

Fault Detection for Cyber-Physical Systems: Smart Grid case

Daniel Silvestre, João P. Hespanha, Carlos Silvestre

Abstract—The problem of fault detection and isolation in cyber-physical systems is growing in importance following the trend to have an ubiquitous presence of sensors and actuators with network capabilities in power networks and other areas. In this context, attacks to power systems or other vital components providing basic needs might either present a serious threat or at least cost a lot of resources. In this paper, we tackle the problem of having an intruder corrupting a smart grid in two different scenarios: a centralized detector for a portion of the network and a fully distributed solution that only has limited neighbor information. For both cases, differences in strategies using Set-Valued Observers are discussed and theoretical results regarding a bound on the maximum magnitude of the attacker's signal are provided. Performance is assessed through simulation, illustrating, in particular, the detection time for various types of faults in IEEE testbed scenarios.

I. INTRODUCTION

Performing fault detection in the context of cyber-physical systems is a challenging task, in particular due to the large size of the network or its sensibility to attacks. In the case of a smart grid, a network failure or malignant action can compromise its service and is a fundamental challenge in real applications [1], [2]. Besides failures and attacks to the physical power grid infrastructure, one must also consider cyber attacks to its communication layer. Therefore, the problem of detecting faults and identifying where they are occurring in a network is considered in this paper. We adopt the linearized small signal version of the structure-preserving model, composed by the linearized swing and the DC power flow equations. A comprehensive survey can be found in [3] regarding different aspects of the design of smart grids. The importance of the problem addressed here has been noted in [1] and later in [2].

D. Silvestre is with the Department of Electrical and Computer Engineering of the Faculty of Science and Technology of the University of Macau, Macau, China, and with the Institute for Systems and Robotics (ISR), Instituto Superior Técnico, University of Lisbon, Lisbon, Portugal. D. Silvestre was supported by the project MYRG2016- 00097-FST from 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. dsilvestre@umac.mo

C. Silvestre is with the Department of Electrical and Computer Engineering of the Faculty of Science and Technology of the University of Macau, Macau, China, on leave from Instituto Superior Técnico/Technical University of Lisbon, 1049-001 Lisbon, Portugal. The work was supported by project MYRG2016- 00097-FST of the University of Macau. csilvestre@umac.mo

João P. Hespanha is with the Dept. of Electrical and Computer Eng., University of California, Santa Barbara, CA 93106-9560, USA. 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. This material is based upon work partially supported by the National Science Foundation under Grant No. ECCS-1608880. hespanha@ece.ucsb.edu

In [4], the use of Set-Valued Observers (SVOs) for distributed fault detection was firstly introduced for the distributed consensus problem. The algorithm is modeled as a Linear Parameter-Varying (LPV) system where communications are seen as a parameter-dependent dynamics matrix. Whereas in [4], each node has access to its own state and one of the neighbor states to which it communicates, 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 [5].

The SVOs framework, whose concept was introduced in [6] and [7] (further information can be found in [8] and [9] and references therein) is used to represent and propagate the set-valued state estimates for linear systems with disturbances and model uncertainties.

For the particular case of smart grids, other proposals have been presented by the research community as alternative fault detection methods. A survey focused in fault location methods for both transmission and distribution systems can be found in [10].

In [11], faults are detected by constructing a χ^2 -detector that constructs the χ^2 statistics from a Kalman filter and compares them to perform statistical hypothesis testing. 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.

Fault detection in smart grids has also been performed resorting to the concept of Petri Nets [12]. The procedure consists in modeling all possible concurrent actions 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 valid states of the system.

In [13], 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 for the equation dictating the detection and isolation of faults are related. In [14], 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 to the model.

In a different direction, [15] and [16] 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.

The main contributions of this paper are as follows:

- we show how to perform fault detection and isolation with observers from a centralized point-of-view. In this scenario, it is shown that uncertainty associated with the initial state can be reduced to zero in finite time;
- the distributed setting is addressed by adding uncertainty parameters to model the unknown dynamics. Given the stability property of the smart grid, we show that the SVOs asymptotically converge to the true state;
- a bound on the maximum magnitude of the attacker signal is given by formulating the problem as a distinguishability of two systems. Simulations are provided to illustrate how our results could be applied to realistic systems.

The remainder of this paper is organized as follows. In Section II, we describe the smart grid model to be addressed. Section III describes the SVO technique and how it can be improved using tools in the literature for the centralized case. The methodology for tackling the decentralized version is presented in Section IV along with rewriting the problem as a distinguishability of two systems and obtaining bounds on the attacker signal in Section V. The mentioned points are illustrated in simulation in Section VI. Concluding remarks and directions of future work are provided in Section VII.

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

II. PROBLEM STATEMENT

In this section, we introduce the smart grid network as a cyber physical system. The model presented in [14] is considered for the evolution of the state of a smart power grid, namely, a connected power network consisting of n generators and their corresponding n generator terminal buses and m load buses, totaling $n+m$ buses in the network. The dynamics of the network follows the linear small-signal version of the classical structure-preserving power network model discussed in [17], which comprises the dynamic linearized swing equation and the algebraic DC power flow equation. Further details regarding the derivation of such dynamics from the nonlinear model can be found in [18] and [15].

The weighted graph associated with the admittance in the connectivity network induces a Laplacian matrix

$\begin{bmatrix} \mathcal{L}_{gg} & \mathcal{L}_{gl} \\ \mathcal{L}_{gl} & \mathcal{L}_{ll} \end{bmatrix} \in \mathbb{R}^{(n+m) \times (n+m)}$, where the first n rows are associated with the buses connecting to the generators and the remaining rows correspond to the bus network.

The whole system can be described by the differential-algebraic continuous-time dynamic model given by

$$N_c \dot{x}(t) = A_c x(t) + p(t) \quad (1)$$

where the state $x = [\delta^\top \omega^\top \theta^\top]^\top \in \mathbb{R}^{2n+m}$, encompasses the generator rotor angles $\delta \in \mathbb{R}^n$, the frequencies $\omega \in \mathbb{R}^n$, and the bus voltages angles $\theta \in \mathbb{R}^m$. The input term $p(t)$ accounts for the known changes in input power to the generators or power demands of the loads. The matrices of the dynamics are as follows

$$N_c = \begin{bmatrix} I & 0 & 0 \\ 0 & N_g & 0 \\ 0 & 0 & 0 \end{bmatrix}, A_c = - \begin{bmatrix} 0 & -I & 0 \\ \mathcal{L}_{gg} & D_g & \mathcal{L}_{gl} \\ \mathcal{L}_{lg} & 0 & \mathcal{L}_{ll} \end{bmatrix},$$

where N_g and D_g are the diagonal matrices of the generator inertia and damping coefficients.

For detection purposes, we assume that a subset of the state variables being measured is corrupted by sensor noise as modeled next. Let $C \in \mathbb{R}^{p \times n}$ and $\eta \in \mathbb{R}^p$, and the signal f represent cyber-physical attacks in the sensors and/or in the state, leading to the following system equations

$$N_c \dot{x}(t) = A_c x(t) + u(t) + \underbrace{\begin{bmatrix} F & 0 \end{bmatrix}}_{F_c} f(t) + E_c d(t)$$

$$y(t) = C_c x(t) + \underbrace{\begin{bmatrix} 0 & L \end{bmatrix}}_{L_c} f(t) + \eta(t)$$

where $F \in \mathbb{R}^{2n+m \times 2n+m}$, $E_c \in \mathbb{R}^{2n+m \times q}$, $L \in \mathbb{R}^{p \times p}$, $d(t) \in \mathbb{R}^q$, $f(t) \in \mathbb{R}^{2n+m+p}$, $u(t) = p(t)$ and both F and L are full rank matrices. The terms $d(t)$, $\eta(t)$ and $f(t)$ are respectively the disturbance, noise and attack signals.

We assume that the parameters of the network can be estimated as in [19], but, in contrast to [14] where no disturbances and noise are included, we consider the error in the estimation by adding a disturbance term to equation (1).

The next step is to transform the differential-algebraic system in (1) into a standard differential equation model, as described in [14], by resorting to the fact that \mathcal{L}_{ll} is invertible due to the overall network being connected [18]. This implies that the bus voltage angles $\theta(t)$ can be obtained from the remaining variables by simply inverting the algebraic equation in (1).

If we consider the partition of the matrices $F = \begin{bmatrix} F_\delta^\top & F_\omega^\top & F_\theta^\top \end{bmatrix}^\top$, $E_c = \begin{bmatrix} E_\delta^\top & E_\omega^\top & E_\theta^\top \end{bmatrix}^\top$ and $C_c = \begin{bmatrix} C_\delta & C_\omega & C_\theta \end{bmatrix}$, where the dimensions of the submatrices are in accordance to the state $x = [\delta^\top \omega^\top \theta^\top]^\top$, the following set of equations, known as the kron-reduced system, is obtained

$$\begin{aligned}
\begin{bmatrix} \dot{\delta}(t) \\ \dot{\omega}(t) \end{bmatrix} &= \underbrace{\begin{bmatrix} 0 & I \\ -N_g^{-1}(\mathcal{L}_{gg} - \mathcal{L}_{gl}\mathcal{L}_{ll}^{-1}\mathcal{L}_{lg}) & -N_g^{-1}D_g \end{bmatrix}}_{\tilde{A}} \begin{bmatrix} \delta(t) \\ \omega(t) \end{bmatrix} \\
&+ \underbrace{\begin{bmatrix} I & 0 & 0 \\ 0 & N_g^{-1} & -N_g^{-1}\mathcal{L}_{gl}\mathcal{L}_{ll}^{-1} \end{bmatrix}}_{\tilde{B}} u(t) \\
&+ \underbrace{\begin{bmatrix} F_\delta & 0 \\ N_g^{-1}F_\omega - N_g^{-1}\mathcal{L}_{gl}\mathcal{L}_{ll}^{-1}F_\theta & 0 \end{bmatrix}}_{\tilde{F}} f(t) \\
&+ \underbrace{\begin{bmatrix} E_\delta & 0 \\ N_g^{-1}E_\omega - N_g^{-1}\mathcal{L}_{gl}\mathcal{L}_{ll}^{-1}E_\theta & 0 \end{bmatrix}}_{\tilde{E}} \begin{bmatrix} d(t) \\ \eta(t) \end{bmatrix}, \\
y(t) &= \underbrace{\begin{bmatrix} C_\delta - C_\theta\mathcal{L}_{ll}^{-1}\mathcal{L}_{lg} & C_\omega \end{bmatrix}}_{\tilde{C}} \begin{bmatrix} \delta(t) \\ \omega(t) \end{bmatrix} + \underbrace{\begin{bmatrix} 0 & 0 & C_\theta\mathcal{L}_{ll}^{-1} \end{bmatrix}}_{\tilde{D}} u(t) \\
&+ \underbrace{\begin{bmatrix} C_\theta\mathcal{L}_{ll}^{-1}F_\theta & L \end{bmatrix}}_{\tilde{L}} f(t) + \underbrace{\begin{bmatrix} C_\theta\mathcal{L}_{ll}^{-1}E_\theta & I \end{bmatrix}}_{\tilde{N}} \begin{bmatrix} d(t) \\ \eta(t) \end{bmatrix}.
\end{aligned}$$

Thus, the kron reduced system, with its associated tuple of matrices $(\tilde{A}, \tilde{B}, \tilde{C}, \tilde{D}, \tilde{E}, \tilde{F}, \tilde{L}, \tilde{N})$, where $\tilde{B} = I$ and $\tilde{D} = 0$, is in the form of a linear time-invariant system, which after the discretization assumes the form

$$\begin{aligned}
x(k+1) &= Ax(k) + Bu(k) + Ff(k) + Ed(k) \\
y(k) &= Cx(k) + Du(k) + Lf(k) + Nd(k)
\end{aligned}, \quad (2)$$

where $x(k) \in \mathbb{R}^{n_x}$, $y(k) \in \mathbb{R}^{n_y}$, $u(k) \in \mathbb{R}^{n_u}$, $f(k) \in \mathbb{R}^{n_f}$ and $d(k) \in \mathbb{R}^{n_d}$ (which stacks both the previous disturbance and noise signals), with matrices of appropriate size. It is assumed the bound $\forall_{1 \leq i < n_d} : |d_i(k)| \leq 1$ and, given that matrix N is constant, we can also find ν^* such that $\forall_{1 \leq i < n_y} : |[Nd(k)]_i| \leq \nu^*$.

III. CENTRALIZED SETUP

The problem tackled in this paper is that of detecting non-zero signals $f(k)$ in the model (2) based on the output measurements $y(k)$. In the sequel, details are provided for the centralized setup, where a single detecting node in the network has access to the whole output measurement and knowledge of the full dynamics. The main focus is to get a detection algorithm that guarantees a bound on the maximum magnitude of an undetectable attack.

For the design of the proposed fault detection solution, we adopt the Set-Valued Observers (SVOs) framework presented in [20] and [21] which enables the construction of a set where the state of the system is known to belong. Using a worst-case set-based estimator we can study magnitude bounds for undetected fault signals.

To review the steps in the construction of our fault detection mechanism, we define $\text{Set}(M, m) := \{q : Mq \leq m\}$, 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 $X(k)$ containing all possible states of the system at time k , knowing that $\forall_{0 \leq i < H}$, $x(k-i) \in X(k-i)$ for all past H time steps and the dynamics of the system (2) with matrices F and L equal to zero, since the set represents the possible states generated by a fault-free dynamic system.

More precisely, the initial state satisfies $x(0) \in X(0)$, where $X(0) := \text{Set}(M_0, m_0)$ and M_0 and m_0 are selected such that the corresponding polytope is guaranteed to contain the initial state. The notation $\bar{Z} := \begin{bmatrix} Z \\ -Z \end{bmatrix}$, for a matrix Z , and $\bar{v} := \begin{bmatrix} v \\ -v \end{bmatrix}$, for a vector v will be used to shorten the following equations. The information obtained by an additional output measurement $y(k+1)$, results in a set $X(k+1)$ that can be described as the set of points, \mathbf{x} , satisfying

$$\underbrace{\begin{bmatrix} M(k)A^{-1} & -M(k)A^{-1}E \\ \bar{C} & 0 \\ 0 & \bar{I} \end{bmatrix}}_{M(k+1)} \begin{bmatrix} \mathbf{x} \\ \mathbf{d} \end{bmatrix} \leq \underbrace{\begin{bmatrix} m(k) + \bar{u}(k) \\ \bar{y}(k+1) + \nu^* \mathbf{1} \\ 1 \end{bmatrix}}_{m(k+1)} \quad (3)$$

for some \mathbf{d} where we used the notation $\bar{u}(k) := M(k)A^{-1}Bu(k)$.

This procedure assumes an invertible matrix of the dynamics A . When this is not the case, we can adopt the strategy in [22] and solve the inequality

$$\underbrace{\begin{bmatrix} \bar{I} & -\bar{A} & -\bar{E} \\ 0 & 0 & \bar{I} \\ \bar{C} & 0 & 0 \\ 0 & M(k) & 0 \end{bmatrix}}_{M(k+1)} \begin{bmatrix} \mathbf{x} \\ \mathbf{x}^- \\ \mathbf{d} \end{bmatrix} \leq \begin{bmatrix} \bar{B}u(k) \\ 1 \\ \bar{y}(k+1) + \nu^* \mathbf{1} \\ m(k) \end{bmatrix}. \quad (4)$$

By applying the Fourier-Motzkin elimination method [23] to remove the dependence on \mathbf{x}^- , we still obtain a set described by $M(k+1)\mathbf{x} \leq m(k+1)$.

We recall the definition of the Fourier-Motzkin elimination method [24] as

Definition 1 (Fourier-Motzkin elimination method): Take a polytope described by $\left\{ \begin{bmatrix} x \\ y \end{bmatrix} \in \mathbb{R}^{n_x+n_y} : A \begin{bmatrix} x \\ y \end{bmatrix} \leq b \right\}$. The Fourier-Motzkin elimination method is a function

$$(A_{\text{FM}}, b_{\text{FM}}) = \text{FM}(A, b, n_x)$$

such that

$$A_{\text{FM}} y \leq b_{\text{FM}} \Leftrightarrow \exists_{x \in \mathbb{R}^{n_x}} : A \begin{bmatrix} x \\ y \end{bmatrix} \leq b.$$

The above computations assume a horizon value $H = 1$, i.e., only the measurements from time k and the input signal from time $k-1$ are used to compute the set-valued estimate of the state at time k . Due to the uncertainty in the initial state or the use of an approximation, $\tilde{X}(k)$, to set $X(k)$ (for example, to avoid the number of vertices of the polytope to render the calculation of the Fourier-Motzkin elimination method intractable), one might consider including past measurements to improve detection, at the expenses of a higher computational cost, by extending the

previous inequalities to a general horizon H . In doing so, it may reduce the conservatism of the set-valued state estimate, as shown in [25]. Finding $M(k+1)$ for larger horizon values is based on lifting techniques and the formulas can be found in [21].

Constructing the above SVO for the fault free system (i.e., (2) with $f = 0$), a fault can be declared when the set $X(k)$ is empty, which means that there is no fault-free trajectory compatible with the observed measurements.

Resorting to results in [25], [21] and [26], one can use of the concept of left-coprime factors to bound the required horizon and decrease the detection time.

Concatenating all inputs to (2) in a single vector u , this system can be expressed as follows, for appropriately defining matrices A, B, C, D :

$$\begin{aligned} x(k+1) &= Ax(k) + Bu(k) \\ y(k) &= Cx(k) + Du(k) \end{aligned} \quad (5)$$

Proposition 1 (left-coprime factorization [27]): Let a discrete-time dynamic system described by (5) be detectable, with transfer function

$$P(z) := D + C(zI - A)^{-1}B := \left[\begin{array}{c|c} zI - A & B \\ \hline C & D \end{array} \right]$$

and define

$$[G(z) \quad Q(z)] = \left[\begin{array}{c|cc} zI - A + KC & -K & B - KD \\ \hline RC & R & RD \end{array} \right]$$

where R is any nonsingular matrix and K is such that $A - KC$ is stable. Then,

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

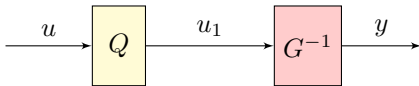


Fig. 1. Schematic representation of the two coprime systems.

The above factorization is depicted in Fig. 1. The left-coprime factorization creates two separate systems Q and G and a fault detection time can be bounded resorting to results from [21]. In [25] and [21], it is shown that if the system is observable, we can select the matrix K such that all eigenvalues of $A - KC$ are equal to zero and the fault detection time is not larger than the number of states of the system (multiplied by the sampling period). The main advantage of the factorization is the appearance of the tunable gain K .

IV. DECENTRALIZED SETUP

In the previous section, we assumed that one detecting agent is present with knowledge of the whole network dynamics and with access to the output measurements. We now consider a decentralized version of this problem, where each node implements a detector based on partial knowledge of the dynamics and a local subset of measurements. In Algorithm 1 it is described the pseudo-code of the detection

algorithm based on a decentralized setup, which convergence can be regarded as that of a consensus system (see [5]). In the sequel, details are provided on the need for an approximation $\tilde{X}(k)$ and how it can be computed.

Algorithm 1 Detection using SSVO

Require: Set $\tilde{X}(0)$, and the output measurement vectors $y^i(k)$ of each detector node i .

Ensure: Distributed fault detection.

```

1: for each  $k \geq 0$  do
2:   for each  $i$  do
3:     /* Find the state estimate  $\tilde{X}^i(k)$  */
4:      $\tilde{X}^i(k) = \text{SVO\_iteration}(\tilde{X}^i(k-1), y^i(k))$ 
5:     /* Exchange and intersect estimates with other
6:     detectors */
7:      $\tilde{X}^i(k) = \bigcap_j \tilde{X}^j(k)$ 
8:     /* Check if  $\tilde{X}^i(k)$  is empty */
9:     if  $\tilde{X}^i(k) = \emptyset$  then
10:      return System is faulty
11:     end if
12:   end for

```

The problem using a decentralized detection can be tackled resorting to the techniques in the literature provided in [28]. The main problem associated with the detector having access to limited local information is that part of the system dynamics is unknown. These uncertainties can be represented by rewriting matrix A in (2) as the sum of a single central matrix A_0 with parameter-dependent terms:

$$A = A_0 + \sum_{\ell=1}^{n_\Delta} \Delta_\ell A_\ell \quad (6)$$

where each Δ_ℓ , $\forall 1 \leq \ell \leq n_\Delta$ is a scalar uncertainty with $|\Delta_\ell| \leq 1$, and the A_ℓ , $\ell \in \{1, 2, \dots, n_\Delta\}$ a sufficiently rich collection of matrices so that all the possible values for A can be written as in (6). This can be achieved through principal component analysis or by directly considering an uncertainty for each of the components unknown to the detector [28]. For the sake of simplicity, we denote by $\Delta = [\Delta_1, \dots, \Delta_{n_\Delta}]^T$ the vector of uncertain parameters.

Detecting a fault in a worst-case scenario amounts to find whether there exists possible values for the disturbance and noise signals, initial value and uncertainty parameters such that the dynamics in (2) with $f(k) = 0$ for $\forall k \geq 0$ produce the output of the system y_k^i .

For a particular value of the uncertainty vector Δ , the next exact set-valued estimates for the state can be obtained using (3) (or (4)). By using the notation $X_\delta(k)$ to denote the set produced by (3) using the uncertainty value δ and $\mathcal{H} := \{\delta \in \mathbb{R}^{n_\Delta H} : |\delta| \leq 1\}$ as the hypercube of all possible values for Δ , the state estimate $X(k)$ is given by:

$$X(k) = \bigcup_{\delta \in \mathcal{H}} X_\delta(k). \quad (7)$$

Remark that the set $X(k)$ in (7) is in general non-convex and an iterative update would be computationally expensive. An alternative is to approximate $X(k)$ by a polytopic $\tilde{X}(k) := \text{Set}(M(k), m(k))$ in order to maintain tractability of the algorithm. The objective is to have polytopical SVOs producing the smallest over-approximation of the sets produced by the ideal SVO that would return $X(k)$. The polytopical approximation of (7) that contains all possible states of the system described by (2), with $|\Delta_\ell| \leq 1$ and $f(\cdot) \equiv 0$, at time $k+1$ can be obtained by

$$\tilde{X}(k+1) = \text{co}\left(\bigcup_{\theta \in \mathcal{H}} \text{Set}(M_\theta(k+1), m_\theta(k+1))\right) \quad (8)$$

where $\text{co}(\cdot)$ denotes the convex hull θ are the vertices of the hypercube \mathcal{H} . The convex hull in (8) can be performed using the methods described in [20]. It is straightforward to conclude that $X(k+1) \subseteq \tilde{X}(k+1)$. Moreover, the set-valued estimates $\tilde{X}(k+1)$ have a uniformly bounded volume for all $k \geq 0$ given that there is a hyper-parallelepiped that contains the set $\tilde{X}(k)$ at each time instant with uniformly bounded distance between any two vertices. This result is given in Proposition 1 in [20] for stable systems.

In terms of complexity, the algorithm to compute the set-valued estimates requires the generation of a polytope for each of the vertices θ of the uncertainty hypercube \mathcal{H} , which grow exponentially on the dimension n_x of the state, since the number of vertices of the hypercube to be considered is $2^{n_\Delta H}$.

The aforementioned method for the distributed case compares with the one presented in Section III as a trade-off between knowledge of the system and performance. The centralized solution takes advantage of knowing the dynamics and avoids uncertainty parameters, which means a computationally lighter algorithm since it does not require a convex hull operation, it is optimal in the sense that no conservatism is added if no measurements are discarded due to the horizon and allowed the introduction of the coprime factorization. The decentralized case favors less centralized operations and global knowledge at the expenses of an approximated solution that requires more demanding computations although some techniques like [29] can be employed to reduce the processing overhead.

V. WORST-CASE ATTACK

The SVO-based approach formulated the fault detection as a distinguishability problem between the last H measurements of the real system and those provided by a fault-free model. Regardless of the adopted solution, it is possible to find theoretical bounds for the worst-case undetected attacker signal. The essence of the process being described in the sequel is to define the set of all inputs and initial states such that the output of the two systems would be the same (i.e., that the faulty and fault-free would not be distinguishable). Then by selecting the largest magnitude of the attacker signal within this polytope one can find the worst-case in terms of undetected faults. To accomplish this, we borrow the

definitions from [30] for the distinguishability of systems S_A and S_B :

Let

$$(A_H, b_H) = \text{RFM} \left\{ \text{LFM} \left(\begin{bmatrix} M_H \\ -M_H \\ \tilde{M}_{X_o} \\ \tilde{M}_W \end{bmatrix}, \begin{bmatrix} 0 \\ 0 \\ \tilde{m}_{X_o} \\ m_W \end{bmatrix}, 2n \right), n_u \right\}.$$

with

$$M_H = \left[\begin{array}{cc|c|c} C_A & -C_B & & \\ C_A A_A & -C_B A_B & & \\ C_A A_A^2 & -C_B A_B^2 & & \\ \vdots & \vdots & & \\ C_A A_A^H & -C_B A_B^H & \bar{R} & \bar{J} \end{array} \right],$$

where

$$\bar{R} = \begin{bmatrix} 0 & 0 & \cdots & 0 \\ R_1^1 & 0 & \cdots & 0 \\ R_1^2 & R_2^2 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ R_1^H & R_2^H & \cdots & R_H^H \end{bmatrix} + \bar{Q},$$

$$\bar{Q} = \text{diag}(Q, Q, \dots, Q), \quad Q = [N_A \quad L \quad -N_B],$$

$$R_i^k = [C_A A_A^{k-i} E_A \quad C_A A_A^{k-i} F \quad -C_B A_B^{k-i} E_B],$$

$$\bar{J} = \begin{bmatrix} 0 & 0 & \cdots & 0 \\ J_1^1 & 0 & \cdots & 0 \\ J_1^2 & J_2^2 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ J_1^H & J_2^H & \cdots & J_H^H \end{bmatrix},$$

$$J_i^k = [C_A A_A^{k-i} B_A - C_B A_B^{k-i} B_B],$$

and

$$\begin{aligned} \tilde{M}_{X_o} &= [\text{diag}(M_{X_o}, M_{X_o}) \quad 0 \quad 0 \quad 0], \quad \tilde{m}_{X_o} = \begin{bmatrix} m_{X_o} \\ m_{X_o} \end{bmatrix}, \\ \tilde{M}_W &= \begin{bmatrix} 0 & \text{diag}(M_n, \dots, M_n) & 0 & 0 \\ 0 & 0 & \text{diag}(M_d, \dots, M_d) & 0 \end{bmatrix}, \\ m_W &= [m_n^T \quad \cdots \quad m_n^T \quad m_d^T \quad \cdots \quad m_d^T]^T. \end{aligned}$$

Matrix M_{X_o} and vector m_{X_o} are those defining the polytope for the initial state of both systems S_A and S_B and similarly M_n , m_n and M_d and m_d for the noise and disturbance signals, respectively. Associating with system A the system with the fault (i.e., (2) with the fault f) and with system B the fault-free system (i.e., (2) with $f = 0$), the following optimization problem can be used to find the worst-case magnitude attack that remains undetectable:

$$\gamma_{\min} \geq \max_{A_H x \leq b_H} x^T P_A x. \quad (9)$$

with

$$P_A = \frac{1}{H} \text{diag}(0_{n_d}, \bar{P}, 0_{n_d}, 0_{n_d}, \bar{P}, 0_{n_d}, \dots, 0_{n_d}, \bar{P}, 0_{n_d}).$$

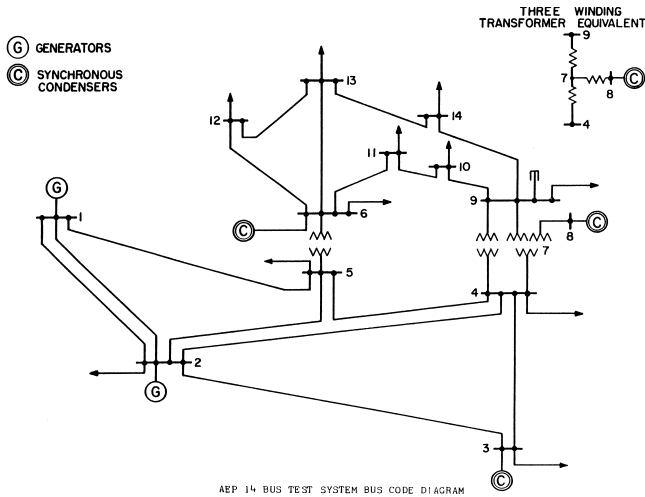


Fig. 2. IEEE 14 bus system test bed example [32]

The matrix \bar{P} defines the quadratic weights to be associated with each fault signal.

The faulty system S_A and fault-free model S_B are $(X_o, \mathbb{R}^{n_u}, W)$ -input distinguishable in H measurements if

$$\frac{1}{H} \sum_{k=0}^H \|\bar{P}f(k)\|^2 > \gamma_{\min}.$$

VI. SIMULATION RESULTS

In this section, simulation results are presented for the testbed network of 14 buses from IEEE with the schematic depicted in Figure 2. The data regarding physical constants from the buses and generator was obtained from MATPOWER 5.0 [31]. We selected a sampling period $T_s = 1s$ to obtain the discrete version of the system corresponding to the model in (2).

The first investigation was to concluded what theoretical bound for the fault signal can be provided when using an SVO-based strategy. To this end, the formulation in Section V was used to solve the optimization problem in (9) and find the value of γ_{\min} that guarantees detection depending on the choice of parameter H . The results are depicted in Figure 3 and where obtained using the BMIBHB solver to solve the concave quadratic problem. The main information to retain from Figure 3 is that a large signal can be concealed in the worst-case for this example if one uses a small value of past measurements.

In order to contrast the theoretical bound with what happens in a typical run (remark that the theoretical bound assumes the worst possible combination of fault signal and disturbance/noise inputs) a value $H = 1$ of past measurements was considered for the next experiments. The centralized solution was simulated with the use of a coprime factorization. A pole placement command in Matlab was used to design the gain K . Results for various constant faults are presented in Figure 4. The main point of interest is the fact that faults are detected in a small number of discrete time instants (less than 10) when the fault constant goes above a

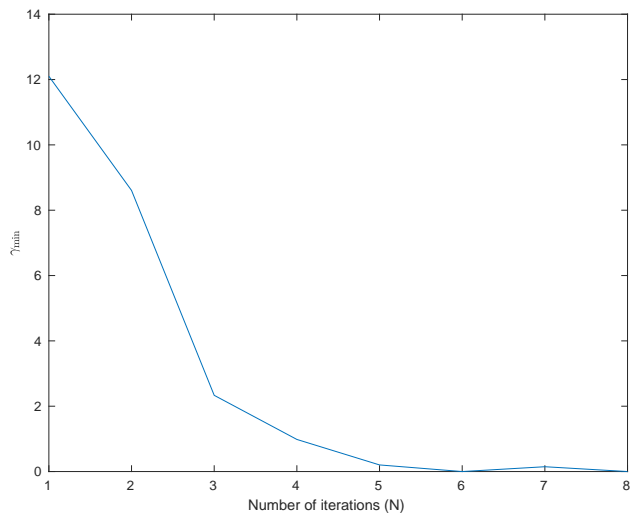


Fig. 3. Evolution of the γ_{\min} as a function of the number of iterations.

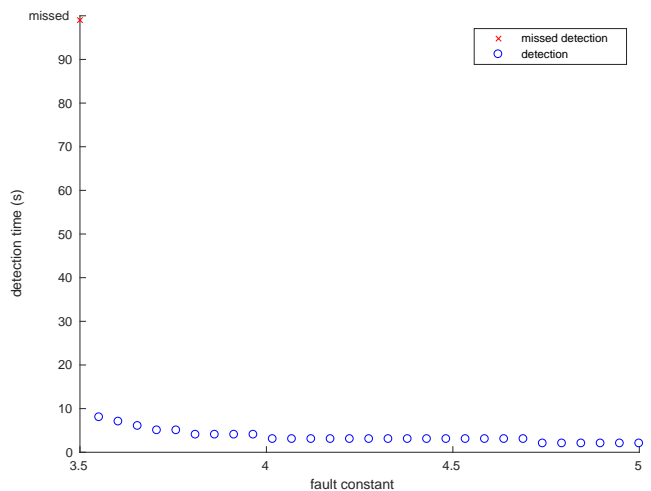


Fig. 4. Detection times for the centralized SVO-based detector employing the coprime technique.

threshold that depends on the actual sequence of disturbance and noise signals.

As a last simulation, 5 detectors with access to a subset of the measurement vector is simulated for the same type of faults. The detection times is depicted in Figure 5. Given that the sets are built using less information, it was expected a worse performance. In this example, the constant fault has to be greater in one unity before a similar detection is achieved. Given that it represents almost a 30% increase, there is a clear need for further research and testing regarding this topic.

VII. CONCLUSIONS

This paper addressed the problem of detecting faults in power networks as an example of a cyber-physical system. By building on results from the literature, it was possible to provide a detector technique based on SVOs that has guarantees in terms of the worst undetectable fault that are obtained using a distinguishability approach. Two scenarios

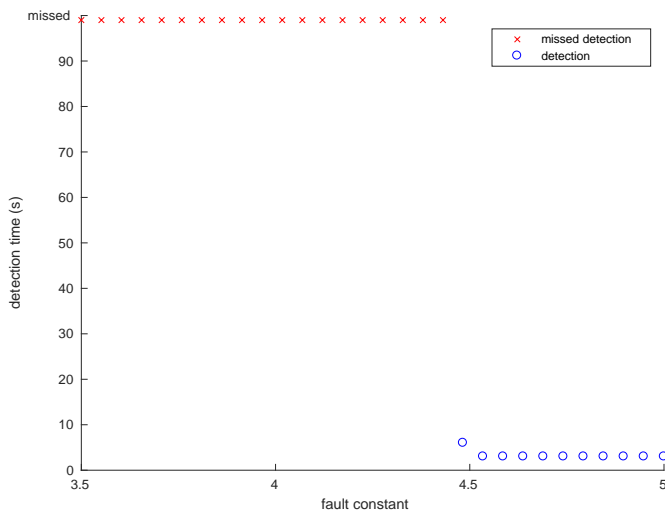


Fig. 5. Detection times for the case of 5 decentralized SVO-based detectors with access to a subset of local measurements.

are presented: a centralized mechanism that builds an SVO for the coprime factorization of the model; and, the decentralized version where just a subset of the measurements are available to the various detectors spread over the network.

Simulation results have shown that for the IEEE 14 bus testbed example, one should select an appropriate horizon size as to avoid large undetected faults that are masked by the disturbance and noise signals. In addition, the experiments suggest that when the detector is successful, it takes a small number of discrete time steps to signal the presence of a fault. In addition, the SVOs are capable of detecting deviations from the model for the disturbances and declaring faults whenever the model is not compatible with the measurements.

REFERENCES

- [1] A. Metke and R. Ekl, "Security technology for smart grid networks," *IEEE Transactions on Smart Grid*, vol. 1, no. 1, pp. 99–107, June 2010.
- [2] M. Amin, "Guaranteeing the security of an increasingly stressed grid," *IEEE Smart Grid Newsletter*, Feb. 2011.
- [3] X. Fang, S. Misra, G. Xue, and D. Yang, "Smart grid 2014; the new and improved power grid: A survey," *IEEE Communications Surveys Tutorials*, vol. 14, no. 4, pp. 944–980, Fourth 2012.
- [4] D. Silvestre, P. Rosa, R. Cunha, J. Hespanha, and C. Silvestre, "Gossip average consensus in a byzantine environment using stochastic set-valued observers," in *52nd IEEE Conference on Decision and Control*, Dec 2013, pp. 4373–4378.
- [5] D. Silvestre, P. Rosa, J. Hespanha, and C. Silvestre, "Finite-time average consensus in a byzantine environment using set-valued observers," in *American Control Conference (ACC), 2014*, June 2014, pp. 3023–3028.
- [6] H. Witsenhausen, "Sets of possible states of linear systems given perturbed observations," *IEEE Transactions on Automatic Control*, vol. 13, no. 5, pp. 556 – 558, oct 1968.
- [7] F. Schweppe, "Recursive state estimation: Unknown but bounded errors and system inputs," *IEEE Transactions on Automatic Control*, vol. 13, no. 1, pp. 22 – 28, feb 1968.
- [8] —, *Uncertain Dynamic Systems*. Prentice-Hall, 1973.
- [9] M. Milanese and A. Vicino, "Optimal estimation theory for dynamic systems with set membership uncertainty: An overview," *Automatica*, vol. 27, no. 6, pp. 997 – 1009, 1991.

- [10] M. Kezunovic, "Smart fault location for smart grids," *IEEE Transactions on Smart Grid*, vol. 2, no. 1, pp. 11–22, March 2011.
- [11] K. Manandhar, X. Cao, F. Hu, and Y. Liu, "Detection of faults and attacks including false data injection attack in smart grid using kalman filter," *IEEE Transactions on Control of Network Systems*, vol. 1, no. 4, pp. 370–379, Dec 2014.
- [12] V. Calderaro, C. Hadjicostis, A. Piccolo, and P. Siano, "Failure identification in smart grids based on petri net modeling," *IEEE Transactions on Industrial Electronics*, vol. 58, no. 10, pp. 4613–4623, Oct 2011.
- [13] A. Giani, E. Bitar, M. Garcia, M. McQueen, P. Khargonekar, and K. Poolla, "Smart grid data integrity attacks: characterizations and countermeasures," in *IEEE International Conference on Smart Grid Communications (SmartGridComm)*, Oct 2011, pp. 232–237.
- [14] F. Pasqualetti, F. Dorfler, and F. Bullo, "Cyber-physical attacks in power networks: Models, fundamental limitations and monitor design," in *50th IEEE Conference on Decision and Control and European Control Conference (CDC-ECC)*, Dec 2011, pp. 2195–2201.
- [15] F. Pasqualetti, A. Bicchi, and F. Bullo, "A graph-theoretical characterization of power network vulnerabilities," in *American Control Conference (ACC), 2011*, June 2011, pp. 3918–3923.
- [16] —, "Consensus computation in unreliable networks: A system theoretic approach," *IEEE Transactions on Automatic Control*, vol. 57, no. 1, pp. 90 –104, jan. 2012.
- [17] P. W. Sauer and M. Pai, *Power system dynamics and stability*. Prentice Hall Upper Saddle River, NJ, 1998, vol. 4.
- [18] E. Scholtz, "Observer-based monitors and distributed wave controllers for electromechanical disturbances in power systems," Ph.D. dissertation, Massachusetts Institute of Technology, 2004.
- [19] A. Chakraborty, J. Chow, and A. Salazar, "A measurement-based framework for dynamic equivalencing of large power systems using wide-area phasor measurements," *IEEE Transactions on Smart Grid*, vol. 2, no. 1, pp. 68–81, March 2011.
- [20] P. Rosa and C. Silvestre, "Fault detection and isolation of LPV systems using set-valued observers: An application to a fixed-wing aircraft," *Control Engineering Practice*, vol. 21, no. 3, pp. 242 – 252, 2013.
- [21] D. Silvestre, P. Rosa, J. P. Hespanha, and C. Silvestre, "Fault detection for LPV systems using set-valued observers: A coprime factorization approach," *Systems & Control Letters*, vol. 106, pp. 32 – 39, 2017.
- [22] J. Shamma and K.-Y. Tu, "Set-valued observers and optimal disturbance rejection," *IEEE Transactions on Automatic Control*, vol. 44, no. 2, pp. 253 –264, feb 1999.
- [23] S. Keerthi and E. Gilbert, "Computation of minimum-time feedback control laws for discrete-time systems with state-control constraints," *IEEE Transactions on Automatic Control*, vol. 32, no. 5, pp. 432 – 435, may 1987.
- [24] J. Telgen, "Minimal representation of convex polyhedral sets," *Journal of Optimization Theory and Applications*, vol. 38, no. 1, pp. 1–24, 1982.
- [25] P. Rosa, C. Silvestre, and M. Athans, "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*, vol. 24, no. 17, pp. 2928–2942, 2014.
- [26] D. Silvestre, P. Rosa, J. P. Hespanha, and C. Silvestre, "Set-based fault detection and isolation for detectable linear parameter-varying systems," *International Journal of Robust and Nonlinear Control*, vol. 27, no. 18, pp. 4381–4397, 2017, rnc.3814.
- [27] K. Zhou, J. C. Doyle, and K. Glover, *Robust and Optimal Control*. Upper Saddle River, NJ, USA: Prentice-Hall, Inc., 1996.
- [28] D. Silvestre, P. Rosa, J. P. Hespanha, and C. Silvestre, "Stochastic and deterministic fault detection for randomized gossip algorithms," *Automatica*, vol. 78, pp. 46 – 60, 2017.
- [29] —, "Self-triggered and event-triggered set-valued observers," *Information Sciences*, vol. 426, pp. 61 – 86, 2018.
- [30] P. Rosa, "Multiple-model adaptive control Multiple-Model Adaptive Control of Uncertain LPV Systems," Ph.D. dissertation, Technical University of Lisbon, Lisbon, Portugal, 2011.
- [31] R. D. Zimmerman, C. E. Murillo-Sanchez, and R. J. Thomas, "Matpower: Steady-state operations, planning, and analysis tools for power systems research and education," *IEEE Transactions on Power Systems*, vol. 26, no. 1, pp. 12–19, Feb 2011.
- [32] U. of Washigton. (2015, March). [Online]. Available: <http://www.ee.washington.edu/research/pstca/>