An LPV framework for chaos synchronization in communication

Meriem Halimi, Gilles Millérioux

EPJ manuscript No.
(will be inserted by the editor)

An LPV framework for chaos synchronization in communication

Meriem Halimi[1] and Gilles Millérioux[1] [a]

Université de Lorraine, Centre de Recherche en Automatique de Nancy, France

Abstract. This paper proposes a unified framework to achieve chaos synchronization of both classes of chaotic discrete-time systems, namely maps involving polynomial nonlinearities and piecewise linear maps. It is shown that all of those chaotic systems can be rewritten as a polytopic Linear Parameter Varying (LPV) system. A unified approach to tackle chaos synchronization problems encountered in communication is derived.

1 Introduction

Most of chaos-based cryptosystems proposed since the 90's require synchronization of complex sequences. Indeed, following the principle of symmetric ciphers [1], they consist in scrambling an information with a chaotic digital sequence. The most popular techniques proposed so far are additive masking, parameter modulation, chaotic switching, two-channel transmission, message-embedding. An overview of the different methods can be found in the survey papers [2–5] or in the book [6]. In the year 1997, it has been shown that chaos synchronization can be formulated as a state reconstruction problem (see the pioneering works [7][8][9][10]). Since then, many classes of observers have been proposed to tackle the synchronization problem. The point lies in that the structure and the design of the observers depend on the nonlinearities involved in the chaotic model. A case-by-case study must be carried out.
The aim of this paper is to show that a unified and efficient framework can be proposed to achieve chaos synchronization for a large class of discrete-time chaotic systems. In particular, the classes of chaotic systems involving polynomial nonlinearities (Duffing map, Henon map, Burger map,...) and piecewise linear maps (Lozi map, Zigzag map, Tent map, Baker map, Cat map, ...) can be addressed within a same framework, called LPV framework. Linear Parameter Varying (LPV) systems are linear models whose state representation depends on a parameter vector which can vary in time. A special attention has been paid on LPV systems for years because they are very handy for control purposes [11] [12] [13] [14] [15] [16] and observation or filtering purposes [17] [18] [19] [20]. In the special context of chaos synchronization, the problem of observers synthesis is particularly important. Indeed, the observers play the role of the receivers. It will be shown that, under some specific conditions, a chaotic system can be rewritten in the form of a polytopic LPV model. A polytopic LPV system is an LPV system such that the time-varying parameter admits a convex description. It turns out that, in such a case, the corresponding observer

[a] gilles.millerioux@univ-lorraine.fr

admits a simple Luenberger-like description called polytopic observer. The gains of the polytopic observer are simply derived from the solution of a convex optimization problem which is expressed in terms of Linear Matrix Inequalities (LMI) [21]. And yet, very efficient numerical tools are available to solve LMI (see [22] or the Yalmip Matlab toolbox). Besides, if we are not only concerned with stability but also with performances like robustness with respect to mismatched parameters or with respect to noise, the structure of the observer is kept unchanged. The gains are still derived from LMI but they are adapted to meet the required performances (see [23] for details). Thus, the simplicity of the observers design, that is of the receiver, is preserved. All those considerations highlight the interest of the LPV framework.
The outline of the paper is the following. In Section 2, background on LPV systems and state reconstruction related problems are recalled. Then, the LPV framework is particularized to chaotic systems and it is shown how the issue of chaos synchronization can be addressed with such a framework. Section 3 is devoted to applications of the LPV framework. Several examples, from basic to advanced ones, are proposed in a tutorial-like form to clarify the main points. An example involving a chaos-based cryptosystem illustrates the use of the LPV framework in communication.

2 Chaotic systems and LPV framework

2.1 Background on polytopic LPV systems

LPV systems are classes of systems obeying the following state space equations

$$\left\{ \begin{array}{l} x_{k+1} = A(\rho_k)x_k + Bu_k \\ \quad y_k = Cx_k + Du_k \end{array} \right. \tag{1}$$

where $x_k \in \mathbb{R}^n$ is the state vector, $u_k \in \mathbb{R}^m$ is the control input, $y_k \in \mathbb{R}^p$ is the output vector, $A \in \mathbb{R}^{n\times n}$ is the dynamical matrix depending on the possibly time varying parameter vector $\rho_k = \left[\rho_k^{(1)}, \rho_k^{(2)}, ..., \rho_k^{(L_\rho)}\right] \in \mathbb{R}^{L_\rho}$, $B \in \mathbb{R}^{n\times m}$ is the input matrix, $C \in \mathbb{R}^{p\times n}$ is the output matrix and $D \in \mathbb{R}^{p\times m}$ is the direct transfer matrix. The parameter ρ_k is assumed to be available at every times k.

Remark 1 *Let us note that* (1) *can be extended to affine systems and the time-varying parameter can be involved in all the state space matrices. In such a case, the following state space equations must be considered*

$$\left\{ \begin{array}{l} x_{k+1} = A(\rho_k)x_k + B(\rho_k)u_k + E(\rho_k) \\ \quad y_k = C(\rho_k)x_k + D(\rho_k)u_k \end{array} \right. \tag{2}$$

In the sequel, we will focus on (1) for simplicity but the results can be extended in a straightforward way to (2).
The dependence of $A(\rho_k)$ with respect to ρ_k can take many forms, in particular, polytopic. The polytopic decomposition refers to a dependence on ρ_k of $A(\rho_k)$ which reads

$$A(\rho_k) = \sum_{i=1}^{N} \xi_k^{(i)}(\rho_k) A_i \tag{3}$$

where ξ_k belongs to the compact set Φ

$$\Phi = \left\{ \mu_k \in \mathbb{R}^N, \mu_k = \left[\mu_k^{(1)}, \ldots, \mu_k^{(N)}\right], \mu_k^{(i)} \geq 0 \ \forall\ i \text{ and } \sum_{i=1}^{N} \mu_k^{(i)} = 1 \right\}$$

Owing to the convexity of Φ, the set of matrices $\{A_1, \ldots, A_N\}$ defines a polytope denoted D_A and the matrices A_i correspond to the vertices of D_A. Hereafter, for the sake of simplicity and whenever possible, the parameter dependency on ρ_k of $\xi_k^{(i)}$ will be omitted, that is the notation $\xi_k^{(i)}$ will be used instead of $\xi_k^{(i)}(\rho_k)$.
The conditions under which a polytopic decomposition can apply are now explained. If the components $\rho_k^{(i)}$ $(i = 1, \ldots, L_\rho)$ of ρ_k belong to a bounded range $[\rho_{min}^{(i)}, \rho_{max}^{(i)}]$, thus ρ_k belongs to a bounded set $\Omega_\rho \subset \mathbb{R}^{L_\rho}$. And then, Ω_ρ can always be embedded in a polytope $\mathcal{D}_\rho$ with vertices $\{\rho_{o_i}, \ldots, \rho_{o_N}\} \in \mathbb{R}^{L_\rho}$. It holds that

$$\rho_k = \sum_{i=1}^{N} \xi_k^{(i)} \rho_{o_i}, \ \xi_k \in \Phi \tag{4}$$

Furthermore, we can notice that $A(\rho_k)$ in (1) can always be written as

$$A(\rho_k) = \bar{A}^{(0)} + \sum_{j=1}^{L_\rho} \rho_k^{(j)} \bar{A}^{(j)} \tag{5}$$

where $\bar{A}^{(0)}$ and $\bar{A}^{(j)}$ are constant matrices obtained from $A(\rho_k)$. $\bar{A}^{(0)}$ is the matrix derived from $A(\rho_k)$ by keeping its constant entries and setting to zero its time varying entries. $\bar{A}^{(j)}$ is the matrix derived from $A(\rho_k)$ by setting to zero its constant entries and to unity the one corresponding to the location of $\rho_k^{(j)}$ in $A(\rho_k)$. Finally, after substituting (4) into (5), the vertices A_i of (3) can be expressed as

$$A_i = \bar{A}^{(0)} + \sum_{j=1}^{L_\rho} \rho_{o_i}^{(j)} \bar{A}^{(j)} \tag{6}$$

2.2 Polytopic LPV description of chaotic systems

Let us consider the general nonlinear dynamical system assumed to exhibit a chaotic dynamics

$$\begin{cases} x_{k+1} = g(x_k, u_k) \\ y_k = Cx_k + Du_k \end{cases} \tag{7}$$

where $x_k \in \mathcal{X} \subseteq \mathbb{R}^n$ is the state vector, $u_k \in \mathbb{R}^m$ is the input, $y_k \in \mathbb{R}^p$ is the measured signal. The aim is to give some conditions under which (7) can be rewritten as (1).

The following proposition applies

Proposition 1 *If the following conditions are fulfilled*

- *i) there exists a function* $\rho : \mathbb{R}^n \to \mathbb{R}^{L_\rho}$ *such that* $A(\rho(x_k))x_k + Bu_k = g(x_k, u_k)$
- *ii)* $\rho(x_k)$ *depends only on measured signals*
- *iii)* $\rho(x_k)$ *lies in a bounded set* Ω_ρ *when* x_k *lies in the admissible set* $\mathcal{X} \subseteq \mathbb{R}^n$

then the nonlinear system (7) *admits an LPV form* (1) *with* $\rho_k = \rho(x_k)$ *and with polytopic description* (3)*.*

Proof 1 *The key point is that, for a chaotic system,* x_k *belongs to a chaotic attractor* Ω *and thus* $\mathcal{X} = \Omega$*. If Condition iii) is satisfied,* Ω_ρ *is bounded and thus can always be embedded in a polytope* $\mathcal{D}_\rho$*. Furthermore, if Condition ii) is satisfied,* ρ_k *is available at every times* k*. Finally, Condition i) is explicit for obtaining an LPV form.*

Two problems must be handled. First, it is worth pointing out that, most often, the LPV description is not unique and multiple functions ρ can be candidates. Such a consideration will be clarified and illustrated in Example 1 of Section 3. Example 1 will also highlight the fact that chaotic systems involving polynomial nonlinearities admit a polytopic LPV description. Secondly, it may happen that obtaining analytically the polytope $\mathcal{D}_\rho$ is either a hard task or is not possible at all. Moreover, we should be concerned, for the sake of conservatism, to get a minimal polytope. Let us assume that we can get, by simulation or experimentally, a sufficient number of vectors ρ_k, collected in a finite set Γ_ρ of cardinality N_ρ, to describe the set Ω_ρ with proper accuracy. The minimal polytope $\mathcal{D}_\rho^*$ wherein Ω_ρ is embedded can thereby be considered as the convex hull of the set of points Γ_ρ. We recall that an element of a finite set of points is an extreme point if it is not a convex combination of other points in this set. Hence, finding $\mathcal{D}_\rho^*$ amounts to finding the extreme points of Γ_ρ. It turns out that the computation can be performed by standard methods. For instance, the built-in function *convhull* of Matlab can be used to that purpose. Such a point will be illustrated in Example 2 of Section 3.

Finally, it is clear that switched linear and switched affine systems also admit a description as (1) (or (2)) with a polytopic dependence (3) of the parameter. The only distinction lies in that the set Ω_ρ is not a continuum but a finite set. Hence, the set Φ still holds with $\mu_k^{(i)}$ taking only extreme values 0 or 1. Such a point will be clarified and illustrated in Example 3 of Section 3.

2.3 Chaos synchronization with polytopic observers

Recalling that chaos synchronization can be formulated as a state reconstruction issue and so as an observer synthesis, we propose below an observer, called polytopic observer. The interest of such an observer is that it is suited for polytopic LPV models and so, for all the chaotic maps admitting such models. The synthesis principle is detailed in the simplest situation but enhancements can be proposed to handle the problems related to mismatch parameters, noisy context, performances guarantees (speed of convergence, ...) [23].
Let us assume that Proposition 1 holds. Hence, the matrix $A(\rho_k)$ in (1) can be rewritten in the polytopic form (3). A polytopic observer for (1) obeys the following state space description

$$\begin{cases} \hat{x}_{k+1} = A(\rho_k)\hat{x}_k + Bu_k + L(\rho_k)(y_k - \hat{y}_k) \\ \hat{y}_k = C\hat{x}_k + Du_k \end{cases} \tag{8}$$

where $\hat{x}_k \in \mathbb{R}^n$, $\hat{y}_k \in \mathbb{R}^p$ and L is a time-varying gain matrix depending on ρ_k which reads

$$L(\rho_k) = \sum_{i=1}^{N} \xi_k^{(i)}(\rho_k) L_i, \quad \xi_k \in \Phi \tag{9}$$

and where the $\xi_k^{(i)}(\rho_k)$ in (9) coincide, for every discrete times k, with the ones involved in the polytopic decomposition (3) of $A(\rho_k)$. Let us point out that, such a requirement can always be satisfied whenever Condition *ii)* of Proposition 1 holds. Indeed, if ρ_k is available, the vertices of the polytope $\mathcal{D}_\rho$ being known, the polytopic decomposition (4) can be performed on-line. Then, it's a simple matter to see that, from (1) and (8), the reconstruction error $e_k = x_k - \hat{x}_k$ is governed by the dynamics

$$e_{k+1} = (A(\rho_k) - L(\rho_k)C)\, e_k \tag{10}$$

The dynamics of the state reconstruction is nonlinear since A and L depend on ρ_k. However, (10) can be viewed as an autonomous LPV polytopic system with state vector $e_k \in \mathbb{R}^n$. Indeed, from (3), (9) and (10), and taking into account the coincidence between the $\xi_k^{(i)}$ involved in (3) and (9), we get that

$$e_{k+1} = \sum_{i=1}^{N} \xi_k^{(i)}(\rho_k)(A_i - L_i C)e_k, \quad \xi_k \in \Phi \tag{11}$$

Global Asymptotical Stability (GAS) around the equilibrium point $e^* = 0$ can be ensured by a suitable choice of the gains L_i $(i = 1, \ldots, N)$. To this end, the following standard theorem involving Linear Matrix Inequalities [21] is recalled.

Theorem 1 *[23] If there exist symmetric matrices P_i, matrices G_i and matrices F_i fulfilling, $\forall (i,j) \in \{1...N\} \times \{1...N\}$, the Linear Matrix Inequalities*

$$\begin{bmatrix} P_i & (\bullet)^T \\ G_i A_i - F_i C & G_i^T + G_i - P_j \end{bmatrix} > 0 \tag{12}$$

then the polytopic observer (8) *with gain $L(\rho_k) = \sum_{i=1}^{N} \xi_k^{(i)}(\rho_k) L_i$ and $L_i = G_i^{-1} F_i$ ensures that the system* (10) *is GAS.*

Actually, (12) ensures the existence of a Lyapunov function $V : \mathbb{R}^n \times \mathbb{R}^L \to \mathbb{R}_+$ defined by $V(e_k, \rho_k) = e_k^T P(\rho_k) e_k$ with $P(\rho_k) = \sum_{i=1}^{N} \xi_k^{(i)}(\rho_k) P_i$ and $\xi_k \in \Phi$, called poly-quadratic Lyapunov function, fulfilling for all $e_k \in \mathbb{R}^n$, for all $\xi_k \in \Phi$

$$V(e_{k+1}, \rho_{k+1}) - V(e_k, \rho_k) < 0 \tag{13}$$

which is sufficient for Global Asymptotical Stability.
Such an observer can be useful for chaos-based communication purposes as it will be illustrated in Example 4 of Section 3.

3 Applications

3.1 Example 1

This example aims at clarifying the problem of the selection of good candidate functions ρ which fulfill conditions of Proposition 1.

Let us consider the chaotic system derived from the Duffing map and involving polynomial nonlinearities

$$\begin{cases} x_{k+1}^{(1)} = x_k^{(2)} \\ x_{k+1}^{(2)} = -2\left(x_k^{(1)}\right)^3 + 2\, x_k^{(1)} + 0.3\, x_k^{(1)} x_k^{(2)} \\ y_k = x_k^{(1)} \end{cases} \tag{14}$$

The corresponding attractor Ω is depicted in Figure 1 (a). Let ρ_k be the time-varying parameter vector defined as

$$\rho_k^{(1)} = -2\left(x_k^{(1)}\right)^2 + 2$$
$$\rho_k^{(2)} = 0.3\, x_k^{(1)}$$

Then, the map (14) can be rewritten as an LPV system (1) with

$$A(\rho_k) = \begin{bmatrix} 0 & 1 \\ \rho_k^{(1)} & \rho_k^{(2)} \end{bmatrix},\ B = \mathbf{0},\ C = [1\ \ 0] \text{ and } D = \mathbf{0}$$

The parameter ρ_k is available from the output y_k. Indeed, $\rho_k^{(1)} = -2\left(y_k\right)^2 + 2$ and $\rho_k^{(2)} = 0.3\ y_k$. Furthermore, ρ_k belongs to a set Ω_ρ as depicted in Figure 1 (b) which clearly highlights the fact that Ω_ρ is bounded and can be embedded in a polytope $\mathcal{D}_\rho$. As a conclusion, such a definition for ρ_k fulfills all the conditions of Proposition 1.

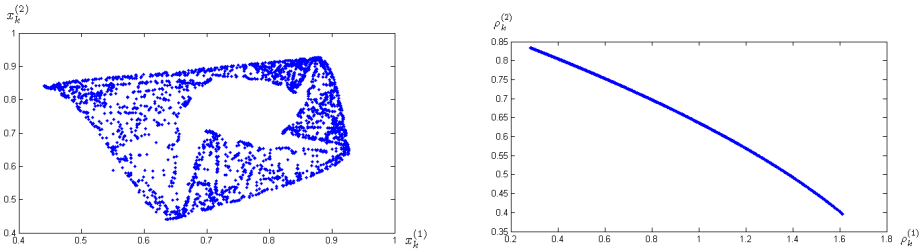

Fig. 1. (a) Chaotic attractor Ω (b) Set Ω_ρ

Another option is to define ρ_k as the one-dimensional vector (scalar) $\rho_k^{(1)} = -2\left(x_k^{(1)}\right)^2 + 2 + 0.3\ x_k^{(2)}$. That gives

$$A(\rho_k) = \begin{bmatrix} 0 & 1 \\ \rho_k^{(1)} & 0 \end{bmatrix},\ B = \mathbf{0},\ C = [1\ \ 0] \text{ and } D = \mathbf{0}$$

However, such a definition does not meet the condition *ii)* of Proposition 1, insofar as $x_k^{(2)}$ is not available from measured signals.

3.2 Example 2

This example aims at illustrating the method to get the minimal polytope $\mathcal{D}_\rho^*$. Let us consider the following system derived from the "Tinkerbell map" given in [25] [24]

$$\begin{cases} x_{k+1}^{(1)} = \left(x_k^{(1)}\right)^2 - \left(x_k^{(2)}\right)^2 + a x_k^{(1)} + b x_k^{(2)} \\ x_{k+1}^{(2)} = 2 x_k^{(1)} x_k^{(2)} + c x_k^{(1)} + d x_k^{(2)} \\ x_{k+1}^{(3)} = 0.1 b x_k^{(2)} - 0.1\left(x_k^{(2)}\right)^2 + 0.1 x_k^{(3)} \\ x_{k+1}^{(4)} = 0.5 x_k^{(1)} + 0.1 x_k^{(2)} + 0.3 x_k^{(4)} \\ y_k^{(1)} = x_k^{(1)} \\ y_k^{(2)} = x_k^{(2)} \end{cases} \tag{15}$$

with $a = 0.9$, $b = -0.6013$, $c = 2$ and $d = 0.5$. For such a setting, the system exhibits a chaotic behavior. The objective is to rewrite (15) in the LPV form (1) with polytopic

dependence (3) and to find the minimal polytope $\mathcal{D}_\rho^*$. To this end, let us define

$$\begin{array}{l} \theta_k^{(1)} = a + x_k^{(1)} \\ \theta_k^{(2)} = b - x_k^{(2)} \end{array} \tag{16}$$

Then, (15) can be rewritten as (1) with the time-varying parameter vector ρ_k such as

$$A(\rho_k) = \begin{bmatrix} \rho_k^{(1)} & \rho_k^{(2)} & 0 & 0 \\ c & \rho_k^{(3)} & 0 & 0 \\ 0 & \rho_k^{(4)} & 0.1 & 0 \\ 0.5 & 0.1 & 0 & 0.3 \end{bmatrix} \text{ where } \begin{cases} \rho_k^{(1)} = \theta_k^{(1)} \\ \rho_k^{(2)} = \theta_k^{(2)} \\ \rho_k^{(3)} = d + 2(\theta_k^{(1)} - a) \\ \rho_k^{(4)} = 0.1\theta_k^{(2)} \end{cases}$$

and

$$C = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \end{bmatrix}$$

The matrices B and D are zero since the system (15) is autonomous. The parameter ρ_k is available from the output y_k and $\rho(x_k)$ is bounded. Indeed, $\theta_k^{(1)} = a + y_k^{(1)}$ and $\theta_k^{(2)} = b - y_k^{(2)}$. By iterating (15), 2000 vectors ρ_k are collected and gathered in the set Γ_ρ which is bounded. The function *convhull* of Matlab is used to find the minimal polytope $\mathcal{D}_\rho^*$ of $\mathcal{D}_\rho$. It succeeds in giving 108 vertices ρ_{o_i}. Both the set Ω_ρ and the minimal polytope $\mathcal{D}_\rho^*$ in the $(\rho_k^{(1)}, \rho_k^{(2)})$ subspace are depicted in Figure 2 (a). Another polytope $\mathcal{D}_\rho$, that is non minimal in such a case, can be defined as depicted in Figure 2 (b). The number of vertices reduces to 5 but the stability conditions (12) would be more conservative. To conclude, such a choice for ρ_k fulfills the conditions of Proposition 1.

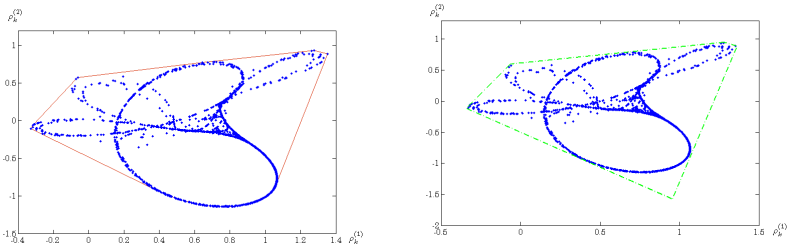

Fig. 2. (a) Set Ω_ρ and polytope $\mathcal{D}_\rho^*$ (b) Polytope $\mathcal{D}_\rho$ with 5 vertices

3.3 Example 3

This example aims at illustrating that a switched linear systems also admits an LPV form like (1) with polytopic description (3). Let us consider the following map derived from the "Lozi map" given in [26] after replacing the affine part "1" by a new

variable $x_k^{(3)}$

$$\begin{cases} x_{k+1}^{(1)} = -1.7 \left| x_k^{(1)} \right| + x_k^{(2)} + x_k^{(3)} \\ x_{k+1}^{(2)} = 0.5\ x_k^{(1)} \\ x_{k+1}^{(3)} = x_k^{(3)} \\ y_k = 2\ x_k^{(1)} \end{cases} \tag{17}$$

Define ρ_k as the one-dimensional time-varying parameter such as $\rho_k = \rho_k^{(1)}$ with

$$\rho_k^{(1)} = \begin{cases} -1.7 & \text{if } x_k^{(1)} \geq 0 \\ 1.7 & \text{if } x_k^{(1)} < 0 \end{cases}$$

Then, (17) can be rewritten in the form (1) with

$$A(\rho_k) = \begin{bmatrix} \rho_k^{(1)} & 1 & 1 \\ 0.5 & 0 & 0 \\ 0 & 0 & 1 \end{bmatrix},\ B = \mathbf{0},\ C = [2\ \ 0] \text{ and } D = \mathbf{0}$$

The vector ρ_k only takes two specific values $\rho_{min} = -1.7$ and $\rho_{max} = 1.7$. Hence, $\Omega_\rho = \{\rho_{min}, \rho_{max}\}$ is not a continuum but reduces to a finite set of two elements. The vertices of the polytope $\mathcal{D}_\rho$ coincide with Ω_ρ. The vertices are $\rho_{o_1} = \rho_{min} = -1.7$ and $\rho_{o_2} = \rho_{max} = 1.7$. Such a choice for ρ_k fulfills all the conditions of Proposition 1. In particular, ρ_k is available from the output y_k. Indeed,

$$\rho_k^{(1)} = \begin{cases} -1.7 & \text{if } y_k \geq 0 \\ 1.7 & \text{if } y_k < 0 \end{cases}$$

Besides, $\rho(x_k)$ is clearly bounded. To conclude, such a choice for ρ_k fulfills the conditions of Proposition 1.

3.4 Example 4

This example aims at illustrating the use of polytopic observers to ensure chaos synchronization for a chaos-based switching cryptosystem.

The general principle is recalled on Figure 3. The transmitters 1 and 2 are de-

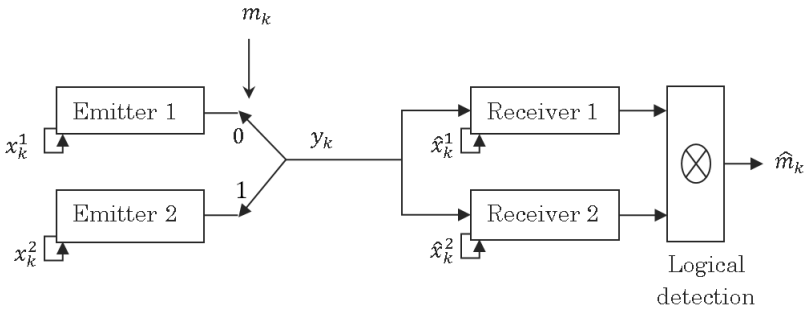

Fig. 3. Secure communication setup

scribed by Υ_1 and Υ_2 respectively. Let us denote with x_k^j the state vector of the system Υ_j and with $x_k^{(i,j)}$ the ith component of x_k^j for the system Υ_j.

$$\Upsilon_1 \begin{cases} x_{k+1}^{(1,1)} = -1.4\left(x_k^{(1,1)}\right)^2 + x_k^{(2,1)} + x_k^{(3,1)} \\ x_{k+1}^{(2,1)} = 0.3\ x_k^{(1,1)} \\ x_{k+1}^{(3,1)} = x_k^{(3,1)} \\ y_k^1 = 0.4\ x_k^{(1,1)} \end{cases} \tag{18}$$

and

$$\Upsilon_2 \begin{cases} x_{k+1}^{(1,2)} = -0.825x_k^{(1,2)} - 0.296\left(x_k^{(1,2)}\right)^2 - x_k^{(2,2)} + 1.04\left(x_k^{(1,2)}\right)^2 x_k^{(2,2)} \\ \qquad\qquad - 1.04\left(x_k^{(1,2)}\right)^4 x_k^{(2,2)} \\ x_{k+1}^{(2,2)} = 1.127\ x_k^{(1,2)} \\ y_k^2 = 0.5\ x_k^{(1,2)} \end{cases} \tag{19}$$

The information m_k is binary and then, only takes two values $m_1 = 0$ or $m_2 = 1$. According to the current value of the information at time k, the output y_k^1 of Υ_1 or y_k^2 of Υ_2 is conveyed through the channel, that is

$$y_k = \begin{cases} y_k^1 & \text{if } \ m_k = m_1 \\ y_k^2 & \text{if } \ m_k = m_2 \end{cases} \tag{20}$$

The objective is to design the receivers assigned to each system in order to recover m_k. To this end, two polytopic observers are well suited. We detail below the off-line step (design) and the on-line step (deciphering).

Off-line step

Υ_1 and Υ_2 admit an LPV polytopic description (1) as shown below.

– **System** Υ_1 (18)

The time-varying parameter for System Υ_1 (18) is denoted ρ_k^1. It is defined as a one-dimensional vector such as $\rho_k^1 = \rho_k^{(1,1)}$ with

$$\rho_k^{(1,1)} = -1.4\ x_k^{(1,1)} \tag{21}$$

Then, (18) can be rewritten in the LPV form (1) with polytopic dependence (3) where

$$A(\rho_k^1) = \begin{bmatrix} \rho_k^{(1,1)} & 1 & 1 \\ 0.3 & 0 & 0 \\ 0 & 0 & 1 \end{bmatrix}, \quad C = \begin{bmatrix} 0.4 & 0 & 0 \end{bmatrix}$$

The matrices B and D are zero since (18) is autonomous. The parameter ρ_k^1 is available from the output y_k^1 since $\rho_k^{(1,1)} = -3.5y_k^1$. Furthermore, the vector ρ_k^1 belongs to the range $\left[\min(\rho_k^{(1,1)})\ \max(\rho_k^{(1,1)})\right]$. As a result, the minimal polytope $\mathcal{D}_{\rho^1}^*$ is obtained in a straightforward way. It involves 2 vertices $\rho_{o_1}^1 = \min(-1.4\ x_k^{(1,1)})$ and $\rho_{o_2}^1 = \max(-1.4\ x_k^{(1,1)})$ ($N = 2$) and the vertices A_i of (3) can be directly derived with (6). As a conclusion, the definition of ρ_k^1 fulfills the conditions of Proposition 1.

– **System Υ_2 (19)**

The time-varying parameter of System Υ_2 (19) is denoted ρ_k^2 and is two-dimensional. It is defined as

$$\begin{aligned}\rho_k^{(1,2)} &= -0.825 - 0.296\ x_k^{(1,2)} \\ \rho_k^{(2,2)} &= -1 + 1.04\left(x_k^{(1,2)}\right)^2 - 1.04\left(x_k^{(1,2)}\right)^4\end{aligned} \tag{22}$$

Then, (19) can be rewritten in the LPV form (1) with polytopic dependence (3) where

$$A(\rho_k^2) = \begin{bmatrix} \rho_k^{(1,2)} & \rho_k^{(2,2)} \\ 1.127 & 0 \end{bmatrix}, \quad C = \begin{bmatrix} 0.5\ 0 \end{bmatrix}$$

The matrices B and D are zero since (19) is autonomous. The parameter ρ_k^2 is available from the output y_k^2 since $\rho_k^{(1,2)} = -0.825 - 0.592\ y_k^2$ and $\rho_k^{(2,2)} = -1 + 4.16\left(y_k^2\right)^2 - 16.64\left(y_k^2\right)^4$. After iterating (19), 500 vectors ρ_k^2 are collected and gathered in Γ_{ρ^2} which is bounded. The function *convhull* of Matlab is used to find the minimal polytope $\mathcal{D}_{\rho^2}^*$ of $\mathcal{D}_{\rho^2}$. It succeeds in giving 121 vertices $\rho_{o_i}^2$. The set Ω_{ρ^2} and the minimal polytope $\mathcal{D}_{\rho^2}^*$ are depicted in Figure 4. The vertices A_i of (3) can be directly derived with (6). As a conclusion, the definition of ρ_k^2 fulfills the conditions of Proposition 1.

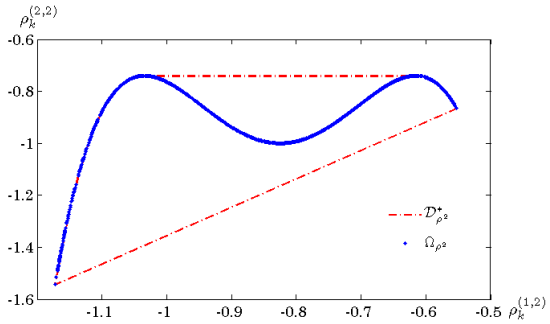

Fig. 4. Set Ω_{ρ^2} and polytope $\mathcal{D}_{\rho^2}^*$ of Υ_2

The receivers 1 and 2 are chosen to take the form of polytopic observers (8) for the respective systems (18) and (19) following the principle as depicted in Figure 3. To this end, the toolbox *Yalmip* of Matlab is used to solve the LMI (12) from which the gains L_1 and L_2 are derived for each system Υ_1 and Υ_2. It turns out that the LMI (12) are feasible and the gains L_1 and L_2 can be performed from by $G_i^{-1}F_i$ according to Theorem 1.

On-line step

a) state reconstruction

The on-line state reconstruction, and so the chaos synchronization, is performed on-line by the polytopic observers (8) for each system Υ_1 and Υ_2. The results are depicted in Figures 5 and 6. Figure 5 highlights the time evolution of the state reconstruction errors $x_k^{(1,1)} - \hat{x}_k^{(1,1)}$, $x_k^{(2,1)} - \hat{x}_k^{(2,1)}$ and $x_k^{(3,1)} - \hat{x}_k^{(3,1)}$ for Υ_1 and Figure 6 highlights the time evolution of the state reconstruction errors $x_k^{(1,2)} - \hat{x}_k^{(1,2)}$ and $x_k^{(2,2)} - \hat{x}_k^{(2,2)}$

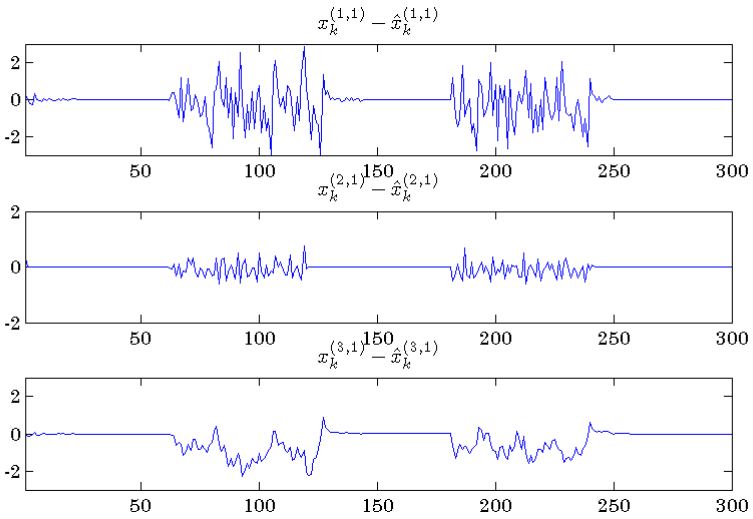

Fig. 5. State reconstruction error for Υ_1

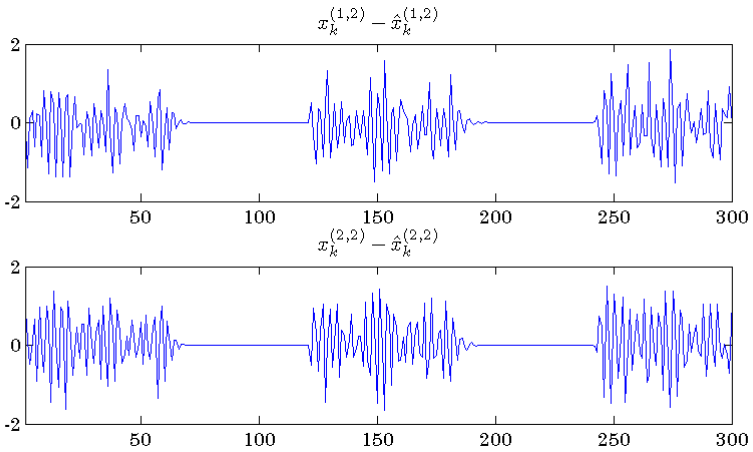

Fig. 6. State reconstruction error for Υ_2

for Υ_2.

b) logical detection
A logical detection based on the state reconstruction error is required for the recovery of m_k. It is defined as follows.

$$\hat{m}_k = \begin{cases} 0 \text{ if } x_k^{(1,1)} - \hat{x}_k^{(1,1)} = \mathbf{0} \text{ and } x_k^{(2,1)} - \hat{x}_k^{(2,1)} = \mathbf{0} \text{ and } x_k^{(3,1)} - \hat{x}_k^{(3,1)} = \mathbf{0} \\ 1 \text{ if } x_k^{(1,2)} - \hat{x}_k^{(1,2)} = \mathbf{0} \text{ and } x_k^{(2,2)} - \hat{x}_k^{(2,2)} = \mathbf{0} \end{cases} \tag{23}$$

Actually, in practice, we should replace 0 by a given tolerance ϵ. The information recovery is illustrated on Figure 7.

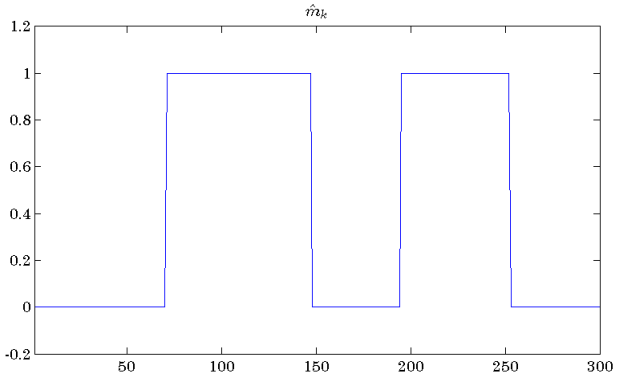

Fig. 7. Recovered information $\hat{m}_k$

4 Conclusion

This paper has presented a unified framework to achieve chaos synchronization of both classes of chaotic discrete-time systems, namely maps involving polynomial nonlinearities and piecewise linear maps which encompass a very large class of chaotic systems. It has been derived conditions under which those chaotic systems can be rewritten as polytopic Linear Parameter Varying (LPV) models. The outcome of the LPV framework lies in that, the observers, which play the role of the receivers, admit a simple Luenberger-like description for all those chaotic systems. Hence, such a framework gives a systematic approach for the design of the receivers. The gains of the polytopic observers are derived from the solution of a close set of Linear Matrix Inequalities for which standard solvers exist. The use of the LPV framework has been illustrated for the chaotic switching cryptosystem but the same methodology applies for all the well-known chaotic cryptosystems, namely, the parameter modulation, the two-channel transmission, the message embedding. Finally, the LPV framework is flexible enough to cope with mismatched parameters or noisy contexts. Indeed, the structure of the observer is kept unchanged. Only the gains must be adapted but it turns out that they are still derived from LMI and so, the ease of design is preserved.

References

1. D. E. Knuth, *The Art of Computer Programming*, **2**, (Addison-Wesley, Reading, MA, 1998)
2. M. J. Ogorzalek, IEEE Trans. Circuits. Syst. I: Fundamental Theo. Appl, **40**, (1993) 693-699
3. M. Hasler, International Journal of Bifurcation and Chaos, **8**, (1998) 647-659
4. T. Yang, Int. J. of Computational Cognition, (2004), (available at http://www.YangSky.com/yangijcc.htm).
5. G. Millérioux, J. M. Amigó, and J. Daafouz, IEEE Trans. on Circuits and Systems I: Regular Papers, **55**, (2008) 1695-1703
6. S. Banerjee, Ed., Chaos Synchronization and Cryptography for Secure Communications: Applications for Encryption, IGI Global, (2010)
7. H. Nijmeijer and I. M. Y. Mareels, IEEE Trans. Circuits. Syst. I: Fundamental Theo. Appl, **44**, (1997) 882-890
8. G. Grassi and S. Mascolo, IEEE Trans. Circuits. Syst. I: Fundamental Theo. Appl, **44**, (1997) 1011-1014

9. M. Itoh, C. W. Wu, and L. O. Chua, International Journal of Bifurcation and Chaos, **7**, (1997) 275-286
10. G. Millérioux, International Journal of Bifurcation and Chaos, **7**, (1997) 1635-1649
11. P. Apkarian, P. Gahinet, and G. Becker, IEEE Transactions on Automatic Control, **40**, (1995) 853-864
12. A. Packard and G. Balas,"Theory and application of linear parameter-varying control techniques", (1997)
13. D.J. Leith and W.E. Leithead, International Journal of Control, **73**, (2000) 1001-1025
14. C. Scherer, Automatica, **37**, (2001) 361-375
15. S. M. Lee and J. H. Park, Applied Mathematics and Computation, **190**, (2007) 671-676
16. M. Farhood and G.E. Dullerud, **44**, (2010) 2108-2119
17. G. I. Bara, J. Daafouz, F. Kratz, and J. Ragot, **74**, no. 16, (2001) 1601-1611
18. M. Heemels, J. Daafouz, and G. Millérioux, IEEE Transactions on Automatic Control, **55**, (2010) 2130-2135
19. R. Toth, F. Felici, P.S.C Heuberger, and P. M. J. Van den Hof, In proceeding of: Proceedings of the European Control Conference, (2007)
20. M. Sato, Automatica, **42**, (2006) 2017-2023
21. S. Boyd, L. El Ghaoui, E. Feron, and V. Balakrishnan, SIAM Studies in Applied Mathematics **15**, (1994)
22. M. C. de Oliveira, D.P. Farias, and J.C. Geromel, LMI solver, http://www.dt.fee.unicamp.br/ carvalho/software.html.
23. M. Halimi, G. Millerioux, and J. Daafouz, *Robust Control and Linear Parameter Varying Approaches* (Springer Berlin Heidelberg, 2013) 97-124
24. A. Goldsztejn, W. Hayes and P. Collins, SIAM J. Applied Dynamical Systems **10**, (2011) 1480-1501
25. H.E. Nusse and J.A. Yorke, *Dynamics: Numerical Explorations*, (Springer, New York, 1994)
26. H. O. Peitgen, H. Jurgens and D. Saupe, *Chaos and fractals: new frontiers of science*, (Springer-Verlag, New York, 1992)