INTERNATIONAL JOURNAL OF ROBUST AND NONLINEAR CONTROL
Int. J. Robust. Nonlinear Control 2016; **00**:1–17
Published online in Wiley InterScience (www.interscience.wiley.com). DOI: 10.1002/rnc

Set-based Fault Detection and Isolation for Detectable Linear Parameter-Varying Systems

Daniel Silvestre[12*], Paulo Rosa [3], João P. Hespanha [4], Carlos Silvestre [12]

[1] *Department of Electrical and Computer Engineering, Faculty of Science and Technology of the University of Macau, Macau, China*
[2] *Institute for Systems and Robotics, Instituto Superior Técnico, Universidade de Lisboa, Lisboa, Portugal*
[3] *Deimos Engenharia, Lisbon, Portugal.*
[4] *Department of Electrical and Computer Eng., University of California, Santa Barbara, CA 93106-9560, USA.*

SUMMARY

In the context of fault detection and isolation of Linear Parameter-Varying (LPV) systems, a challenging task appears when the dynamics and the available measurements render the model unobservable, which invalidates the use of standard Set-Valued Observers (SVOs). Two results are obtained in this paper, namely: using a left-coprime factorization, one can achieve set-valued estimates with ultimately bounded hyper-volume and convergence dependent on the slowest unobservable mode; and, by rewriting the SVO equations and taking advantage of a coprime factorization, it is possible to have a low-complexity fault detection and isolation method. Performance is assessed through simulation, illustrating, in particular, the detection time for various types of faults. Copyright © 2016 John Wiley & Sons, Ltd.

Received . . .

KEY WORDS: Fault Detection and Isolation; Unobservable LPV; Coprime Factorization, Distributed

1. INTRODUCTION

Performing fault detection in the context of cyber-physical systems can be difficult to address because the observability of the system can be affected. For example, having nodes with access to only local information or special network structures along with limited local state measurements can result in unobservable modes for the overall system.

The motivation for this work is to provide tools to detect and isolate faults in cyber physical systems that have unobservable modes but are detectable. Current state-of-the-art techniques using set-valued estimators are not suitable for systems with unobservable modes and non-zero inputs as the disturbances and input signals increase the hypervolume of the set-valued estimates in each iteration, therefore resulting in divergent estimates.

*Correspondence to: Department of Electrical and Computer Engineering of the Faculty of Science and Technology of the University of Macau, Macau, China, and with the Instituto Superior Técnico, Universidade de Lisboa, Lisboa, Portugal. E-mail:dsilvestre@isr.ist.utl.pt

Contract/grant sponsor: [1] This work was supported by grant SFRH//BD/71206/2010, from Fundação para a Ciência e a Tecnologia. [3]J. Hespanha was supported by the U.S. Army Research Laboratory and the U.S. Army Research Office under grants No. W911NF-09-1-0553 and W911NF-09-D-0001. [4] This work was supported in part by the University of Macau, Macao, China, under Project MYRG2015-00126-FST, in part by the Fundação para a Ciência e a Tecnologia under Project FCT [UID/EEA/50009/2013] and in part by ONRg GRANT N62909-15-1-V177.

The importance of addressing the fault detection (or state estimation) of a group of dynamic systems interconnected by a network is reported in [1] and later in [2], where the detection is crucial given that a single malfunctioning node can severely impact on the overall network performance. Applications of such systems span the areas of mobile robots, cooperating unmanned vehicles tasks such as surveillance and reconnaissance, distributed state estimation, among others (see [3] and the references therein).

In the case of a smart grid, a network failure or malignant action can compromise its service which motives the use of efficient fault detection mechanisms [4], [5]. Besides failures and attacks to the physical power grid infrastructure, one must also consider cyber attacks to its communication infrastructure. Therefore, the problem of detecting faults and identifying where they are occurring in a network is considered in this paper. To assess the performance of the techniques developed herein, we adopt the linearized small signal version of the structure-preserving model, composed by the linearized swing equation and the DC power flow equation. A comprehensive survey can be found in [6] regarding different aspects of the design of smart grids. The importance of this problem is reported in [7] and later in [5].

There is a rich state-of-the-art for some specific problems regarding cyber-physical systems that can be described by the Linear Parameter-Varying (LPV) model adopted in this paper. In [3], one of the main results is showing that the overall system of a group of dynamic systems is unobservable when only considering relative information of the states. A transformation is introduced that allows to perform fault detection and isolation by considering the observable subspace of the overall system. The algorithm requires a centralized detection scheme and is only applicable to the specific Linear Time-Invariant (LTI) model. In this paper, we derive an alternative approach based on Set-Valued Observers (SVOs), which enables a distributed detection for the observable subspace if we consider a strategy such that of [8].

In [8], the use of SVOs for distributed fault detection were firstly introduced for the specific case of consensus. The overall system is modeled as an uncertain LPV system where communications are seen as a parameter-dependent dynamics matrix. Even though, the whole system is not observable in every time instant, for a sufficiently long time interval, the system is observable, as long as the underlying network topology is strongly connected. Whereas in [8], each node has access to its own state, and the state of one neighbor to which it communicates, in this paper, it is assumed that nodes have access only to relative information. The distributed detection can also be improved by resorting to exchanging state estimates whenever the systems communicate or take measurements by using a similar algorithm to the one presented in [8].

The SVOs framework, whose concept was introduced in [9] and [10] (further information can be found in [11] and [12] and references therein) is used as a way to represent and propagate the set-valued state estimates. The approach allows us to consider virtually any kind of linear dynamics for the agents, and also to incorporate disturbances and model uncertainties.

An alternative method to the SVOs is the use of the reachability concept to construct set-valued estimates. The proposals in [13] and [14] both resort to this concept and use zonotopes to define the sets where the state belongs. Zonotopes are a compromise of accuracy for performance in the sense that they are a subclass within polytopes. In addition, unions can be computed efficiently when compared to polytopes whereas intersections are much more efficient using polytopes. Our proposal focus on the use of polytopes since operations introduce less conservatism than zonotopes.

For the particular case of smart grids, other proposals have also been presented by the research community as alternative fault detection methods motived by the increased interest for this topic by the industry. A survey focused on fault location methods for both transmission and distribution systems can be found in [15].

In [16], faults are detected by constructing a χ^2-detector that computes the χ^2 statistics of the residuals from a Kalman filter and compares them with the thresholds obtained from the standard distribution. Such a strategy is stochastic in nature and includes potential false-positives with a certain probability. The alternative approach presented in this paper is deterministic and relies on a worst-case detection. A similar stochastic detection strategy can achieved with the extension of the framework proposed here, following the methodology described in [8].

DOI: 10.1002/rnc

Fault detection in smart grids has also been performed resorting to the concept of Petri Nets [17]. The procedure consists in mapping the possible concurrent actions of each of the nodes in the network to determine the current state of the system and checking if it is compatible with the measurements. In this article, we adopt a different methodology although the objective is the same, in the sense that we are computing a set of all possible states of the system.

In [18], the authors study the problem of undetectable faults due to the unobservable modes of the system. The fault detection is based on ensuring that the network is observable for a fixed number of compromised nodes by carefully selecting which states to measure. Although the focus is slightly different, the definition of the equation dictating the detection and isolation of faults are related. In [19], one of the main results is to characterize detectability of faults both using dynamic and static procedures considering the dynamics of the network and no disturbances in the model.

In a different direction, [20] and [21] show that the theoretical condition for fault detectability and identifiability in the context of smart power grids is similar to that of detecting faults in consensus problems and amounts to studying the zero dynamics of the system given by the difference between the nominal "fault-free" and the one with the input fault signal. In this paper, we rewrite the equations describing the set-valued estimates in a similar fashion, which describe *fast* SVO (fSVO) in the sense they are low-complexity methods by avoiding the need to resort to the Fourier-Motzkin elimination algorithm.

In order of importance, the contributions of this paper are as follows:

- we show how to perform fault detection and isolation with SVOs for unobservable but detectable systems taking advantage of a coprime factorization;
- reformulation of the theoretical conditions for fault detection and isolation, which leads to a different set of SVO equations that when coupled together with a coprime factorization represents a more efficient method for fault detection without adding conservatism.

The remainder of this paper is organized as follows. In Section 2, we describe the generic model for the systems to be addressed and state the problem of constructing set-valued estimates for unobservable but detectable systems. Section 3 reviews the definitions of SVOs pointing out the related issues. The methodology for tackling detectable systems is presented in Section 4 along with the rewritten SVO equations to reduce the computational complexity in Section 5. The mentioned points are illustrated in simulation in Section 6. Concluding remarks and directions for future work are provided in Section 7.

Notation : The transpose of a matrix A is denoted by $A^\intercal$. We let $1_n := [1 \dots 1]^\intercal$ and $0_n := [0 \dots 0]^\intercal$ indicate n-dimensional vector of ones and zeros, respectively, and I_n denotes the identity matrix of dimension n. Dimensions will be omitted when clear from context. The vector e_i denotes the canonical vector whose components are equal to zero, except for the ith component. The symbol $\otimes$ denotes the Kronecker product. The notation $||.||$ refers to $\|v\| := \sup_i |v_i|$ for a vector, and $\|A\| := \bar{\sigma}(A)$, for the maximum singular value $\bar{\sigma}$. The ith coordinate of a vector v is denoted by $[v]_i$.

2. PROBLEM STATEMENT

In this section, we introduce the problem of detecting faults in the context of unobservable but detectable Linear Parameter-Varying (LPV) systems subject to disturbances and noise signals. A major issue for current SVO-based methods is the requirement for system observability, which we discuss later in this section.

We are interested in detecting and isolating faults for systems described by the model

$$\begin{aligned} x(k+1) &= A(\rho(k))x(k) + B(\rho(k))u(k) + E(\rho(k))d(k) \\ y(k) &= C(\rho(k))x(k) + D(\rho(k))u(k) + \nu(k) \end{aligned} \tag{1}$$

where $x \in \mathbb{R}^{n_x}$, $u \in \mathbb{R}^m$, represent the state and input signal of the system, respectively. Without loss of generality, we assume that $|d_i(k)| \leq 1$ and $|\nu_i(k)| \leq \bar{\nu}, \forall k \geq 0$.

DOI: 10.1002/rnc

The model in (1) is a "fault-free" version of the system. When considering an unknown fault signal $f(\cdot)$, it can be added through the term $F(\rho(k))f(k)$ to the state equation and through $L(\rho(k))f(k)$ to the output equation. The signal $f(k)$ models a fault affecting the components of the system according to the matrices $F(\rho(k))$ and being reflected in the output through $L(\rho(k))$. This will be used for the fault isolation in order to create a model accepting each of the faults. However, notice that for fault detection the SVO framework is able to detect any generic fault provided that such fault creates a sequence of measurements that cannot be produced by the "fault-free" model and the known bounds for the initial state, disturbances and noise signals. In the remainder of the paper, whenever clear from context, we omit the dependence on the parameter ρ and represent as A_k the matrix $A(\rho(k))$.

In [22], one of the results states that knowing an initial set containing the initial conditions for a stable system with input $u(k) = 0, \forall k \geq 0$ is sufficient to guarantee that the hyper-volume of the set-valued estimates is bounded. However, if the system has unobservable modes and non-zero input u, the theorem does not apply and the estimates hyper-volume can diverge. The main problem to be addressed in this paper is how to construct set-valued estimates for detectable systems.

3. REVIEW OF SET-VALUED OBSERVERS

For the design of the proposed fault detection solution, we adopt the Set-Valued Observers (SVOs) framework presented in [23] and in [24] which enables multiple nodes to perform the fault detection using the local information available to them.

The remainder of this section is devoted to reviewing the type of SVOs selected, as well as its applicability to fault detection. We define Set$(M, m) := \{q : Mq \leq m\}$, which represents a convex polytope, with the operator $\leq$ being a component-wise operation between the two vectors. The aim of an SVO is to find the smallest set containing all possible states of the system at time k, $X(k)$ using the previous set-valued estimates and measurements of the system.

More precisely, the initial state satisfies $x(0) \in X(0)$ where $X(0) :=$ Set(M_0, m_0), for some M_0 and m_0. Let us introduce the notation $X_H(k+1) :=$ Set$(M_H(k+1), m_H(k+1))$ for the set containing all the possible states of the system at time $k+1$ compliant with the dynamics and measurements over the last H iterations, the *horizon*. Considering an horizon greater than 1 reduces the conservatism of the set-valued state estimate given by the initial uncertainty, as shown in [22].

The set $X_H(k+1)$, when A_k is non-singular, are all the points for which the following inequality holds

$$\left[\begin{array}{cc} \multicolumn{2}{c}{M_H(k+1)} \\ \hline C_{k+1} & 0 \\ 0 & I \otimes \bar{I} \end{array}\right] \begin{bmatrix} \mathbf{x} \\ d(k) \\ \vdots \\ d(k-H+1) \end{bmatrix} \leq \underbrace{\begin{bmatrix} m(k) + \tilde{u}(k,1) \\ \vdots \\ m(k-H+1) + \tilde{u}(k,H) \\ \bar{y}(k+1) + \bar{\nu}1 \\ 1 \\ \vdots \\ 1 \end{bmatrix}}_{m(k+1)}.$$

where $M_H(k+1)$ is defined by

$$M_H(k+1) := \left[\begin{array}{cccc} \multicolumn{4}{c}{M_{H-1}(k+1)} \\ \hline M(k-H+1)A_k^{-H} & -M(k-H+1)A_k^{-H}E_k & \cdots & -M(k-H+1)A_{k-H+1}^{-1}E_{k-H+1} \end{array}\right]$$

DOI: 10.1002/rnc

where $\tilde{u}(k,H) := \sum_{\tau=1}^{H} M(k-H+1)A_{k-\tau+1}^{-(H-\tau+1)}B_{k-\tau+1}u(k-\tau+1)$; the notation $\bar{Z}$ stands for $\bar{Z} := \begin{bmatrix} Z \\ -Z \end{bmatrix}$ for a matrix Z; and with a slight abuse of notation $A_k^H := A_k \cdots A_{k-H+1}$ and $A_k^{-H} := (A_k \cdots A_{k-H+1})^{-1}$ for $H > 0$.

If, however, A_k is non-invertible, we can adopt the strategy in [25] and solve the inequality

$$\left[\begin{array}{cc} \multicolumn{2}{c}{M_H(k+1)} \\ \hline \bar{C}_{k+1} & 0 \end{array}\right] \begin{bmatrix} \mathbf{x}(k+1) \\ \mathbf{x}(k) \\ d(k) \\ \mathbf{x}(k-1) \\ d(k-1) \\ \vdots \\ \mathbf{x}(k-H+1) \\ d(k-H+1) \end{bmatrix} \leq \begin{bmatrix} m_H(k+1) \\ \bar{y}(k+1) + \bar{\nu}1 \end{bmatrix}$$

where

$$M_H(k+1) := \left[\begin{array}{cccccc|cc} \multicolumn{6}{c|}{M_{H-1}(k+1)} & \multicolumn{2}{c}{0} \\ \hline \bar{I} & 0 & -\overline{E_k} & \cdots & 0 & -\overline{A_k^{H-2}E_{k-H+2}} & -\overline{A_k^H} & -\overline{A_k^{H-1}E_{k-H+1}} \\ 0 & 0 & 0 & \cdots & 0 & 0 & 0 & \bar{I} \\ 0 & 0 & 0 & \cdots & 0 & 0 & M(k-H+1) & 0 \end{array}\right]$$

with the base case

$$M_1(k+1) := \begin{bmatrix} \bar{I} & -\overline{A_k} & -\overline{E_k} \\ 0 & 0 & \bar{I} \\ 0 & M(k) & 0 \end{bmatrix}$$

and

$$m_H(k+1) := \begin{bmatrix} m_{H-1}(k+1) \\ \sum_{\tau=0}^{H-1} \overline{A_k^{\tau}B_{k-\tau}}u(k-\tau) \\ 1 \\ m(k-H+1) \end{bmatrix}.$$

The dependence on $\mathbf{x}(k), \cdots, \mathbf{x}(k-H+1)$ can be removed by applying the Fourier-Motzkin elimination method [26] and obtain the set described by $M(k+1)\mathbf{x}(k+1) \leq m(k+1)$.

Lemma 1 (fault detection)
Consider a dynamic system as in (1) and an SVO that produces set-valued estimates, $X_H(k)$, for $x(k)$, given horizon H and $|d_i(k)| \leq 1, \forall k \geq 0$. A fault occurred if $X_H(k) = \emptyset$.

Lemma 1 is a direct consequence of the definition of the SVO, as an empty set means there is no instantiation of $\mathbf{x}(k)$ such that the measurements are compliant with the "fault-free" model where the signal $f(k) = 0, \forall_{k\geq 0}$.

There are two major issues using the standard procedure for the aforementioned SVOs: boundedness of the hyper-volume of the sets is only guaranteed if the system is stable with zero input [22] (requiring the system to be observable also yields boundedness of the sets); and, the computational time associated with the use of the Fourier-Motzkin elimination method which is of intrinsically double exponential complexity.

4. SVOS FOR DETECTABLE SYSTEMS

In [22], it was proposed the use of the concept of left-coprime factors to bound the horizon required for detection. This result is going to be a building block for faster SVOs (i.e., with diminished

Int. J. Robust. Nonlinear Control (2016)
DOI: 10.1002/rnc

computational requirements) in the next section. In this section, we exploit additional characteristics of the coprime factorization to provide a guaranteed rate of convergence of the set-valued state estimates, for the case of detectable systems (i.e. all unobservable modes of the system are stable).

Consider the system (1) but where all the exogenous signals are concatenated in u (and correspondingly for matrices B_k and D_k) so that we get the following dynamics

$$\begin{aligned} x(k+1) &= A_k x(k) + B_k u(k) \\ y(k) &= C_k x(k) + D_k u(k) \end{aligned} \tag{2}$$

Proposition 1 (left-coprime factorization [27])
Let a discrete-time dynamic system described by (2) be detectable, which can be written in a compact matrix notation as

$$P(k) := \left[\begin{array}{c|c} A_k & B_k \\ \hline C_k & D_k \end{array}\right]$$

and define

$$G(k) = \left[\begin{array}{c|c} A_k - K_k C_k & -K_k \\ \hline R_k C_k & R_k \end{array}\right], Q(k) = \left[\begin{array}{c|c} A_k - K_k C_k & B_k - K_k D_k \\ \hline R_k C_k & R_k D_k \end{array}\right]$$

where R_k must always be a nonsingular matrix and K_k is such that $A_k - K_k C_k$ is stable. Then,

$$P(k) = G^{-1}(k) Q(k).$$

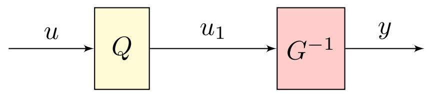

Figure 1. Schematic representation of the two coprime systems.

The above factorization is depicted in Fig. 1. The left-coprime factorization creates two separate systems $Q(k)$ and $G(k)$ and a fault is detected whenever appropriately set-valued estimates for the signal u_1 (see Fig. 1) for the two systems do not intersect.

The aforementioned technique allows to establish two convergence results for the sets produced by the SVOs. If the system is observable, we can select the matrices K_k such that all eigenvalues of $(A_k - K_k C_k)^{n_x}$ are equal to zero for any $k \geq n_x$ with n_x being the number of states of the system [22]. If the system is detectable, the rate of convergence is governed by the slowest of the unobservable modes, as shown next.

Definition 1
A sequence of sets, $U(1), U(2), \cdots$, is said to have *ultimately bounded hyper-volume* if there exist $\epsilon > 0, k_o \geq 1$ such that $vol(U(k)) < \epsilon$ for all $k \geq k_o$. Moreover, if $vol(U(k)) < \Gamma_o \frac{1-\lambda^k}{1-\lambda}$, for some $\Gamma_o, \lambda > 0$, then the sequence of sets is said to have $1/\lambda$ *convergence*.

The next theorem summarizes the convergence properties of the SVOs. When referring to an SVO producing estimates for the output signal, we mean the set of all points obtained by applying the output equation to any point in the set-valued estimates of its internal state, i.e., for a coprime factor $Q(k)$, with internal state $x_Q(k)$, an SVO will return the set $X_Q(k)$ such that $x_Q(k) \in X_Q(k)$ and the estimates for the output $u_1(k)$, considering $R = I$, is the set defined $\{u_1(k) : p(k) \in X_Q(k), u_1(k) = C_k p(k) + D_k u(k)\}$.

Theorem 1 (estimate convergence)
Consider a system P with dynamic model as in (1), with $f \equiv 0$, where $x(k) \in \mathbb{R}^n$. Further suppose that a left-coprime factorization as in Proposition 1 exists, and that an SVO constructed for $Q(k)$ and $G(k)$, providing estimates of $u_1(k)$, is designed. Finally, assume that $x(0) \in X(0)$, and both $|d_i(k)| \leq 1$, $|\nu_i(k)| \leq 1$. Then:

DOI: 10.1002/rnc

i) if P is observable, the hyper-volume of the set-valued estimates of $u_1(k)$ is ultimately bounded and converge in a finite number of steps;
ii) if P is detectable, the hyper-volume of the set-valued estimates of $u_1(k)$ is ultimately bounded with convergence governed by $\frac{1}{\sigma_{\text{max}}}$, where $\sigma_{\text{max}} := \max_k \|A_k - K_k C_k\|$.

Proof

i) The proof can be found in [22] for the LTI case. It revolves around the fact that, for an observable pair (A, C), one can place the eigenvalues of $A - KC$ at the origin and thus obtain a deadbeat observer such that $(A - KC)^n = 0$. For the LPV case, a similar statement is true but for the product of matrices in the last n_x time instants, i.e., $(A_k - K_k C_k)^{n_x} = 0$.
ii) Since the system is detectable, one can build a state observer satisfying

$$\hat{x}(k+1) = (A_k - K_k C_k)\hat{x}(k) + \begin{bmatrix} L_k & B_k \end{bmatrix} \begin{bmatrix} y(k) \\ u(k) \end{bmatrix},$$

with $A_k - K_k C_k$ being stable, which means that the state estimate can be written based on the initial estimate as

$$\hat{x}(k) = (A_k - K_k C_k)^k \hat{x}(0) + \sum_{\tau=0}^{k-1} (A_k - K_k C_k)^{k-1-\tau} \begin{bmatrix} L_k & B_k \end{bmatrix} \begin{bmatrix} y(\tau) \\ u(\tau) \end{bmatrix}.$$

Since the system is detectable, take σ_{max} as defined in the statement of the theorem, which means $||(A_k - K_k C_k)^k \hat{x}(0)|| \leq \sigma_{\text{max}}^k \|\hat{x}(0)\|$ and, therefore, an overbound for the set-valued estimate can be written as

$$|\hat{x}(k)| \leq \sum_{\tau=0}^{k-1} \left\|(A_k - K_k C_k)^{k-1-\tau}\right\| \left\|\begin{bmatrix} L_k & B_k \end{bmatrix}\right\| \left\| \begin{bmatrix} y(\tau) \\ u(\tau) \end{bmatrix} \right\| + \sigma_{\text{max}}^k \|\hat{x}(0)\|.$$

Given the exponential rate of convergence associated with the term in $\hat{x}(0)$ let us look at the remaining term

$$\begin{aligned} \sum_{\tau=0}^{k-1} \left\|(A_k - K_k C_k)^{k-1-\tau}\right\| \left\|\begin{bmatrix} L_k & B_k \end{bmatrix}\right\| \left\| \begin{bmatrix} y(\tau) \\ u(\tau) \end{bmatrix} \right\| &\leq \sum_{\tau=0}^{k-1} \sigma_{\text{max}}^{k-1-\tau} \left\|\begin{bmatrix} L_k & B_k \end{bmatrix}\right\| \left\| \begin{bmatrix} y(\tau) \\ u(\tau) \end{bmatrix} \right\| \\ &\leq \frac{(1 - \sigma_{\text{max}}^k)}{1 - \sigma_{\text{max}}} \left\|\begin{bmatrix} L_k & B_k \end{bmatrix}\right\| \max_{0 \leq \tau \leq k} \left\| \begin{bmatrix} y(\tau) \\ u(\tau) \end{bmatrix} \right\| \end{aligned}$$

which concludes the proof since the set-valued estimates are bounded and its worst-case is governed by $1/\sigma_{\text{max}}$.

□

5. FAST SVOS

In the previous section, a left-coprime factorization was used to obtain a bound on the necessary horizon for the SVO-based fault detection approach, thus eliminating unnecessary computational complexity of considering all past measurements. However, the computational complexity is also tied to the use of the Fourier-Motzkin elimination method (see Section 3) to remove the dependence on past instants, which has a doubly exponential complexity. In this section, we reformulate the SVO equations in order to have the dependency on a single point in time and avoid the use of Fourier-Motzkin elimination method. The new set of equations make the computation of the sets lose its iterative property which is resolved by using the left-coprime factorization to remove the conservatism added by discarding the restrictions associated with the previous sets.

DOI: 10.1002/rnc

Consider the faulty system with no noise, no disturbances, and no other inputs apart from the fault (which to avoid misinterpretations, we label as f and corresponds to u in the notation of [19] and [21]). Then, the dynamics in (1) becomes

$$\begin{aligned} x(k+1) &= A_k x(k) + F_k f(k) \\ y(k) &= C_k x(k) + L_k f(k). \end{aligned}$$

To include other signals such as a disturbance affecting the state and a noise factor, we can use $\begin{bmatrix} f(k) \\ d(k) \end{bmatrix}$ and replace accordingly the matrix F_k by $\begin{bmatrix} F_k & E_k \end{bmatrix}$ and L_k by $\begin{bmatrix} L_k & N_k \end{bmatrix}$.

By resorting to the factorization in Proposition 1 and the results in Theorem 1, i.e., convergence in finite-time if the system is observable or an asymptotic rate of convergence if the system is detectable, it is possible to remove the use of the projection step. The main advantage is avoiding the Fourier-Motzkin elimination method at the expenses of not maintaining an estimate for the current state.

In the construction of the proposed SVO, it is helpful to introduce the definitions of fault detectability and fault identifiability. These definitions do not resemble to SVOs for all possible time-varying system matrices and the objective is not to check if the equations to all such possible sequences. However, given a specific sequence of system matrices, they correspond to the SVO equation.

Definition 2 (fault detectability [19])
Consider a system with model given by (2) and a fault profile $f_1(k), 0 \leq k \leq k_t$. A fault f_1 is detectable in k_t time instants if there does not exist $x(0) \in \mathbb{R}^{n_x}$ that satisfies

$$C_k A_k^k x(0) + \sum_{\tau=0}^{k-1} C_k A_k^{k-1-\tau} F_k f_1(\tau) + L_k f_1(k) = 0 \tag{3}$$

for all $0 \leq k \leq k_t$.

Notice that (3) can be rewritten in vectorial form as

$$\begin{bmatrix} C_k \\ C_k A_k \\ \vdots \\ C_k A_k^{k_t} \end{bmatrix} x(0) = \begin{bmatrix} -L_k f_1(0) \\ -C_k F_k f_1(0) - L_k f_1(1) \\ \vdots \\ -\sum_{\tau=0}^{k_t-1} C_k A_k^{k_t-1-\tau} F_k f_1(\tau) - L_k f_1(k_t) \end{bmatrix}.$$

We also introduce a similar definition regarding the identifiability of the faults.

Definition 3 (fault distinguishability)
Take a system with model given by equation (2) and a fault profile $f_2(k), 0 \leq k \leq k_t$. Fault f_2 is distinguishable in k_t time instants from fault f_1 if there does not exist $x(0) \in \mathbb{R}^{n_x}$ that satisfies

$$\begin{bmatrix} C_k & L_k^{f_1} & 0 & \cdots & 0 \\ C_k A_k & C_k F_k^{f_1} & 0 & \cdots & 0 \\ \vdots & \ddots & \ddots & \ddots & \vdots \\ C_k A_k^{k_t} & C_k A_k^{k_t-1} F_k^{f_1} & \cdots & C_k F_k^{f_1} & L_k^{f_1} \end{bmatrix} \begin{bmatrix} x(0) \\ f_1(1) \\ \vdots \\ f_1(k_t) \end{bmatrix} = m_{f_2}$$

where $F_k^{f_1}$ and $L_k^{f_1}$ are the matrices associated with fault f_1 and

$$m_{f_2} = \begin{bmatrix} -L_k f_2(0) \\ -C_k F_k f_2(0) - L_k f_2(1) \\ \vdots \\ -\sum_{\tau=0}^{k_t-1} C_k A_k^{k_t-1-\tau} F_k f_2(\tau) - L_k f_2(k_t) \end{bmatrix}.$$

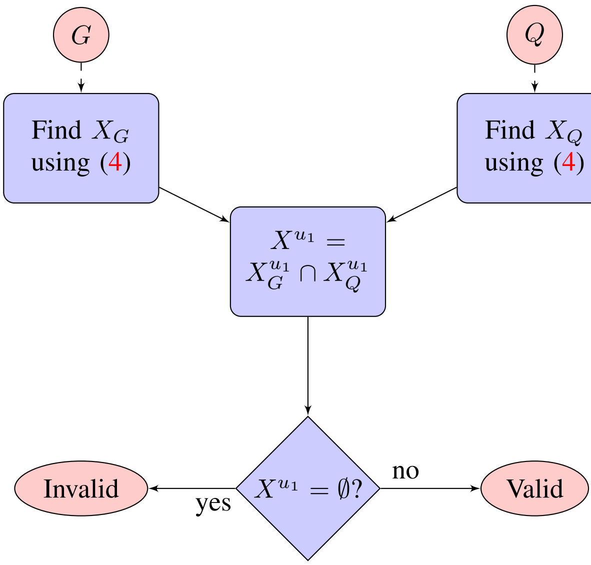

Figure 2. Flowchart of an iteration of the Fast SVO algorithm which takes as input the coprime factorization and decides if the model is invalid or still valid.

In the above definitions, for two different fault signals f_1 and f_2, we define $x(0) = x_1(0) - x_2(0)$ where $x_1(0)$ and $x_2(0)$ are the initial conditions for the system using f_1 and f_2 respectively.

In order to perform fault detection, we will have to consider the nominal "fault-free" model and distinguish it from the actual system for which we have measurements $y(k)$. Considering model (1) with disturbances and noise signals and using the above definitions, we can rewrite the SVO equations so as to make all the inequalities be written using a single time instant, i.e., all inequalities pose constraints on the $x(k-H)$ variable. The new set of inequalities for the SVOs are:

$$\begin{bmatrix} \bar{C}_k & \bar{L}_k & 0 & \cdots & 0 \\ \bar{C}_k A_k & \bar{C}_k F_k & 0 & \cdots & 0 \\ \vdots & \ddots & \ddots & \ddots & \vdots \\ \bar{C}_k A_k^n & \bar{C}_k A_k^{n-1} F_k & \cdots & \bar{C}_k F_k & \bar{L}_k \\ 0 & \bar{I} & 0 & \cdots & 0 \\ \vdots & \ddots & \ddots & \ddots & \vdots \\ 0 & 0 & 0 & \cdots & \bar{I} \\ M(k-H) & 0 & 0 & \cdots & 0 \end{bmatrix} \begin{bmatrix} x(k-H) \\ d(k-H) \\ \vdots \\ d(k) \end{bmatrix} \leq \begin{bmatrix} \bar{y}(k-H) \\ \vdots \\ \bar{y}(k) \\ 1 \\ \vdots \\ 1 \\ m(k-H) \end{bmatrix} \tag{4}$$

The above SVO equation is no longer an iterative solution since it is not possible to obtain estimates for $x(k-H)$ and obtain $M(k-H)$ and $m(k-H)$. Nevertheless, we can assume a sufficiently *large* set and use the coprime factorization presented in the previous section to remove the conservatism of that overbound. In essence, (4) will be applied to the LPV models of the coprime factors of (1) by replacing the matrices according to Proposition 1.

The Lemma 1 can be reformulated for the novel SVO equations obtaining:

Lemma 2 (fault detection)
Consider a dynamic system as in (1) and an fSVO defining the inequalities for $x_Q(k-H)$ and $x_G(k-H)$ of the coprime factors $Q(k)$ and $G(k)$ given by Proposition 1 with sufficiently large sets such that $x_Q(k-H) \in X_Q(k-H)$ and $x_G(k-H) \in X_G(k-H)$. A fault occurred if there is no solution to the inequalities (4) for both coprime factors.

Lemma (2) comes directly from the fact that if there are no solutions to (4), the "fault-free" model does not correspond to the real system. Fault isolation can be performed by invalidating the models for all the remaining faults. For each of the ℓ considered faults, we define pairs of matrices (F_k, L_k) such that only that fault is modeled, thus creating ℓ possible models for the system. If the faults are identifiable, then all SVOs become empty except for the one which represents the correct fault model. If multiple faults are to be considered we could use a scheme such as the one presented in [28].

A decision regarding the model for each possible fault being compliant with the measurements is made based on the algorithm presented in Fig. 2. The sets $X_G^{u_1}$ and $X_Q^{u_1}$ denote, respectively, the set of possible

DOI: 10.1002/rnc

values of output u_1 for the cofactor system $G(k)$ and $Q(k)$. Testing if X^{u_1} is the empty set amounts to solving a feasibility program of existing a point in X_G and another in X_Q such that the outputs of the subsystems $G(k)$ and $Q(k)$ are the same.

An important issue regarding the fSVOs is that they are not suitable for state estimation. As all the inequalities are written with respect to $x(k-H)$, no estimates are available for $x(k)$. In the standard SVOs, restrictions concerning the state in all last H iterations are then projected to depend solely on the current time instant. Following this reasoning, no iterative computation of the set-valued estimates is possible, which makes them not suitable for state estimation. In addition, following the factorization, the two SVOs for subsystems $Q(k)$ and $G(k)$ have states that are internal to each of the subsystems and, therefore, are not related to the original system state $x(k)$. Nevertheless, for applications such as fault detection and isolation and model invalidation, they are suitable as the state itself may be disregarded.

6. SIMULATION RESULTS

In this section, we present a set of simulations illustrating the fault detection mechanism described in this article. In particular, we are interested in comparing against the approach of performing a canonical Kalman decomposition, which is valid only for the LTI case whereas our proposal addresses the broader class of LPV systems. This distributed fault detection architecture reduces the dependability on a single centralized point of detection, offering a more robust fault detection strategy but increasing the aggregated computational power, since each node acts itself as a detector. We start by analyzing the example described in [3] which resorts to the Kalman decomposition for a particular example.

Recovering the example, each subsystem is a flexible link robot dynamic system modeled as:

$$\begin{bmatrix} \dot{\theta}^i_m \\ \dot{\omega}^{i_m} \\ \dot{\theta}^i_\ell \\ \dot{\omega}^{i_\ell} \end{bmatrix} = \begin{bmatrix} 0 & 1 & 0 & 0 \\ -\frac{K_\ell}{J_m} & -\frac{B}{J_m} & \frac{K_\ell}{J_m} & 0 \\ 0 & 0 & 0 & 1 \\ -\frac{K_\ell}{J_\ell} & 0 & -\frac{L_\ell}{J_m} - \frac{mgh}{J_\ell} & 0 \end{bmatrix} \begin{bmatrix} \theta^i_m \\ \omega^{i_m} \\ \theta^i_\ell \\ \omega^{i_\ell} \end{bmatrix} + \begin{bmatrix} 0 \\ \frac{K_\tau}{J_m} \\ 0 \\ 0 \end{bmatrix} u^i + \begin{bmatrix} 0 \\ \frac{K_\tau}{J_m} \\ 0 \\ 0 \end{bmatrix} f^i + \begin{bmatrix} 0 \\ 0 \\ 0 \\ \frac{mgh}{J_\ell} \end{bmatrix} d^i$$

$$y_i = \sum_{j \in \mathcal{J}_i} C(x_i - x_j)$$

for $i \leq N$ and $C = [I_3\ 0_{3\times 1}]$. The states represent the angular position and velocity of the motor shaft (θ^i_m and ω^{i_m}), and the angular position and velocity of the link (θ^i_ℓ and ω^{i_ℓ}). For further details on the subsystems dynamical models, the interested reader is referred to [3] and the references therein. The network topology is selected at random in each time instant with 25 nodes, a minimum and maximum degree of the interconnection graph of 1 and 3, respectively. We assume that the topology is available to the nodes so that the parameter ρ can be determined. The system is discretized using a sampling time of 0.01 seconds, and the simulations are run for 100 discrete time steps. The simulations displayed are the result from the computations at node 1.

We consider three different scenarios: one where a subsystem has an actuator fault represented by a constant fault signal; a second where this fault is random across time; and a last one where no fault is injected, but the predefined bounds for the disturbance are not satisfied. Each scenario aims to illustrate a different aspect of the detection algorithm.

We start by considering a fixed topology so that the system becomes a Linear Time-Invariant (LTI) model. The Kalman decomposition is performed by applying the state transformation specific to the case of subsystems with relative measurements [3]. A standard SVO is then designed for the observable subspace. The aim is to show that detection for this case is possible although the conservatism is not removed since we did not perform the coprime factorization. Figure 3 depicts the detection of the algorithm using SVOs. The red and green lines represent the upper and lower bounds of the state variable for the angular position of node 1. These are obtained by projecting the set of estimates onto the coordinate corresponding to this variable. When the state of the system crosses one of the bounds, the corresponding observation will produce an empty set, as none of the admissible state realizations is compatible with the input/output sequences.

In the simulation, we also designed the SVOs for the coprime factors obtained from the system corresponding to the observable subspace and compared it with the proposed method of designing the SVOs for the original detectable system. The two strategies produced the same results for the LTI case. However, the Kalman decomposition is defined only for LTI systems and, therefore, one of the advantages of the proposed technique is to make it possible to construct the SVOs *oblivious* to unobservable modes as long as they are stable.

The next simulations were conducted using the proposed factorization-based implementations of the SVOs for the LPV system. In Fig. 4, it is shown the detection time for the case of a constant actuator fault, as a function of the associated amplitude. As soon as the magnitude of the signal rises slightly above the

DOI: 10.1002/rnc

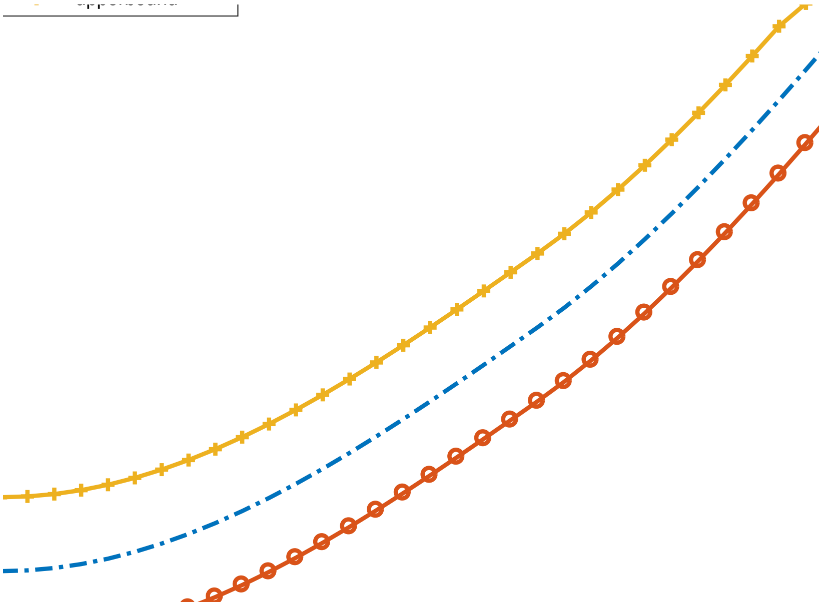

Figure 3. Example of a simple fault detection where the state of the system (blue line) crosses the upperbound (red line) of the state given through the projection of the set-valued estimate onto the corresponding coordinate.

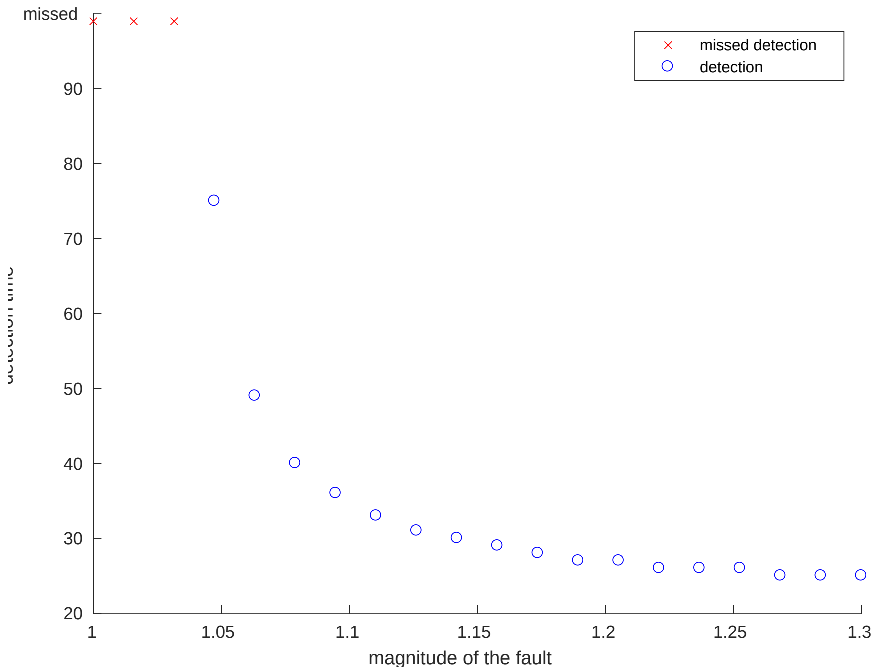

Figure 4. Detection times when varying the magnitude of a constant fault.

bound considered for the disturbances, the fault is detected, as the model with $f = 0$ is not able to generate state realizations compatible with this fault.

Based on the previous results, we investigate fault profiles that hinder detection. Intuitively, the faults harder to detect are likely to behave as modeled disturbances. Following this reasoning, we consider the case where the fault is stochastic with uniform distribution with support on the interval from zero to the maximum magnitude in order to determine its impact. Figure 5 shows the mean detection time for the simulated case for a Monte Carlo experiment with 1000 runs. It is noticeable that the detection requires a

DOI: 10.1002/rnc

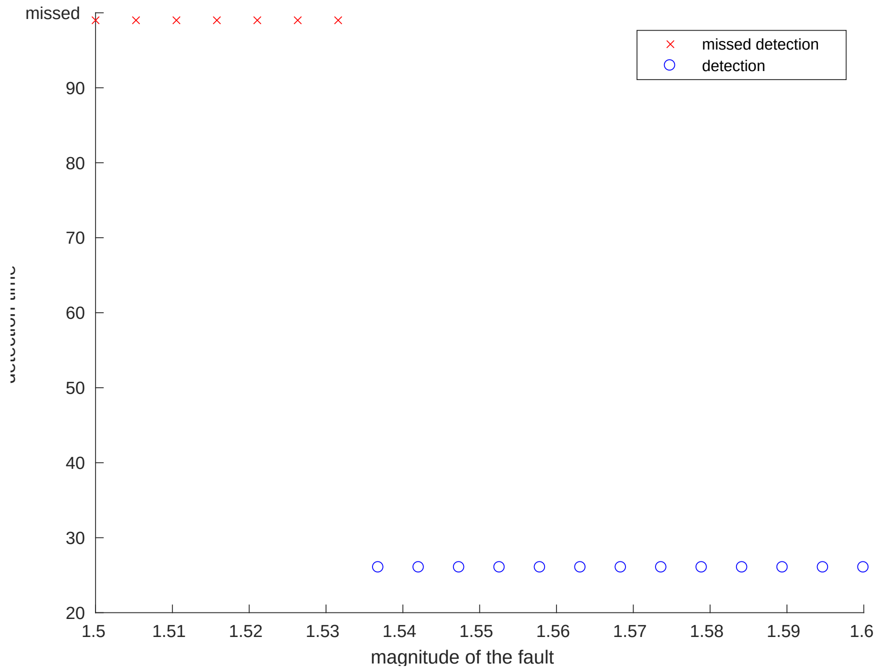

Figure 5. Mean detection times when varying the maximum magnitude of a random fault.

higher magnitude than the constant case, due to the fact that the fault signal magnitude is lower than the deterministic case most of the times.

It should be stressed that the SVOs provide means to tackle a wide range of models for the dynamic system. We take advantage of this fact to further evaluate the proposed method in a more demanding scenario. By definition, every fault is going to be detected as long as the measurements do not comply with the assumed fault-free model. For this reason, we introduced unmodeled stochastic uniformly distributed disturbances, with support on the interval from zero to the maximum magnitude, to the state of the system. Notice that in the dynamics of the subsystems, the disturbances only affect the variable ω^{i_ℓ} which makes the detection troublesome.

Figure 6 shows the mean detection times for the unmodeled disturbances case for a Monte Carlo experiment with 1000 runs. The fault is only detected when its maximum magnitude reaches above 1, which is clearly above the previous required magnitude values for the fault signal.

The fault isolation scheme was also simulated using the aforementioned example. Two different faults were considered, namely $f_1(k) := [c \quad 0]^\intercal$ and $f_2(k) := [0 \quad c]^\intercal$, for a varying constant c. The simulation run 3 SVOs: an SVO for the "fault-free" model for fault detection; another that considered $B_k f_1(k)$ for determining that f_1 is not the current fault; and, a similar to the latter but considering $f_2(k)$. Fault detection means the first SVO produced an empty set and upon that event, isolation of the faults is determined when only one of the SVOs is not producing the empty set. In this simulation, after 20 time instants, fault f_1 is injected in the system.

Figure 7 reports the detection and isolation times for fault f_1. We point out that the constant c cannot be directly compared with the bound for the disturbances without taking into account the small values in matrices B_k. Figure 7 presents 1000 montecarlo runs, but is interesting that in some of the runs, isolation (i.e., SVO for f_2 reports the empty set) happens before the detection as both fault signals have different directions and contribute to a quicker violation of the bounds for the disturbances.

In order to illustrate our main result for detectable systems, we simulated a simple example where by construction the system is unobservable but we can tune the eigenvalues of the dynamics matrix. Consider the dynamic system given by

$$A = \begin{bmatrix} \lambda_{\max} & 1 \\ 0 & -\frac{1}{2} \end{bmatrix}, B = \begin{bmatrix} 0 \\ 1 \end{bmatrix}, C = \begin{bmatrix} 0 & 4 \end{bmatrix}, D = 0.$$

where by selecting the value of $\lambda_{\max}$, we tune the unobservable mode. For this example of a system with two states, it is always unobservable and we resort to the left-coprime factorization proposed in [29]. In Fig. 8, it is depicted the hypervolume of the sets for the case of fast unobservable modes (selecting $\lambda_{\max} = 0$ yields eigenvalues of $A - KC$ equal to zero and slow unobservable eigenvalues of the term $A - KC$, by

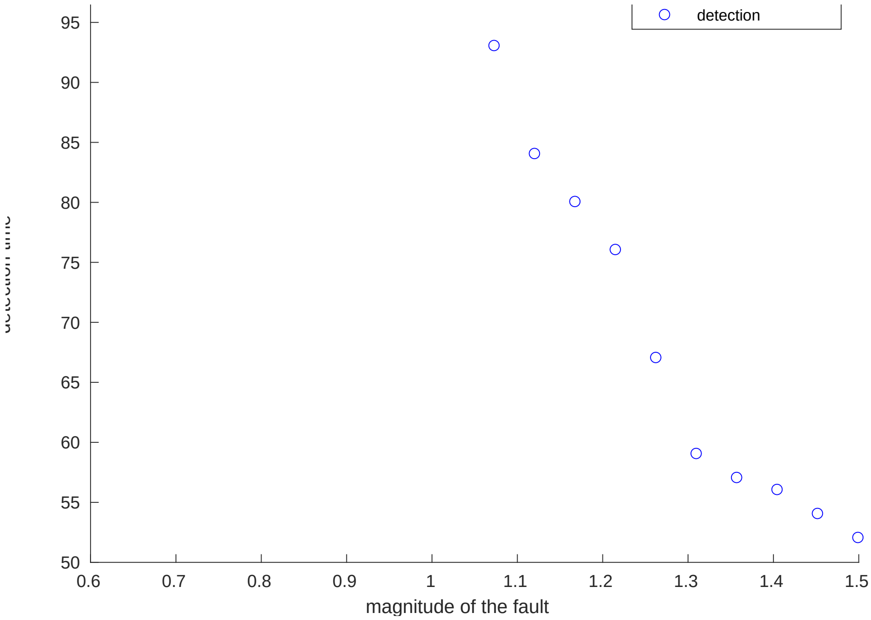

Figure 6. Detection time for a fault free system but with unmodeled disturbances.

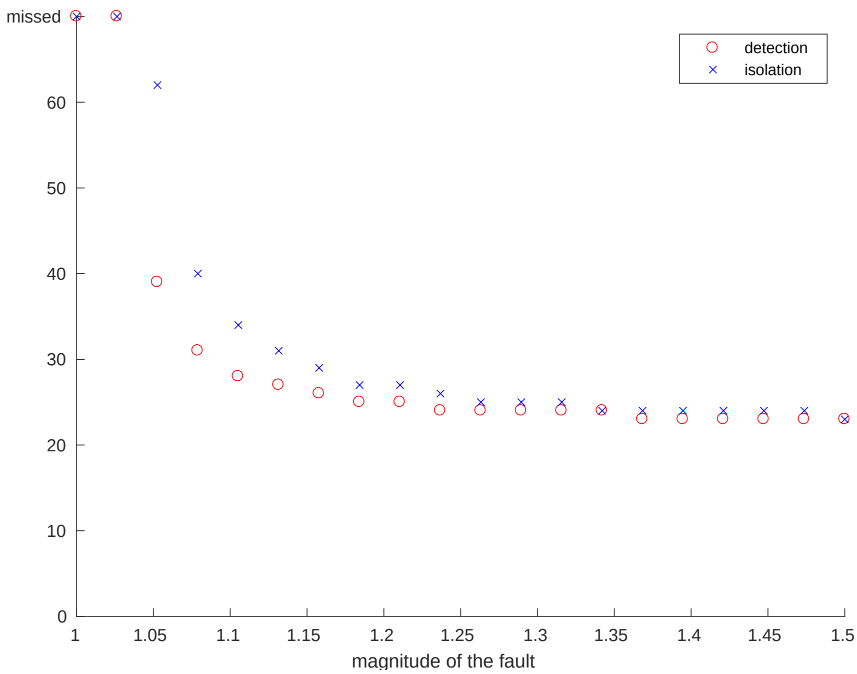

Figure 7. Detection and isolation of fault f_1 in the system.

setting $\lambda_{\max} = 0.74$). For the fast unobservable modes case, the size becomes constant after 2 time instants corresponding to the size of the state space and following the results in Theorem 1. When the eigenvalues are slow, the convergence is asymptotic, in the sense of Definition 1, and slower when compared to the fast mode case.

The key point to note when using the fSVOs is that the uncertainty of the initial state is removed after the horizon as given by Theorem 1. This feature is crucial for the procedure since by not having an iterative algorithm there is no available estimate for the state $x(k-H)$. However, Fig. 9 illustrates the results for the

DOI: 10.1002/rnc

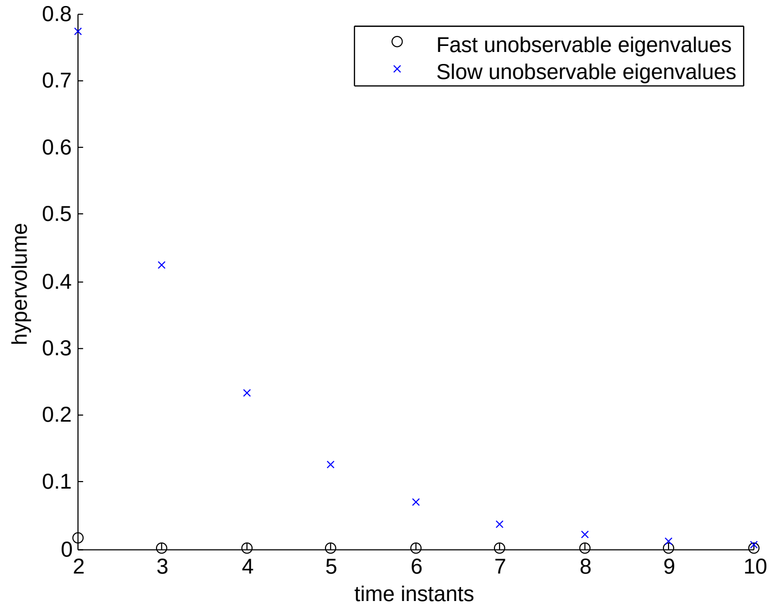

Figure 8. Hypervolume of the set corresponding to the system G for eigenvalues of $A - KC$ close to zero (magnitude under 2.3×10^{-2}) and with $\lambda_{\max} = 0.74$.

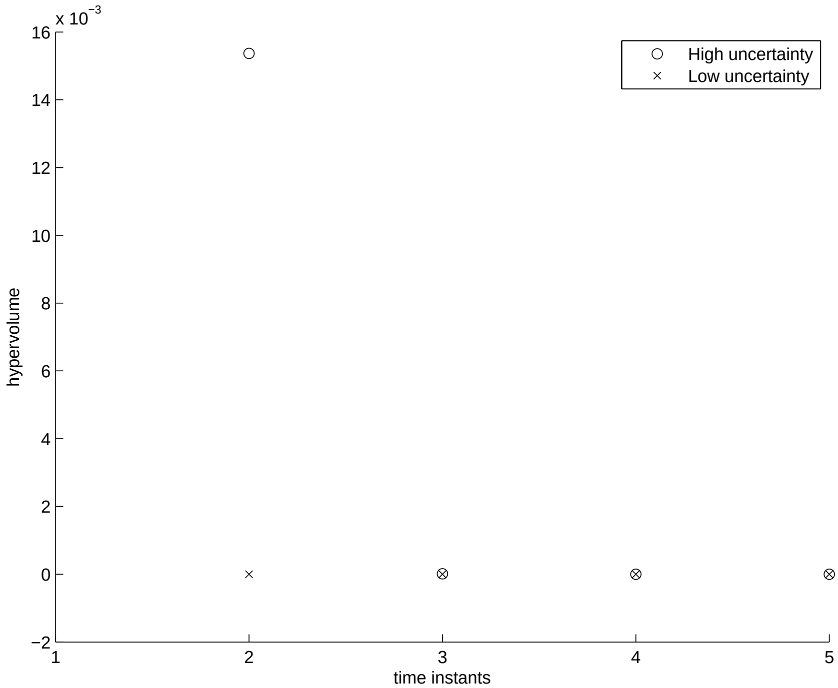

Figure 9. Hypervolume of the set corresponding to the system G for eigenvalues of $A - KC$ close to zero (magnitude under 2.3×10^{-2}) and uncertainty of 1 and 10^6 for the initial state.

fast unobservable modes case when we start with an uncertainty equal to a hypercube of side 1 and 10^6. As expected, after two time instants the size of both set-valued estimates for the internal state of system G are equal and remain constant for the rest of the simulation. In Fig. 10, we present the median and quartiles (25% and 75%) for the running time of a single iteration of the SVOs against the fSVOs for 1000 runs. It is worth pointing out that the small horizon and the fact that we are using hyper-parallelepiped approximations for the projections already make the SVOs considerably efficient. Nevertheless, fSVOs

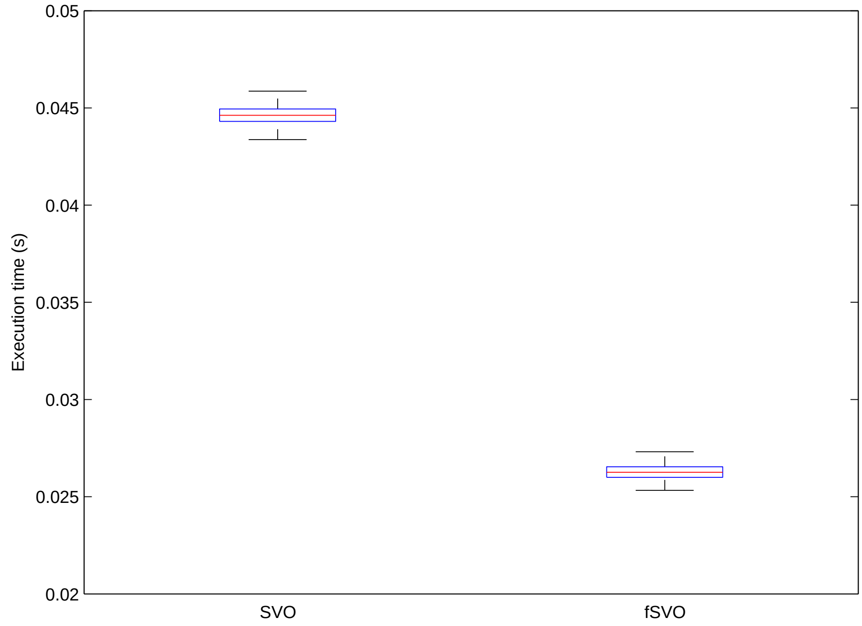

Figure 10. Running time of the SVOs compared with the fSVOs.

still reduce the computational time to almost half when compared to the SVOs using the same coprime factorization.

We also simulated the smart power grid network case, as another example of a cyber physical system. We consider the well-known test bed example IEEE 14 bus system [30] with sampling period of 1 second and run the simulations for 20 seconds.

Another interesting point to be illustrated is how SVOs can isolate faults. In the former simulations the ability of the method was presented for fault detection and a simple strategy would be to design an SVO for each of the faults and when only one SVO is active, the fault is identified. However, such procedure entails a combinatorial number of SVOs. As an example, for 5 generators and assuming a maximum of 2 simultaneous faulty generators would require 15 SVOs (one for each single generator failing and one for each pair of faulty generators). We now illustrate that by designing an SVO aggregating generator faults, it is possible to identify faults resorting to fewer SVOs. We consider two SVOs: 1) all generators are injecting random signals; 2) generators 1, 2 and 3 do not suffer any fault and their rotor angles are not corrupted.

In simulation, a fault was reported after two seconds by SVO 2 (i.e., its estimated set was empty), which means a fault occurred in at least one of the first 3 generators. By applying iteratively this method it is possible to isolate a fault by constructing SVOs using the past measurements and perform a binary search over the possible faults. If we assume only 1 generator can fail at a time, we need $\lceil \log_2 n \rceil$ steps in the binary search and design two SVOs at each step mapping half of the faulty nodes. For the general case of F possible faulty generators, we have the expression $\lceil F \log_2 n \rceil$.

7. CONCLUSIONS

This paper addressed the problem of detecting faults in a distributed environment when the overall system of systems has stable unobservable modes (i.e. it is detectable). Standard SVOs require observability, otherwise the estimates might diverge, which means that the hypervolume of the produced set-valued estimates can tend to infinity as time progresses. In addition, standard SVOs include operations that are very costly in terms of computational time, which diminishes their applicability to time-sensitive plants.

Nevertheless, SVOs were adopted due to their ability to cope with asynchronous measurements and allow general models that can incorporate both physical systems and their interconnection with networks. By performing a left-coprime factorization, we were able to show that these observers can also be designed for detectable systems with guaranteed convergence rates for the estimates. These are of prime interest as they mean that conservatism in prior estimates has an effect that is at least exponentially going to zero. Building

DOI: 10.1002/rnc

on this result, we were able to rewrite the equations of the SVOs to mimic the theoretical conditions for fault detectability and identifiability and, therefore, avoid the use of the Fourier-Motzkin elimination method, as the whole set was written in terms of a fixed time instant, thus speeding up the computations. The initial uncertainty also vanished due to the convergence property of the estimates.

Simulation results have shown that when the maximum magnitude of a fault exceeds the disturbance bounds, the detection occurs and the time before declaring the faulty state goes to near the size of the state space. Both constant and stochastic faults were simulated using a group of flexible link robotic models. In addition, the SVOs were capable of detecting deviations from the model for the disturbances and declaring faults whenever the model was not compatible with the measurements. An application to a smart grid was used to illustrate the effectiveness of the detection procedure for cyber-physical systems.

ACKNOWLEDGEMENTS

This work was partially supported by the project MYRG2016- 00097-FST of the University of Macau; by the Portuguese Fundação para a Ciência e a Tecnologia (FCT) through Institute for Systems and Robotics (ISR), under Laboratory for Robotics and Engineering Systems (LARSyS) project UID/EEA/50009/2013; and by U.S. Army Research Laboratory and the U.S. Army Research Office under grants No. W911NF-09-1-0553 and W911NF-09-D-0001. The work of Daniel Silvestre was supported by the FCT PhD grant SFRH/BD/71206/2010. Carlos Silvestre is on leave from the Instituto Superior Técnico, Universidade de Lisboa, Lisboa, Portugal.

REFERENCES

1. Fax J, Murray R. Information flow and cooperative control of vehicle formations. *IEEE Transactions on Automatic Control* Sept 2004; **49**(9):1465–1476, doi:10.1109/TAC.2004.834433.
2. Massioni P, Verhaegen M. Distributed control for identical dynamically coupled systems: A decomposition approach. *IEEE Transactions on Automatic Control* Jan 2009; **54**(1):124–135, doi:10.1109/TAC.2008.2009574.
3. Menon P, Edwards C. Robust fault estimation using relative information in linear multi-agent networks. *IEEE Transactions on Automatic Control* Feb 2014; **59**(2):477–482, doi:10.1109/TAC.2013.2274689.
4. Metke A, Ekl R. Security technology for smart grid networks. *IEEE Transactions on Smart Grid* June 2010; **1**(1):99–107, doi:10.1109/TSG.2010.2046347.
5. Amin M. Guaranteeing the security of an increasingly stressed grid. *Smart Grid Newsletter, IEEE* Feb 2011; .
6. Fang X, Misra S, Xue G, Yang D. Smart grid 2014; the new and improved power grid: A survey. *Communications Surveys Tutorials, IEEE* Fourth 2012; **14**(4):944–980, doi:10.1109/SURV.2011.101911.00087.
7. Metke A, Ekl R. Security technology for smart grid networks. *IEEE Transactions on Smart Grid* June 2010; **1**(1):99–107, doi:10.1109/TSG.2010.2046347.
8. Silvestre D, Rosa P, Hespanha JP, Silvestre C. Stochastic and deterministic fault detection for randomized gossip algorithms. *Automatica* 2017; **78**:46 – 60, doi:http://doi.org/10.1016/j.automatica.2016.12.011. URL http://www.sciencedirect.com/science/article/pii/S0005109816305192.
9. Witsenhausen H. Sets of possible states of linear systems given perturbed observations. *IEEE Transactions on Automatic Control* oct 1968; **13**(5):556 – 558, doi:10.1109/TAC.1968.1098995.
10. Schweppe F. Recursive state estimation: Unknown but bounded errors and system inputs. *IEEE Transactions on Automatic Control* feb 1968; **13**(1):22 – 28, doi:10.1109/TAC.1968.1098790.
11. Schweppe F. *Uncertain Dynamic Systems*. Prentice-Hall, 1973.
12. Milanese M, Vicino A. Optimal estimation theory for dynamic systems with set membership uncertainty: An overview. *Automatica* 1991; **27**(6):997 – 1009, doi:10.1016/0005-1098(91)90134-N.
13. Althoff M, Stursberg O, Buss M. Reachability analysis of linear systems with uncertain parameters and inputs. *Decision and Control, 2007 46th IEEE Conference on*, 2007; 726–732, doi:10.1109/CDC.2007.4434084.
14. Su J, Chen WH. Fault diagnosis for vehicle lateral dynamics with robust threshold. *2016 IEEE International Conference on Industrial Technology (ICIT)*, 2016; 1777–1782, doi:10.1109/ICIT.2016.7475033.
15. Kezunovic M. Smart fault location for smart grids. *IEEE Transactions on Smart Grid* March 2011; **2**(1):11–22, doi:10.1109/TSG.2011.2118774.
16. Manandhar K, Cao X, Hu F, Liu Y. Detection of faults and attacks including false data injection attack in smart grid using kalman filter. *IEEE Transactions on Control of Network Systems* Dec 2014; **1**(4):370–379, doi:10.1109/TCNS.2014.2357531.
17. Calderaro V, Hadjicostis C, Piccolo A, Siano P. Failure identification in smart grids based on petri net modeling. *IEEE Transactions on Industrial Electronics* Oct 2011; **58**(10):4613–4623, doi:10.1109/TIE.2011.2109335.
18. Giani A, Bitar E, Garcia M, McQueen M, Khargonekar P, Poolla K. Smart grid data integrity attacks: characterizations and countermeasures. *Smart Grid Communications (SmartGridComm), 2011 IEEE International Conference on*, 2011; 232–237, doi:10.1109/SmartGridComm.2011.6102324.
19. Pasqualetti F, Dorfler F, Bullo F. Cyber-physical attacks in power networks: Models, fundamental limitations and monitor design. *Decision and Control and European Control Conference (CDC-ECC), 2011 50th IEEE Conference on*, 2011; 2195–2201, doi:10.1109/CDC.2011.6160641.
20. Pasqualetti F, Bicchi A, Bullo F. A graph-theoretical characterization of power network vulnerabilities. *American Control Conference (ACC), 2011*, 2011; 3918–3923, doi:10.1109/ACC.2011.5991344.

DOI: 10.1002/rnc

21. Pasqualetti F, Bicchi A, Bullo F. Consensus computation in unreliable networks: A system theoretic approach. *IEEE Transactions on Automatic Control* jan 2012; **57**(1):90 –104, doi:10.1109/TAC.2011.2158130.
22. Rosa P, Silvestre C, Athans M. Model falsification using set-valued observers for a class of discrete-time dynamic systems: a coprime factorization approach. *International Journal of Robust and Nonlinear Control* 2014; **24**(17):2928–2942, doi:10.1002/rnc.3033.
23. Rosa P, Silvestre C. On the distinguishability of discrete linear time-invariant dynamic systems. *50th IEEE Conference on Decision and Control*, 2011.
24. Rosa P. Multiple-model adaptive control Multiple-Model Adaptive Control of Uncertain LPV Systems. PhD Thesis, Technical University of Lisbon, Lisbon, Portugal 2011.
25. Shamma J, Tu KY. Set-valued observers and optimal disturbance rejection. *IEEE Transactions on Automatic Control* feb 1999; **44**(2):253 –264, doi:10.1109/9.746252.
26. Keerthi S, Gilbert E. Computation of minimum-time feedback control laws for discrete-time systems with state-control constraints. *IEEE Transactions on Automatic Control* may 1987; **32**(5):432 – 435, doi:10.1109/TAC.1987.1104625.
27. Zhou K, Doyle JC, Glover K. *Robust and Optimal Control*. Prentice-Hall, Inc.: Upper Saddle River, NJ, USA, 1996.
28. Bras S, Rosa P, Silvestre C, Oliveira P. Fault detection and isolation in inertial measurement units based on bounding sets. *IEEE Transactions on Automatic Control* July 2015; **60**(7):1933–1938, doi:10.1109/TAC.2014.2363300.
29. Ravi R, Pascoal A, Khargonekar P. Normalized coprime factorizations and the graph metric for linear time-varying systems. *Decision and Control, 1990., Proceedings of the 29th IEEE Conference on*, 1990; 1241–1246 vol.3, doi:10.1109/CDC.1990.203807.
30. University of Washigton. March 2015. URL http://www.ee.washington.edu/research/pstca/.

DOI: 10.1002/rnc