Polytopic observer design for LPV systems based on minimal convex polytope finding

Floriane Anstett, Gilles Millérioux, Gérard Bloch

Polytopic observer design for LPV systems based on minimal convex polytope finding

Floriane Anstett* , Gilles Millérioux*, Gérard Bloch*

***Abstract*— Linear Parameter Varying (LPV) systems are models widely encountered in the engineering field. In this paper, a systematic method is provided to design a polytopic observer whose goal is to reconstruct the state of discrete-time LPV systems. The method incorporates in an original manner a minimal convex polytope finding and thereby confers efficiency to the reconstruction technique. The proposed approach is illustrated in the context of secure communications based on chaotic parameter modulation.**

***Index Terms*— Linear Parameter Varying (LPV) systems, minimal convex polytope, polytopic observers, chaotic systems**

I. Introduction

Linear Parameter Varying (LPV) systems are models widely encountered in the engineering field. They are characterized by a dynamics which is linear with respect to the state vector but, unlike pure linear systems, the dynamical matrix depends on a time-varying parameter. A LPV description may result from a system which smoothly switches between time-invariant models assigned to distinct operating conditions. LPV models may also result from the rewriting of the dynamics governing a nonlinear system. This is typically the case when dealing with chaotic systems [1]. Even though analyzing or guaranteeing the stability of LPV systems is not a simple matter in general, some tractable stability conditions in terms of Linear Matrix Inequalities have been successfully derived in [2] under the assumption that a polytopic decomposition of the parameter dependent dynamical matrix can be carried out. Actually, such a decomposition is possible whenever the time-varying parameter is bounded. Indeed, if so, the parameter lies in a compact set which can always be embedded in a polytope. However, such a polytope is not unique. And yet, the conservatism of the LMI conditions, and then the efficiency of the related control or observer design, highly depend on the polytopic decomposition. Recently, it has been shown [1] that the minimal convex polytope guarantees the best decomposition in terms of conservatism.

There exist different algorithms to find the minimal convex polytope of a finite set of points, to mention a few, the Graham scan [3], Quick Hull [4] [5] [6], the random sampling [7] or the linear programming approach [8]. Those algorithms have been proposed in some totally distinct contexts but have never been used for control purpose. The aim of this paper is to review some of the most relevant and to show that they can be incorporated into the design of polytopic observers, i.e. state reconstructors of LPV systems admitting a polytopic description.

The paper is organized as follows. In Section II, some recalls on discrete-time LPV systems, polytopic description and polytopic observers are carried out. Then, a general approach for designing a polytopic observer is presented. In Section III, different algorithms for minimal convex polytope finding and polytopic decomposition are first reviewed. Then, it is shown how those algorithms can be systematically incorporated into the design of a polytopic observer to improve the state reconstruction efficiency. Finally, in Section IV, the proposed approach is applied in a chaos-based secure communication scheme. In this context, a polytopic observer achieves a joint state and parameter estimation for recovering the information masked through a chaotic parameter modulation.

II. LPV polytopic systems and polytopic observers

Let us first recall some important definitions which shall be used in the sequel. The convex hull of a set of points is the minimal convex set containing this set. The minimal convex polytope of a finite set of points is the convex hull of this set. The vertices of the minimal convex polytope are called extreme points. Finding the minimal convex polytope of a finite set of points consists in determining the set of extreme points.

A. LPV polytopic form

Consider the discrete-time LPV system:

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

where $x_k \in \mathbb{R}^n$ is the state vector, $y_k \in \mathbb{R}^p$ the output, $\mathscr{A} \in \mathbb{R}^{n\times n}$ the dynamical matrix, $C \in \mathbb{R}^{p\times n}$ the output matrix, $\rho_k = [\rho_k^{(1)} \dots \rho_k^{(j)} \dots \rho_k^{(L)}]^T \in \mathbb{R}^L$ the time-varying parameter. We recall the usual assumptions related to LPV systems:

i) ρ_k is bounded,
ii) $\mathscr{A}$ is of class C^1 with respect to the entries of ρ_k,
iii) ρ_k is on-line accessible.

By virtue of assumption i), ρ_k evolves in a compact set Ω_ρ and thereby can be always included in a convex polytope $\mathscr{D}_\rho$. Hence, ρ_k can be expressed as

$$\rho_k = \sum_{i=1}^{N} \xi_k^{(i)} \theta_i \tag{2}$$

* The authors are with the Centre de Recherche en Automatique de Nancy (CRAN), Nancy-University, CNRS. Address: CRAN-ESSTIN, 2 rue Jean Lamour, 54519 Vandoeuvre lès Nancy, France. Email: {firstname.lastname}@esstin.uhp-nancy.fr.

where the vector ξ_k belongs to the convex set $S = \{\mu_k \in \mathbb{R}^N, \mu_k = [\mu_k^{(1)} \dots \mu_k^{(N)}]^T, \mu_k^{(i)} \geq 0 \quad \forall i, \sum_{i=1}^{N} \mu_k^{(i)} = 1\}$. The constant vectors $\theta_i, \dots, \theta_N$ are the N vertices of the convex polytope $\mathscr{D}_\rho$. Hereafter, the notation $\xi_k(\rho_k)$ will be used to reflect the implicit dependence of ξ_k on ρ_k expressed by Eq. (2).
It is shown in [1] that, by virtue of the assumption ii), $\mathscr{A}(\rho_k)$ can always be decomposed as

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

with

$$A^{(i)} = \mathscr{A}_0 + \sum_{j=1}^{L} \theta_i^{(j)} A^{I_j} \tag{4}$$

and where $\mathscr{A}_0$ is a matrix derived from $\mathscr{A}$ by keeping its constant entries while setting to zero its time-varying entries. $\theta_i^{(j)}$ represents the component j of the vertex θ_i of the convex polytope $\mathscr{D}_\rho$. A^{I_j} is the matrix whose entries are all zero except the one corresponding to the position of $\rho_k^{(j)}$ in $\mathscr{A}$, which equals to unity.
Note that the vector ξ_k coincides with the one involved in (2). The constant matrices $A^{(1)}, \dots, A^{(N)}$ are the N vertices of the convex polytope $\mathscr{D}_\mathscr{A}$ associated to the polytope decomposition (3).
In the next section, a state reconstruction technique for LPV systems like (1) admitting a polytopic description is provided. The reconstruction is achieved by resorting to a so-called polytopic observer. The reader can refer to [9][10][11] for instance to get acquainted with the use of polytopic observers over distinct contexts.

B. Polytopic observer

A polytopic observer reads

$$\begin{cases} \hat{x}_{k+1} = \mathscr{A}(\rho_k)\hat{x}_k + \mathscr{L}(\rho_k)(y_k - \hat{y}_k) \\ \hat{y}_k \quad\quad = C\hat{x}_k \end{cases} \tag{5}$$

where $\mathscr{L}$ is a time-varying gain depending on ρ_k. The state reconstruction error $\varepsilon_k = x_k - \hat{x}_k$, obtained from (1) and (5), is governed by:

$$\varepsilon_{k+1} = \big(\mathscr{A}(\rho_k) - \mathscr{L}(\rho_k)C\big)\varepsilon_k \tag{6}$$

The dynamics of the state reconstruction is nonlinear since the matrices $\mathscr{A}$ and $\mathscr{L}$ depend on ρ_k. Thus (6) is in turn a LPV system. Its global stability around zero can be guaranteed by a suitable choice of the gain matrix $\mathscr{L}$. Let the gain $\mathscr{L}$ admit the following form:

$$\mathscr{L}(\rho_k) = \sum_{i=1}^{N} \xi_k^{(i)}(\rho_k) L_i \tag{7}$$

If the vector ξ_k of (7) is chosen so as it coincides with the one involved in (3), then (6) turns into :

$$\varepsilon_{k+1} = \sum_{i=1}^{N} \xi_k^{(i)}(\rho_k)(A^{(i)} - L_i C)\varepsilon_k \tag{8}$$

Then, global conditions for convergence toward zero are ensured from Theorem 1.

Theorem 1 ([11]): Global convergence of (8) is achieved whenever the following set of Linear Matrix Inequalities

$$\begin{bmatrix} P_i & A^{(i)T}G_i^T - C^T F_i^T \\ G_i A^{(i)} - F_i C & G_i + G_i^T - P_j \end{bmatrix} > 0 \tag{9}$$

is feasible for all $(i, j) \in \{1, \dots, N\} \times \{1, \dots, N\}$.
The G_i's, F_i's and P_i's are unknown matrices of appropriate dimensions. The resulting gains are given by:

$$L_i = G_i^{-1} F_i \tag{10}$$

Actually, it can be shown that (9) ensures the existence of a so-called polyquadratic Lyapunov function $V : \mathbb{R}^n \to \mathbb{R}^+$, defined by $V(\varepsilon_k) = \varepsilon_k^T \mathscr{P}_k \varepsilon_k$, with $\mathscr{P}_k = \sum_{i=1}^{N} \xi_k^{(i)} P_i$, $\xi_k \in S$, fulfilling

$$V(\varepsilon_{k+1}) - V(\varepsilon_k) < 0 \tag{11}$$

The existence of such a Lyapunov function guarantees the polyquadratic stability (of the state reconstruction error in our context) which is sufficient for global convergence.

Remark 1: Alternatively, we could be interested in seeking for a constant gain $\mathscr{L}$ which does not depend on ρ_k, i.e $\mathscr{L}(\rho_k) = L$. In such a case, (6) would turn into

$$\varepsilon_{k+1} = \big(\mathscr{A}(\rho_k) - LC\big)\varepsilon_k \tag{12}$$

which can be, without any effort, written in a LPV polytopic form. Hence, we can resort to the following theorem

Theorem 2: Global convergence of (12) is achieved whenever the following set of Linear Matrix Inequalities

$$\begin{bmatrix} P_i & A^{(i)T}G^T - C^T F^T \\ GA^{(i)} - FC & G + G^T - P_j \end{bmatrix} > 0 \tag{13}$$

is feasible for all $(i, j) \in \{1, \dots, N\} \times \{1, \dots, N\}$.
The matrix G, the matrix F and the matrices P_i's are unknown. The gain L is given by:

$$L = G^{-1} F \tag{14}$$

Actually, (13) still ensures the existence of a polyquadratic Lyapunov function V fulfilling (11) but the conditions are more conservative.

A key point is that the polytope $\mathscr{D}_\rho$ and so $\mathscr{D}_\mathscr{A}$ is not unique. And yet, the conservatism of the LMI conditions highly depends on the polytopic decomposition. It turns out that the conservatism is directly related to the size of the polytope $\mathscr{D}_\rho$ which must be minimal [1]. As a result, we must seek for the vertices θ_i of this minimal convex polytope which will be hereafter denoted $\mathscr{D}_\rho^*$. Besides, for good efficiency of polytopic observers, we must propose a relevant method for the on-line computation of the ξ_k involved in the gain $\mathscr{L}$ of (7). Those two issues are discussed in the next section.

III. Polytopic observer design

A. Minimal convex polytope finding

The most relevant algorithms for finding the minimal convex polytope of a finite set of points, i.e. for finding the set of extreme points, are first presented here in dimension two. However, their extension to greater dimension whenever possible is then sketched. Throughout this section, a finite set of K points $\Lambda = \{\theta_0 \dots \theta_{K-1}\}$ is called a list. $\theta_i^{(j)}$ $(j = 1, \dots, L)$ stands for the j^{th} component of θ_i. When dealing with some angles α_i, they will be considered, by convention, as positive if measured counterclockwise.

Graham scan

The Graham scan [3] is based on the principle that two consecutive faces, made by three consecutive extreme points, form an angle less than π. The algorithm is divided into two steps, the sort of the consecutive points and the computation of the angles between two consecutive faces.

The algorithm starts by picking out a point of the set Λ which is known to be an extreme point. This point, denoted θ_0, will be a reference for the sort of the other points. One can choose, for instance, the point of minimal ordinate. If there exist several points with the same minimal ordinate, one can choose the one which has the greatest abscissa.

Having selected the reference point, the first step consists in sorting the other points θ_i of Λ by increasing angle α_i that the line $(\theta_0\theta_i)$ forms with the x-axis. The list of such ordered points is denoted Λ_t. This step is illustrated on Fig. 1(a), where $\Lambda_t = \{\theta_0\theta_1\theta_5\theta_2\theta_4\theta_3\}$. The sort of two points θ_i and θ_j does not require the explicit computation of the corresponding angles α_i and α_j because the following equivalence applies:

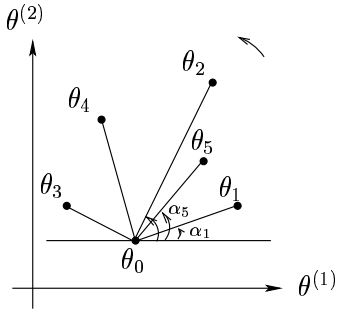
$$\begin{aligned}\alpha_i < \alpha_j \Leftrightarrow (\theta_i^{(2)} - \theta_0^{(2)})(\theta_j^{(1)} - \theta_0^{(1)}) \\ - (\theta_j^{(2)} - \theta_0^{(2)})(\theta_i^{(1)} - \theta_0^{(1)}) < 0\end{aligned} \tag{15}$$

where the evaluation of the right hand side involving a crossproduct requires only fast accurate operations (additions, multiplications).

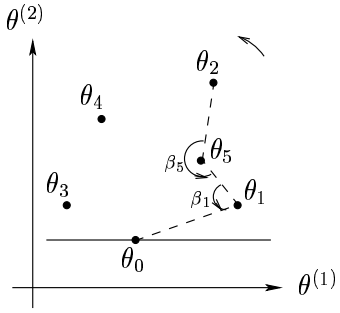
The second step consists in testing whether the angle β_j between two consecutive faces, made by three sorted consecutive points θ_i, θ_j and θ_l, is less than π. If $\beta_j < \pi$, the point θ_j is an extreme point. If $\beta_j \geq \pi$, θ_j is not an extreme point and it is removed from Λ_t. The algorithm proceeds again with the new list until all the points have been tested. At the end, Λ_t contains only the extreme points. As previously, the test can be made without computing explicitly the angles, but by exploiting the equivalence:

$$\begin{aligned}\beta_j < \pi \Leftrightarrow (\theta_j^{(1)} - \theta_i^{(1)})(\theta_l^{(2)} - \theta_i^{(2)}) \\ - (\theta_l^{(1)} - \theta_i^{(1)})(\theta_j^{(2)} - \theta_i^{(2)}) < 0\end{aligned} \tag{16}$$

Figure 1(b) illustrates the selection of extreme points. On this figure, θ_1 is an extreme point since $\beta_1 < \pi$, but not θ_5 since $\beta_5 > \pi$. Thus, θ_5 is removed from the list Λ_t and the test proceeds again with the new list $\Lambda_t = \{\theta_0\theta_1\theta_2\theta_4\theta_3\}$, until all the points of Λ_t have been tested. Finally, the vertices of the minimal convex polytope of Λ, represented on Fig. 2, are $\{\theta_0\theta_1\theta_2\theta_4\theta_3\}$.



(a) Sort of the points



(b) Selection of extreme points

Fig. 1. The two steps of the Graham scan

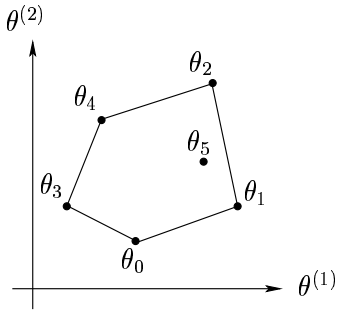


Fig. 2. Minimal convex polytope

This algorithm has a low complexity $\sigma(K \log K)$, K being the number of points in Λ, but it cannot be generalized to dimensions greater than 2.

Quick Hull

Several versions of Quick Hull have been proposed [4][5]. This algorithm is based on the approach "divide and conquer". Indeed, the points located inside a triangle formed with three points of Λ known as extreme points do not belong to the set of extreme points and can be no longer considered.

The algorithm starts by picking out two points of Λ, θ_0 and θ_1, which are known to be extreme points. For instance, the points of minimal and maximal abscissa, respectively, can be chosen. The line $(\theta_0\theta_1)$ passing through these two reference points divides the set Λ into two subsets. In every subset, we

seek for the point which has the greatest euclidean distance to the line $(\theta_0\theta_1)$. These two points, denoted θ_i and θ_j, are extreme points. The points located inside the triangles $\theta_0\theta_1\theta_i$ and $\theta_0\theta_1\theta_j$ are not vertices of the minimal convex polytope, and thus are removed from the list Λ. The algorithm proceeds again with new reference lines passing through two arbitrary chosen points which are known to be extreme points. This procedure is repeated until all the possible lines have been tested.

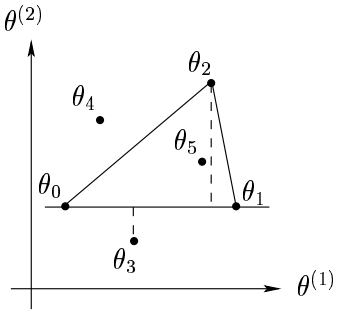


Fig. 3. Quick Hull

Figure 3 illustrates this approach. The line $(\theta_0\theta_1)$ divides the set of points into two subsets. θ_2 and θ_3 have, respectively in each subset, the greatest euclidean distance to this line and are extreme points. θ_5, located inside the triangle $\theta_0\theta_1\theta_2$, is not an extreme point and is discarded. The algorithm proceeds again with a new reference line, for example $(\theta_0\theta_2)$. Finally, the extreme points are $\{\theta_0\theta_1\theta_2\theta_3\theta_4\}$.

The algorithm has the same complexity $\sigma(K \log K)$ as the one of the Graham scan, but it can be extended to dimensions greater than 2.

In dimension 3, the algorithm has been studied in [6]. The principle is that the points located inside a tetrahedron formed with four points of Λ known as extreme points do not belong to the set of extreme points and are no longer considered. To start the division, three reference points, θ_0, θ_1 and θ_2, which are known to be extreme points, are chosen. These three points form a triangular face which divides the space. In every subspace, the point θ_i of greatest euclidean distance to the initial face is found. The points located inside the tetrahedron $\theta_0\theta_1\theta_2\theta_i$ are not extreme points and are discarded. The procedure is repeated until all the points of Λ are tested. In dimension 3, the algorithm complexity is $\sigma(K^2)$.

Random sampling

Random sampling is reported in [7]. Its principle consists in projecting the points of the set Λ on a line chosen randomly. The two points projected on the line with minimal and maximal abscissas are extreme points. The procedure is repeated with new random lines until no new extreme point can be found.

Since some projections on different lines can lead to find the same pair of extreme points, the projections which do not lead to a new pair of extreme points are eliminated. This elimination is based on the following principle. If two arbitrary lines, which form respectively angles α_1 and α_2 with the x-axis, lead to the same pair of extreme points, then every line forming an angle α with the x-axis, $\alpha_1 < \alpha < \alpha_2$, will also lead to the same pair and will not be tested since it does not bring any more new extreme points.

This approach is illustrated on Fig. 4. In this example, the projections of the points of Λ on the line D_1 show that θ_2 and θ_3 are extreme points. The projection on D_2 delivers the same pair. Thus, any line which forms an angle α with the x-axis, $\alpha_1 < \alpha < \alpha_2$, will not be tested. On the other hand, the projection on D_3 shows that θ_1 and θ_4 belong to the set of extreme points of Λ.

This approach can be extended to dimension $L > 2$. In this case, the points of Λ are projected on arbitrary hyperplanes of dimension $L-1$.

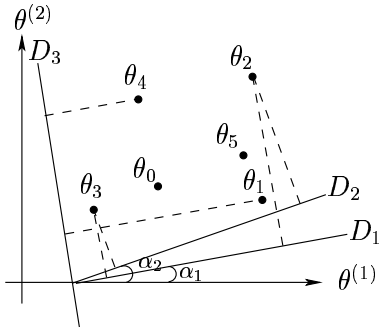


Fig. 4. Random sampling

Linear programming approach

Finding the minimal convex polytope of a finite set of points can be viewed as a linear programming problem, whatever the dimension L is. The following theorem, stated in [8], gives a necessary and sufficient condition for a point θ_j to be an extreme point of the convex hull of $\Lambda = \{\theta_0 \dots \theta_{K-1}\}$.

Theorem 3: The solution of the linear program

$$\begin{aligned} &\min \quad z_j \\ &\text{s. t.} \sum_{i=0}^{K-1} z_i\theta_i = \theta_j, \ \sum_{i=0}^{K-1} z_i = 1, \ z_i \geq 0, \ i = 0,\dots,K-1 \end{aligned} \tag{17}$$

is positive if and only if θ_j is an extreme point of the convex hull of Λ.

By definition, if θ_j is an extreme point of Λ, it is not a convex combination of the other points of Λ and 1 is the unique optimal solution of (17). Conversely, if θ_j is not an extreme point of Λ, it is a convex combination of the other points of Λ and 0 is always the optimal solution of (17). In this case, the point θ_j is removed from the set Λ and the procedure is repeated until all the points of Λ have been tested.

Now, let us turn back to our special context. It is recalled that the time-varying parameter ρ_k of the LPV system can be written in the polytopic form (2). Actually, the above mentioned finding approaches appear to be relevant to determine the vertices θ_i of the minimal convex polytope $\mathscr{D}_\rho^*$ including Ω_ρ. And yet, in order to compute $\mathscr{L}(\rho_k)$ (Eq.7), it is necessary to determine on-line the vector ξ_k. It is the purpose of the next section.

B. On-line polytopic decomposition

The vertices θ_i being known, the decomposition problem can be reformulated as follows.
Find the vector $\xi_k = \left[\xi_k^{(1)} \dots \xi_k^{(N)}\right]^T$ such that:

$$u_k = Z\xi_k, \quad \xi_k^{(i)} \geq 0, \quad i = 1,\dots,N \tag{18}$$

with $u_k = \left[\rho_k^T \quad 1\right]^T = \left[\rho_k^{(1)} \dots \rho_k^{(L)} \quad 1\right]^T$ and

$$Z = \begin{bmatrix} \theta_1^{(1)} & \dots & \theta_i^{(1)} & \dots & \theta_N^{(1)} \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ \theta_1^{(L)} & \dots & \theta_i^{(L)} & \dots & \theta_N^{(L)} \\ 1 & \dots & 1 & \dots & 1 \end{bmatrix}$$

The last row entries of u_k and Z correspond to the constraint $\sum_{i=1}^{N} \xi_k^{(i)} = 1$. Usually, the number N of vertices and the dimension L of the polytope are not correlated and most often $N > L+1$, meaning that there are more unknowns (N) than equations $(L+1)$. To determine ξ_k, a brute solution would consist in computing the pseudo-inverse of Z. However, the problem lies in that the number of vertices N can be very large and so Z can be huge.
An alternative to overcome this problem is proposed. Although the principle is detailed for the dimension $L = 2$, it can be extended to greater dimensions. A trivial situation occurs when ρ_k is an extreme point. If so, by definition, all the $\xi_k^{(i)}$ equal zero except the one corresponding to θ_i that equals 1. Otherwise we can rest on the key idea that every point ρ_k located strictly inside the minimal convex polytope $\mathscr{D}_\rho^*$ is also included inside a triangle formed by three vertices of the polytope. Those vertices are denoted θ_p, θ_q and θ_r. As a result, ρ_k can be merely rewritten as a linear combination of these three vertices. Let

$$\underline{Z} = \begin{bmatrix} \theta_p^{(1)} & \theta_q^{(1)} & \theta_r^{(1)} \\ \theta_p^{(2)} & \theta_q^{(2)} & \theta_r^{(2)} \\ 1 & 1 & 1 \end{bmatrix}, \quad u_k = \begin{bmatrix} \rho_k^{(1)} \\ \rho_k^{(2)} \\ 1 \end{bmatrix} \tag{19}$$

Then, $w_k = \left[\xi_k^{(p)} \xi_k^{(q)} \xi_k^{(r)}\right]^T$ is solution of

$$u_k = \underline{Z} w_k \tag{20}$$

The constraint $\xi_k^{(p)}, \xi_k^{(q)}, \xi_k^{(r)} \geq 0$ will be actually always fulfilled since ρ_k is inside the triangle.
In order to find the vertices θ_p, θ_q and θ_r of a triangle including ρ_k, the position of ρ_k with respect to the *oriented* lines $(\theta_p\theta_q)$, $(\theta_p\theta_r)$ and $(\theta_q\theta_r)$, where θ_p, θ_q and θ_r are extreme points arbitrarily chosen, can be tested by computing:

$$Q_1 = (\theta_q^{(1)} - \theta_p^{(1)})(\rho_k^{(2)} - \theta_p^{(2)}) - (\rho_k^{(1)} - \theta_p^{(1)})(\theta_q^{(2)} - \theta_p^{(2)}) \tag{21}$$

$$Q_2 = (\theta_r^{(1)} - \theta_q^{(1)})(\rho_k^{(2)} - \theta_q^{(2)}) - (\rho_k^{(1)} - \theta_q^{(1)})(\theta_r^{(2)} - \theta_q^{(2)}) \tag{22}$$

$$Q_3 = (\theta_p^{(1)} - \theta_r^{(1)})(\rho_k^{(2)} - \theta_r^{(2)}) - (\rho_k^{(1)} - \theta_r^{(1)})(\theta_p^{(2)} - \theta_r^{(2)}) \tag{23}$$

If Q_1 (resp. Q_2 and Q_3) is less than zero, ρ_k is on the right side of $(\theta_p\theta_q)$ (resp. $(\theta_q\theta_r)$ and $(\theta_r\theta_p)$). If Q_1 (resp. Q_2 and Q_3) is greater than zero, ρ_k is on the left side of $(\theta_p\theta_q)$ (resp. $(\theta_q\theta_r)$ and $(\theta_r\theta_p)$). If the three quantities Q_1, Q_2 and Q_3 are of the same sign, ρ_k is located inside the triangle $\theta_p\theta_q\theta_r$; if not, ρ_k is located outside.
In the example illustrated on Fig. 5, for the extreme points θ_1, θ_3, θ_5, that is $p = 1$, $q = 3$, and $r = 5$, $Q_1 > 0$, $Q_2 > 0$, $Q_3 > 0$, meaning that ρ_k is on the left side of $(\theta_1\theta_3)$, $(\theta_3\theta_5)$, $(\theta_5\theta_1)$, respectively. ρ_k is located inside the triangle $\theta_1\theta_3\theta_5$.
On the contrary, for the extreme points θ_3, θ_4, θ_5, that is $p = 3$, $q = 4$, and $r = 5$, $Q_1 > 0$ and $Q_2 > 0$, meaning that ρ_k is on the left side of $(\theta_3\theta_4)$ and $(\theta_4\theta_5)$, respectively. However, since $Q_3 < 0$, meaning that ρ_k is on the right side of $(\theta_5\theta_3)$, ρ_k is not included in the triangle $\theta_3\theta_4\theta_5$.

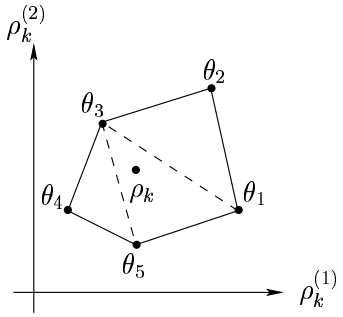


Fig. 5. Localization of ρ_k in a triangle

As mentioned above, this approach can be extended to a dimension L greater than 2. In such a case, ρ_k should be a linear combination of $(L+1)$ vertices of the minimal convex polytope when ρ_k is not an extreme point and a polyhedron with $(L+1)$ vertices including ρ_k has to be found.

C. Summary for the polytopic observer design

The design and the use of a polytopic observer involves two steps: the first one is achieved off-line whereas the second one is performed on-line at each time instant k.

1) **Off-line step**
   - Constitution of the list Λ of points ρ_k by simulating system (1)
   - Finding of the vertices θ_i of the minimal convex polytope $\mathscr{D}_\rho^*$ including ρ_k with one of the approaches presented in Section III-A
   - Determination of the matrices $A^{(i)}$ by (4)
   - Resolution of the LMI (9) and computation of the gain matrices L_i by (10)
2) **On-line step**
   - Computation of ξ_k by (18) or (20)
   - Computation of the gain $\mathscr{L}$ by (7)
   - Computation of $\hat{x}_k$ by (5)

In the next section, an example illustrates the proposed method in the context of secure communications based on chaotic parameter modulation.

IV. Application to secure communications based on chaotic parameter modulation

A. Chaotic parameter modulation

Chaotic behavior is one of the most complex dynamics a nonlinear system can exhibit. Because the signals resulting from chaotic systems are broadband, noiselike, difficult to predict, the idea of using chaotic systems for information masking has received much attention since the pioneering work of [12]. Several methods for "hiding" an information signal into a chaotic signal have been proposed in the literature. An overview can be found according to the chronology in [13][14][15][16] including the chaotic masking, the chaotic switching, the parameter modulation, the message embedding. These methods are defined either for continuous-time or discrete-time systems. Here, we focus on the parameter modulation. For such a scheme, at the transmitter side, a parameter of a chaotic dynamical system is modulated by the information to be masked, also called the plaintext, according to a prescribed rule. For binary messages, the parameter of the transmitter only takes two distinct values [17][18][19].

A general chaotic transmitter system reads:

$$\left\{ \begin{array}{ll} x_{k+1} = f(x_k, \lambda_k(m_k)) \\ y_k \quad = h(x_k) \end{array} \right. \tag{24}$$

where $x_k \in \mathbb{R}^n$ is the state vector, $y_k \in \mathbb{R}$ is the scalar output also called the ciphertext, $m_k \in \mathscr{M}$, a countable set, is called the plaintext, $\lambda_k \in \mathbb{R}^l$ is the (scalar or vectorial) parameter modulated by the information m_k. f is the nonlinear chaotic dynamics and h is the output function.

In such a scheme, m_k must be constant during the time interval $[jT,(j+1)T[$ $(j \in \mathbb{N})$ with T sufficiently large. More details about the choice of T will be provided later on in this section. The modulation obeys the following simple rule. According to the current value of the symbol m_k in the time interval $[jT,(j+1)T[$, $\lambda_k = \lambda^i$ when $m_k = m_i$ where λ^i belongs to a set of same cardinality as $\mathscr{M}$.

Here, we focus on a special set of chaotic systems (24) given by

$$\left\{ \begin{array}{ll} x_{k+1} = A(x_k)x_k + \psi(x_k)\lambda_k \\ y_k \quad = Cx_k \end{array} \right. \tag{25}$$

where $A \in \mathbb{R}^{n\times n}$ is a dynamical matrix depending in a nonlinear way on x_k and ψ a nonlinear function. $C \in \mathbb{R}^{1\times n}$ is the output matrix. The description (25) includes a lot of chaotic systems [1].

A solution to the recovering of m_k at the receiver side consists in estimating both the state vector x_k and the parameter λ^i. The simplified block diagram of a parameter modulation scheme is depicted on Fig. 6. The issue of estimating both the state vector x_k and the parameter λ^i is known in control theory as the joint state and parameter estimation. It involves the use of adaptive observers. It is also similar to the problem of adaptive chaos synchronization. This relevant issue has been widely investigated in the literature [1][20][21][22][23][24]. Many works usually resort to the Extended Kalman Filter (EKF) to handle the problem (see for instance [19]). Nevertheless, most adaptive methods hold whenever the chaotic system verify some special properties such as nonlinearities with Lipschitz conditions, special structure such as output injection. In [1], a new adaptive synchronization scheme, incorporating chaos specificities, has been suggested within the framework of polytopic observers. The advantage lies in that we can get rid of the above mentionned restrictive assumptions. The main results are recalled below.

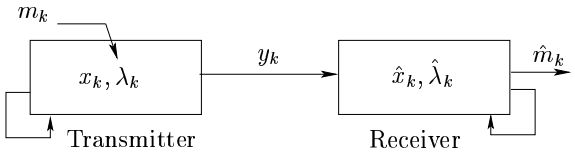


Fig. 6. Parameter modulation

Let introduce the extended state vector $\bar{x}_k$:

$$\bar{x}_k = \left[\begin{array}{c} x_k \\ \lambda^i \end{array} \right] \tag{26}$$

Equation (25) can be rewritten as:

$$\left\{ \begin{array}{ll} \bar{x}_{k+1} = \bar{A}(x_k)\bar{x}_k \\ y_k \quad = \bar{C}\bar{x}_k \end{array} \right. \tag{27}$$

with:

$$\bar{A}(x_k) = \left[\begin{array}{cc} A(x_k) & \psi(x_k) \\ \mathbf{0} & \mathbf{1} \end{array} \right], \quad \bar{C} = \left[\begin{array}{cc} C & \mathbf{0} \end{array} \right] \tag{28}$$

$\mathbf{1}$ and $\mathbf{0}$ being respectively the identity and the null matrix of proper dimension.

Assume that when x_k lies in a chaotic attractor Ω, there exists a function $\varphi : \mathbb{R}^n \to \mathbb{R}^L$ defined as $\rho_k = \varphi(x_k)$ such that:

1) ρ_k is bounded when x_k is bounded,
2) $\mathscr{A}$ defined as $\mathscr{A}(\rho_k) = \mathscr{A}(\varphi(x_k)) = A(x_k)$ and Φ defined as $\Phi(\rho_k) = \Phi(\varphi(x_k)) = \psi(x_k)$ are both of class C^1 with respect to ρ_k,
3) ρ_k is on-line accessible.

If so, (27) can be rewritten as

$$\left\{ \begin{array}{ll} \bar{x}_{k+1} = \bar{\mathscr{A}}(\rho_k)\bar{x}_k \\ y_k \quad = \bar{C}\bar{x}_k \end{array} \right. \tag{29}$$

with:

$$\bar{\mathscr{A}}(\rho_k) = \left[\begin{array}{cc} \mathscr{A}(\rho_k) & \Phi(\rho_k) \\ \mathbf{0} & \mathbf{1} \end{array} \right] = \sum_{i=1}^{N} \xi_k^{(i)}(\rho_k)\bar{A}^{(i)} \tag{30}$$

and we enter the assumptions i) to iii) when considering $\bar{\mathscr{A}}(\rho_k)$. Similarly to (4), the constant matrices $\bar{A}^{(i)}$ are given by:

$$\bar{A}^{(i)} = \bar{\mathscr{A}}_0 + \sum_{j=1}^{L} \theta_i^{(j)} \bar{A}^{I_j} \tag{31}$$

System (29) is of the form (1). Hence, Theorem 1 can be applied to ensure the global convergence of the state reconstruction error by replacing $A^{(i)}$ by $\bar{A}^{(i)}$. Moreover, replacing x_k by $\bar{x}_k$ and (3) by (30), the observer (5) becomes:

$$\left\{\begin{array}{ll}\hat{\bar{x}}_{k+1} & =\bar{\mathscr{A}}(\rho_k)\hat{\bar{x}}_k+\bar{\mathscr{L}}(\rho_k)(y_k-\hat{y}_k)\\ \hat{y}_k & =\bar{C}\hat{\bar{x}}_k\end{array}\right. \tag{32}$$

The quantity T related to the window length must be large enough to guarantee the convergence of $\hat{\bar{x}}_k$ toward $\bar{x}_k$ with good accuracy.

B. Example

Consider the chaotic modulator given by:

$$\left\{\begin{array}{l}x_{k+1}^{(1)}=\cos(\phi)x_k^{(1)}-\sin(\phi)x_k^{(2)}\\ x_{k+1}^{(2)}=\sin(\phi)x_k^{(1)}-(\cos(\phi)-0.3\gamma)x_k^{(2)}+2\gamma(x_k^{(2)})^2\\ \qquad\quad +4\lambda_k\gamma((x_k^{(2)})^3+0.005)\\ y_k \quad =x_k^{(2)}\end{array}\right. \tag{33}$$

with $\phi=3.03$, $\gamma=2.7$ and $x_k=[x_k^{(1)}\quad x_k^{(2)}]^T$. x_k evolves in a chaotic attractor Ω depicted on Fig 7(a). The scalar parameter λ_k is modulated by the binary plaintext $m_k\in\{0,1\}$. λ_k is piecewise constant. Indeed, during the interval $[jT,(j+1)T[$ with $T=200$, $\lambda_k=\lambda^1$ when $m_k=1$ and $\lambda_k=\lambda^2$ when $m_k=0$. Only the state $x_k^{(2)}$ is transmitted.
In the intervals $[jT,(j+1)T[$ $(j\in\mathbb{N})$, the recovering of the information m_k can be achieved by reconstructing the state $x_k^{(1)}$ and the modulated parameter λ^i, as proposed above. To this end, we must rewrite (33) into the appropriate form (29). We first point out that (33) is of the form (25) with:

$$\begin{array}{l}A(x_k)=\left[\begin{array}{cc}\cos(\phi) & -\sin(\phi)\\ \sin(\phi) & -\cos(\phi)+0.3\gamma+2\gamma x_k^{(2)}\end{array}\right],\\ \psi(x_k)=\left[\begin{array}{c}0\\ 4\gamma((x_k^{(2)})^3+0.005)\end{array}\right],\\ C=\left[\begin{array}{cc}0 & 1\end{array}\right]\end{array} \tag{34}$$

Then, let us define the extended state vector $\bar{x}_k$:

$$\bar{x}_k=\left[\begin{array}{c}x_k^{(1)}\\ x_k^{(2)}\\ \lambda^i\end{array}\right] \tag{35}$$

System (33) can thereby be rewritten as (27) with:

$$\bar{A}(x_k)=\left[\begin{array}{cc}A(x_k) & \psi(x_k)\\ \mathbf{0} & 1\end{array}\right],\quad \bar{C}=\left[\begin{array}{ccc}0 & 1 & 0\end{array}\right] \tag{36}$$

We must find out a function $\varphi=[\varphi_1\quad\varphi_2]^T$ such that assumptions 1), 2) and 3) are fulfilled. We take $\rho_k^{(1)}=\varphi_1(x_k)=\cos(\phi)-0.3\gamma+2\gamma x_k^{(2)}$ and $\rho_k^{(2)}=\varphi_2(x_k)=4\gamma((x_k^{(2)})^3+0.005)$. It is clear that since x_k evolves in the chaotic attractor Ω, it is bounded and thus, ρ_k is also bounded (assumption 1)). With such a choice, one has $A(x_k)=\mathscr{A}(\varphi(x_k))=\mathscr{A}(\rho_k)$ and $\psi(x_k)=\Phi(\varphi(x_k))=\Phi(\rho_k)$ and $\bar{\mathscr{A}}(\rho_k)$ reads:

$$\bar{\mathscr{A}}(\rho_k)=\left[\begin{array}{cc}\mathscr{A}(\rho_k) & \Phi(\rho_k)\\ \mathbf{0} & 1\end{array}\right]=\left[\begin{array}{ccc:c}\cos(\phi) & -\sin(\phi) & 0 & \\ \sin(\phi) & \rho_k^{(1)} & \rho_k^{(2)} & \\ 0 & 0 & 1 & \end{array}\right] \tag{37}$$

$\mathscr{A}$ and Φ are of class C^1 with respect to ρ_k (assumption 2)). Finally, since $x_k^{(2)}$ is transmitted, ρ_k is actually on-line accessible (assumption 3)). As a result, system (33) can be rewritten in the polytopic form (29)-(30)-(31).
Now, we can design the polytopic observer (32) as summarized in Section III-C which involves an off-line step and an on-line step.

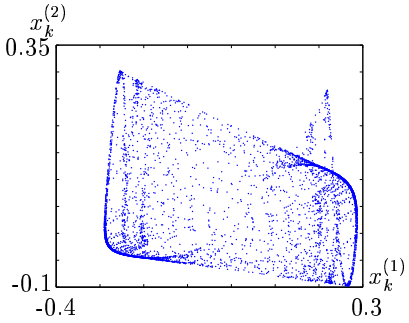
1. Off-line step

1.1 Constitution of the list Λ of points ρ_k

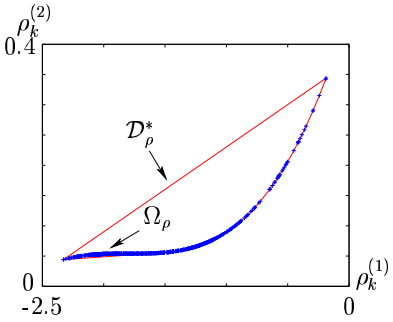
The points ρ_k have been obtained by simulated system (33) from an initial condition inside the chaotic attractor Ω, over 600 iterations. This number of iterations is considered sufficiently large for describing the nonlinearity ρ_k with good accuracy.

1.2 Finding of the vertices of the minimal convex polytope $\mathscr{D}_\rho^*$

When x_k evolves in the chaotic attractor Ω (Fig. 7(a)), ρ_k evolves in the compact set Ω_ρ, the image of Ω by the function φ (Fig. 7(b)). The Quick Hull algorithm is applied in order



(a) Chaotic attractor Ω



(b) Minimal convex polytope $\mathscr{D}_\rho^*$ including Ω_ρ

Fig. 7. Chaotic attractor and minimal polytope

to find the minimal convex polytope $\mathscr{D}_\rho^*$ including Ω_ρ, also depicted on Fig. 7(b). The finding has been achieved with the software Matlab (function `convhull`) and gives $N=269$ vertices.

1.3 Determination of the matrices $\bar{A}^{(i)}$

The matrices $\bar{A}^{(i)}$ are computed according to (31) with $L=2$

and:

$$\bar{\mathscr{A}}_0 = \begin{bmatrix} \cos(\phi) & -\sin(\phi) & 0 \\ \sin(\phi) & 0 & 0 \\ 0 & 0 & 1 \end{bmatrix}, \quad \bar{A}^{I_1} = \begin{bmatrix} 0 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 0 \end{bmatrix},$$
$$\bar{A}^{I_2} = \begin{bmatrix} 0 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 0 & 0 \end{bmatrix} \tag{38}$$

1.4 Computation of the gain matrices L_i

The software LMISol, available for free at http://www.dt.fee.unicamp.br/∼mauricio/lmisol10.html, solves the LMI (9) with the matrices $\bar{A}^{(i)}$. It turns out that the LMI are feasible. Thus the gains can be computed by (10). It is worth emphasizing that with the minimal triangle and rectangle including ρ_k as polytopes, the LMI are no longer feasible stressing the importance of seeking for the minimal polytope to obtain the less conservative LMI conditions.

2. On-line step

2.1 Computation of ξ_k

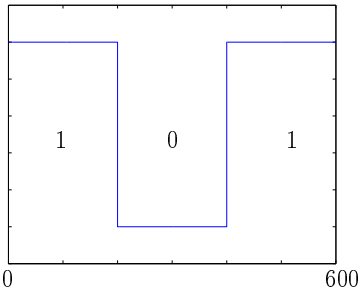
The vector ξ_k is computed at each time step by solving (20).

2.2 Computation of the gain $\mathscr{L}$

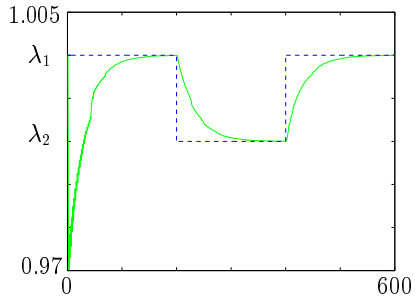
The polytopic gain $\mathscr{L}$ is given by (7) with L_i and ξ_k computed previously.

2.3 Computation of $\hat{\bar{x}}_k$

The extended state vector reconstruction is performed by (32).

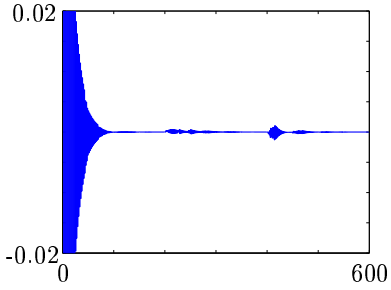


(a) Binary information m_k

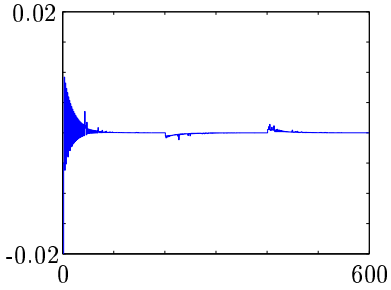


(b) Dashed line: λ_k, solid line: $\hat{\lambda}_k$

Fig. 8. Binary information and modulated parameter



(a) $x_k^{(1)} - \hat{x}_k^{(1)}$



(b) $x_k^{(2)} - \hat{x}_k^{(2)}$

Fig. 9. State reconstruction errors

Figure 8(a) represents the binary information m_k. Figure 8(b) represents the modulated parameter λ_k (dashed line) and the reconstructed parameter $\hat{\lambda}_k$ (solid line). On Fig. 9(a) and 9(b) are depicted the reconstruction errors of $x_k^{(1)}$ and $x_k^{(2)}$, respectively. As it turns out, T is sufficiently large to cope with the transients.

V. Conclusion

A systematic method to design a polytopic observer, that is an observer for LPV systems admitting a polytopic description, has been provided. The conservatism of the conditions ensuring a global state reconstruction can be reduced when the corresponding LMIs involve the vertices of the minimal polytope including the time-varying parameter. Based on this central consideration, we have proposed an enhancement of the polytopic observer design by incorporating a minimal convex polytope finding step. A lot of chaotic maps may admit a strictly equivalent LPV polytopic description by means of a suitable change of variable. As an illustration, a chaos-based secure communication scheme has been investigated. It has been shown that the retrieving of an information masked by a chaotic parameter modulation can be achieved by resorting to a polytopic observer obeying the proposed design. Finally, let us mention that the approach would also apply in some more general contexts, in particular state feedback control or merely stability analysis.

Acknowledgments

The authors wish to thank J.-R. Roche of the “Institut de Mathématiques Elie Cartan de Nancy” (IECN) for helpful

discussions on computational geometry.

REFERENCES

[1] G. Millérioux, F. Anstett, and G. Bloch, "Considering the attractor structure of chaotic maps for observer-based synchronization problems," *Mathematics and Computers in Simulation*, vol. 68, no. 1, pp. 67–85, 2005.

[2] J. Daafouz and J. Bernussou, "Parameter dependent Lyapunov functions for discrete time systems with time varying parametric uncertainties," *Systems and Control Letters*, vol. 43, no. 45, pp. 355–359, 2001.

[3] R. L. Graham, "An efficient algorithm for determinig the convex hull of a finite planar set," *Information Processing Letters*, vol. 2, no. 1, pp. 132–133, 1973.

[4] W. F. Eddy, "A new convex hull algorithm for planar sets," *ACM Transactions on Mathematical Software*, vol. 3, no. 4, pp. 398–403, December 1977.

[5] F. P. Preparata and M. I. Shamos, *Computational geometry*. Springer-Verlag, October 1985.

[6] D. C. S. Allison and M. T. Noga, "Computing the three-dimensional convex hull," *Computer Physics Communications*, vol. 103, no. 1, pp. 74–82, 1997.

[7] S. Chatterjee and S. Chatterjee, "A note of finding extreme points in multivariate space," *Computational Statistics and Data Analysis*, vol. 10, no. 1, pp. 87–92, 1990.

[8] P. M. Pardalos, Y. Li, and W. W. Hager, "Linear programming approaches to the convex hull problem in $\mathbb{R}^n$," *Computers Math. Applic.*, vol. 29, no. 7, pp. 23–29, 1995.

[9] G. Millérioux and J. Daafouz, "Polytopic observer for global synchronization of systems with output measurable nonlinearities," *International Journal of Bifurcation and Chaos*, vol. 13, no. 3, pp. 703–712, March 2003.

[10] G. Millérioux, L. Rosier, G. Bloch, and J. Daafouz, "Bounded state reconstruction error for LPV systems with estimated parameters," *IEEE Trans. on Automatic Control*, vol. 49, no. 8, pp. 1385–1389, August 2004.

[11] G. Millérioux and J. Daafouz, *Chaos in Automatic Control*, ser. Control Engineering Series. CRC Press, 2006, ch. Polytopic observers for synchronization of chaotic maps, pp. 323–344.

[12] T. L. Carroll and L. M. Pecora, "Synchronizing chaotic circuits," *IEEE Trans. Circuits and Systems*, vol. 38, no. 4, pp. 453–456, April 1991.

[13] M. J. Ogorzalek, "Taming chaos - part I: synchronization," *IEEE Trans. Circuits. Syst. I: Fundamental Theo. Appl*, vol. 40, no. 10, pp. 693–699, 1993.

[14] M. Hasler, "Synchronization of chaotic systems and transmission of information," *International Journal of Bifurcation and Chaos*, vol. 8, no. 4, pp. 647–659, April 1998.

[15] T. Yang, "A survey of chaotic secure communication systems," *Int. J. of Computational Cognition*, vol. 2, no. 2, pp. 81–130, 2004, (available at `http://www.YangSky.com/yangijcc.htm`).

[16] G. Millérioux, A. Hernandez, and J. Amigó, "Conventional cryptography and message-embedding," in *Proc. of the 2005 International Symposium on Nonlinear Theory and its Applications (NOLTA 2005)*, Bruges, Belgium, 18-21 October 2005, pp. 469–472.

[17] H. Dedieu, M. P. Kennedy, and M. Hasler, "Chaos shift keying: modulation and demodulation of a chaotic carrier using self-synchronizing Chua's circuits," *IEEE Trans. Circuits Syst. II: Anal. Digit. Sign. Process.*, vol. 40, no. 10, pp. 634–642, 1993.

[18] U. Parlitz, L. Chua, L. Kocarev, K. S. Halle, and A. Shang, "Transmission of digital signals by chaotic synchronization," *International Journal of Bifurcation and Chaos*, vol. 3, no. 2, pp. 973–977, 1993.

[19] C. Cruz and H. Nijmeijer, "Synchronization through filtering," *International Journal of Bifurcation and Chaos*, vol. 10, no. 4, pp. 763–775, 2000.

[20] R. Marino and P. Tomei, "Global adaptive observers for nonlinear systems via filtered transformations," *IEEE Trans. on Automatic Control*, vol. 37, no. 8, pp. 1239–1245, 1992.

[21] A. Fradkov, H. Nijmeijer, and A. Markov, "Adaptive observer-based synchronization for communication," *International Journal of Bifurcation and Chaos*, vol. 10, no. 12, pp. 2807–2813, 2000.

[22] Q. Zhang and A. Xu, "Global adaptive observer for a class of nonlinear systems," in *Proc. of the 40th IEEE Conf. on Decision and Control*, vol. 4, Orlando, Florida, 4-7 dec. 2001, pp. 3360–3365.

[23] A. Guyader and Q. Zhang, "Adaptive observer for discrete time linear time varying systems," in *Proc. of 13th IFAC Symposium on System Identification, SYSID'2003*, Rotterdam, The Netherlands, August 2003, pp. 1743–1748.

[24] F. Anstett, G. Millérioux, and G. Bloch, "Global adaptive synchronization based upon polytopic observers," in *Proc. of IEEE International symposium on circuit and systems, ISCAS'04*, vol. 4, Vancouver, Canada, May 2004, pp. 728 – 731.