Preprints of the 19th World Congress
The International Federation of Automatic Control
Cape Town, South Africa. August 24-29, 2014

Distributed Detection of Cyber Attacks and Faults for Power Systems

Hiroaki Nishino and Hideaki Ishii *

* *Department of Computational Intelligence and Systems Science Tokyo Institute of Technology, Yokohama 226-8502, Japan*
E-mails: nishino@sc.dis.titech.ac.jp, ishii@dis.titech.ac.jp

Abstract: We consider distributed methods for detection of cyber attacks and faults in power networks. The approach is based on grouping of buses in the system, and for each group, we design filters for detection and isolation of faults applied to the buses within the group. The scheme is distributed in the sense that it uses only locally available data such as the generated power, loads, and power flows. Specifically, a fault detection method based on a geometric approach is applied to two different settings. Depending on the availability of phasor measurement units, we develop indirect and direct methods and compare their characteristics in performance and computation. A numerical example is provided to illustrate the results.

Keywords: Power systems, Cyber security, Fault detection and isolation, Distributed systems

1. INTRODUCTION

In recent years, various large-scale networked control systems have been connected to general purpose networks such as the Internet. While this type of changes in the system structure enables monitoring and operation from remote locations, it has raised serious issues related to cyber security. Control systems have traditionally been secure from malicious intruders mostly because the networks have been closed dedicated ones based on special protocols. Security problems have been studied from control theoretic viewpoints in, e.g., (Mo and Sinopoli (2010); Zhang and Sundaram (2012); Dibagi and Ishii (2014)).

In this context, power systems have received special attention. In addition to being part of the critical infrastructure, the introduction of renewable energies such as solar and wind power will necessarily increase the amount of communication to maintain the safety and the stability of the power grid. Monitoring of power systems is important for its reliable operation. One of the main functions there is state estimation, which provides information regarding the level of synchronization among buses and the power flows in the grid. Due to the slow sampling and the limitation in computation, state estimation has commonly been done in the steady state (Abur and Gómez-Expósito (2004)).

The work of (Liu et al. (2011)) pointed out the vulnerability in such static state estimation techniques. In particular, it was demonstrated that through malicious manipulation of sensor measurement data, estimated states can be modified significantly without being noticed. This result motivated studies on related problems such as (Giani et al. (2011); Sou et al. (2011)). The new sensors known as phasor measurement units (PMUs) allow direct sensing of the phase in the power frequency at high sampling frequencies. Some works such as Zhang et al. (2013) formulate estimation problems assuming that PMUs are available at some buses, resulting in more accurate and robust estimation.

On the other hand, attacks on power systems can also be detected and isolated based on dynamical models of the grid. A common model of active power flows is that of swing equations. In (Shames et al. (2011)), a distributed approach was proposed for such a model with the underlying assumption that at all buses, PMUs are available; this in turn enables the use of fault detection and isolation (FDI) filters employing observers with unknown inputs. In contrast, in (Hashimoto and Hayakawa (2011)), no PMU is assumed and instead only conventional measurements of generated power and loads are utilized. Distributed detection of faults and attacks at each bus is realized through a geometric approach of (Massoumnia et al. (1989)). The work of (Pasqualetti et al. (2011)) proposes a framework for general models of power networks expressed as linear descriptor systems and FDI schemes with robustness properties. For more on general FDI methods, see, e.g., (Ding (2008)).

In this paper, we consider distributed attack detection for power systems with the following features. First, we introduce grouping of the buses and construct an FDI filter for each group. The relation between the sizes of the groups and the achievable level of detection performance is discussed. Second, we aim at detecting highly malicious attacks where sensing data of multiple buses may be manipulated simultaneously in a coordinated manner. Third, we consider two classes of settings in terms of the available measurements. One is based on the conventional measurements as in (Hashimoto and Hayakawa (2011)), and the other is the case when PMUs are placed at some buses. While in both cases, detection of faults and attacks is possible, the difference lies in the quality of isolation by each FDI filter, and consequently in the number of filters necessary for the full FDI.

⋆ This work was supported in part by the Aihara Project, the FIRST program from JSPS, initiated by CSTP and by the CREST program of Japan Science and Technology Agency.

The paper is organized as follows. In Section 2, we introduce the model of power systems subject to attacks/faults and state the problem of fault detection and isolation. In Section 3, the FDI filter technique employed in this paper is reviewed. In Section 4, we provide an indirect detection method for power system. The results are then extended in Section 5 to the case when PMU measurements are available. In Section 6, we examine the proposed method through a numerical example. Concluding remarks are given in Section 7.

We list the notation employed in this paper: For a given matrix $X \in \mathbb{R}^{n\times m}$, the matrix after removing the ith column from X is denoted by $X^i \in \mathbb{R}^{n\times(m-1)}$. Similarly, let $X^{i,j} \in \mathbb{R}^{n\times(m-2)}$ be the matrix after the removal of the ith and jth columns from X. The identity matrix of size $n \times n$ is given by I_n. Let $\mathbf{1}_n$ be the vector in $\mathbb{R}^n$ with all entries equal to 1. The standard basis of $\mathbb{R}^n$ is denoted by $\{e_n^i\}_{i=1}^n$. The Kronecker product is expressed by $\otimes$.

2. PROBLEM FORMATION

In this section, we present the modeling of the power network and the grouping of buses for distributed detection. The problem considered in the paper is then formulated.

2.1 Power System Model with Faults and Grouping

Consider a power system whose network structure is represented by a graph, denoted by $\mathcal{G} := (\mathcal{V}, \mathcal{E})$. Here, the nodes correspond to the buses and the edges are the transmission lines. The total number of buses is n. The node set and the edge set are respectively given by $\mathcal{V} := \{1, \cdots, n\}$ and $\mathcal{E} \subset \mathcal{V} \times \mathcal{V}$. We assume that all nodes are connected to generators or motors. Then, the dynamics of the phase of the complex voltage of the ith bus can be described by the socalled swing equation as (Machowski et al. (2008))

$$m_i\ddot{\delta}_i(t) + d_i\dot{\delta}_i(t) = u_i(t) + f_i(t) - \sum_{j\in\mathcal{N}_i} p_{ij}(t), \quad i = 1, 2, \ldots, n, \tag{1}$$

where m_i is the inertia coefficient, d_i is the damping coefficient, δ_i is the phase angle, u_i represent the power input (the mechanical input minus the load), $\mathcal{N}_i$ is the set of nodes connected to bus i directly (that is, the neighborhood of bus i), p_{ij} is the active power flow from bus i to bus j. Under the condition $\delta_i - \delta_j \approx 0$, this p_{ij} can be approximated through linearization as

$$p_{ij}(t) = |\hat{v}_i||\hat{v}_j|\hat{b}_{ij}(\delta_i(t) - \delta_j(t)),$$

where $|\hat{v}_i|$ and $|\hat{v}_j|$ are respectively the magnitudes of the voltages at buses i and j, $\hat{b}_{ij}$ is the susceptance of the transmission line connecting buses i and j. For simplicity of notation, let $z_{ij} := |\hat{v}_i||\hat{v}_j|\hat{b}_{ij}$ and let $p_{ij}(t) = z_{ij}(\delta_i(t) - \delta_j(t))$.

In this model, faults occurred at bus i are denoted by the signal f_i. This represents unexpected changes in the power generation or consumption. More precisely, f_i is the difference between the true value of the input power and its measured data obtained as u_i. Hence, if any data manipulation is made in the injection power, f_i takes a nonzero value. For example, suppose that the true values of generated power and load are 1200 [W] and 1000 [W], respectively. Then the true power input is $u_i = 1200 - 1000 = 200$. However, if due to manipulation in data, the measured value becomes -100 [W], then we have $u_i = -100$. The difference between these values is represented by the fault signal $f_i = 200 - (-100) = 300$.

It is noted that, in general power systems, some buses are not connected to generators or motors, resulting in algebraic constraints in the system. In the model above, one way to include such load buses in an approximated sense is to set the inertia and damping coefficients small.

In this paper, we develop a detection and isolation method for the fault signals f_i in the power system (1). In particular, the faults may be caused by highly coordinated attacks by malicious intruders. Therefore, we must explicitly consider cases when multiple faults occur simultaneously.

Moreover, the detection is to be done in a distributed manner by using only local information of the system. We introduce a cover of the node set $\mathcal{V}$, denoted by $\{\tilde{\mathcal{V}}_i\}_{i=1}^N$, that is, $\tilde{\mathcal{V}}_i \subset \mathcal{V}$ for $i = 1, \ldots, N$ and $\mathcal{V} = \cup_i \tilde{\mathcal{V}}_i$. Each set $\tilde{\mathcal{V}}_i \subset \mathcal{V}$ in the cover is called a group, and the subgraph consisting of nodes in $\tilde{\mathcal{V}}_i$ is assumed to be connected. Hence, the N groups may have overlaps so that nodes can belong to multiple groups. The design procedure provided in the following is to be applied to each group $\tilde{\mathcal{V}}_i$. Hence, for the ease of notation, we omit the index i and consider a group with g nodes denoted as $\tilde{\mathcal{V}} := \{v_1, \cdots, v_g\}$.

For the detection of faults occurring in the group, locally available data are used. This includes the power inputs u_i and the power flows p_{ij} from all buses in the group as well as those from the immediate neighbors of the group. We will explain more on this point in the next subsection.

2.2 Dynamics of Buses in a Group

Here, we rewrite the model of the power system in (1) for group $\tilde{\mathcal{V}}$ in the vector form. Let the state x be given by $x(t) := \left[x_{v_1}(t)^T \cdots x_{v_g}(t)^T\right]^T$ where $x_i(t) := \left[\delta_i(t)\ \dot{\delta}_i(t)\right]^T$, $i \in \tilde{\mathcal{V}}$. And, let the input be $u(t) := \left[\overline{u}_{v_1}(t) \cdots \overline{u}_{v_g}(t)\right]^T$. Here, we have introduced the modified input $\overline{u}_i(t) := u_i(t) - \sum_{j\in\mathcal{N}_i, j\notin\tilde{\mathcal{V}}} p_{ij}(t)$ by adding the power input and the power flowing from outside the group. Under this modification, we can regard the dynamics of this group to be a closed system and thus can reduce the order of this system.

Besides, we define the fault vector f by

$$f(t) := \left[f_{v_1}(t) \cdots f_{v_g}(t)\right]^T.$$

Based on the setting above, the overall state-space equation of group $\tilde{\mathcal{V}}$ becomes as follows:

$$\dot{x}(t) = (A + L \otimes D)x(t) + Bu(t) + Bf(t), \tag{2}$$

where the matrices A, B, and D are given by

$$A := \begin{bmatrix} \overline{A}_{v_1} & & O \\ & \ddots & \\ O & & \overline{A}_{v_g} \end{bmatrix},\ B := \begin{bmatrix} \overline{B}_{v_1} & & O \\ & \ddots & \\ O & & \overline{B}_{v_g} \end{bmatrix},\ D := \begin{bmatrix} 0 & 0 \\ 1 & 0 \end{bmatrix}.$$

Here, for each $i \in \{v_1, \ldots, v_g\}$, the submatrices $\overline{A}_i$ and $\overline{B}_i$ are defined as

$$\overline{A}_i := \begin{bmatrix} 0 & 1 \\ 0 & -\dfrac{d_i}{m_i} \end{bmatrix}, \ \overline{B}_i := \begin{bmatrix} 0 \\ \dfrac{1}{m_i} \end{bmatrix}.$$

Moreover, in (2), the matrix L is the weighted Laplacian given by

$$[L]_{i,j} := \begin{cases} -\displaystyle\sum_{j \in \mathcal{N}_i \cap \tilde{\mathcal{V}}} \frac{z_{ij}}{m_i} & \text{if } i = j, \\ \dfrac{z_{ij}}{m_i} & \text{if } j \in \mathcal{N}_i \cap \tilde{\mathcal{V}}, \\ 0 & \text{otherwise.} \end{cases}$$

As the output $y(t)$ at the group $\tilde{\mathcal{V}}$, we consider two cases depending on the use of PMUs. In both cases, the power flows p_{ij}, $i, j \in \tilde{\mathcal{V}}$, within the group are assumed available.

(1) The first case is when no PMU is used in the group. The output $y(t)$ is given by

$$y(t) = Cx(t), \tag{3}$$

where the matrix C is given by $C := \begin{bmatrix} \overline{C}_{v_1}^T & \cdots & \overline{C}_{v_g}^T \end{bmatrix}^T$. The submatrices $\overline{C}_i$ are defined in the form of $\overline{C}_i := \Gamma_i \otimes [1 \ 0]$, where $\Gamma_i := \begin{bmatrix} \Gamma_{ii_1}^T \cdots \Gamma_{ii_{n_i}}^T \end{bmatrix}^T$, with $\{i_1, \cdots, i_{n_i}\} := \mathcal{N}_i \cap \tilde{\mathcal{V}}$. Note that Γ_{ii_j} is a g-dimensional row vector whose ith entry is $-z_{ii_j}$, i_jth entry is z_{ii_j}, and the rest are 0.

(2) In the second case, it is assumed that phase measurements from PMUs can be used at the FDI filter. To simplify the discussion and notation, we assume that within the group $\tilde{\mathcal{V}}$, one bus, say v_j, is equipped with a PMU. Then, the phase $\delta_j(t)$ becomes available in addition to the original output $y(t)$. This approach can be easily generalized to the case with an arbitrary number of PMU measurements.

Hence, in this case, the dynamics of the buses in this group is slightly modified from (5) to

$$\hat{y}(t) := \begin{bmatrix} \delta_j(t) \\ y(t) \end{bmatrix} = \hat{C}x(t), \quad \text{where } \hat{C} := \begin{bmatrix} (e_{2g}^{2j-1})^T \\ C \end{bmatrix}. \tag{4}$$

2.3 Distributed Attack Detection Problem

The distributed attack detection problem considered in this paper can be stated as follows: For the power system (2) of the group $\tilde{\mathcal{V}}$, construct an FDI filter for each fault signal f_i to detect whether f_i is nonzero using the measurements of the power input u and the power flow y or $\hat{y}$ obtained within the group $\tilde{\mathcal{V}}$. The two cases in the outputs are studied separately in Sections 4 and 5.

3. FAULT DETECTION FILTER DESIGN PROBLEM

In this section, we provide a brief review on the geometric approach for the FDI method from (Massoumnia et al. (1989)). This forms the basis for the development of attack detection methods for power systems.

Consider the linear time-invariant system given by

$$\begin{aligned} \dot{x}(t) &= Ax(t) + Bu(t) + \sum_{i=1}^{k} L_i f_i(t), \\ y(t) &= Cx(t), \end{aligned} \tag{5}$$

where $x(t) \in \mathbb{R}^n$ is the state, $u(t) \in \mathbb{R}^m$ is the input, $y(t) \in \mathbb{R}^q$ is the output, $f_i(t)$, $i = 1, \ldots, k$, denote the fault signals, and L_i is a matrix describing how f_i affects the system.

The FDI problem is to design a bank of filters to detect whether any of the fault signals are being applied to the system (5) based on the information of its input u and output y. Specifically, for each i, we design an FDI filter generating the residual r_i which takes a nonzero value if and only if the ith fault signal f_i becomes nonzero. Note that in this FDI filter, the residual r_i is affected only by one fault signal f_i, while other signals f_j have no influence.

For detecting the fault f_i, we consider the FDI filter described in the form as

$$\begin{aligned} \dot{w}_i(t) &= F_i w_i(t) - E_i y(t) + G_i u(t), \\ r_i(t) &= M_i w_i(t) - H_i y(t) + K_i u(t), \end{aligned} \tag{6}$$

where $w_i \in \mathbb{R}^{d_i}$ is the state of this filter, and the matrices F_i, E_i, G_i, M_i, H_i, and K_i are of appropriate sizes.

In solving this problem, we use the notions of (C, A)-invariant subspace and (C, A)-unobservability subspace, which are briefly introduced from (Wonham (1985)). For the system (5), we say that the subspace $\mathcal{W} \subset \mathbb{R}^n$ is a (C, A)-invariant subspace if there exists a matrix $D \in \mathbb{R}^{n \times q}$ such that

$$(A + DC)\mathcal{W} \subset \mathcal{W}.$$

For any given subspace $\mathcal{R} \subset \mathbb{R}^n$, a (C, A)-invariant subspace that contains $\mathcal{R}$ can be found. Denote by $\mathcal{W}^*(\mathcal{R})$ the minimum dimensional (C, A)-invariant subspace containing $\mathcal{R}$. It can be calculated through the following iteration known as the (C, A)-invariant subspace algorithm (CAISA):

$$\mathcal{W}^{k+1} = \mathcal{R} + A(\mathcal{W}^k \cap \mathrm{Ker} C), \quad \mathcal{W}^0 = 0. \tag{7}$$

It is noted that $\mathcal{W}^k \subset \mathcal{W}^{k+1}$ and for some $k^* \leq n$, it holds that $\mathcal{W}^{k^*} = \mathcal{W}^*(\mathcal{R})$.

On the other hand, we say that a subspace $\mathcal{S} \subset \mathbb{R}^n$ is a (C, A)-unobservability subspace if it is an unobservable subspace of the pair $(HC, A + DC)$ for some matrices $D \in \mathbb{R}^{n \times q}$ and $H \in \mathbb{R}^{q \times q}$. Given any subspace $\mathcal{R} \subset \mathbb{R}^n$, a (C, A)-observability subspace that contains $\mathcal{R}$ can be found. Denote by $\mathcal{S}^*(\mathcal{R})$ the minimum dimensional (C, A)-unobservability subspace containing $\mathcal{R}$. Its calculation can be carried out based on the following procedure called unobservable subspace algorithm (UOSA):

$$\mathcal{S}^{k+1} = \mathcal{W}^*(\mathcal{R}) + (A^{-1}\mathcal{S}^k) \cap \mathrm{Ker} C, \quad \mathcal{S}^0 = \mathbb{R}^n. \tag{8}$$

We can show that $\mathcal{S}^k \supset \mathcal{S}^{k+1}$ and for some $k^* \leq n$, it holds that $\mathcal{S}^{k^*} = \mathcal{S}^*(\mathcal{R})$.

The following proposition provides a necessary and sufficient condition for the existence of the FDI filter to detect faults (Massoumnia et al. (1989)).

Proposition 1. For the system (5), the FDI filter (6) can be designed to detect the ith fault signal f_i if and only if

$$\mathcal{S}^*\left(\sum_{j \neq i} \mathrm{Im}\ L_j\right) \bigcap \mathrm{Im}\ L_i = 0.$$

When the condition in the proposition is satisfied, the corresponding FDI filter can be designed through a modified version of an algorithm given in (Wonham (1985)). It is noted that the dimension d_i of the filter (6) is given by

$$d_i = n - \dim(\mathcal{S}_i^*), \tag{9}$$

where $\mathcal{S}_i^* := \mathcal{S}^*\big(\sum_{j\neq i} \mathrm{Im} L_j\big)$. In fact, the state w_i of the filter has the following property: Let $\mathbb{R}^n/\mathcal{S}_i^*$ be the quotient space and let P_i be the corresponding canonical projection. Then, we focus on the error s_i between the state w_i and the projection of x via P_i, that is, $s_i(t) := w_i(t) - P_i x(t)$. The dynamics of the FDI filter can be expressed by this error and the residual as

$$\begin{aligned} \dot{s}_i(t) &= F_i s_i(t) - P_i L_i f_i(t), \\ r_i(t) &= M_i s_i(t). \end{aligned}$$

Hence, the filter is driven only by the ith fault signal and is completely decoupled from other faults. Note that F_i is a stable matrix by design, and thus the error will converge to zero as long as f_i is zero even if initially $s_i(0) \neq 0$.

4. FAULT DETECTION FOR POWER SYSTEMS

In this section, we develop the distributed detection filters for attack detection in power systems based on the method introduced in the previous section. Here, we focus on the case of (3) where the output does not contain PMU measurements.

4.1 Limitation on Direct Detection

A natural way to approach the problem is to find an FDI filter of the form in (6) to detect the fault signal f_i based on the input u and the output y of the power system (2) and (3). However, in (Hashimoto and Hayakawa (2011)), it is shown that such an FDI filter does not exist. This fact is stated in the next proposition.

Proposition 2. For the power system (2) and (3) without PMUs, it is not possible to design an FDI filter to directly detect the fault signal f_i for each i.

This result presents a limitation in the FDI design in the context of power systems. In particular, it shows that regardless of the way groups are formed, detection of faults that occurred within a group cannot be detected from the local information collected within the group. This result is based on Proposition 1 and can be shown by establishing that

$$\mathcal{S}^*\left(\sum_{j\neq i} \mathrm{Im}\, B_j\right) \bigcap \mathrm{Im}\, B_i \neq 0,$$

where B_i is the ith column of the B-matrix in (2). Intuitively, the reason for this impossibility result can be explained by the fact that all measurements related to the phases δ_j are obtained through the power flows in (3).

In (Hashimoto and Hayakawa (2011)), an indirect approach is proposed where an FDI filter is designed for detecting the difference $f_i - f_j$ for each pair f_i and f_j. Such a filter however has the problem of not being sensitive to the case when two fault signals are the same, i.e., $f_i = f_j$. This can potentially become a weakness in the system from the viewpoint of cyber security, where malicious attacks may be expected in a highly coordinated manner. The situation is quite different from multiple faults occurring simultaneously by chance.

4.2 Indirect Detection Approach

Here, we propose an alternative indirect approach and clarify conditions under which FDI filters can be designed. Specifically, we consider designing a filter which generates a residual r_{ij} which takes nonzero value if and only if either f_i or f_j or both becomes nonzero for $i, j \in \tilde{\mathcal{V}}$ with $i \neq j$. The distributed FDI filter for detecting the pair f_i and f_j is expressed by

$$\begin{aligned} \dot{w}_{ij}(t) &= F_{ij} w_{ij}(t) - E_{ij} y(t) + G_{ij} u(t), \\ r_{ij}(t) &= M_{ij} w_{ij}(t) - H_{ij} y(t) + K_{ij} u(t), \end{aligned} \tag{10}$$

where w_{ij} is the state, and r_{ij} is the residual signal.

Though this filter alone is not able to detect attacks on one bus, we propose a method that identifies the attacked buses by (i) designing the above filter for all pairs $i, j \in \tilde{\mathcal{V}}$, $i \neq j$), and then (ii) checking the combination of nonzero residuals r_{ij}. Notice that, for example, if all residuals which have the index $i \in \tilde{\mathcal{V}}$ take nonzero values, then we can conclude that bus i is being attacked. If the level of maliciousness is high, multiple buses may be attacked simultaneously. We show that such attacks can also be identified to a certain extent, depending on the number of buses being attacked.

We are now ready to state the main result of the paper, showing a sufficient condition to apply this method.

Theorem 4.1. For the power system (2) and (3) without PMUs, the distributed indirect fault detection filter (10) can be designed if for the pair $v_i, v_j \in \tilde{\mathcal{V}}$, $i \neq j$, it holds that

$$\frac{d_{v_i}}{m_{v_i}} \neq \frac{d_{v_j}}{m_{v_j}}. \tag{11}$$

This result shows that for malicious attack detection in a group without PMUs, the indirect approach can be useful. In particular, we can verify the possibility of designing the FDI filter through the sufficient condition in the theorem, which requires only all ratios of inertia to damping coefficients to be different. This is a mild condition, which should hold in general, because of individual differences in the parameters of generators and motors. Thus, we do not need to check the condition given in Proposition 1, involving the computation of the (C, A)-unobservability subspace.

4.3 Issues Related to Performance and Computation

Before finishing this section, we examine the tradeoff between the performance in the attack detections and the amount of computation with respect to the group sizes.

In the indirect approach for fault detection discussed so far, an FDI filter is designed for each pair of buses in the group. Hence, in a group consisting of g buses, the total number of FDI filters to be constructed becomes ${}_gC_2 = g(g-1)/2$. As mentioned earlier, the fault in bus i can be identified when all residuals r_{jk} whose indices contain i take nonzero values. This holds true even in the case when multiple buses experience faults. However, note that the maximum number of simultaneous attacks that can be identified is $g - 2$ (Meskin and Khorasani (2009)); see also the example in Section 6. If the number of

simultaneous attacks is more than $g-1$, all of the residuals of this group will take nonzero values, which makes it impossible to identify the attacked buses. In such a case, nevertheless, almost all buses are attacked, so the system is in a very dangerous situation.

Next, we look at the total order of the distributed FDI filters for carrying out the full detection. By (9), the order d_{ij} of the FDI filter (10) for detecting f_i and f_j can be determined as

$$d_{ij} = 2g - \dim\Big(\mathcal{S}^*\Big(\sum_{k\neq i,j} \text{Im } B_k\Big)\Big).$$

We can show that the dimension of $\mathcal{W}^*\big(\sum_{k\neq i,j} \text{Im } B_k\big)$ is $2g-4$. Then, because of the fact $\mathcal{W}^*\big(\sum_{k\neq i,j} \text{Im } B_k\big) \subset \mathcal{S}^*\big(\sum_{k\neq i,j} \text{Im } B_k\big)$, it holds that $d_{ij} \in [1, 4]$. Therefore, we conclude that the total order of filters in group $\tilde{\mathcal{V}}$ satisfies the inequality

$$\frac{g(g-1)}{2} \leq \sum_{i,j} d_{ij} \leq 4 \times \frac{g(g-1)}{2}. \tag{12}$$

In summary, when the size g of the group is larger, one obtains more information in detection and isolation, but the necessary computation increases. That is, there is a tradeoff between the detectability of attacks and the calculation amount.

5. FAULT DETECTION WITH PMU DATA

In this section, we extend our FDI design approach for cyber security in power systems to the case where further measurements are available from PMUs. It is demonstrated that under this scenario, direct detection is possible even if such measurements are partial and not placed at all buses in the system.

The problem of this section is to design an FDI filter for directly detecting whether the fault signal f_i is nonzero based on the input u and the output $\hat{y}$ in (4) of the system. That is, we would like to construct the filter generating the residual r_i that responds whenever f_i takes nonzero values. Similarly to the previous case, the FDI filter is given by

$$\begin{aligned} \dot{w}_i(t) &= F_i w_{ij}(t) - E_i \hat{y}(t) + G_i u(t), \\ r_i(t) &= M_i w_{ij}(t) - H_i \hat{y}(t) + K_i u(t). \end{aligned} \tag{13}$$

When the measurement contains PMU data, the following theorem can be established.

Theorem 5.1. For the power system (2) and (4), distributed direct fault detection filter (13) can be designed.

Though the theorem statement is limited to the case with one PMU, the result can be extended to the general case with multiple PMUs. This result clarifies that direct detection can be achieved within a group if any of the buses are equipped with PMUs, measuring the values of the phases. Such detection will enhance the efficiency for detection of malicious attacks.

Moreover, direct detection implies that the number of FDI filters can be significantly reduced and is in fact equal to that of the buses, g. In the current case, the orders of the filters can be explicitly calculated. Similarly to the discussion in Subsection 4.3, the order of the FDI filter for detecting f_i is equal to

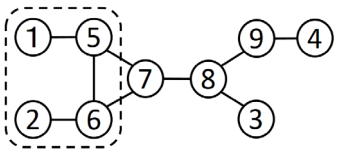

Fig. 1. 9-bus power system

$$d_i = 2g - \dim\Big(\mathcal{S}^*\Big(\sum_{k\neq i} \text{Im } B_k\Big)\Big) = 2g - (2g-2) = 2.$$

As a consequence, the total order of the filters in group $\tilde{\mathcal{V}}$ becomes $\sum_i d_i = 2g$, which is much smaller than that for the indirect detection case in (12). However, introducing PMUs in the power system especially in a large quantity can be costly. These are factors that need to be considered when implementing this direct detection method.

6. NUMERICAL EXAMPLE

In this section, we verify the effectiveness of the proposed distributed fault detection methods through a numerical example.

We consider the power system depicted in Fig. 1 with nine buses. Here, we focus on the group indicated by the dashed line, consisting of four buses 1, 2, 5, and 6 ($g = 4$). In this case, the group node set is given by $\tilde{\mathcal{V}} = \{1, 2, 5, 6\}$. The two cases depending on the availability of PMU data are examined.

(1) Indirect detection without PMU data: In view of Theorem 4.1, we set the ratios of inertia and damping coefficients of the buses to take different values. The input data to the FDI filter for this group is as follows:

- Injection powers: u_1, u_2, u_5, u_6.
- Power flows within the group: p_{15}, p_{26}, p_{56}.
- Power flows to/from external buses: p_{57}, p_{67}.

We constructed the indirect FDI filters which generate six residual signals as r_{12}, r_{15}, r_{16}, r_{25}, r_{26}, and r_{56}. By observing the residuals taking nonzero values, we can identify the buses that experience faults and/or attacks at the time. As mentioned earlier, this can be done as long as the number of buses being attacked is less than $g - 2 = 2$.

For the simulation, we set the attack scenario as follows:

- For $t \in [0, 4)$, there is no fault signal injected to the buses.
- For $t \geq 4$, the injection power data of u_5 is manipulated as -100 [W] $\to -50$ [W].
- For $t \geq 8$, the injection power data of u_6 is manipulated as -100 [W] $\to 0$ [W].

The responses of the six residuals are indicated in Fig. 2. From these plots, we can conclude that the attacks are detected successfully. In Fig. 2, we observe the following:

- For $t \in [0, 4]$, all residuals remain zero.
- For $t \in [4, 8]$, the residuals r_{15}, r_{25}, and r_{56} become nonzero.
- For $t > 8$, the residuals r_{15}, r_{16}, r_{25}, r_{26}, and r_{56} take nonzero values.

We can confirm that (i) during the time interval $t \in [0, 4]$, none of the buses is attacked, (ii) during $t \in [4, 8]$, bus 5

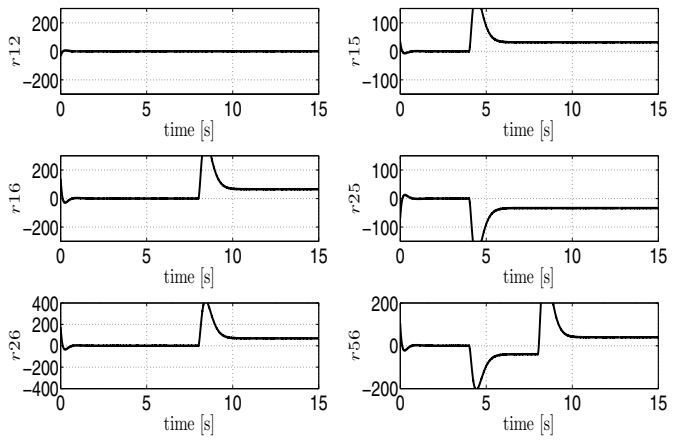

Fig. 2. Time responses of the residue signals r_{ij} of the indirect detection filters (with no PMU)

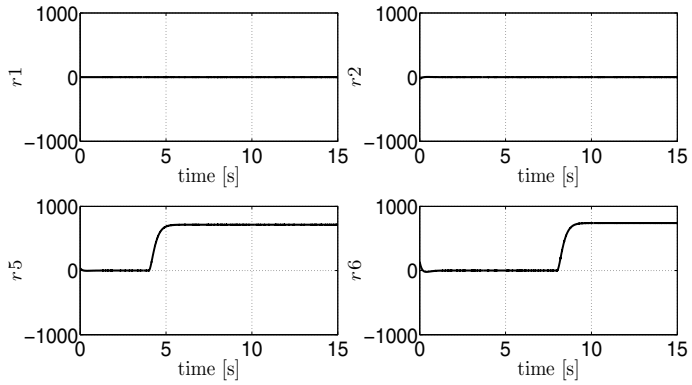

Fig. 3. Time responses of the residue signals r_i of the direct detection filters (with a PMU)

is being manipulated, and (iii) during $t \geq 8$, both buses 5 and 6 are attacked.

(2) Direct detection with PMU data: Here, bus 1 is equipped with a PMU so that in addition to the measurements in case (1) above, the phase δ_1 is available to the FDI filters. After designing the filters, we ran the simulation under the same attack scenario as above. The behaviors of the four residuals r_1, r_2, r_5, and r_6 are shown in Fig. 3. From the plots, we can easily verify that the attacks could be detected and isolated. Clearly, r_5 responds to f_5 at time $t = 4$, and then r_6 becomes nonzero after time $t = 8$. The other two residuals r_1 and r_2 remained almost constant at zero as expected.

7. CONCLUSION

In this paper, we have proposed a distributed attack detection method by using the scheme of grouping of buses and modeling of a power system by the swing equation. We have considered two problem settings depending on the presence of PMUs. When such sensors are not available, a sufficient condition has been developed for realizing indirect detection of faults. It has then been shown that even if PMUs are placed only at a limited number of buses, direct detection is possible; this is a more advantageous situation since the number of necessary filters can be reduced. In future research, we will study applying other FDI methods to enhance performance and robustness.

REFERENCES

Abur, A. and Gómez-Expósito, A. (2004). *Power System State Estimation: Theory and Implementation*. Marcel Dekker, New York.

Dibagi, S. and Ishii, H. (2014). Resilient consensus of double-integrator multi-agent systems. In *Proc. American Control Conf.*, to appear.

Ding, S. (2008). *Model-based Fault Diagnosis Techniques: Design Schemes, Algorithms, and Tools*. Springer, London.

Giani, A., Bitar, E., Garcia, M., McQueen, M., Khargonekar, P., and Poolla, K. (2011). Smart grid data integrity attacks: Characterizations and countermeasures. In *Proc. IEEE Smart Grid Comm.*, 232–237.

Hashimoto, H. and Hayakawa, T. (2011). Distributed cyber attack detection for power network systems. In *Proc. 50th IEEE Conf. on Decision and Control*, 5820–5824.

Liu, Y., Ning, P., and Reiter, M. (2011). False data injection attacks against state estimation in electric power grids. *ACM Trans. Information and System Security*, 14, 13: 1–33.

Machowski, J., Bialek, J., and Bumby, J. (2008). *Power System Dynamics: Stability and Control,* 2nd edition. Wiley.

Massoumnia, M., Verghese, G., and Willsky, A. (1989). Fault detection and identification. *IEEE Trans. Autom. Control*, 34, 316–321.

Meskin, N. and Khorasani, K. (2009). Actuator fault detection and isolation for a network of unmanned vehicles. *IEEE Trans. Autom. Control*, 54, 835–840.

Mo, Y. and Sinopoli, B. (2010). False data injection attacks in control systems. In *Proc. 1st Workshop on Secure Control Systems*.

Pasqualetti, F., Bicchi, A., and Bullo, F. (2011). A graph-theoretical characterization of power network vulnerabilities. In *Proc. American Control Conf.* 3918–3923.

Shames, I., Teixeira, A., Sandberg, H., and Johansson, K. (2011). Distributed fault detection for interconnected second-order systems. *Automatica*, 47, 2757–2764.

Sou, K., Sandberg, H., and Johansson, K. (2011). Electric power network security analysis via minimum cut relaxation. In *Proc. 50th IEEE Conf. on Decision and Control*, 4054–4059.

Wonham, W. (1985). *Linear Multivariable Control: A Geometric Approach,* Third Edition. Springer, New York.

Zhang, H. and Sundaram, S. (2012). Robustness of complex networks with implications for consensus and contagion. In *Proc. 51st IEEE Conf. on Decision and Control*, 3426–3432.

Zhang, Q., Chakhchoukh, Y., Vittal, V., Heydt, G., Logic, N., and Sturgill, S. (2013). Impact of PMU measurement buffer length on state estimation and its optimization. *IEEE Trans. Power Systems*, 28, 1657–1665.