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

G. Zheng\textsuperscript{1}, D. Boutat\textsuperscript{1}, T. Floquet\textsuperscript{3,5} and J.-P. Barbot\textsuperscript{4,5}
\textsuperscript{1}INRIA Rhône-Alpes, 655 avenue de l’Europe, 38334 St Ismier Cedex, France
\textsuperscript{2}LVR, ENSI-Bourges/Université d’Orléans, 10, Bd. Lahitolle, 18020 Bourges, France
\textsuperscript{3}LAGIS UMR CNRS 8146, Ecole Centrale de Lille, BP 48, Cité Scientifique, 59651 Villeneuve-d’Ascq, France
\textsuperscript{4}Equipe Commande des Systèmes (ECS), ENSEA, 6 Av. du Ponceau, 95014 Cergy, France
\textsuperscript{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, some 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 \textit{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 \textit{et al.}, 1992), chaotic masking with delays (Lee \textit{et al.}, 2003), chaotic switching (Parlitz \textit{et al.}, 1992), chaotic modulation (Wu \textit{et al.}, 1993) and inverse system approach (Feldmann \textit{et al.}, 1996)....

Since the work (Nijmeijer \textit{et al.}, 1997), synchronization can be viewed as a special case of observer design problem, i.e the state reconstruction from mea-
measurements of an output variable under the assumption that the system structure and parameters are known. For a synchronization based chaos-based cryptosystem, a receiver (observer design 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 (unknown inputs of the chaotic system from a control theory point of view). Many techniques issued 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 decreases the risk of known plain-text attack, 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, one input is accessible to every user in the group and another input is accessible only by the administrator of the group. 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 (Nijmeijer et al., 1997), for chaotic system but with unknown inputs. Actually, 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 multi-inputs possess different risks to be broken, i.e., even if message $M_{N1}$ 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. Under this 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 as follows. The next section is devoted to analyze 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) highlights the proposed well-founded 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 $n$-dimensional chaotic system without delays in the following generic form:

$$\dot{x} = f(x)$$  \hspace{1cm} (1)

$x \in U$ is the state vector, $U$ is an open set of $\mathbb{R}^n$, and $f : \mathbb{R}^n \rightarrow \mathbb{R}^n$ is analytic.

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

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

where $k \in \mathbb{R}^q$ is the key vector, $y \in \mathbb{R}^p$ is the output vector and $u = [u_1, \ldots, u_m]^T \in \mathbb{R}^m$ 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 $f_i, h_j \in \mathbb{R}$, $g_l \in \mathbb{R}^n$, $i \in [1, n]$, $j \in [1, p]$, $l \in [1, m]$. Without loss of generality, it is assumed that, for all $x \in U$, the distribution $\text{span} \{g_1, \ldots, g_m\}$ and the codistribution $\text{span} \{dh_1, \ldots, dh_p\}$ 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 $\rho$ of the system (2) is defined by $\rho = \{\rho_1, \ldots, \rho_p\}$, where $\rho_i = \min \{s \text{ such that } L_{g_i} L_f^{s-1} h_i \neq 0 \text{ for } k = 1 : m\}$, $i = 1 : p$.

- $\Phi$ is the codistribution spanned by the time derivatives of the measured outputs not affected by the inputs:

$$\Phi = \text{span} \{dh_1, \ldots, L_f^{\rho_1-1} h_1, \ldots, dh_p, \ldots, L_f^{\rho_p-1} h_p\}$$

- $\Omega$ is a basis of $\Phi$:

$$\Omega = \{dh_1, \ldots, L_f^{\rho_1-1} h_1, \ldots, dh_p, \ldots, L_f^{\rho_p-1} h_p\}$$

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

$\mathcal{L}$ is the commutative algebra of the considered output and their allowed related derivatives:

$$\mathcal{L} = \text{span} \{h_1, \ldots, L_f^{\rho_1-1} h_1, \ldots, h_p, \ldots, L_f^{\rho_p-1} h_p\}$$  \hspace{1cm} (3)
• \( \Omega \) is the module spanned by \( \Omega \) over \( \mathcal{E} \), and \( \Omega^1 \) is the submodule spanned by 
\[
\{ dh_1, ..., dL_i^{-2}h_1, ..., dh_p, ..., dL_i^{-2}h_p \}
\]
over \( \mathcal{E} \) where by definition \( L_i^{-1}h_j = 0 \) and \( L_i^0h_j = h_j \).

• \( G \) is the smallest involutive distribution that contains \( \{ g_1(x), ..., g_m(x) \} \). Denote \( k = \dim G, \ m \leq k \leq n \).

• \( G^\perp \) is the annihilator of \( G \), i.e.
\[
G^\perp = \text{span}\{ \alpha_1, ..., \alpha_{n-k} \}
\]
where the \( \alpha_i \) 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 \( \lambda \) and \( \alpha \).

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

\[
\begin{align*}
\dot{\xi}_1 &= \xi_2 \\
\vdots & \\
\dot{\xi}_{r_1-1} &= \xi_{r_1} \\
\dot{\xi}_{r_1} &= L_i^0 h_i(x) + \sum_{j=1}^m L_j L_i^{-1} h_i(x) u_j \\
\eta &= p(\xi, \eta) + q(\xi, \eta) u \\
y_i &= \xi_i^i 
\end{align*}
\]

where

\[
\xi = \left[ (\xi^1)^T \cdots (\xi^p)^T \right]^T
\]

and

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

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 \( \text{span} \{ g_1, \ldots, g_m \} \) 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 \( \text{span} \{ g_1, \ldots, g_m \} \) 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:

\[
V = \begin{bmatrix}
L_i^{r_1} h_1(x) & \cdots & L_i^{r_p} h_p(x)
\end{bmatrix}^T + \Gamma(x) u
\]

\[
= \begin{bmatrix}
y_1^{(r_1)} & \cdots & y_p^{(r_p)}
\end{bmatrix}^T
\]
with
\[
\Gamma(x) = \begin{bmatrix} \mathcal{L}g_1 L_f^{r-1} h_1(x) & \ldots & \mathcal{L}g_m L_f^{r-1} h_1(x) \\ \vdots & \ddots & \vdots \\ \mathcal{L}g_1 L_f^{m-1} h_p(x) & \ldots & \mathcal{L}g_m L_f^{m-1} h_p(x) \end{bmatrix}
\]
that can be known using the normal form (4). Assume there exists a 1 × \(p\) vector function \(K(x) = [k_1(x), \ldots, k_p(x)] \neq 0\), with \(k_i \in \mathcal{L}, i = 1, \ldots, p\) such that
\[
K \Gamma = 0 \quad (6)
\]
and define a dummy output as follows:
\[
\bar{y} = \bar{h}(x) = KV = \sum_{i=1}^{p} k_i(x) L_f^r h_i(x).
\]
If \(\bar{y} \notin \mathcal{L}\), it can be considered as a suitable dummy output in order to estimate more states. The system has a new vector relative degree with respect to this output. If \(r = n\) (with this new \(y\)), 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 Eq. (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 \(\bar{y} = KV \notin \mathcal{L}\).

ii) the set of equivalence classes \(E = \mathcal{G}^\perp \cap \Omega \mathcal{L} \mathcal{G}^\perp \cap \Omega \mathcal{L}\) of elements of \(\mathcal{G}^\perp \cap \Omega \mathcal{L}\) modulo \(\mathcal{G}^\perp \cap \Omega \mathcal{L}\) is such that \(E \neq \emptyset\).

iii) \(\Xi = \{\alpha \in \mathcal{G}^\perp \cap \Omega \mathcal{L} \text{ such that } l_f \alpha \notin \mathcal{L}\} \neq \emptyset\).

**Remark 1** A complete description of the algorithm can be found in (Barbot et al., 2005).

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 \(y\) and their time derivatives
\footnote{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.}:
\[
\begin{align*}
\{ x &= \Xi (y, \dot{y}, \ldots, y^{(n-1)}, k) \\
u &= \Psi (y, \dot{y}, \ldots, y^{(n-1)}, k) \}
\end{align*}
\quad (7)
\]
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 formally find 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.

3 Cryptanalysis and identifiability

Equation (7) and consequently the proposed scheme cannot 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. It is possible to obtain several independent equations with respect to \( k \):

\[
\begin{align*}
    u(t_1) &= \Psi (y(t_1), \dot{y}(t_1), ..., y^{(n-1)}(t_1), k) \\
    u(t_2) &= \Psi (y(t_2), \dot{y}(t_2), ..., y^{(n-1)}(t_2), k) \\
    \vdots & \quad \vdots \\
    u(t_l) &= \Psi (y(t_l), \dot{y}(t_l), ..., y^{(n-1)}(t_l), k)
\end{align*}
\]

(8)

Then, two cases appear:

- there exist \( q = l \) independent equations, which is equivalent to:

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

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.

Thus, 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:

\[
\begin{cases}
    u(t_1) &= \Psi(y(t_1), \dot{y}(t_1), ..., y^{(n-1)}(t_1), \\
    &\quad y(t_1 - \tau), ..., y^{(l)}(t_1 - \tau), k) \\
    u(t_2) &= \Psi(y(t_2), \dot{y}(t_2), ..., y^{(n-1)}(t_2), \\
    &\quad y(t_2 - \tau), ..., y^{(l)}(t_2 - \tau), k) \\
    \vdots &\vdots \\
    u(t_l) &= \Psi(y(t_l), \dot{y}(t_l), ..., y^{(n-1)}(t_l), \\
    &\quad y(t_l - \tau), ..., y^{(l)}(t_l - \tau), k)
\end{cases}
\]  

(9)

with \( j \leq n - 1 \). From (9), it is obvious that there are more unknown inputs, \( y^{(o)}(t - \tau) \) 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:

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

(10)

where the \( l \) delays are also 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:

\[
\begin{cases}
    \dot{\xi}_1 = \xi_2 \\
    \vdots \\
    \dot{\xi}_{l-1} = \xi_l \\
    \dot{\xi}_l = L_f^{-1} h_i(x) + \sum_{j=1}^{m} L_{g_j} L_f^{-1} h_i(x) u_j \\
    \eta = p(\xi, \eta) + q(\xi, \eta, y(t-\tau_1), ..., y(t-\tau_l)) u \\
y_i = \xi_l
\end{cases}
\]

(11)

where \( L_{g_j} L_f^{-1} h_i \) is given by:

\[
L_{g_j} L_f^{-1} h_i = \frac{\partial L_f^{-1} h_i}{\partial x} g_j(x, y(t-\tau_1), ..., y(t-\tau_l), k).
\]
Then Equation (5) becomes
\[
V = [ L_1 h_1(x) \cdots L_p h_p(x) ]^T + \Gamma(x, y(t), y(t - \tau_1), \ldots, y(t - \tau_l), k)u
\]
\[
= \begin{bmatrix} y_1(\tau_1) & \cdots & y_p(\tau_p) \end{bmatrix}^T
\] (12)

Since \( y(t) \) and all the \( y(t - \tau_s) \) are known if all \( \tau_s \) are known, it is possible to find \( K(x, y(t - \tau_1), \ldots, y(t - \tau_l), k) \) such that
\[
K(x, y(t - \tau_1), \ldots, y(t - \tau_l), k).\Gamma(x, y(t), y(t - \tau_1), \ldots, y(t - \tau_l), k) = 0.
\]

Nevertheless, the resulting dummy output may be function of the delays and this may introduce some obstacles for the next step of the algorithm. This is due to the fact that the time derivative of outputs with delays is in general a function of the delayed state which is not a known output function. Consequently, a sufficient condition in order to overcome this problem is to find \( K(x, k) \) independent of delays. Thus, one can proceed as follows: first, use Proposition 1 including the outputs with delays as elements of (3); then check whether or not it is possible to find \( K \) without delayed outputs.

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:
\[
\begin{align*}
\dot{x}_1 &= a(x_2 - x_1) + x_2 x_3 x_4 \\
\dot{x}_2 &= b(x_1 + x_2) - x_1 x_2 x_4 + (1 + e(x_1(t - \tau))^2)m_1 \\
\dot{x}_3 &= -cx_3 + x_1 x_2 x_4 \\
\dot{x}_4 &= -dx_4 + x_1 x_2 x_3 - x_4 m_2
\end{align*}
\] (13)

where \( x_i \ (i = 1, \ldots, 4) \) 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):
\[
\begin{align*}
\dot{x}_1 &= a(x_2 - x_1) + x_2 x_3 x_4 \\
\dot{x}_2 &= b(x_1 + x_2) - x_1 x_3 x_4 \\
\dot{x}_3 &= -cx_3 + x_1 x_2 x_4 \\
\dot{x}_4 &= -dx_4 + x_1 x_2 x_3 - x_4 m_2
\end{align*}
\] (14)

where \( e \) is a positive real constant, \( \tau \) 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:

\[
d - c - \beta > 0.
\]

(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), let us calculate

\[
\Gamma = \begin{pmatrix}
L_{g_1} & L_{g_2} \\
L_f h_2 & L_{g_1} L_f h_2
\end{pmatrix}

= \begin{pmatrix}
(1 + e(x_1(t - \tau))^2) & 0 \\
(1 + e(x_1(t - \tau))^2)(b - x_3 x_4) & 0
\end{pmatrix}.
\]

Thus, one can choose

\[
K = (b - x_3 x_4, -1)
\]

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). Set

\[
\mathcal{L} = \text{span}\{h_1, h_1(t - \tau), h_2, L_f h_2\}
\]

Since

\[
L_f h_2 = b(x_1 + x_2) - x_1 x_3 x_4 = x_3 x_4 \mod \{x_1, x_2\}
\]

one has

\[
\mathcal{L} = \text{span}\{x_1, x_1(t - \tau), x_2, x_3 x_4\}.
\]

Then, the following dummy output can be defined:

\[
\tilde{y} = K \begin{bmatrix} L_f h_1 \\ L_f h_2 \end{bmatrix} = (b - x_3 x_4) \hat{y}_1 - \hat{y}_2 = (x_3^2 + x_4^2 \mod \mathcal{L}(x)
\]

because \( \tilde{y} \notin \mathcal{L} \). 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

\[
\Phi = \text{span}\{dx_1, dx_2, dx_3 x_4, d(x_3^2 + x_4^2)\}
\]

is equal to 4. This means that one can recover all the state in finite time. A straightforward consequence of the fact that \( \text{span}\{g_1, g_2\} \) 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:

\[
\begin{aligned}
\dot{x}_1 &= a(x_2 - x_1) + x_2 \dot{x}_3 \dot{x}_4 + E_1 \lambda_1 \text{sign}(x_1 - \dot{x}_1) \\
\dot{x}_2 &= b(x_1 + x_2) + \lambda_2 \text{sign}(x_2 - \dot{x}_2) \\
\frac{d(\ddot{x}_3 \ddot{x}_4)}{dt} &= -(c + d) \ddot{x}_3 \ddot{x}_4 \\
\frac{d(\ddot{x}_3 \ddot{x}_4)}{dt} &= -2c\ddot{x}_3^2 - 2d\ddot{x}_4^2 + 4x_1x_2 \ddot{x}_3 \ddot{x}_4 \\
&+ 2E_3 \lambda_4 \text{sign}\left((\ddot{x}_3^2 + \ddot{x}_4^2) - (\dot{x}_3^2 + \dot{x}_4^2)\right)
\end{aligned}
\]  

(16)

with:

\[
\lambda_i > 0, \quad i = 1, \ldots, 4
\]

\[
E_1 = \begin{cases} 
1 & x_2 = \dot{x}_2 \\
0 & \text{otherwise}
\end{cases}
\]

\[
E_2 = \begin{cases} 
1 & \text{if } E_1 = 1 \text{ and } x_1 = \dot{x}_1 \\
0 & \text{otherwise}
\end{cases}
\]

\[
E_3 = \begin{cases} 
1 & \text{if } E_2 = 1 \text{ and } \ddot{x}_3 \ddot{x}_4 = \ddot{x}_3 \ddot{x}_4 \\
0 & \text{otherwise}
\end{cases}
\]

and with the auxiliary states:

\[
\ddot{x}_3 \ddot{x}_4 = -\frac{\lambda_2 \text{sign}(x_2 - \dot{x}_2)}{x_1}
\]

(17)

\[
\ddot{x}_3^2 + \ddot{x}_4^2 = \frac{E_2 \lambda_3 \text{sign}(\ddot{x}_3 \ddot{x}_4 - \ddot{x}_3 \ddot{x}_4)}{x_1 x_2}.
\]

(18)

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

\[
S = \{x_1 = 0\} \cup \{x_1 x_2 = 0\}.
\]

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:

\[
\begin{aligned}
\tilde{m}_1 &= \frac{E_2 \lambda_1 \text{sign}(x_1 - \dot{x}_1)}{1 + e(x_1(t - \tau))^2} \\
\tilde{m}_2 &= \frac{E_4 \lambda_4 \text{sign}\left((\ddot{x}_3^2 + \ddot{x}_4^2) - (\dot{x}_3^2 + \dot{x}_4^2)\right)}{\ddot{x}_3^2 - \ddot{x}_4^2}
\end{aligned}
\]

(19)

(20)

where

\[
E_4 = \begin{cases} 
1 & \text{if } E_3 = 1 \text{ and } \ddot{x}_3^2 + \ddot{x}_4^2 = \ddot{x}_3^2 + \ddot{x}_4^2 \\
0 & \text{otherwise}
\end{cases}
\]

The observation errors are defined by:

\[
\begin{aligned}
e_1 &= x_1 - \dot{x}_1 \\
e_2 &= x_2 - \dot{x}_2 \\
e_{34} &= x_3 x_4 - \dot{x}_3 \dot{x}_4 \\
e_{34^2} &= (x_3^2 + x_4^2) - (\dot{x}_3^2 + \dot{x}_4^2)
\end{aligned}
\]
From system (14), it can be computed that:

\[
\frac{d(x_3 x_4)}{dt} = -(c + d) x_3 x_4 + x_1 x_2 (x_3^2 + x_4^2)
\]

and

\[
\frac{d(x_3^2 + x_4^2)}{dt} = -2c x_3^2 + 4x_1 x_2 x_3 x_4 - 2dx_4^2 + 2 (x_3^2 - x_4^2) m_2.
\] (21)

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

\[
\begin{aligned}
\dot{e}_1 &= x_2 (x_3 x_4 - \tilde{x}_3 \tilde{x}_4) + (1 + e (x_1 (t - \tau))^2) m_1 - E_1 \lambda_1 \text{sign}(e_1) \\
\dot{e}_2 &= -x_1 x_3 x_4 - \lambda_2 \text{sign}(e_2) \\
\dot{e}_{34} &= -(c + d) (x_3 x_4 - \tilde{x}_3 \tilde{x}_4) + x_1 x_2 (x_3^2 + x_4^2) - E_2 \lambda_3 \text{sign}(\tilde{x}_3 \tilde{x}_4 - \tilde{x}_3 \tilde{x}_1) \\
\dot{e}_{34} &= -2e (x_3^2 - \tilde{x}_3^2) - 2d (x_4^2 - \tilde{x}_4^2) + 4x_1 x_2 (x_3 x_4 - \tilde{x}_3 \tilde{x}_4) + 2 (x_3^2 - x_4^2) m_2 - 2E_3 \lambda_4 \text{sign}((\tilde{x}_3^2 + \tilde{x}_4^2) - (\tilde{x}_3^2 + \tilde{x}_4^2))
\end{aligned}
\]

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

**First step:** one has:

\[
\dot{e}_2 = -x_1 x_3 x_4 - \lambda_2 \text{sign}(e_2).
\]

All the states are bounded. So, one can choose the gain \(\lambda_2 > \sup_{t\geq 0} |x_1 x_3 x_4|\) so that a sliding motion appears after a finite time \(t_1\) on \(e_2 = 0\). Writing that \(\dot{e}_2 = 0\) gives:

\[-x_1 x_3 x_4 = \lambda_2 \text{sign}(e_2).\]

Then

\[\tilde{x}_3 \tilde{x}_4 = -\frac{\lambda_2 \text{sign}(e_2)}{x_1} = x_3 x_4\] (22)

and

\[E_1 = 1.\] (23)

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

\[\dot{e}_1 = (1 + e (x_1 (t - \tau))^2) m_1 - \lambda_1 \text{sign}(e_1).\]

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

\[\dot{e}_1 = (1 + e (x_1 (t - \tau))^2) m_1 - \lambda_1 \text{sign}(e_1) = 0\]

and

\[E_2 = 1.\] (24)

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

\[\dot{m}_1 = \frac{E_2 \lambda_1 \text{sign}(e_1)}{(1 + e (x_1 (t - \tau))^2)} = m_1.\]
Third step: for \( t > t_2 \), using (22) and (24), one has:

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

If \( \lambda_3 \) is chosen such that

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

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

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

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

\[
\dot{x}_3 + \dot{x}_4 = \frac{\lambda_3 \text{sign}(e_{34})}{x_1x_2} = x_3 + x_4.
\]

The possibility to estimate \( m_2 \) requires the knowledge of \( \tilde{x}_3 \) and \( \tilde{x}_4 \). Define

\[
\tilde{x}_3 \tilde{x}_4 = A \\
\tilde{x}_3^2 + \tilde{x}_4^2 = B
\]

There are two groups of solutions:

\[
S_1 : \left\{ \begin{array}{l}
\dot{x}_{3_1} = \frac{B + \sqrt{B^2 - 4A^2}}{2} \\
\dot{x}_{4_1} = \frac{B - \sqrt{B^2 - 4A^2}}{2}
\end{array} \right.
\]

and

\[
S_2 : \left\{ \begin{array}{l}
\dot{x}_{3_2} = \frac{B - \sqrt{B^2 - 4A^2}}{2} \\
\dot{x}_{4_2} = \frac{B + \sqrt{B^2 - 4A^2}}{2}
\end{array} \right. \tag{25}
\]

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

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

In this case, one has for \( S_2 \):

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

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

\[
m_{2_2} = \frac{\left[ -c\tilde{x}_{3_1}^2 - d\tilde{x}_{4_1}^2 + (\tilde{x}_{3_1}^2 - \tilde{x}_{4_1}^2) m_{2_1} \right]}{\left( \tilde{x}_{3_2}^2 - \tilde{x}_{4_2}^2 \right)}.
\]

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

\[
m_{2_2} = \frac{\left[ -c\tilde{x}_{3_1}^2 - d\tilde{x}_{4_1}^2 + (\tilde{x}_{3_1}^2 - \tilde{x}_{4_1}^2) m_{2_1} \right]}{\left( \tilde{x}_{4_1}^2 - \tilde{x}_{3_1}^2 \right)}
\]

\[
= c - d - m_{2_1}
\]

\[13\]
If $m_{21}$ is the correct solution, then $m_{22} < 0$ according to Eq. (15) and this excludes the solution $m_{22}$. Following this way, the correct solution corresponding to $\hat{x}_3^2$ and $\hat{x}_4^2$ can be found.

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

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

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

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

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

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

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.

6 Conclusion

In this article, a new multiple secure data transmission system based on multi-input multi-output chaotic delayed systems was proposed. The aim of this
Figure 3: simulation of $x_2$ and its estimate

Figure 4: simulation of $x_3 x_4$ 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
scheme is to reduce the risk to be broken because it is more difficult to know all the inputs at the same time in order to realize a full known plain-text attack. Moreover, some delays were introduced in order to improve the robustness of the secure data transmission.

References


