INTERNATIONAL JOURNAL OF ROBUST AND NONLINEAR CONTROL
Int. J. Robust. Nonlinear Control 2016; **00**:1–4
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 hypervolume 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.

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

[†]E-mail:dsilvestre@isr.ist.utl.pt
*Correspondence to: Contact the author D. Silvestre through dsilvestre@isr.ist.utl.pt for a free unformatted copy of this article or go to http://onlinelibrary.wiley.com/doi/10.1002/rnc.3814/full for the final formatted version.

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].

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

DOI: 10.1002/rnc

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.

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.
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.