Distributed Fault Detection and Isolation with Imprecise Network Models

Iman Shames, André M. H. Teixeira, Henrik Sandberg, Karl H. Johansson

***Abstract*— In this paper we consider the problem of Distributed Fault Detection and Isolation (D-FDI) in large networked systems with imprecise models. Taking a previously proposed D-FDI scheme for a given initial network model, we analyze its performance under small changes in the network graph, namely the addition or removal of edges. Under some assumptions, it is shown that for this kind of perturbations there exist suitable thresholds for which fault detection and isolation is achieved. As our second contribution, we propose solutions to accomplish D-FDI with considerably lower computational burden, while handling imprecise network models. Numerical experiments demonstrating the effectiveness of the proposed solution are presented, taking the IEEE 118 bus power network as an example.**

I. Introduction

Critical infrastructures such as power grids, water distribution networks, and transport systems are examples of cyber-physical systems. These systems consist of large-scale physical processes monitored and controlled by SCADA (supervisory control and data acquisition) systems running over a heterogeneous set of communication networks and computers. Although the use of such powerful software systems adds flexibility and scalability, it also increases the vulnerability to hackers and other malicious entities who may perform cyber attacks through the IT systems [1], [2].

A holistic approach to security of SCADA systems is important because of the complex coupling between the physical process and the distributed software system. Unfortunately a theory for such system security lacking. Increasing the security by adding encryption and authentication schemes helps to prevent some cyber attacks by making them harder to succeed but it would be a mistake to rely solely on such methods, as it is well-known that the overall system is not secured because some of its components are. A method to increase security of networked control systems involve the design of control algorithms that are robust to the effects of cyber attacks [3]–[6] and monitoring schemes to detect anomalies in the system caused by attacks [7]. This paper focus on the latter and uses fault detection and isolation (FDI) to design a distributed FDI scheme for a network of interconnected second-order linear systems *where the exact model of the network is not known to the nodes*.

There are various ways to detect and isolate a fault in a system [8]–[11]. Observer-based approaches have been well studied and some of these methods have been proposed for power systems [12], [13]. However, distributed FDI for systems comprised of a network of autonomous nodes is still in its infancy. The results is presented in [7], [14]–[16] can be considered as the first steps in distributed fault detection and isolation in networks.

In this paper, we first consider the case where a fault detection mechanism as outlined in [15] is in place. In this case we address the question of how to accomplish the task of distributed fault detection and isolation if the precise model of the network is not available to each of the nodes. More precisely, we outline the minimum amount of information that is sufficient for a node to achieve fault detection and isolation using its local measurements.

The outline of the paper is as follows. In the next section we describe the distributed fault detection and isolation (D-FDI) method that this work is based on. In Section III we study the problem of interest that is how to distributedly detect and isolate faults when the network model is not precise using the method outlined in Section II. In Section IV we propose methods to reduce the computational burden of the method described in Section II. In doing so, we propose a distributed fault detection and isolation method that requires less computation than the one presented in III and is capable of handling imprecise network models. Some numerical examples are given in Section V. Concluding remarks are presented in the last section.

II. D-FDI for Faulty Nodes

Consider a network of N interconnected systems and let $\mathcal{G}(\mathcal{V}, \mathcal{E}, \mathcal{A})$ be the underlying graph of this network, where $\mathcal{V} = \{i\}_1^N$ is the vertex set with $i \in \mathcal{V}$ corresponding to node i, $\mathcal{E} \subseteq \mathcal{V} \times \mathcal{V}$ is the edge set of the graph, and $\mathcal{A} \in \mathbb{R}^{N \times N}$ is the weighted adjacency matrix with nonnegative entries. The undirected edge $\{i, j\}$ is incident on vertices i and j if nodes i and j share a communication link, in which case the corresponding entry in the adjacency matrix $[\mathcal{A}]_{ij}$ is positive and reflects the edge weight. The out-degree of node i is $\deg(i) = \sum_{j \in \mathcal{N}_i} [\mathcal{A}]_{ij}$, where $N_i = \{j \in \mathcal{V} : \{i, j\} \in \mathcal{E}\}$ is the neighbourhood set of i. The degree matrix $\Delta(\mathcal{G}) \in \mathbb{R}^{N \times N}$ is a diagonal matrix defined as

$$[\Delta]_{ij} = \begin{cases} \deg(i) & , \ i = j \\ 0 & , \ i \neq j \end{cases} .$$

The weighted Laplacian of $\mathcal{G}$ is defined as $\mathcal{L}(\mathcal{G}) = \Delta - \mathcal{A}$. Moreover, assume that of state each node is given by $x_i(t) \in \mathbb{R}^2$. Furthermore, we introduce the following definitions.

This work was supported in part by the European Commission through the VIKING project, the Swedish Research Council, the Swedish Foundation for Strategic Research, the Knut and Alice Wallenberg Foundation

The authors are with ACCESS Linnaeus Centre, Electrical Engineering, Royal Institute of Technology, Stockholm, Sweden. {imansh,andretei,hsan,kallej}@kth.se

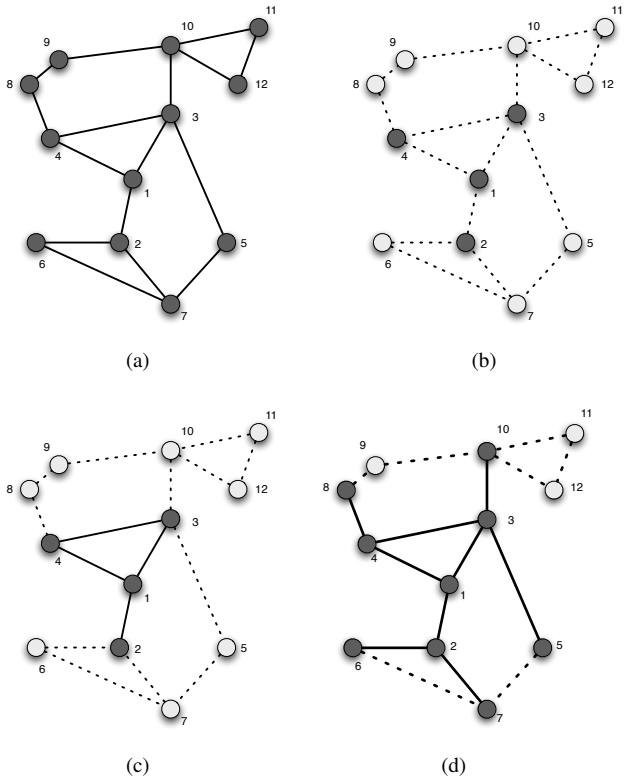


Fig. 1. (a) A network with 12 nodes. (b) The set of one-hop neighbours of node 1 are nodes $\{2, 3, 4\}$ and are coloured darker. (c) The one-hop neighbourhood graph of node 1 is the set of dark nodes connected by solid lines. (d) The graph represented by dark nodes that are connected to each other by solid lines is the proximity graph of node 1.

Definition 1 (ℓ-hop Neighbour Set of Node i): We call the set $\mathcal{N}_i^\ell \subset \mathcal{V}$ the ℓ-hop neighbour set of node i where $v \in \mathcal{N}_i^\ell$ if there is a path of length at most ℓ between i and v.

Definition 2 (ℓ-hop Neighbourhood Graph of Node i): We call the graph $\mathcal{G}_i^\ell(\mathcal{N}_i^\ell, \mathcal{E}_i^\ell) \subset \mathcal{G}(\mathcal{V}, \mathcal{E})$ the ℓ-hop neighbourhood graph of node i where $\{v, u\} \in \mathcal{E}_i^\ell$ if $\{v, u\} \in \mathcal{E}$ and $u, v \in \mathcal{N}_i^\ell$.

Remark 1: For the case where $\ell = 1$, we drop the superscript 1 for the ease of notation. Moreover, $N_i \triangleq |\mathcal{N}_i|$.

Definition 3 (Proximity Graph of Node i): We call the graph $\mathcal{P}_i(\mathcal{N}_i \cup \overline{\mathcal{N}}_i, \mathcal{E}_i \cup \overline{\mathcal{E}}_i) \subset \mathcal{G}(\mathcal{V}, \mathcal{E})$ the proximity graph of node i where $\{v, u\} \in \mathcal{E}_i$ if $\{v, u\} \in \mathcal{E}$ and $u, v \in \mathcal{N}_i$. Moreover, $\overline{\mathcal{N}}_i$ is the set of all the nodes in the network that are not in $\mathcal{N}_i$ but share a link with at least one of the nodes in $\mathcal{N}_i$, and $\overline{\mathcal{E}}_i$ is the set of all edges incident on at least one of the nodes in $\mathcal{N}_i$ that are not in $\mathcal{E}_i$.

Examples for the objects defined in Definitions 1-3 are given in Fig. 1.

In this paper we focus on the case where $n = 2$. For the case where $n = 2$ the state of each node, $x_i(t) = [\xi_i(t)\ \zeta_i(t)]^\top$, is governed by

$$\dot{\xi}_i(t) = \zeta_i(t) \tag{1a}$$

$$\dot{\zeta}_i(t) = u_i(t) + v_i(t), \tag{1b}$$

where $v_i(t)$ is a scalar known external input, ξ_i, ζ_i are the scalar states, and u_i is the control given by the linear control law

$$u_i(t) = -\kappa_i \zeta_i(t) + \sum_{j \in N_i} w_{ij} \left[(\xi_j(t) - \xi_i(t)) + \mu(\zeta_j(t) - \zeta_i(t)) \right], \tag{2}$$

where $w_{ij} \in \mathbb{R}_{>0}$, and $\kappa_i, \mu \in \mathbb{R}_{\geq 0}$ for $i, j = 1, \ldots, N$. In this case, assume each node i measures

$$y_i(t) = C_i x(t) \tag{3}$$

where $x(t) = [\xi_1(t), \ldots, \xi_N(t), \zeta_1(t), \ldots, \zeta_N(t)]^\top$, and $C_i = [\bar{C}_i^\top \ \bar{C}_i^\top]^\top$, with $\bar{C}_i \in \mathbb{R}^{N_i \times N}$ being a full row rank matrix where each of the rows have all zero entries except for one entry at the j-th position that corresponds to those nodes that are neighbours of i. The overall equation of the network becomes:

$$\dot{x}(t) = Ax(t) + Bv(t) \tag{4}$$

where

$$A = \begin{bmatrix} 0_N & I_N \\ -\mathcal{L} & -\mu\mathcal{L} - \overline{K} \end{bmatrix}, \tag{5}$$

$\mathcal{L}$ is the weighted Laplacian matrix associated with the network where w_{ij} is the weight of edge $\{i, j\}$, and $\overline{K} = diag(\kappa_1, \ldots, \kappa_N)$. We say that node $k \in \mathcal{V}$ is faulty if for some functions $f_{\xi k}(t)$ and $f_{\zeta k}(t)$ not identical to zero either $\dot{\xi}_k(t) = \zeta_k(t) + f_{\xi k}(t)$, or $\dot{\zeta}_k(t) = u_k(t) + v_k(t) + f_{\zeta k}(t)$.

Remark 2: The variables ξ_i and ζ_i can be interpreted as position and velocity of node i, respectively, for a mobile system, or as phase and frequency in the context of interconnected synchronous power system generators and motors.

Assumption 1: We focus on the case where there is at most one faulty node, $j \in \mathcal{V}$, in the formation.

Remark 3: The control law described by (2) is a general form of the following well-known control laws:

$$u_i^1(t) = -\kappa_i \zeta_i(t) + \sum_{j \in \mathcal{N}_i} w_{ij}(\xi_j(t) - \xi_i(t)), \tag{6}$$

$$u_i^2(t) = \sum_{j \in \mathcal{N}_i} w_{ij} \left[(\xi_j(t) - \xi_i(t)) + \mu(\zeta_j(t) - \zeta_i(t)) \right]. \tag{7}$$

The functions $f_{\xi k}(t)$ and $f_{\zeta k}(t)$ are denoted fault signals. It is assumed that the faulty node injects fault in only one of the states and we focus on the case where the fault occurs in $\dot{\zeta}_k(t)$. The case where the fault may occur in $\dot{\xi}_k(t)$ is very similar.

To achieve the fault detection and isolation task each node i considers $|\mathcal{N}_i|$ different models of the form:

$$\dot{x}^i(t) = Ax^i(t) + Bv(t) + b_k^i f_k(t) \tag{8}$$

where b_k^i is a vector of zeros except for the k-th entry, and $k \in \mathcal{N}_i$. For each of these systems an observer is constructed such that the estimates are insensitive to $b_k^i f_k(t)$. Note that, each node is monitoring its closest neighbors for misbehavior. Let $\hat{x}_k^i(t)$ denote the estimate of the states of the model with its associated b_k^i and calculated by node i.

An unknown input observer (UIO) for each of these systems is described by:

$$\begin{aligned} \dot{z}_k^i(t) &= F_k^i z_k^i(t) + T_k^i B v(t) + K y_i(t) \\ \hat{x}_k^i(t) &= z_k^i(t) + H_k^i y_i(t), \end{aligned} \tag{9}$$

where $z_k^i(t) \in \mathbb{R}^n$ is the observer's state. The observer matrices must be designed to achieve the decoupling from the unknown input and meet requirements on the stability of the observer. Choosing the matrices $F_k^i, T_k^i, K_k^i, H_k^i$ to satisfy the following conditions [11]

$$\begin{aligned} &F_k^i = (A - H_k^i C_i A - K_k^i C), \quad T_k^i = (I - H_k^i C_i) \\ &K_k^i = K_k^i + K_k'^i, \quad K_k'^i = F_k^i H_k^i, \quad (H_k^i C_i - I) b_k^i = 0, \end{aligned} \tag{10}$$

and F_k^i be Hurwitz, we have the estimation error dynamics

$$\dot{e}_k^i(t) = F_k^i e_k^i(t) - T_k^i \sum_{m \in \mathcal{N}_i \setminus \{k\}} b_m f_m(t). \tag{11}$$

Define

$$r_k^i(t) \triangleq C_i e_k^i(t), \tag{12}$$

where $e_k^i(t) = x(t) - \hat{x}_k^i(t)$.

Definition 4: A residual $r_j^i(t)$ is a fault indicator function that satisfies

$$\|r_j^i(t)\| = 0 \Leftrightarrow \|f_k(t)\| = 0 \quad \forall j \neq k \in \mathcal{N}_i.$$

Note that the residual dynamics are driven by the j-th fault if $T_k^i b_{f_j} \neq 0, k \neq j$.

We introduce the following detection and isolation condition for fault $f_j(t)$,

$$\begin{aligned} &\left\|r_j^i(t)\right\| < \Theta_i \\ &\left\|r_k^i(t)\right\| \geq \Theta_i \ , \forall j \neq k, \end{aligned} \tag{13}$$

where $\Theta_i > 0$ is an isolation threshold.

Now, using Algorithm 1 a faulty node j can be detected by all the nodes in $\mathcal{N}_j$. However, all the other nodes in the network only detect the existence of a fault in the network and the exact identity of the faulty node is unknown to them. For the proof of existence of the required UIOs in the aforementioned interconnected systems see [15].

Remark 4: For the ease of notation we drop the superscript i from the variable names for the rest of this paper.

Algorithm 1 D-FDI of Faulty Nodes at Node i

for $k \in \mathcal{N}_i$ **do**
  Generate $r_k(t)$.
end for
if $\exists j : \ \|r_j(t)\| < \Theta_{f_j} \ \& \ \|r_k(t)\| \geq \Theta_{f_k} \ \forall k \in \mathcal{N}_i \neq j$ **then**
  Node j is faulty.
else if $\|r_k(t)\| \geq \Theta_{f_k} \ \forall k \in \mathcal{N}_i$ **then**
  There exists a faulty node $\ell \in \mathcal{V} \setminus \mathcal{N}_i$.
else if $\|r_k(t)\| < \Theta_{f_k} \ \forall k \in \mathcal{N}_i$ **then**
  There is no faulty node in the network.
end if

We conclude this section with the following remark.

Remark 5: If a node j is faulty, all the nodes in the network detect that there exists a faulty node in the network unless the fault signal happens to coincide with a system zero. However, only the nodes in the one-hope neighbourhood of j can isolate node j as the faulty node in the network.

III. D-FDI in the Presence of Imprecise Network Model

As described earlier to construct the bank of observers to achieve D-FDI the knowledge of matrix A and as a result the full knowledge of the network model and the interconnection of the nodes is necessary. In this section we consider the case where after the observers are designed under a known network model and interconnection graph, some edges are removed. Later, we show that to be able to have a functioning D-FDI scheme the full knowledge of the network is not necessary.

Now we are ready to pose the first problem of interest.

Problem 1: Consider the network described above, and a bank of observers as described in Section II for fault detection using the known graph of the network. Now, consider that the network loses $l \in \mathbb{N}$ edges. What are the conditions that ensure that the existing observers at node i still can detect the occurrence of fault in the network?

Then we address this more general problem.

Problem 2: What is the minimum sufficient knowledge about a network that should be available to each node i to be able to design the necessary UIOs to implement Algorithm 1 ?

We first address Problem 1. Consider the case where we design a bank of UIO to estimate the states of the neighbours of node i, recall that we have the following observer error and residual dynamics

$$\begin{aligned} \dot{e}_k(t) &= F_k e_k(t) - T_k \sum_{m \in \mathcal{N}_i \setminus \{k\}} b_m f_m(t) \\ r_k(t) &= C_i e_k(t). \end{aligned} \tag{14}$$

Imagine l edges are lost in the network, hence

$$\begin{aligned} A_\ell &= A + \Delta A \\ C_{i\ell} &= C_i + \Delta C_i \end{aligned} \tag{15}$$

where A_ℓ is the new coupling matrix after the edge loss, ΔA is a perturbation matrix corresponding to the lost edges, $C_{i\ell}$ is the new measurement matrix and ΔC_i is the associated perturbation. We have the following assumption.

Assumption 2: The network remains connected after losing l edges.

Using the existing parameters of the aforementioned UIO (computed under the assumption of no edge loss) for the error dynamics we have

$$\begin{aligned} \dot{e}_k(t) =& F_k e_k(t) + \Delta A x(t) + H_k C_i \Delta A x(t) \\ &+ H_k \Delta C_i \Delta A x(t) - K_k \Delta C_i x(t) \\ &- T_k \sum_{m \in \mathcal{N}_i \setminus \{k\}} b_m f_m(t). \end{aligned} \tag{16}$$

If any of the removed edges had been connecting i to one of its neighbours, the error dynamics is not necessarily stable

and the observers do not converge. Hence, the following observation.

Observation 1: If a bank of observers is constructed at node i with the full knowledge of the network and at least one of the lost edges is in $\mathcal{E}_i$, the bank of observers should be calculated again taking into account the new network.

However, if the link had not been connecting i to any of its neighbours, we have $\Delta C_i = 0$. It is easy to check

$$\begin{aligned}\dot{e}_k(t) =& F_k e_k(t) + \Delta A x(t) + H_k C_i \Delta A x(t) \\ & - T_k \sum_{m \in \mathcal{N}_i \setminus \{k\}} b_m f_m(t).\end{aligned} \tag{17}$$

The error dynamics described by (17), in the presence of no faults for $m \in \mathcal{V} \setminus \{k\}$, $f_m(t) = 0$, becomes

$$\dot{e}_k(t) = F_k e_k(t) + (I + H_k C_i)\Delta A x(t). \tag{18}$$

The error dynamics described by (18) is stable due to F_k being Hurwitz and the fact that $\Delta A x(t)$ goes exponentially fast to zero when there is no fault in the network. Consequently $r_k(t) = C_i(t)e_k(t)$ goes to zero when there is no fault in the system, although, the UIO parameters are designed for a different interconnection network. This result helps us to address Problem 2. The knowledge of the interconnection network beyond the proximity graph of a node i is not necessary for Algorithm 1 to be used for detection of a faulty node. Formally, we have the following result.

Proposition 1: Consider a node i in an arbitrary connected network of N interconnected nodes and Algorithm 1 with the bank of UIOs calculated for this network. Using Algorithm 1 and the existing bank of observers, node i can detect the existence of a faulty node in any connected network where the proximity graph of node i is the same as the original network.

However, the faulty node cannot be isolated using the condition given by (13) when the network model is imprecise. Before proposing a rationale for this assertion we recall this result from [17]:

Proposition 2: If the coefficient matrix $A(t)$ is continuous for all $t \in [0, \infty)$ and constants $a > 0$, $b > 0$ exist such that for every solution of the homogeneous differential equation

$$\dot{x}(t) = A(t)x(t)$$

one has

$$\|x(t)\| \leq \beta \|x(t_0)\| e^{-\alpha(t-t_0)}, \qquad 0 \leq t_0 < t < \infty$$

then for each $f(t)$ bounded and continuous on $[0, \infty)$, every solution of the nonhomogeneous equation

$$\dot{x}(t) = A(t)x(t) + f(t), \qquad x(t_0) = 0$$

is also bounded for $t \in [0, \infty)$.

It is also proved in [17] that if $\|f(t)\| \leq \sigma_f < \infty$ then the solution of the perturbed system satisfies

$$\|x(t)\| \leq \beta \|x(t_0)\| e^{-\alpha(t-t_0)} + \frac{\beta \sigma_f}{\alpha}\left(1 - e^{-a(t-t_0)}\right). \tag{19}$$

In the problems that we address in this paper matrix system A is time-invariant and the differences between states go to zero exponentially fast, i.e. for all $i, j \in \mathcal{V}$, $|\xi_i - \xi_j| \to 0$ and $|\zeta_i - \zeta_j| \to 0$ exponentially fast. Hence, in the presence of fault signal $f(t)$, where $\|f(t)\| \leq \sigma_f < \infty$, from [17] there exists a τ such that

$$\|\bar{x}(\tau)\| \leq \frac{\beta \sigma_f}{\alpha} + \bar{\delta} \tag{20}$$

where $\bar{x} = [\xi_1 - \xi_n, \ldots, \xi_{n-1} - \xi_n, \zeta_1 - \zeta_n, \ldots, \zeta_{n-1} - \zeta_n]^\top$, α and β are described in Proposition 2, and $\delta \ll 1$. Thus, for all $i, j \in \mathcal{V}$ there exists a $\delta \leq \frac{b\sigma_f}{a} + \bar{\delta}$ where $|\xi_i - \xi_j| \leq \delta$ and $|\zeta_i - \zeta_j| \leq \delta$. Now assume that for $m \in \mathcal{V} \setminus \{j\}$, $f_m(t) = 0$, and $f_j(t) \neq 0$; then $f(t) = b_j f_j(t)$. Now, we focus on $\|(I + H_k C_i)\Delta A x\|$. Further, assume that ΔA corresponds to the uncertainty in (or loss of) l links, then we have, $\|(I + H_k C_i)\Delta A x\| \leq 4l\delta$ (Note that $\|I + H_k C_i\| \leq 2$). Under the assumption that only node j is faulty, for the error dynamics of the UIOs we have

$$\begin{aligned}\dot{e}_k(t) &= F_k e_k(t) + (I + H_k C_i)\Delta A x(t) \\ &\quad - T_k b_j f_j(t), \quad k \in \mathcal{N}_i \setminus \{j\} \\ \dot{e}_j(t) &= F_j e_j(t) + (I + H_k C_i)\Delta A x(t).\end{aligned} \tag{21}$$

The same as before according to Proposition 2 the error of the UIO monitoring the neighbour node $k \neq j$ converges to a ball around zero and a radius ρ_k such that

$$\rho_k \leq \frac{\beta_k \gamma_k}{\alpha_k} + \bar{\delta} \tag{22}$$

for some α_k and δ_k, and $\|Ax(t) - T_k b_j f_j(t)\| \leq \gamma_k$. Assuming that the values of α_k and β_k are the same for all UIOs and equal to $\bar{\alpha}$ and $\bar{\beta}$ [1] we have

$$\begin{aligned}\rho_k &\leq \frac{\bar{\beta}\|(I + H_k C_i)\Delta A x(t) - T_k b_j f_j(t)\|}{\bar{\alpha}} + \bar{\delta} \\ &\leq \frac{\bar{\beta}\|(I + H_k C_i)\Delta A x(t)\| + \bar{f}_i}{\alpha} + \bar{\delta} \\ &\leq \frac{4\bar{\beta} l\delta + \bar{f}_i}{\bar{\alpha}} + \bar{\delta}\end{aligned} \tag{23}$$

where $\bar{f}_i = \max_{k \in \mathcal{N}_i \setminus \{j\}} (\|T_k b_j f_j(t)\|)$. The error dynamics converges to a ball around zero with the radius ρ_j where

$$\rho_j \leq \frac{\bar{\beta}\gamma_j}{\bar{\alpha}} + \bar{\delta}, \tag{24}$$

and $\gamma_j = 4l\delta$. Assuming that none of lost (uncertain) edges belongs to $\mathcal{P}_i$, then one can get a tighter value on γ_j, that is $\gamma_j = 2l\delta$.

The difference between the values of the upper bound on the magnitude of error in observers monitoring the faulty node comparing with the magnitude of the error in the observers monitoring other nodes serves as a guideline to choose the threshold for the fault detection conditions as described by (13). In what comes next, we propose another method to circumvent the issue of selecting a proper threshold value in the face of uncertainty in links.

[1] This assumption is in fact a feasible one and we elaborate on it later in the paper.

Observation 2: For a given monitoring node i, the poles of F_k^i can be placed arbitrarily provided that $(A - H_k^i C_i A,\ C_i)$ is observable, which is equivalent to say that the system (A, b_k^i, C_i) does not have transmission zeros. If this is the case for all k, then $\{F_k^i\}$ can be designed to have the same poles and consequently we have $\alpha_k = \alpha$ and $\beta_k = \beta$ for all k.

IV. Reducing the Complexity of the Proposed D-FDI Method

For implementation of the method introduced earlier in this paper, at each node it is required to have one observer corresponding to each of the neighbours. Each of these observers has $2N$ states. So at each node i, $2N|N_i|$ states are estimated, which puts a heavy computational burden on each of the nodes as N increases. For example a network with 10 nodes the observer bank in node a node with 5 neighbours would require a total of 100 states. So it is desired to reduce the amount of computation necessary for the FDI scheme to succeed in detection the existence of a fault in the general network and isolation of the faulty node among the neighbours of a given node $i \in \mathcal{V}$. This is achieved via reducing the dimensions of the UIOs used in D-FDI where only local models of the network are considered.

Consider a fault free network as before:

$$\dot{x}(t) = Ax(t) + Bv(t) \tag{25}$$

For the subnetwork of this network with $\mathcal{P}_i$ as its graph we have

$$\dot{\phi}^i(t) = A_{\mathcal{P}}^i \phi^i(t) + \psi^i(t) + B_{\mathcal{P}}^i v_{\mathcal{P}}^i(t), \tag{26}$$

where $\phi_i = [\xi_i, \xi_{i_1}, \ldots, \xi_{i_{N_i}}, \zeta_i, \zeta_{i_1}, \ldots, \zeta_{i_{N_i}}]$, $\psi_i = [\xi_{\bar{i}_1}, \ldots, \xi_{\bar{i}_{N_i}}, \zeta_{\bar{i}_1}, \ldots, \zeta_{\bar{i}_{N_i}}]$, $\bar{i}_m, i_m \in \mathcal{N}_i \cup \overline{\mathcal{N}}_i$, and particularly $i_{|\mathcal{N}_i|+1}$ to $i_{|\mathcal{N}_i \cup \overline{\mathcal{N}}_i|}$ correspond to the nodes in $\overline{\mathcal{N}}_i$. Moreover, $A_{\mathcal{P}}^i$ is the matrix associated with the network with $\mathcal{P}_i$ as its graph, $\psi^i(t)$ is a vector with zero entries except for the entries corresponding to nodes $m \in \overline{\mathcal{N}}_i$, $v_{\mathcal{P}}^i(t)$ is the known input vector in this subnetwork, and $B_{\mathcal{P}}^i$ is the input matrix associated with these inputs. We have the following straightforward result for $\psi^i(t)$.

Proposition 3: In the network induced by the proximity graph of node i as described by (26), that is the subnetwork of the fault-free network described by (4), $\psi^i(t)$ goes to zero exponentially fast.

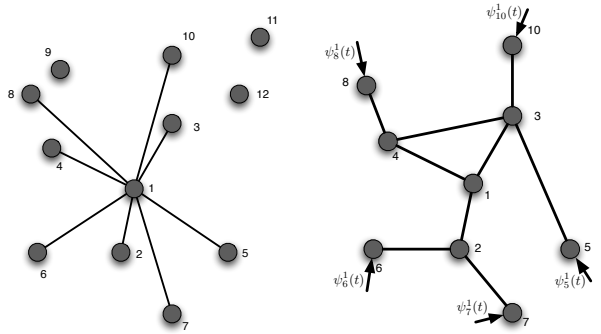
The bank of UIOs at i can be designed for only the subnetwork with $\mathcal{P}_i$ as its graph described by (26). An example of such a subnetwork for the network of Fig. 1 is given in Fig. 2 (b).

In the case where there is no fault in the network, the unknown parts of the real network enter the equation dynamics, as in the previous section, as exponentially decaying signals. So, as before, in this case the detection of a fault in the network can be determined using the bank of UIOs for $\mathcal{P}_i$. Moreover, isolation can be achieved as well via choosing an appropriate threshold value.

However, the selection of the aforementioned threshold might prove be cumbersome, and requires a knowledge of the magnitude of the fault. In what comes next we propose a method to achieve D-FDI using only the full knowledge of the proximity graph without resorting to complicated ways of choosing the threshold value. We first make the following assumption that will be valid until the end of this section.

Assumption 3: Each node $i \in \mathcal{V}$ measures the states of all the nodes in its proximity graph.

An example for the measurement graph of node i is given in Fig. 2(a). As before, to achieve the fault detection and



(a) (b)

Fig. 2. (a) An example for the measurement graph of node i in the network of Fig. 1 under Assumption 3. (b) The subnetwork model for designing a bank of UIOs at node 1 of the network depicted in Fig. 1.

isolation task each node i considers $|\mathcal{N}_i|$ different models of the form:

$$\dot{\phi}^i(t) = A_{\mathcal{P}}^i \phi^i(t) + \psi^i(t) + B_{\mathcal{P}}^i v_{\mathcal{P}}^i(t) + b_k^{i\star} f_k(t) \tag{27}$$

where $b_k^{i\star}$ is a vector of zeros except for the entry corresponding to node $k \in \mathcal{N}_i$ that is equal to one. We rewrite (27) as

$$\dot{\phi}^i(t) = A_{\mathcal{P}}^i \phi^i(t) + B_{\mathcal{P}}^i v_{\mathcal{P}}^i(t) + \begin{bmatrix} B^{i\star} & b_k^{i\star} \end{bmatrix} \begin{bmatrix} \psi^i(t) \\ f_k(t) \end{bmatrix}, \tag{28}$$

with $B^{i\star} = [b_{m_1}^{i\star} \ \ldots \ b_{m_{|\overline{\mathcal{N}}|}}^{i\star}]$, where $b_{m_l}^{i\star}$, $m_l \in \overline{\mathcal{N}}_i$, is a vector of zeros except for the entry corresponding to node $m_l \in \overline{\mathcal{N}}_i$ that is equal to one. For each of these models a UIO is defined that is insensitive to the unknown input $\begin{bmatrix} B^{i\star} & b_k^{i\star} \end{bmatrix} \begin{bmatrix} \psi^i(t) \\ f_k(t) \end{bmatrix}$.

Proposition 4: Consider the distributed control system with a fault in node j given by (26) and local measurments satisfying Assumption 3. If $\mathcal{P}_i$ is connected and $j \in \mathcal{N}_i$, then there exists a UIO for system (28) constructed at node i.

Applying Algorithm 1 for the residuals obtained from these UIOs that their existence is guaranteed by Proposition 4 solves the problem of distributed fault detection and isolation via only local models and measurements.

The method introduced in this section not only reduces the size of the observers, but also it eliminates the need to have an exact network model beyond the proximity graph of a given node for that node to detect and isolate faults in its one-hop neighbourhood. However, it is established that it is possible under the assumption that the node has access to the measurements of the states of its two-hop neighbours.

V. Numerical Examples

In this section we illustrate the solution proposed in Section IV with a power network example. The simulations were carried out using the IEEE 118 bus network example available with the MATPOWER toolbox [18]. The graph of the power network is shown in Fig. 3.

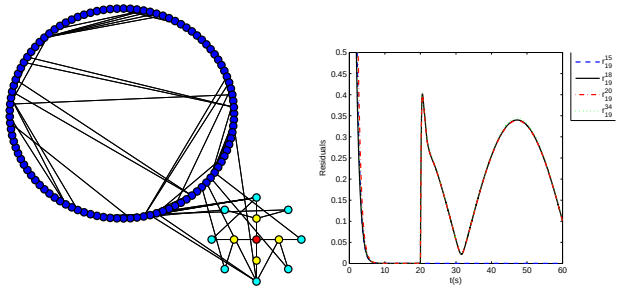


Fig. 3. [left] The graph of the IEEE 118 bus network. Node 19 (red) is the node at the center of the smaller cluster to the right, monitoring its $1-$hop neighbours (yellow). This cluster represents the $2-$hop neighbourhood of node 19. [right] Residuals generated by the UIO bank at node 19.

We considered the classical synchronous machine model [19] for each node of the power network, leading to the global network dynamics as in (4) with

$$A = \begin{bmatrix} 0_N & I_N \\ -\bar{M}\mathcal{L} & -\bar{M}\bar{D} \end{bmatrix}, \quad B = \begin{bmatrix} 0_N & \bar{M} \end{bmatrix}^\top,$$
$$\bar{M} = \text{diag}\left(\frac{1}{m_1}, \cdots, \frac{1}{m_N}\right), \bar{D} = \text{diag}\left(d_1, \cdots, d_N\right),$$

where $m_i > 0$ and $d_i > 0$ are the inertia and damping coefficients of node i and $N = 118$ is the number of buses. Since these coefficients were not available in the example data files, they were randomly generated so that the load buses had considerably lower values than the generator buses, namely $m_g \approx 10^3 m_l$ and $d_g \approx 10^3 d_l$.

In this example, node 19 is monitoring its $1-$hop neighbours for faulty behaviours using the method proposed in Section IV. Thus the only network model knowledge needed is its $2-$hop neighbourhood, the smaller cluster in Fig. 3, which consists of 26 states, as opposed to the 236 states of the global network. Using this smaller model, a bank of UIO was generated according to the discussion in Section II and Section IV.

In the simulations, node 15 exhibits a faulty behaviour after $t = 20s$, which is successfully detected by node 19 as seen in Fig. 3. Furthermore, all the residuals corresponding to other neighbouring nodes become large while the one for node 15 remains at zero. Following Algorithm 1, node 15 is then detected and identified as the faulty node.

VI. Conclusions

The D-FDI scheme proposed in [15] designed using a given initial network model was shown to be robust to the addition or removal of edges. Namely, fault detection and isolation can be achieved using this scheme by choosing suitable thresholds, provided that the proximity graph of the monitoring nodes remains constant.

A solution to reduce the computational complexity of the D-FDI scheme was proposed that reduces the network model required for each observer bank, thus, in addition to being less computationally expensive, is resilient to imprecise network models. Numerical experiments demonstrating the effectiveness of the proposed solution are presented, taking the IEEE 118 bus power network as an example. In this example and for a particular monitoring node, D-FDI was accomplished using models with only 11% of the dimension of the global model.

References

[1] A. A. Cárdenas, S. Amin, and S. S. Sastry, "Secure control: Towards survivable cyber-physical systems," in *First International Workshop on Cyber-Physical Systems (WCPS2008)*, Beijing, China, June 2008, pp. 495–500. [Online]. Available: http://www.truststc.org/pubs/345.html

[2] T. G. Roosta, "Attacks and defenses of ubiquitous sensor networks," Ph.D. dissertation, EECS Department, University of California, Berkeley, May 2008. [Online]. Available: http://www.eecs.berkeley.edu/Pubs/TechRpts/2008/EECS-2008-58.html

[3] N. Lynch, *Distributed Algorithms*, 1st ed. Morgan Kaufmann, 1997. [Online]. Available: http://www.amazon.com/exec/obidos/redirect?tag=citeulike07-20&path=ASIN/1558603484

[4] D. Bauso, L. Giarre, and R. Pesenti, "Lazy consensus for networks with unknown but bounded disturbances," in *Proceedings of the IEEE Conf. on Decision and Control*, New Orleans, LA, December 2007, pp. 2283–2288.

[5] S. Amin, A. Cárdenas, and S. Sastry, "Safe and secure networked control systems under denial-of-service attacks." in *Hybrid Systems: Computation and Control*. Lecture Notes in Computer Science. Springer Berlin / Heidelberg, April 2009, pp. 31–45.

[6] S. Sundaram and C. Hadjicostis, "Distributed function calculation via linear iterations in the presence of malicious agents - part II: Overcoming malicious behavior," in *Proceedings of the American Control Conference*, Seatle, WA, June 2008, pp. 1356–1361.

[7] F. Pasqualetti, A. Bicchi, and F. Bullo, "Distributed intrusion detection for secure consensus computations," in *Proceedings of Control and Decision Conference*, 2007, pp. 5594–5599.

[8] M. A. Massoumnia and G. C. Verghese, "Failure detection and identification," *IEEE Transactions on Automatic Control*, vol. 34, pp. 316–321, 1989.

[9] J. Chen and R. J. Patton, *Robust Model-Based Fault Diagnosis for Dynamic Systems*. Kluwer Academic Publishers, 1999.

[10] R. Isermann, "Model-based fault detection and diagnosis: status and applications," in *Proceedings of the 16th IFAC Symposium on Automatic Control in Aerospace*, St. Petersburg, Russia, June 2004, pp. 71–85.

[11] S. X. Ding, *Model-based Fault Diagnosis Techniques: Design Schemes*. Springer Verlag, 2008.

[12] E. Scholtz and B. Lesieutre, "Graphical observer design suitable for large-scale DAE power systems," in *Proceedings of the IEEE Conf. on Decision and Control*, Cancun, Dec. 2008, pp. 2955–2960.

[13] M. Aldeen and F. Crusca, "Observer-based fault detection and identification scheme for power systems," in *IEE Proceedings - Generation, Transmission and Distribution*, vol. 153, no. 1, Jan. 2006, pp. 71–79.

[14] F. Pasqualetti, A. Bicchi, and F. Bullo, "Consensus computation in unreliable networks: A system theoretic approach," *IEEE Transactions on Automatic Control*, 2010, submitted, available online at http://www.fabiopas.it/papers/FP-AB-FB-10a.pdf.

[15] I. Shames, A. M. H. Teixeira, H. Sandberg, and K. H. Johansson, "Distributed Fault Detection for Interconnected Second-Order Systems ," *Automatica*, 2011, to appear.

[16] R. Smith, "A decoupled feedback structure for covertly appropriating networked control systems," in *Proceedings of the 18th IFAC World Congress*, Milano, Italy, August-September 2011.

[17] H. D'Angelo, *Linear Time-Varying Systems: Analysis and Synthesis*. Allyn and Bacon, 1970.

[18] R. D. Zimmerman, C. E. Murillo-Sánchez, and R. J. Thomas, "MATPOWER's extensible optimal power flow architecture," in *Power and Energy Society General Meeting*. IEEE, July 2009, pp. 1–7.

[19] P. Kundur, *Power System Stability and Control*. McGraw-Hill Professional, 1994.