "Impulsive stabilization for control and synchronization of chaotic systems: Theory and application to secure communication", *IEEE Trans. Circuits and Systems-I 44, 976-988.*

Yang T., Yang L. B. et al. [1998] "Breaking chaotic switching using generalized synchronization: Examples", *IEEE Trans. Circuits and Systems-I 45, 1062-1067.*

Yang T., (2004), A survey of chaotic secure communication systems", *Int. J. Comp. Cognition, vol. 2, No. 2, 81-130, 2004.*