



HAL
open science

A hybrid approach for the estimation of time-varying delays of discrete-time systems

Meriem Halimi, Gilles Millérioux, Jamal Daafouz

► **To cite this version:**

Meriem Halimi, Gilles Millérioux, Jamal Daafouz. A hybrid approach for the estimation of time-varying delays of discrete-time systems. 5th Symposium on System Structure and Control, IFAC Joint Conference 2013 SSSC, TDS, FDA, Feb 2013, Grenoble, France. pp.CDROM. hal-00842996

HAL Id: hal-00842996

<https://hal.science/hal-00842996>

Submitted on 10 Jul 2013

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

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

A hybrid approach for the estimation of time-varying delays of discrete-time systems

M. Halimi* G. Millerioux* J. Daafouz*

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

Abstract: This paper addresses the problem of the estimation of unknown time-varying delays of discrete-time systems. The problem is reformulated as a mode detection for hybrid systems with a switching law depending on the unknown delay. Some existing data-based residual methods used for the estimation of the mode of switching linear discrete-time systems are briefly reviewed and presented in a unified way. Furthermore, it is shown that the usual existence conditions of some detectors can be relaxed. Next, results concerning the so-called discernibility property are particularized to the hybrid formulation of the estimation problem. Finally, it is shown that the issue is especially interesting in the context of chaotic secure communications both for information recovery and cryptanalysis purposes.

1. INTRODUCTION

Time-delay systems have been the subject of intensive researches over the years. This is due to the fact that time delays are inherent in many real physical systems, such as mechanical systems, chemical processes, biology, transportation or communication systems and econometric models. The estimation of time delays of dynamical systems has received considerable attention in automatic control. However, most of the available methods are dedicated to continuous systems. A review and a comparison of the estimation techniques is proposed in Bjorklund and Ljung [2003]. In the two last decades, there has been an increasing interest in delayed chaotic systems for communication purposes. Indeed, the delays increase the system complexity and so is interesting for enhancing confidentiality. A pioneering work dealing with opto-electronic communication systems has been first reported in Mirasso et al. [1996]. Since then, performances have been improved and nowadays, very high throughputs communication systems can be designed as in Lavrov et al. [2010]. An overview on this topic can be found in Uchida et al. [2005] where the interest of non-linear delayed feedback chaotic laser systems is pointed out. The estimation of the delay is an important issue in this context since it might play the role of the secret parameter in secure communication. Discrete-time delayed systems have been proposed to increase the security of chaotic communications in Zheng et al. [2008]. However, the question of the security in terms of the complexity for the recovery of the time-varying delayed sequence injected into a chaotic systems is not discussed. As it turns out, the general problem of the estimation of the delay for discrete-time systems is rather scarce. This motivates the present work.

The key idea of this paper consists in formulating the estimation problem of time varying delays as a mode detection problem for an equivalent switched linear system. To this end, it is used the switched system transformation approach of Hetel et al. [2008] Nikolakopoulos et al. [2005] Tzes et al. [2005] where the switching signal changes ac-

ording to the delay. The delay is assumed to be unknown but lies in a finite and known set.

This paper is organized as follows. In Section 2, the problem of the estimation of the delay is formulated as a mode detection for hybrid systems. Some existing data-based residual methods used for the estimation of the switching law are briefly reviewed and presented in a unified way. Then, a new detector is proposed. The problem of uniqueness of the mode detection is discussed in Section 3. The corresponding notions of Discernibility and Backward Discernibility are recalled. Then, the discernibility property is particularized to the case of the hybrid formulation of the estimation problem. In Section 4, a comparison between the different estimators is carried out. Section 5 is devoted to a summary of the step by step procedure for the estimation. It is followed by an application where delay estimation is particularly useful: chaotic-based communication. The example involving chaotic signals is well suited to highlight the efficiency of the method which applies without any restrictions on the time variation of the delay. In particular, no assumption on the dwell-time is required. *Notation:* \mathbb{R}^n is the n -dimensional set of real numbers and \mathbb{Z}^+ is the set of positive integers. $\mathbf{1}$ is the identity matrix and $\mathbf{0}$ is the zero matrix, both being of appropriate dimension when unspecified. X^T is the transpose of the matrix X . The matrix X^\dagger stands for the generalized inverse (Moore-Penrose) of X satisfying $X^\dagger X$ symmetric, XX^\dagger symmetric, $XX^\dagger X = X$ and $X^\dagger XX^\dagger = X^\dagger$. $\ker(X)$ stands for the kernel of the matrix X .

2. HYBRID FORMULATION

2.1 Problem statement

Let us consider the discrete time delayed system given by

$$\begin{cases} x_{k+1} = A_1 x_k + A_2 x_{k-\tau(k)} + B u_k \\ y_k = C x_k \end{cases} \quad (1)$$

where k is the natural number standing for the discrete-time, $x_k \in \mathbb{R}^n$ is the state vector, $y_k \in \mathbb{R}^m$ is the

output, $u_k \in \mathbb{R}^p$ is the input. The matrices $A_1 \in \mathbb{R}^{n \times n}$, $A_2 \in \mathbb{R}^{n \times n}$, $B \in \mathbb{R}^{n \times p}$ and $C \in \mathbb{R}^{m \times n}$ are respectively the dynamical, the input and the output matrices. The quantity $\tau(k)$ is the time-varying delay. It is assumed to take values in a finite set assumed to be known: $\tau(k) \in \{0, 1, \dots, \alpha\}$. The time variation is arbitrary. The case when $\tau(k)$ is not directly accessible is considered. The objective is to estimate $\tau(k)$ based on the knowledge of the model, the sequences of u_k and y_k . To this end, we propose to rewrite (1) as a hybrid system. That constitutes the central starting point of the approach. Defining

$$X_k = \begin{bmatrix} x_k \\ x_{k-1} \\ x_{k-2} \\ \vdots \\ x_{k-\alpha} \end{bmatrix}, \quad U_k = u_k, \quad Y_k = y_k \quad (2)$$

system (1) can be equivalently rewritten as

$$\begin{cases} X_{k+1} = \mathcal{A}_{\tau(k)} X_k + \mathcal{B}_{\tau(k)} U_k \\ Y_k = \mathcal{C} X_k \end{cases} \quad (3)$$

where $X_k \in \mathbb{R}^N$ with $N = (\alpha+1)n$, $Y_k \in \mathbb{R}^m$ and $U_k \in \mathbb{R}^p$

$$\mathcal{A}_{\tau(k)} = \begin{bmatrix} V & V_\alpha \\ \mathbf{1}_{n,\alpha} & \mathbf{0} \end{bmatrix}, \quad \mathcal{B}_{\tau(k)} = \begin{bmatrix} B \\ \mathbf{0} \end{bmatrix}, \quad \mathcal{C} = [C \ \mathbf{0}]$$

with

$$V = [V_0 \ V_1 \ \dots \ V_{\alpha-1}]$$

and V_i defined as

$$V_0 = \begin{cases} A_1 + A_2 & \text{if } \tau(k) = 0 \\ A_1 & \text{if } \tau(k) \neq 0 \end{cases}$$

$$V_{i \neq 0} = \begin{cases} A_2 & \text{if } \tau(k) = i \\ \mathbf{0} & \text{if } \tau(k) \neq i \end{cases}$$

System (3) can be considered as a switching linear system that switches between " $\alpha + 1$ " modes depending on the value of the unknown delay $\tau(k)$.

This being the case, estimating $\tau(k)$ amounts to estimate the mode of the hybrid equivalent system (3). Hereafter, $\tau_{[k_1, k_h]} = \{\tau(k_1) \dots \tau(k_h)\}$ will denote the finite sequence of delays in the interval of time $[k_1, k_2]$. Based on the equivalent hybrid formulation, $\tau_{[k_1, k_h]}$ is referred to as a sequence (or a path) of modes. In the following, we review some different mode detection methodologies which apply for switched linear systems and present them in a unified way. Then, a new detector is proposed.

2.2 Mode detectors

There mainly exist two approaches to perform a mode detection for switched linear systems. All are based on the consideration of the following equation, obtained by stacking up the successive outputs Y_k in the interval of time $[k-h, k]$.

$$Y_{k-h, k} = \mathcal{O}_{\tau_{[k-h, k]}} X_{k-h} + T_{\tau_{[k-h, k]}} U_{k-h, k} \quad (4)$$

where

$$\mathcal{A}_{k_1}^{k_h} = \mathcal{A}_{k_1} \mathcal{A}_{k_2} \dots \mathcal{A}_{k_h}$$

$$\mathcal{B}_{k_1}^{k_h} = \begin{bmatrix} \mathcal{A}_{k_1}^{k_h-1} \mathcal{B}_{k_h} & \dots & \mathcal{A}_{k_1}^{k_2} \mathcal{B}_{k_3} & \mathcal{A}_{k_1} \mathcal{B}_{k_2} & \mathcal{B}_{k_1} \end{bmatrix}$$

$$Y_{k_1, k_2} = \begin{bmatrix} Y_{k_1} \\ Y_{k_1+1} \\ \vdots \\ Y_{k_2} \end{bmatrix}, \quad U_{k_1, k_2} = \begin{bmatrix} U_{k_1} \\ U_{k_1+1} \\ \vdots \\ U_{k_2} \end{bmatrix}$$

$\mathcal{O}_{\tau_{[k-h, k]}}$ is the observability matrix in the finite observation window $[k-h, k]$ defined as

$$\mathcal{O}_{\tau_{[k-h, k]}} = \begin{bmatrix} \mathcal{C} \\ \mathcal{C} \mathcal{A}_{\tau(k-h)} \\ \vdots \\ \mathcal{C} \mathcal{A}_{\tau(k-2)} \\ \mathcal{C} \mathcal{A}_{\tau(k-h)} \end{bmatrix}$$

$$T_{\tau_{[k-h, k]}} = \begin{bmatrix} \mathbf{0} & \mathbf{0} \\ \mathcal{C} \mathcal{B}_{\tau(k-h)} & \mathbf{0} \\ \vdots & \vdots \\ \mathcal{C} \mathcal{B}_{\tau(k-2)} & \mathbf{0} \\ \mathcal{C} \mathcal{B}_{\tau(k-h)} & \mathbf{0} \end{bmatrix}$$

Detector 1 A first mode detector has been proposed in Babaali and Egerstedt [2005]. The mode detector delivers the true mode $\tau^*(k-1)$ whenever the mode fulfills

$$\tau^*(k-1) = \{j \in \{0, \dots, \alpha\} \mid Y_{k-h, k} - T_{\tau_{[k-h, k]}} U_{k-h, k} \in \mathcal{R}(\mathcal{O}_{\tau_{[k-h, k]}})\} \quad (5)$$

where $\mathcal{R}(\bullet)$ is the "column range space" of matrix.

A way of verifying (5) is derived from the following equivalence. Given a vector Y' and a matrix \mathcal{O} , X being unknown, it holds that

$$Y' \in \mathcal{R}(\mathcal{O}) \Leftrightarrow \exists X \mid Y' = \mathcal{O}X \Leftrightarrow (\mathcal{O}^\dagger - \mathbf{1})Y' = 0$$

Now, letting $Y' = Y_{k-h, k} - T_{\tau_{[k-h, k]}} U_{k-h, k}$ and $\mathcal{O} = \mathcal{O}_{\tau_{[k-h, k]}}$, it can be defined a quantity called residual having the following form

$$r_{h, \tau}^1 = (\mathcal{O}_{\tau_{[k-h, k]}} \mathcal{O}_{\tau_{[k-h, k]}}^\dagger - \mathbf{1})(Y_{k-h, k} - T_{\tau_{[k-h, k]}} U_{k-h, k}) \quad (6)$$

If the estimation of $\tau(k)$ is correct up to the time $k-2$, the true mode $\tau^*(k-1)$ is such that the corresponding residual fulfills

$$r_{h, \tau^*}^1 = 0 \quad (7)$$

Detector 2 Another detector has been introduced in Domlan et al. [2007]. For such a detector, it is assumed a so-called pathwise observability (PWO) first introduced in Babaali and Egerstedt [2003].

Definition 1. (Babaali and Egerstedt [2003])

The system (3) is pathwise observable (PWO) if there exists an integer h such that every path $\tau_{[k-h, k-1]}$ of length h is observable, i.e. satisfies $\text{rank}(\mathcal{O}_{\tau_{[k-h, k]}}) = N$. The smallest integer h is called the index of PWO.

Then, assuming that system (3) is PWO, it is defined a so-called projection matrix fulfilling

$$\Omega_{\tau_{[k-h, k]}} \mathcal{O}_{\tau_{[k-h, k]}} = \mathbf{0} \quad (8)$$

It turns out that $\Omega_{\tau_{[k-h, k]}}$ corresponds to the left null space of $\mathcal{O}_{\tau_{[k-h, k]}}$. Finally, a residual having the following form is proposed

$$r_{h, \tau}^2 = \Omega_{\tau_{[k-h, k]}} [Y_{k-h, k} - T_{\tau_{[k-h, k]}} U_{k-h, k}] \quad (9)$$

If the estimation of $\tau(k)$ is correct up to the time $k-2$, the true mode $\tau^*(k-1)$ is such that the corresponding residual fulfills

$$r_{h, \tau^*}^2 = 0 \quad (10)$$

3. UNICITY OF RESIDUALS

3.1 Discernibility

Detector 3 Before proceeding further, let us recall a result provided in Paoletti et al. [2008]. Let us notice that it is restated here with the notation of the present paper.

Theorem 1. System (3) admits an equivalent SARX representation if and only if there is $h \in \mathbb{Z}^+$ such that for every mode sequences $\tau_{[k-h, k-1]}$, there exists a vector Ξ verifying

$$\Xi \mathcal{O}_{\tau_{[k-h, k-1]}} = \mathcal{C} \mathcal{A}_{\tau_{(k-1)}}^{\tau(k-h)} \quad (11)$$

Whenever Theorem 1 is fulfilled, the SARX model is given by

$$Y_k = \Theta_{\tau_{[k-h, k]}} v_k \quad (12)$$

with

$$\Theta_{\tau_{[k-h, k]}} = \begin{bmatrix} \Xi_l^{(1)} \\ \Xi_l^{(2)} \end{bmatrix}$$

and

$$v_k = [Y_{k-h} \cdots Y_{k-1} \quad U_{k-h} \cdots U_{k-1} \quad U_k]^T$$

where

- $\Xi_l^{(1)}$: solution of (11),
- $\Xi_l^{(2)} = \left[\mathcal{C} \mathcal{B}_{\tau_{(k-1)}}^{\tau(k-h)} \quad \mathbf{0} \right] - \Xi_l^{(1)} T_{\tau_{[k-h, k-1]}}$.

The solution of the equation (11) reads

$$\Xi_l^{(1)} = \mathcal{C} \mathcal{A}_{\tau_{(k-1)}}^{\tau(k-h)} \mathcal{O}_{\tau_{[k-h, k-1]}}^\dagger + Q_\tau^T (\mathbf{1} - \mathcal{O}_{\tau_{[k-h, k-1]}} \mathcal{O}_{\tau_{[k-h, k-1]}}^\dagger) \quad (13)$$

with Q_τ an arbitrary matrix.

If Theorem 1 is fulfilled, the following residual can be proposed

$$r_{h, \tau}^3 = \begin{bmatrix} -\Xi_l^{(1)} & \mathbf{1} \end{bmatrix} (Y_{k-h, k} - T_{\tau_{[k-h, k]}} U_{k-h, k}) \quad (14)$$

Hence, a new mode detector can be proposed as defined in the following proposition.

Proposition 1. Whenever Theorem 1 is fulfilled, if the estimation of $\tau(k)$ is correct up to the time $k-2$, the true mode $\tau^*(k-1)$ is such that the corresponding residual fulfills

$$r_{h, \tau^*}^3 = 0 \quad (15)$$

Proof 1. From (12), if Theorem 1 is fulfilled, the following equality holds

$$\Delta = Y_k - \Theta_{\tau_{[k-h, k]}^*} v_k = 0 \quad (16)$$

The quantity Δ can be rewritten as follows

$$\begin{aligned} \Delta &= Y_k - \begin{bmatrix} \Xi_l^{(1)} & \Xi_l^{(2)} \end{bmatrix} \begin{bmatrix} Y_{k-h, k-1} \\ U_{k-h, k} \end{bmatrix} \\ &= Y_k - \Xi_l^{(1)} Y_{k-h, k-1} - \Xi_l^{(2)} U_{k-h, k} \\ &= \begin{bmatrix} -\Xi_l^{(1)} & \mathbf{1} \end{bmatrix} \begin{bmatrix} Y_{k-h, k-1} \\ Y_k \end{bmatrix} - \left(\left[\mathcal{C} \mathcal{B}_{\tau^*(k-1)}^{\tau^*(k-h)} \quad \mathbf{0} \right] \right. \\ &\quad \left. - \Xi_l^{(1)} T_{\tau_{[k-h, k-1]}^*} \right) U_{k-h, k} \\ &= \begin{bmatrix} -\Xi_l^{(1)} & \mathbf{1} \end{bmatrix} Y_{k-h, k} - \begin{bmatrix} -\Xi_l^{(1)} & \mathbf{1} \end{bmatrix} \\ &\quad \begin{bmatrix} T_{\tau_{[k-h, k-1]}^*} \\ \mathcal{C} \mathcal{B}_{\tau^*(k-1)}^{\tau^*(k-h)} \quad \mathbf{0} \end{bmatrix} U_{k-h, k} \\ &= \begin{bmatrix} -\Xi_l^{(1)} & \mathbf{1} \end{bmatrix} (Y_{k-h, k} - T_{\tau_{[k-h, k]}^*} U_{k-h, k}) \end{aligned}$$

Finally, we get that

$$\Delta = r_{h, \tau^*}^3 = 0$$

which completes the proof.

The important question which arises is the unicity of the solution delivered by the detectors. In other words, it is worth checking whether a mode detector is able to discriminate the true sequence from any other ones. Such an issue is known as the discernibility and is discussed in Babaali and Egerstedt [2005] and Domlan et al. [2007]. Formally, discernibility obeys the following definition.

Definition 2. For a given detector delivering a residual $r_{h, \tau}$, two modes sequences τ^1 and τ^2 are discernible on an observation window of length $h+1$, if the corresponding residuals r_{h, τ^1} et r_{h, τ^2} are not simultaneously zero when one of the sequence τ^1 or τ^2 is the true one.

A necessary and sufficient condition for discernibility of two sequences is proven in Domlan et al. [2007] and is recalled below.

Theorem 2. (Domlan et al. [2007]) Two modes sequences τ^1 and τ^2 of a switching system are discernible on an observation window of length $h+1$, for almost all initial conditions X_{k-h} if:

$$\Omega_{\tau^i} \mathcal{O}_{\tau^j} \neq \mathbf{0}, \quad i, j \in \{1, 2\}, \quad i \neq j \quad (17)$$

or

$$\Omega_{\tau^i} (T_{\tau^j} - T_{\tau^i}) U_{k-h, k} \neq 0, \quad i, j \in \{1, 2\}, \quad i \neq j \quad (18)$$

Such a condition depends on the structure of the detector since it involves the matrices Ω_{τ^i} . Other conditions have been established regardless of the structure of the detector, see in particular Babaali and Egerstedt [2004] and the following rank condition.

Definition 3. (Babaali and Egerstedt [2004]) A path τ^1 is discernible from another path τ^2 of the same length if

$$\text{rank}([\mathcal{O}_{\tau^1} \quad \mathcal{O}_{\tau^2}]) > \text{rank}(\mathcal{O}_{\tau^2}) \quad (19)$$

where $[\mathcal{O}_{\tau^1} \quad \mathcal{O}_{\tau^2}]$ denotes the horizontal concatenation of \mathcal{O}_{τ^1} and \mathcal{O}_{τ^2} . The degree of discernibility is defined as the integer d satisfying

$$d = \text{rank}([\mathcal{O}_{\tau^1} \quad \mathcal{O}_{\tau^2}]) - \text{rank}(\mathcal{O}_{\tau^2})$$

Whenever (19) is fulfilled, it is said that τ^1 is d -discernible from τ^2 .

3.2 Backward Discernibility BD

A less restrictive condition to guarantee the unicity of the solution delivered by the detectors is the so-called Backward Discernibility (BD). It has been introduced in Babaali and Egerstedt [2005] and recalled here. We restrict our attention to the case of autonomous systems since it will correspond to the situation of our expected application. The reader shall refer to Babaali and Egerstedt [2005] to get further details.

Definition 4. (Babaali and Egerstedt [2005]) A mode i is BD from another mode j , if there is an integer h such that for every sequence τ of length h , τi is discernible from τj . The smallest of such integer h is the index of BD of i from j .

Clearly, discernibility implies backward discernibility but the converse is not true. To check backward discernibility

of a mode i from another mode j , it suffices to prove the following condition which is directly derived from Definition 3.

Condition 1. A mode i is backward discernible from another mode j if for every sequence τ of length h

$$\text{rank}([\mathcal{O}_{\tau i} \ \mathcal{O}_{\tau j}]) > \text{rank}(\mathcal{O}_{\tau j}) \quad (20)$$

3.3 Specificity for time-delayed systems

In this section, it is shown that for the switched linear system (3) resulting from the equivalent formulation of the delay estimation, discernibility cannot hold for every paths. From this perspective, it suffices to show that there exist sequences for which the rank condition (19) cannot be fulfilled when $\tau(k) \in \{0, 1, \dots, \alpha\}$ with $\alpha > 0$.

Let us consider the sequences $\tau^1 = 0 \dots 0$ and $\tau^2 = 10 \dots 0$ of length h . The two respective observability matrices denoted \mathcal{O}_{τ^1} et \mathcal{O}_{τ^2} read

$$\begin{aligned} \mathcal{O}_{\tau^1} &= \begin{bmatrix} C \\ \mathcal{CA}_0 \\ \vdots \\ \mathcal{CA}_0^h \end{bmatrix} = \begin{bmatrix} C & \mathbf{0} \dots \mathbf{0} \\ C(A_1 + A_2) & \mathbf{0} \dots \mathbf{0} \\ C(A_1 + A_2)^2 & \mathbf{0} \dots \mathbf{0} \\ \vdots & \vdots \\ C(A_1 + A_2)^h & \mathbf{0} \dots \mathbf{0} \end{bmatrix} \\ \mathcal{O}_{\tau^2} &= \begin{bmatrix} C \\ \mathcal{CA}_1 \\ \vdots \\ \mathcal{CA}_0^{h-1} A_1 \end{bmatrix} \\ &= \begin{bmatrix} C & \mathbf{0} & \mathbf{0} \dots \mathbf{0} \\ \mathcal{CA}_1 & \mathcal{CA}_2 & \mathbf{0} \dots \mathbf{0} \\ C(A_1 + A_2)A_1 & C(A_1 + A_2)A_2 & \mathbf{0} \dots \mathbf{0} \\ \vdots & \vdots & \vdots \\ C(A_1 + A_2)^{h-1} A_1 & C(A_1 + A_2)^{h-1} A_2 & \mathbf{0} \dots \mathbf{0} \end{bmatrix} \end{aligned}$$

Denote V_1 the first column of \mathcal{O}_{τ^1} , and V_2, V_2' the first and the second column of \mathcal{O}_{τ^2} respectively. It can be clearly seen that $V_1 = V_2 + V_2'$. As a result,

$$\text{rank}([\mathcal{O}_{\tau^1} \ \mathcal{O}_{\tau^2}]) = \text{rank}(\mathcal{O}_{\tau^2})$$

and according to Definition 3, the paths τ^1 and τ^2 are not discernible.

4. COMPARATIVE STUDY

This section aims at comparing the different aforementioned mode detectors.

4.1 Comparison of detector 3 and detector 2

Let us show that the detector 3 is a particular case of the detector 2. Let us first notice that the conditions (10) and (15) are based on residuals which get the same form except that $\Omega_{\tau[k-h,k]}$ is replaced by $\begin{bmatrix} -\Xi_l^{(1)} & \mathbf{1} \end{bmatrix}$. Then, it suffices to show that any solution of the detector 3 is also a solution of the detector 2. To this end, it must be shown that $\begin{bmatrix} -\Xi_l^{(1)} & \mathbf{1} \end{bmatrix}^T$ is in the kernel of $\mathcal{O}_{\tau[k-h,k]}^T$.

Let H_2 be defined as

$$H_2 = \begin{bmatrix} -\Xi_l^{(1)} & \mathbf{1} \end{bmatrix}^T$$

The following equalities are in order.

$$\begin{aligned} \mathcal{O}_{\tau[k-h,k]}^T H_2 &= \begin{bmatrix} \mathcal{O}_{\tau[k-h,k]} \\ \mathcal{CA}_{\tau(k-1)}^\tau \end{bmatrix}^T H_2 \\ &= \begin{bmatrix} \mathcal{O}_{\tau[k-h,k-1]}^T & (\mathcal{CA}_{\tau(k-1)}^\tau)^T \\ -\Xi_l^{(1)T} \\ \mathbf{1} \end{bmatrix} \\ &= -\mathcal{O}_{\tau[k-h,k-1]}^T \Xi_l^{(1)T} + (\mathcal{CA}_{\tau(k-1)}^\tau)^T \\ &= -(\Xi_l^{(1)} \mathcal{O}_{\tau[k-h,k-1]}^T)^T + (\mathcal{CA}_{\tau(k-1)}^\tau)^T \\ &= -(\mathcal{CA}_{\tau(k-1)}^\tau)^T + (\mathcal{CA}_{\tau(k-1)}^\tau)^T \\ &= \mathbf{0} \end{aligned}$$

meaning that $\begin{bmatrix} -\Xi_l^{(1)} & \mathbf{1} \end{bmatrix}^T$ is in the kernel of $\mathcal{O}_{\tau[k-h,k]}^T$.

4.2 Comparison of detector 2 and detector 1

Now, we show that the detector 2 is equivalent to the detector 1. We recall that the residual $r_{h,\tau}^2$ is built from the matrices $\Omega_{\tau[k-h,k]}$ verifying

$$\Omega_{\tau[k-h,k]} \mathcal{O}_{\tau[k-h,k]} = \mathbf{0}$$

This equality can be equivalently rewritten as

$$\mathcal{O}_{\tau[k-h,k]}^T \Omega_{\tau[k-h,k]}^T = \mathbf{0}$$

We first notice that the conditions (7) and (10) are based on residuals which get the same form except that $\Omega_{\tau[k-h,k]}$ is replaced by $(\mathcal{O}_{\tau[k-h,k]} \mathcal{O}_{\tau[k-h,k]}^\dagger - \mathbf{1})$. Let us show that a solution of detector 1 is also a solution of detector 2 and vice-versa. To this end, define H_1 as

$$H_1 = (\mathcal{O}_{\tau[k-h,k]} \mathcal{O}_{\tau[k-h,k]}^\dagger - \mathbf{1})^T$$

We get that

$$\begin{aligned} \mathcal{O}_{\tau[k-h,k]}^T H_1 &= \mathcal{O}_{\tau[k-h,k]}^T (\mathcal{O}_{\tau[k-h,k]} \mathcal{O}_{\tau[k-h,k]}^\dagger - \mathbf{1})^T \\ &= \mathcal{O}_{\tau[k-h,k]}^T ((\mathcal{O}_{\tau[k-h,k]}^\dagger)^T \mathcal{O}_{\tau[k-h,k]}^T - \mathbf{1}) \\ &= \mathcal{O}_{\tau[k-h,k]}^T (\mathcal{O}_{\tau[k-h,k]}^\dagger)^T \mathcal{O}_{\tau[k-h,k]}^T - \mathcal{O}_{\tau[k-h,k]}^T \\ &= \mathbf{0} \end{aligned}$$

The last equality stems from the definition of the Moore generalized inverse. Hence, $(\mathcal{O}_{\tau[k-h,k]} \mathcal{O}_{\tau[k-h,k]}^\dagger - \mathbf{1})^T$ is in the kernel of $\mathcal{O}_{\tau[k-h,k]}^T$.

Besides, we have that

$$\dim(\Omega_{\tau[k-h,k]}) = (m(h+1) - \text{rank}(\mathcal{O}_{\tau[k-h,k]})) \times m \cdot (h+1)$$

and

$$\dim(\mathcal{O}_{\tau[k-h,k]} \mathcal{O}_{\tau[k-h,k]}^\dagger - \mathbf{1}) = m(h+1) \times m(h+1)$$

As a result, whenever $\mathcal{O}_{\tau[k-h,k]} \neq \mathbf{0}$ which always holds since $C \neq \mathbf{0}$ (no sense otherwise), one has

$$\dim(\Omega_{\tau[k-h,k]}) < \dim(\mathcal{O}_{\tau[k-h,k]} \mathcal{O}_{\tau[k-h,k]}^\dagger - \mathbf{1})$$

meaning that every row $(\mathcal{O}_{\tau[k-h,k]} \mathcal{O}_{\tau[k-h,k]}^\dagger - \mathbf{1})$ can be obtained by a linear combination of the rows of $\Omega_{\tau[k-h,k]}$ and then, span the kernel of $\mathcal{O}_{\tau[k-h,k]}^T$, which proves the equivalence.

Besides, we can show that the existence condition stated in terms of PWO for the mode detector 2 (and so detector 1)

to exist, as required in Domlan et al. [2007], can be relaxed. From this perspective, we can again resort to condition (11) which is reformulated. First, the following standard lemma is recalled.

Lemma 3. For any two matrices (W, Z) , the equation $W X = Z$, with X unknown, has a solution if and only if $\text{rank}([W \ Z]) = \text{rank}(W)$.

Based on Lemma 3, checking whether Equation (11) has a solution is equivalent to check the rank condition below

$$\text{rank}\left(\begin{bmatrix} \mathcal{O}_{\tau[k-h, k-1]}^T & (\mathcal{C}\mathcal{A}_{\tau(k-h)}^T)^T \end{bmatrix}\right) = \text{rank}(\mathcal{O}_{\tau[k-h, k-1]}^T)$$

which is equivalent to

$$\text{rank}\left(\begin{bmatrix} \mathcal{O}_{\tau[k-h, k-1]} \\ \mathcal{C}\mathcal{A}_{\tau(k-h)} \end{bmatrix}\right) = \text{rank}(\mathcal{O}_{\tau[k-h, k-1]})$$

and finally means that

$$\text{rank}(\mathcal{O}_{\tau[k-h, k]}) = \text{rank}(\mathcal{O}_{\tau[k-h, k-1]}) \quad (21)$$

Hence, the lower bound h given in Domlan et al. [2007] and corresponding to $\text{rank}(\mathcal{O}_{\tau[k-h, k]}) = N$ is too restrictive. Clearly, if the condition of observability is verified, i.e., $\text{rank}(\mathcal{O}_{\tau[k-h, k-1]}) = N$ for all sequences, (11) has always a solution. However, we can consider $h < N$, h verifying (21) for the detector 2 and so detector 1 to exist. In other words, the detection horizon h can be chosen such that the rank of the observability matrices is kept unchanged considering the horizons of length $h-1$ and h .

5. OVERALL PROCEDURE AND APPLICATION TO CHAOTIC COMMUNICATIONS

5.1 Overall delay estimation procedure

Step 1: hybrid formulation - rewrite system (1) in the form (3).

Step 2: detection horizon h - find out the minimal integer h such that (21) is satisfied.

Step 3: discernibility - check whether (19) is fulfilled or in last resort, find out the sequences which are discernible.

Step 4: backward discernibility - check whether (20) is satisfied for the non discernible sequences.

Step 5: mode detection - given a detector $i = 1, 2$ or 3 , find out the residuals $r_{h, \tau}^i$ which vanish and infer the corresponding true mode. Let us notice that, if backward discernibility is verified for every sequences, an approach based on a sliding window can be used. Indeed, only the residuals of the sequences τ^*j ($j \in \{0, \dots, \alpha\}$) with τ^* resulting from the previous estimation have to be checked. That allows to drastically reduce the number of tests.

5.2 Application to chaotic-based communications

The block diagram of the considered communication setup is depicted in Figure 1. It corresponds to two distinct usual problems addressed in the literature and solved here in a unified way. The delay may correspond to, according to a bijective rule, the information to be encrypted at the transmitter side. If so, the objective at the receiver side is to recover the information. The scheme can alternatively be considered as two cascaded systems. The time-varying delay results from a chaotic sequence delivered by an external system supposed to be secret (at least its initial

condition). In this context, we are interested in recovering the “hidden” time-varying sequence for cryptanalysis purposes. In both situations, a mode detector is needed. As an example, let us consider the discrete-time delayed

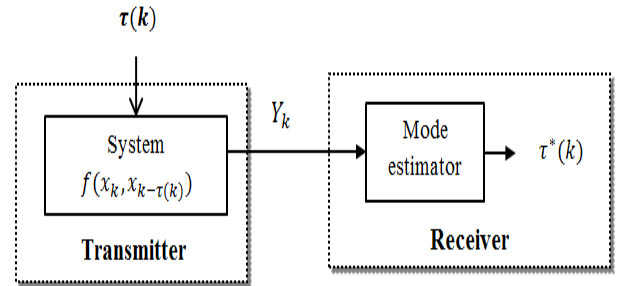


Fig. 1. Communication setup

system given by:

$$\begin{cases} x_1(k+1) = -0.21x_1(k) + 0.1x_2(k) + 0.69x_1(k - \tau(k)) \\ x_2(k+1) = x_2(k) - 0.1x_1(k - \tau(k)) \\ y_k = 2x_1(k) + x_2(k) \end{cases} \quad (22)$$

where $\tau(k) \in \{0, 1\}$ results from a binarized sequences of the chaotic Lozi map. Chaoticity induces that no dwell time is guaranteed. The equations for the chaotic Lozi map read

$$\begin{cases} z_1(k+1) = -1.7|z_1(k)| + z_2(k) + 1 \\ z_2(k+1) = 0.5z_1(k) \end{cases} \quad (23)$$

and its chaotic attractor is shown in Fig. 2.

Hybrid formulation: the switched linear equivalent system (3) is obtained with

$$X_k = \begin{bmatrix} x_k \\ x_{k-1} \end{bmatrix} \quad \text{and} \quad x_k = \begin{bmatrix} x_1(k) \\ x_2(k) \end{bmatrix}$$

$$A_0 = \begin{bmatrix} 0.48 & 0.1 & 0 & 0 \\ -0.1 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \end{bmatrix}, \quad A_1 = \begin{bmatrix} -0.21 & 0.1 & 0.69 & 0 \\ 0 & 1 & -0.1 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \end{bmatrix}$$

$$C = [2 \ 1 \ 0 \ 0]$$

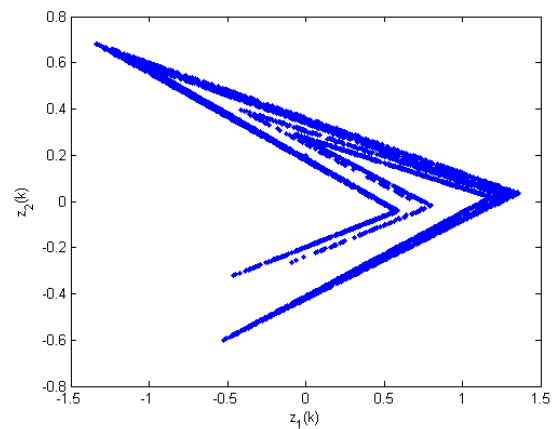


Fig. 2. Chaotic attractor of Lozi map

Detection horizon: the smallest detection horizon h which verifies (21) is $h = 3$. As stressed in Subsection 4.2, it can be noticed that $h < N$ with $N = 4$.

Discernibility: discernibility is checked using (19). The result is shown in Table 1. For every true sequence τ^* of length 3, the corresponding non discernible sequences of the same length, if any, are reported on the same line. From

True sequence τ^*	Sequences τ non discernible from τ^*
000	100
001	101
010	110
011	111
100	none
101	none
110	none
111	none

Table 1. Discernible sequences

this table, it is clear that condition (19) does not hold for all sequences, and thus the system is not discernible for $h = 3$. Actually, even if we would increase h , discernibility would never be verified as it is proven in Section 3.3.

For the non discernible sequences, we should check whether at least Backward Discernibility would be fulfilled. To this end, we must resort to the rank test (20). It turns out that BD is verified because for every pairs $(i, j) \in \{0, 1\}^2$, the following rank condition holds

$$\text{rank}\left(\begin{bmatrix} \mathcal{O}_{\tau_{[1,2]i}^*} & \mathcal{O}_{\tau_{[1,2]j}} \end{bmatrix}\right) - \text{rank}(\mathcal{O}_{\tau_{[1,2]j}}) > 0$$

Delay estimation: since discernibility is not fulfilled for all sequences, it is not guaranteed that the mode detector delivers the true first sequence $\tau^*(0), \tau^*(1), \tau^*(2)$. An exhaustive search over the 2^3 possible sequences must be performed. After $k = 3$, the detector successfully recovers the “hidden” chaotic sequence as depicted on Figure 3.

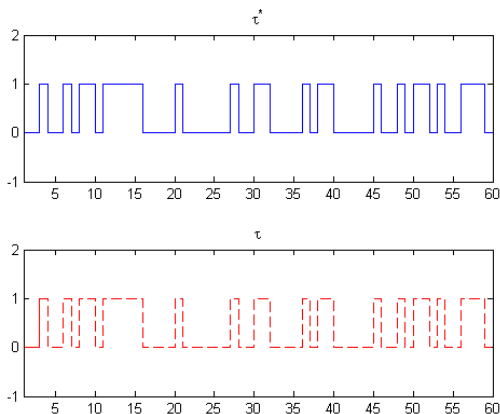


Fig. 3. True sequence τ^* and reconstructed sequence τ

6. CONCLUSION

We have presented an approach to estimate time-varying delays of discrete-time systems. The problem has been turned into an equivalent mode detection problem for switched linear systems. A brief overview of mode detection existing methods has been provided and unified. Some conditions on the existence of detectors have been

relaxed and a new detector has been proposed. Conditions on discernibility have been particularized to our special context taking into account the particular structures of the matrices resulting from the hybrid formulation of the delay estimation. Finally, a step-by-step approach has been proposed and the efficiency of the method has been highlighted in a chaotic-based communication problem. The method can be extended in a straightforward way to switched linear delayed systems.

REFERENCES

- M. Babaali and M. Egerstedt. Pathwise Observability and Controllability are decidable. In *Proceedings 42nd IEEE Conference on Decision and Control (CDC'03)*, volume 6, pages 5771–5776, Maui, Hawaii, 2003.
- M. Babaali and M. Egerstedt. Observability of Switched Linear Systems. *Hybrids Systems: Computation and Control*, pages 48–63, 2004.
- M. Babaali and M. Egerstedt. Asymptotic Observers for Discrete-Time Switched Linear Systems. In *Proceedings of the 16th IFAC World Congress*, Czech Republic, 2005.
- S. Bjorklund and L. Ljung. A Review of Time-Delay Estimation Techniques. In *Proceedings 42nd IEEE Conference on Decision and Control*, 2003.
- E. A. Domlan, J. Ragot, and D. Maquin. Switching Systems Mode Estimation using a Model-based Diagnosis Method. In *8th Conference on Diagnostics of Processes and Systems*, Slubice, Poland, 2007.
- L. Hetel, J. Daafouz, and C. Iung. Equivalence Between the Lyapunov-Krasovskii Functional Approach for Discrete Delay Systems and the Stability Conditions for Switched Systems. *Nonlinear Analysis: Hybrids Systems*, pages 697–705, 2008.
- R. Lavrov, M. Jacquot, and L. Larger. Nonlocal non-Linear Electro-optic Phase Dynamics Demonstrating 10 gb/s Chaos Communications. *IEEE Journal of Quant. Electron*, 46(10):1430–1435, 2010.
- C. R. Mirasso, P. Colet, and P. Garcia-Fernandez. Synchronization of Chaotic Semiconductor Lasers: Application to Encoded Communications. *IEEE Photon. Technol. Lett*, 8(2):299–301, 1996.
- G. Nikolakopoulos, A. Panousopoulou, A. Tzes, and J. Lygeros. Multi-Hopping Induced Gain Scheduling for Wireless Networked Controlled Systems. In *Proceedings 44th IEEE Conference on Decision and Control (CDC'05)*, Seville, 2005.
- S. Paoletti, A. Garulli, J. Roll, and A. Vicino. A Necessary and Sufficient Condition for Input Realization of Switched Affine State Space Models. In *Proceeding 47th IEEE conference on decision and control*, Cancun, Mexico, December 2008.
- A. Tzes, G. Nikolakopoulos, and I. Koutroulis. Development and Experimental Verification of a Mobile Client-Client Networked Controlled System. *European Journal of Control*, 11(3):229–241, 2005.
- A. Uchida, F. Rogister, J. Garcia-Ojalvoand, and R. Roy. Synchronization and Communication with Chaotic Laser systems. In *Progress in Optics*, pages 48:203–341, 2005.
- G. Zheng, D. Boutat, T. Floquet, and J.-P. Barbot. Secure Data Transmission Based on Multi-Input Multi-Output Delayed Chaotic System. *International Journal of Bifurcation and Chaos*, 18(7):2063–2072, 2008.