2011 50th IEEE Conference on Decision and Control and
European Control Conference (CDC-ECC)
Orlando, FL, USA, December 12-15, 2011

# Distributed Cyber Attack Detection for Power Network Systems

**Hideaki Hashimoto and Tomohisa Hayakawa**

Department of Mechanical and Environmental Informatics
Tokyo Institute of Technology, Tokyo 152-8552, JAPAN
hayakawa@mei.titech.ac.jp

**Abstract**

In this paper, a framework of distributed fault detection for network systems is developed. Specifically, a framework of distributed cyber attack detection system for synchronized large-scale power network is constructed, where active power flow in power network system is modeled by the swing equation and cyber attacks are modeled as unknown power generation or consumption. The approach is based on fault detection and identification (FDI) filter so that malicious cyber attacks in the neighborhood of a node are identified through local information that consists of local power consumption, generation, and power flow. The FDI filter is a special Luenberger observer whose parameter is selected in such a way that residual between the sensed power flow and the FDI filter's output is only affected by specific cyber attacks. Residual indicates the existence of the cyber attack. A sufficient condition is provided for the existence of the FDI filter with the local input and the output to detect fault in the network system. A numerical example is provided to demonstrate efficacy of the proposed approach.

## 1. Introduction

Power network is a large-scale network system where the generators and the loads are disorderly connected. In the face of increasing demands of stable electric power supply and global environmental problems, modernization of power network, such as smart grid, has been drawing much attention. Specifically, sensing, billing, load prediction, and load control can be modernized by utilizing information technology [1]. Installations of renewable energy such as solar and wind power which have fluctuating power generation would increase if accurate load prediction and advanced load control are properly handled [2].

On the other hand, power grid will be more likely to be exposed to malicious attacks (cyber attacks), because information such as power consumption data and control signal to distributed generators can be shared and communicated with the modernization of the power network. For example, illegal electricity usage based on smart metering [3], false data injection into sensing data [4], cyber attack on energy generation control signal in the power network [5] have been investigated. In fact, several cyber attacks on the power grid in the U.S. has been reported [6].

In general, active power flow on power network system is modeled by the swing equation [7]. In the power network system, local phenomena can be propagated so that the entire system is affected by the phenomena due to its characteristic as a network system. Therefore, bad effects by cyber attacks such as unknown power consumption and power insertion into local power network give rise to global instability of the power network. Recently, impact analysis of cyber attacks on the power network system is investigated [8]. Both prevention and detection methods against cyber attacks turn out to seem extremely important.

In [9], centralized detection methods of false data injection attack on the power network system modeled by swing equation were proposed. Furthermore, in [10] semi-decentralized scheme to detect and isolate cyber attacks with unknown power injection and consumption using local sensing information, the whole power generation, and consumption data is investigated. Power network system is a large-scale system so that distributed scheme to detect cyber attacks from local power generation, power consumption, and power flow sensing data is valuable from the point of view of load distribution and robust detection.

Cyber attack can be viewed as a special class of fault at the point in that unknown disturbance happens on a system. There are a number of researches on fault detection for dynamical systems [11]. For example, fault detection and estimation scheme with sliding observer for vehicle formation [12] and distributed fault detection with overlapping decompositions for nonlinear systems is investigated [11]. In [13], an approach based on the fault detection and identification (FDI) filter is proposed. The FDI filter is a special Luenberger observer whose parameters are selected in such a way that residual between system output and the FDI filter's output is only affected by a specific fault [14]. The residual indicates the existence of the cyber attacks. For this problem, some necessary and sufficient conditions of existence of the FDI filter has been derived [14, 15]. Furthermore, the sufficient condition of existence for distributed the FDI filter [16] and that for vehicle formation problem with the information of relative location is derived [17].

In this paper, a framework of distributed cyber attack detection for synchronized large-scale power network is

developed, where active power flow in the power network system is modeled by the swing equation and cyber attacks are modeled as unknown power generation and/or consumption. A new scheme for constructing the FDI filter against malicious cyber attacks in the neighborhood are identified through local information which consists of power consumption, power generation, and power flow. The residual term indicates the existence of cyber attacks. Finally, a numerical example is provided to demonstrate efficacy of the proposed approach, where power network system of IEEE 9-buses benchmark is employed in a numerical example.

In this paper following notations are used. We refer to the matrix $I_n$ as $n \times n$ a dimensional identity matrix, the matrix $0_{n\times m}$ as $n \times m$ a dimensional zero matrix, the vector $\mathbf{1}_n \triangleq [1, \dots, 1]^{\mathrm{T}} \in \mathbb{R}^n$ as a vector with all 1 entry, the vector $\mathbf{e}_N^i \in \mathbb{R}^N$ as a vector with only all 0 entry except 1 entry of 1th column, and the operator $\otimes$ as the Kronecker product.

## 2. Mathematical Preliminary

In this section we introduce notation, several definitions, and some key results concerning geometric approach that are necessary for developing the main results of this paper in regards to the detectability of cyber attacks and faults [18]. Specifically, letting $\mathcal{U}, \mathcal{V}$ be the subspaces of the linear space $\mathcal{X}$ on the real field $\mathbb{R}^n$, addition and intersection of the subspaces are defined as $\mathcal{U} + \mathcal{V} \triangleq \{u + v : u \in \mathcal{U}, v \in \mathcal{V}\}$ and $\mathcal{U} \cap \mathcal{V} \triangleq \{x : x \in \mathcal{U}, x \in \mathcal{V}\}$, respectively.

Let $A : \mathcal{X} \to \mathcal{Y}$ be a map from the linear space $\mathcal{X}$ to another linear space $\mathcal{Y}$. The subspaces $\mathcal{R}(A)$ and $\mathcal{N}(A)$ are referred to as its null space and range space, respectively. When $\mathcal{U}$ is a subspace of the linear space $\mathcal{X}$ and $\mathcal{V}$ is a subspace of the linear space $\mathcal{Y}$, respectively, the image and the inverse image of the subspaces associated with $A$ is defined as

$$A\mathcal{U} \triangleq \{Ax : x \in \mathcal{U}\}, \tag{1}$$

$$A^{-1}\mathcal{V} \triangleq \{x \in \mathcal{X} : Ax \in \mathcal{V}\}. \tag{2}$$

Consider the linear time-invariant system $\mathcal{G}$ described by

$$\dot{x}(t) = Ax(t) + Bu(t), \tag{3}$$

$$y(t) = Cx(t), \tag{4}$$

where $x \in \mathbb{R}^n$, $u \in \mathbb{R}^m$, $y \in \mathbb{R}^q$ are the state, the input, and the output of the system, respectively, and $A \in \mathbb{R}^{n\times n}, B \in \mathbb{R}^{n\times m}$, and $C \in \mathbb{R}^{q\times n}$, are constant matrices. A subspace $\mathcal{W} \subset \mathbb{R}^n$ is called a $(C, A)$-invariant subspace if there exists a map $D \in \mathbb{R}^{n\times q}$ such that $(A + DC)\mathcal{W} \subset \mathcal{W}$. The smallest $(C, A)$-invariant subspace which contains the given subspace $\mathcal{U}$ is denoted as $\mathcal{W}^*(\mathcal{U})$ (or $\mathcal{W}^*(\mathcal{U}, C, A)$). The smallest $(C, A)$-invariant subspace $\mathcal{W}^*(\mathcal{U})$ is given by the following $(C, A)$-invariant subspace algorithm (CAISA)

$$\mathcal{W}^{k+1} = \mathcal{U} + A(\mathcal{W}^k \cap \mathcal{N}(C)), \quad \mathcal{W}^0 = 0. \tag{5}$$

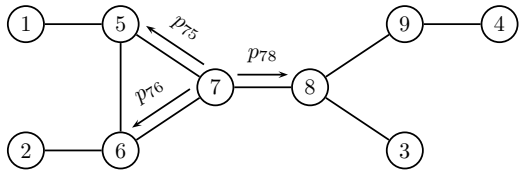


**Figure 3.1**: Electric power network system

Note that for some $k \leq n$, $\mathcal{W}^0 \subset \mathcal{W}^1 \subset \cdots \subset \mathcal{W}^k = \mathcal{W}^{k+1}$ is satisfied so that $\mathcal{W}^*(\mathcal{U}) = \mathcal{W}^k$ [18].

Let $\langle \mathcal{N}(C)|A\rangle = \mathcal{N}(C) \cap A^{-1}\mathcal{N}(C) \cap \cdots \cap A^{-n+1}\mathcal{N}(C)$. A subspace $\mathcal{M} \triangleq \langle \mathcal{N}(C)|A\rangle$ is called a $(C, A)$-unobservable subspace. A subspace $\mathcal{S} \subset \mathbb{R}^n$ is called a $(C, A)$-unobservability subspace if there exist maps $D \in \mathbb{R}^{n\times q}$ and $H \in \mathbb{R}^{q\times q}$ such that $\mathcal{S} = \langle \mathcal{N}(HC)|A + DC\rangle$. Note that $(C, A)$-unobservability subspace $\mathcal{S}$ is the $(HC, A + DC)$-unobservable subspace.[1] The smallest $(C, A)$-unobservability subspace which contains the given subspace $\mathcal{U} \subset \mathbb{R}^n$ is denoted by $S^*(\mathcal{U})$. The smallest $(C, A)$-unobservability subspace $S^*(\mathcal{U})$ is given by the following unobservability subspace algorithm (UOSA)

$$\mathcal{S}^{k+1} = \mathcal{W}^*(\mathcal{U}) + (A^{-1}\mathcal{S}^k) \cap \mathcal{N}(C), \quad \mathcal{S}^0 = \mathbb{R}^n. \tag{6}$$

Note that for some $k \leq n$, $\mathcal{S}^0 \supset \mathcal{S}^1 \supset \cdots \supset \mathcal{S}^k = \mathcal{S}^{k+1}$ is satisfied so that $\mathcal{S}^*(\mathcal{U}) = \mathcal{S}^k$ [18].

## 3. Node Dynamics

Electric power transmission system where the generators and the loads are connected through transmission lines can be seen as a network system with the nodes which consist of buses of the generators and the loads, and the edges which represent connections between the buses (Figure 3.1). We assume that the loads are general motor loads and the graph which represents the network is connected. Let the power network system consists of $N$ nodes, and the active power flows at each node $i$ is modeled by the swing dynamics given by

$$\begin{aligned} \dot{\delta}_i(t) =& \omega_i(t), \\ m_i\dot{\omega}_i(t) + d_i\omega_i(t) - u_i(t) =& -\sum_{j\in\mathcal{N}_i} p_{ij}(t) + f_i(t), \\ \delta_i(0) = \delta_{i0}, \quad \omega_i(0) =& \omega_{i0}, \quad t \geq 0, \quad i = 1, \dots, N, \end{aligned} \tag{7}$$

where $\delta_i \in \mathbb{R}$ denotes the phase angle of node $i$, $\omega_i \in \mathbb{R}$ denotes the phase angle speed of node $i$, $m_i$ denotes the inertia of node $i$, $d_i$ denotes the damping constant of node $i$, $u_i \in \mathbb{R}$ denotes the active power injected/consumed through node $i$ which is termed input in this paper, $p_{ij} \in \mathbb{R}$ denotes the active power flow from node $i$ to node $j$. The set of all nodes connected to node $i$ is denoted by $\mathcal{N}_i = \{i_1, \dots, i_{n_i}\} \subset \{1, \dots, N\}$, where $n_i$ is the number of nodes connected to node $i$ and is same as the cardinal number $|\mathcal{N}_i|$ of the set $\mathcal{N}_i$.

[1] In this paper it is important to distinguish between a $(C, A)$-unobservability subspace and a $(C, A)$-unobservable subspace.

Unknown time variant function $f_i \in \mathbb{R}$ represents the cyber attack (unknown active power injection or consumption), where $f_i(t) = 0$ indicates no cyber attack to node $i$ and $f_i(t) \neq 0$ indicates the cyber to attack node $i$ at time $t$.

The complex voltage at node $i$ is $v_i(t) = |v_i|e^{j\delta_i(t)}$ [10]. Assuming that there are no power losses in transmission, the active power flow from node $i$ to node $j$ is given by

$$p_{ij}(t) = w_{ij}\sin(\delta_i(t) - \delta_j(t)), \tag{8}$$

where the constant $w_{ij}$ satisfies $w_{ij} = |v_i||v_j|b_{ij}$ with $b_{ij}$ denoting the susceptance transmission line connecting nodes $i$ and $j$. We assume that the voltages $|v_i|$, $i = 1, \ldots, N$, are constant. Since the differences $\delta_i(t) - \delta_j(t)$, $j = 1, \ldots, n_i$, between the phase angle $\delta_i$ and the phase angles of the neighbor nodes $\mathcal{N}_i$ are small, the active power flow from node $i$ to node $j$ is assumed to be linearized so that (8) is rewritten as

$$p_{ij}(t) = w_{ij}(\delta_i(t) - \delta_j(t)). \tag{9}$$

We assume that at each node $i$, the active power supplied from node $i$ to node $j$ are measured and denoted by $\bar{y}_i \in \mathbb{R}^{n_i}$ as sensing data. Writing the state at node $i$ as $x_i \triangleq [\delta_i, \omega_i]^{\mathrm{T}} \in \mathbb{R}^2$ and the sensing data at node $i$ as

$$\bar{y}_i(t) = \bar{C}_i x(t), \tag{10}$$

where $x \triangleq [x_1^{\mathrm{T}}, \ldots, x_N^{\mathrm{T}}]^{\mathrm{T}}$,

$$\bar{C}_i \triangleq (\Gamma_i \otimes [1, 0]) \in \mathbb{R}^{n_i \times 2N}, \tag{11}$$

and matrix $\Gamma_i \in \mathbb{R}^{n_i \times N}$ is given by

$$\Gamma_i(j,k) \triangleq \begin{cases} -w_{ij}, & k = i, \\ w_{ij}, & k = i_j, \\ 0, & \text{otherwise.} \end{cases} \tag{12}$$

In this paper, we assume that each node $i$ can get the sensing data of its neighbors $\bar{y}_j$, $j \in \mathcal{N}_i$,. Therefore, the sensing data at node $i$ is defined as

$$y_i(t) = [\bar{y}_i^{\mathrm{T}}(t), \bar{y}_{i_1}^{\mathrm{T}}(t), \ldots, \bar{y}_{i_{n_i}}^{\mathrm{T}}(t)] = C_i x(t), \tag{13}$$

where

$$C_i \triangleq [\bar{C}_i^{\mathrm{T}}, \bar{C}_{i_1}^{\mathrm{T}}, \ldots, \bar{C}_{i_{n_i}}^{\mathrm{T}}]^{\mathrm{T}} \in \mathbb{R}^{(\sum_{j \in \{i\} \cup \mathcal{N}_i} n_j) \times 2N}. \tag{14}$$

## 4. Dynamics of Power Network System

In the power network system, the global input is denoted by $u \triangleq [u_1, \ldots, u_N]^{\mathrm{T}} =\in \mathbb{R}^N$ and cyber attacks to the whole power network system is denoted by $f \triangleq [f_1, \ldots, f_N]^{\mathrm{T}} \in \mathbb{R}^N$, the global sensing data is denoted by $y \triangleq [\bar{y}_1^{\mathrm{T}}, \ldots, \bar{y}_N^{\mathrm{T}}]^{\mathrm{T}} \in \mathbb{R}^{\sum_{i=1}^N n_i}$, then power network system dynamic is given by

$$\dot{x}(t) = (A + (L \otimes D))x(t) + Bu(t) + Bf(t), \tag{15}$$

$$y(t) = Cx(t), \tag{16}$$

where

$$A_i \triangleq \begin{bmatrix} 0 & 1 \\ 0 & -\frac{d_i}{m_i} \end{bmatrix}, \quad A \triangleq \begin{bmatrix} A_1 & & \\ & \ddots & \\ & & A_N \end{bmatrix} \in \mathbb{R}^{2N \times 2N}, \tag{17}$$

$$B_i \triangleq \begin{bmatrix} 0 \\ \frac{1}{m_i} \end{bmatrix}, \quad B \triangleq \begin{bmatrix} B_1 & & \\ & \ddots & \\ & & B_N \end{bmatrix} \in \mathbb{R}^{2N \times N}, \tag{18}$$

$$D \triangleq \begin{bmatrix} 0 & 0 \\ 1 & 0 \end{bmatrix}, \quad C \triangleq \left[\bar{C}_1^{\mathrm{T}}, \ldots, \bar{C}_N^{\mathrm{T}}\right]^{\mathrm{T}}, \tag{19}$$

and weighted graph Laplacian $L \in \mathbb{R}^{N \times N}$ is defined as

$$L_{(i,j)} \triangleq \begin{cases} -\sum_{j \in \mathcal{N}_i} \frac{w_{ij}}{m_i}, & i = j, \\ \frac{w_{ij}}{m_i}, & j \in \mathcal{N}_i, \\ 0, & \text{otherwise.} \end{cases} \tag{20}$$

## 5. Detection of Cyber Attacks

In this section, we characterize the framework of cyber attack detection with the FDI filter utilizing the inputs at node $i$ and its neighbors $\bar{u}_i \triangleq [u_i, u_{i_1}, \ldots, u_{i_{n_i}}]$ and the sensing data $y_i$.

### 5.1. Works Related to Cyber Attack Detection

A general fault detection and identification methodology with the FDI filter has been proposed in [13]. Specifically, the FDI filter and residual $r_i \in \mathbb{R}$ is constructed with the design parameters $F_i, E_i, G_i, M_i, H_i, K_i$ as

$$\dot{w}_i(t) = F_i w_i(t) - E_i y(t) + G_i u(t), \tag{21}$$

$$r_i(t) = M_i w_i(t) - H_i y(t) + K_i u(t), \tag{22}$$

where $w_i \in \mathbb{R}^{m_i}$ denotes the state of the FDI filter. Note that the FDI filter (21), (22) utilizing the global input $u$ and the global sensing data $y$ is considered to be a centralized detection framework.

Detection of a cyber attack is achieved by generating a residual $r_i(t)$ with the following characteristics:

- If there is no cyber attack to node $i$ ($f_i(t) \equiv 0$), the residual $r_i(t)$ converges to 0, even if there are cyber attacks to other nodes, i.e., $f_j \neq 0$, $j \in \{1, \ldots, N\}$, $j \neq i$.
- If node $i$ is under a cyber attack ($f_i(t) \neq 0$), then the residual $r_i$ has a value except 0 ($r_i(t) \neq 0$).

When the residual with these characteristics can be generated, the residual equal to 0 indicates that there is no cyber attack to node $i$, also the residual not equal to 0 indicates that there is a cyber attack to node $i$. Assuming the centralized detector, problem to find parameters $F_i, E_i, G_i, M_i, H_i, K_i$ results in designing the residual $r_i(t)$ with above-mentioned characteristics called an

extension of the fundamental problem in residual generation (EFPRG). Existence of these parameters is denoted by a solvability of EFPRG. The necessary and sufficient condition was developed for EFPRG.

**Lemma 1** [14, Theorem 6]. EFPRG to detect cyber attack $f_i$ to the system (15), (16) is solvable if and only if there exists the smallest $(C, A+(L\otimes D))$-unobservability subspace $\mathcal{S}^*(\mathcal{R}(\bar{B}_i))$ containing $j \neq i$ subspace $\mathcal{R}(\bar{B}_i)$ such that

$$\mathcal{S}^*(\mathcal{R}(\bar{B}_i)) \cap \mathcal{R}(b_i) = 0, \tag{23}$$

where $\bar{B}_i \in \mathbb{R}^{2N\times(N-1)}$ denotes the matrix of $B$ with $i$th row is eliminated and $b_i \in \mathbb{R}^{2N}$ denotes a vector of $i$th row of $B$.

As mentioned before, in this paper we are aiming to develop a framework of cyber attack detection with FDI filter utilizing the local inputs $\bar{u}_i$ and the local sensing data $y_i$. To this end, consider the special FDI filter and residual

$$\dot{w}_i(t) = F_i w_i(t) - E_i y_i(t) + G_i \bar{u}_i(t), \tag{24}$$

$$r_i(t) = M_i w_i(t) - H_i y_i(t) + K_i \bar{u}_i(t), \tag{25}$$

where only $\bar{u}_i$ and $y_i$ are used at the local detector. In this paper constructing the detector (25) and (24) is called as a *distributed EFPRG* where we find parameters $F_i, E_i, G_i, , M_i, H_i, K_i$ of the FDI filter. The sufficient condition for solvability of distributed EFPRG is given as follows:

**Lemma 2** [16, Theorem 2.3]. Distributed EFPRG to detect a cyber attack $f_i$ for the system (13), (15) wit the local inputs $\bar{u}_i$ and the local sensing data $y_i$ at node $i$ is solvable if there exists the smallest $(C_i, A+(L\otimes D))$-unobservability subspace containing $\mathcal{R}(\bar{B}_i)$ such that

$$\mathcal{S}_i^*(\mathcal{R}(\bar{B}_i)) \cap \mathcal{R}(b_i) = 0. \tag{26}$$

### 5.2. Unsolvability of Direct Cyber Attack Detection Problem

Unsolvability of distributed EFPRG for the system (13), (15) with the inputs of node $i$ and its neighbors $\bar{u}_i$ is concluded by the following Theorem.

**Theorem 1.** Consider the system given by (15), (16). Then EFPRG to detect the cyber attack $f_i$ is not solvable for $i = 1, \ldots, N$.

From Theorem 1, it is obvious that the distributed EFPRG which is a special case of EFPRG restricting the design parameter structure, is not solvable, either.

### 5.3. Problem Statement (Indirect Cyber Attack Detection Problem)

The objective of this paper is to develop a framework of cyber attack detection with the FDI filter utilizing inputs at node $i$ and its neighbors $\bar{u}_i$ and the sensing data $y_i$. In Section 5.2, however, it is demonstrated that the distributed EFPRG to detect a cyber attack $f_i$ with the input $\bar{u}_i$ for the system (13), (15) is not solvable.

In this section, we come up with another approach which is not to detect a cyber attack to node $i$ but to detect a cyber attack to node $i$ *or* one of its neighbor $\alpha \in \mathcal{N}_i$. In other words, we define the new function

$$f_{i\alpha} \triangleq f_i(t) - f_\alpha(t) \tag{27}$$

which represents a cyber attack to node $i$ or one of its neighbor $\alpha \in \mathcal{N}_i$ and detect whether $f_{i\alpha}$ is 0 or not. In this framework, if we can generate a residual $r_{i\alpha}(t)$ which becomes nonzero only if $f_{i\alpha}(t)$ is nonzero, we can detect a cyber attacks to node $i$ or node $\alpha$ but the case of $f_i(t) \equiv f_\alpha(t)$.

For example, consider the power network system with $N(\geq 5)$ nodes and the neighbors of the node 1 are equal to $\mathcal{N}_1 = \{2, 3, 4\}$. Consider the cyber attack detection at the node 1. First of all, we define the functions which express a cyber attack to node $i$ or one of its neighbors $\mathcal{N}_1$ as $f_{12}, f_{13}, f_{14}$. Assuming residuals $r_{12}, r_{13}, r_{14}$ be generated, such that each of them has a nonzero value only if respective $f_{12}, f_{13}, f_{14}$ has nonzero value. Then, when the node 1 is under cyber attack ($f_1(t) \neq 0$), the residuals $r_{12}(t), r_{13}(t), r_{14}(t)$ become nonzero. When node $j \in \mathcal{N}_1$ is suffered by a cyber attack, the residuals $r_{1j}(t)$, $j \in \mathcal{N}_1$, become nonzero. On the other hand, when the nodes except for the node 1 and its neighbors are under cyber attack, all the residuals are not affected at all. In this framework, we can detect cyber attacks to the node 1 or its neighbors $\mathcal{N}_1$ respectively but the case of $f_1(t) \equiv f_{1_j}(t)$, $j \in \mathcal{N}_1$.

The following fact is known. Let $n_i > 1$, define the new $\binom{n_i+1}{2}$ functions which represents cyber attacks to two of node $i$ and/or its neighbors. If we can generate the corresponding $\binom{n_i+1}{2}$ residuals, then we can detect at most $n_i - 1$ cyber attacks to node $i$ and its neighbors firing at the same time [17]. Furthermore, in the case of $n_i = 1$, one cannot distinguish cyber attack to node $i$ from cyber attack to its neighbor [17].

On the same setting as the above example, define $f_{23}, f_{24}, f_{34}$ and if $r_{23}, r_{24}, r_{34}$ are generated successfully, then a cyber attack to the node 1 is detectable. Furthermore, cyber attacks to the node 1 and its neighbors firing at the same time at most 2 can be identified. This facts are confirmed by the TABLE 5.1 which shows the relationship between the cyber attacked nodes and the residuals. In Table 5.1, when more than one nodes $\mathcal{I} \subset \{1\}\cup\mathcal{N}_1$ are cyber attacked, the residuals which become nonzero are indicated by $\circ$. By Table 5.1, it can be checked that $n_1 - 1 = 2$ cyber attacks firing at the same time are detectable and identifiable, but more than 3 cyber attacks firing at the same time is not identifiable.

In this paper, given the system (13), (15), we will analyzes the problem to find the design parameters $F_{jk}, E_{jk}, G_{jk}, M_{jk}, H_{jk}, K_{jk}$ to design $\binom{n_i+1}{2}$ pairs of

**Table 5.1**: Cyber attacks and residuals

| | Cyber attacked nodes | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| | 1 | 2 | 3 | 4 | 1,2 | 1,3 | $\cdots$ | 1,2,4 | 2,3,4 |
| $r_{12}$ | ○ | ○ | | | ○ | ○ | $\cdots$ | ○ | ○ |
| $r_{13}$ | ○ | | ○ | | ○ | ○ | $\cdots$ | ○ | ○ |
| $r_{14}$ | ○ | | | ○ | ○ | ○ | $\cdots$ | ○ | ○ |
| $r_{23}$ | | ○ | ○ | | ○ | ○ | $\cdots$ | ○ | ○ |
| $r_{24}$ | | ○ | | ○ | ○ | | $\cdots$ | ○ | ○ |
| $r_{34}$ | | | ○ | ○ | | ○ | $\cdots$ | ○ | ○ |

the FDI filters and the residuals as

$$\begin{aligned} \dot{w}_{jk}(t) &= F_{jk}w_{jk}(t) - E_{jk}y_i(t) + G_{jk}\bar{u}_i(t), \\ r_{jk}(t) &= M_{jk}w_{jk}(t) - H_{jk}y_i(t) + K_{jk}\bar{u}_i(t), \\ j &= i,i_1,\ldots,i_{n_i}, \quad k = i_1,\ldots,i_{n_i}, \quad j > k, \end{aligned} \tag{28}$$

such that the residuals become nonzero only if cyber attack $f_{jk} \triangleq f_j - f_k$ become nonzero at node $i$ with the input $\bar{u}_i(t)$.

### 5.4. Solvability of Indirect Cyber Attack Detection

The following theorem is a main result of this paper.

**Theorem 2.** Consider the network system (13), (15). Indirect distributed EFPRG at node $i$ with the input $\bar{u}_i$ to detect cyber attacks $f_i$, $i \in \{1\} \cup \mathcal{N}_i$, is solvable.

## 6. Conclusion

A framework of cyber attack detection with the FDI filter utilizing local information was proposed. First of all, cyber attack to the power network system is regarded as unknown power generation or consumption. We analyze the method to directly detect cyber attacks utilizing the information of local power generation or consumption and power flow with the FDI filter. We demonstrate the unsolvability of construction of the FDI filter and residual which only is affected by specific cyber attack. Furthermore, we propose a framework that we construct the FDI filters and residuals not detect cyber attack directly but to detect cyber attacks to the node or its neighbors. We illustrate the solvability of the indirect distributed EFPRG with local power generation and consumption data and power flow data. Finally, numerical simulation of the power network system presents the validity of the proposed method. Future work includes the development of detection methods which deal robustness, and detection method for power system modeled by probabilistic system.

## References


[1] D. Butler, "Super savers: Meters to manage the future," *Nature*, vol. 445, pp. 586–588, 2007.

[2] H. Ryan, "How green is the smart grid?," *Elect. J.*, vol. 22, no. 3, pp. 29–41, 2009.

[3] A. Pasdar and S. Mirzakuchaki, "A solution to remote detecting of illegal electricity usage based on smart metering," in *Proc. Int. Workshop Soft Compu. Appl.*, (Hungary, Romania), pp. 163–167, August 2007.

[4] Y. Liu, M. Reiter, and P. Ning, "False data injection attacks against state estimation in electric power grids," in *Proc. ACM Conf. Compu. Commu. Security*, (Chicago, IL), pp. 21–32, 2009.

[5] P. Mohajerin Esfahani, M. Vrakopoulou, K. Margellos, J. Lygeros, and G. Andersson, "A robust policy for automatic generation control cyber attack in two area power network," in *Proc. IEEE Conf. Dec. Contr.*, (Atlanta, GA), pp. 5973–5978, December 2010.

[6] S. Gorman, "Electricity grid in U.S. penetrated by spies," *The Wall Street Journal*, April 8th, 2009.

[7] P. Kundur, N. Balu, and M. Lauby, *Power System Stability and Control*. McGraw-Hill New York, 1994.

[8] D. Kundur, X. Feng, S. Liu, T. Zourntos, and K. Butler-Purry, "Towards a framework for cyber attack impact analysis of the electric smart grid," in *Proc. IEEE Int. Conf. Smart Grid Commu.*, (Gaithersburg, MD), pp. 244–249, Octorber 2010.

[9] O. Kosut, L. Jia, R. Thomas, and L. Tong, "Malicious data attacks on smart grid state estimation: Attack strategies and countermeasures," in *Proc. IEEE Int. Conf. Smart Grid Commu.*, (Gaithersburg, MD), Octorber 2010.

[10] A. Teixeira, H. Sandberg, and K. Johansson, "Networked control systems under cyber attacks with applications to power networks," in *Proc. IEEE Amer. Contr. Conf.*, (Baltimore, MD), pp. 3690–3696, June 2010.

[11] A. Shui, W. Chen, P. Zhang, S. Hu, and X. Huang, "Review of fault diagnosis in control systems," in *Proc. IEEE Conf. Dec. Contr.*, (Shanghai, China), pp. 5324–5329, Dec 2009.

[12] P. Menon and C. Edwards, "Fault estimation using relative information for a formation of dynamical systems," in *Proc. IEEE Conf. Dec. Contr.*, (Atlanta, GA), pp. 738–743, December 2010.

[13] R. V. Beard, *Failure accommodation in linear systems through self-reorganization*. PhD thesis, Massachusetts Institute of Technology, 1971.

[14] M. Massoumnia, G. Verghese, and A. Willsky, "Failure detection and identification," *IEEE Trans. Autom. Contr.*, vol. 34, no. 3, pp. 316–321, 1989.

[15] M. Massoumnia, "A geometric approach to the synthesis of failure detection filters," *IEEE Trans. Autom. Contr.*, vol. 31, no. 9, pp. 839–846, 1986.

[16] N. Meskin and K. Khorasani, "Fault detection and isolation of actuator faults in spacecraft formation flight," in *Proc. IEEE Conf. Dec. Contr.*, (San Diego, CA), pp. 1159–1164, December 2006.

[17] N. Meskin and K. Khorasani, "Actuator fault detection and isolation for a network of unmanned vehicles," *IEEE Trans. Autom. Contr.*, vol. 54, no. 4, pp. 835–840, 2009.

[18] W. Wonham, *Linear Multivariable Control: A Geometric Approach*. New York: Springer-Verlag, 1979.