HOKKAIDO UNIVERSITY

Title	Detection of False Data Injection Attacks in Distributed State Estimation of Power Networks
Author(s)	Obata, Sho; Kobayashi, Koichi; Yamashita, Yuh
Citation	IEICE transactions on fundamentals of electronics communications and computer sciences, E106A(5), 729-735 https://doi.org/10.1587/transfun.2022MAP0010
Issue Date	2023-05-01
Doc URL	https://hdl.handle.net/2115/90179
Rights	copyright©2023 IEICE
Type	journal article
File Information	Detection of False Data Injection Attacks in Distributed State Estimation ...tworks.pdf

Hokkaido University Collection of Scholarly and Academic Papers : HUSCAP

PAPER Special Section on Mathematical Systems Science and its Applications

Detection of False Data Injection Attacks in Distributed State Estimation of Power Networks*

Sho OBATA†, *Nonmember*, **Koichi KOBAYASHI**†a), *and* **Yuh YAMASHITA**†, *Members*

SUMMARY In a power network, it is important to detect a cyber attack. In this paper, we propose a method for detecting false data injection (FDI) attacks in distributed state estimation. An FDI attack is well known as one of the typical cyber attacks in a power network. As a method of FDI attack detection, we consider calculating the residual (i.e., the difference between the observed and estimated values). In the proposed detection method, the tentative residual (estimated error) in ADMM (Alternating Direction Method of Multipliers), which is one of the powerful methods in distributed optimization, is applied. First, the effect of an FDI attack is analyzed. Next, based on the analysis result, a detection parameter is introduced based on the residual. A detection method using this parameter is then proposed. Finally, the proposed method is demonstrated through a numerical example on the IEEE 14-bus system.

key words: *power networks, distributed state estimation, false data injection attacks, ADMM (Alternating Direction Method of Multipliers)*

1. Introduction

Cyber attacks against various control systems have attracted much attention (see, e.g., [9]–[13]). In a power network, the state estimation problem in the steady-state aims to estimate the state (the vector consisting of the bus phase angles) from the measured value (the vector consisting of active power flow measurements). In state estimation of steady-state power networks, a false data injection (FDI) attack that cannot be detected from the residual (i.e., the difference between the observed and estimated values) is well known [4], [6], [11], [14]. FDI attacks can be realized by attacking multiple sensors simultaneously under the assumption that an attacker knows the structure (i.e., the sensor placement) of a given power network. The effects of FDI attacks are then eliminated from the estimation error. An attacker can change the state, while the control system cannot detect this change from the value of the residual.

On the other hand, distributed optimization is effective in state estimation and control of large-scale systems. In the conventional distributed optimization method, a given system is decomposed into multiple subsystems. Each subsystem (slave node) solves the local optimization problem. An aggregator (master node) collects the computation results of subsystems, and updates the optimal value. Several methods for distributed optimization have been proposed (see, e.g., [3], [5], [15]). In particular, ADMM (Alternating Direction Method of Multipliers) [1] is well known as one of the powerful methods in distributed optimization. In [2], the ADMM-based distributed state estimation method has been proposed for a power network. In this method, it is assumed that there exist data deception attacks and denial of service (DoS) attacks. However, FDI attacks have been not considered.

In this paper, we propose a method for detecting FDI attacks in distributed state estimation using ADMM. FDI attacks cannot be detected from the converged estimated state obtained by ADMM. This is because elimination of FDI attacks from the residual occurs in the converged estimated state. On other hand, the effects of FDI attacks may be detected from the tentative estimated state before convergence. This is because elimination of the attack effect does not occur when starting ADMM. In the proposed method, the tentative residual in ADMM is used. First, the effect of FDI attacks is analyzed. Next, based on the analysis result, a detection parameter is introduced based on the residual. A detection method using this parameter is proposed. Finally, the proposed method is demonstrated through a numerical example on the IEEE 14-bus system. We show that a simple distributed solution method based on the least squares method is ineffective in the detection of FDI attacks in the IEEE 14-bus system (see Sect. 4.2 for further details of this method). Using the proposed method, FDI attacks can be detected.

This paper is organized as follows. In Sect. 2, state estimation of power networks, FDI attacks, and distributed state estimation are summarized as preliminaries. In Sect. 3, the effects of FDI attacks in ADMM are analyzed. Based on the results, a detection method is proposed. In Sect. 4, a numerical example is presented. In Sect. 5, we conclude this paper.

Notation: Let $\mathcal{R}$ denote the set of real numbers. Let $0_{m\times n}$ ($1_{m\times n}$) denote the $m\times n$ matrix whose element is 0 (1). Let I_n denote the $n\times n$ identity matrix. For the vector x, let $\|x\|$ denote the Euclidean norm of x.

2. Preliminaries

2.1 State Estimation of Power Networks

Consider state estimation of power networks with $n+1$ buses

Manuscript received April 15, 2022.
Manuscript revised August 31, 2022.
Manuscript publicized October 24, 2022.

†The authors are with the Graduate School of Information Science and Technology, Hokkaido University, Sapporo-shi, 060-0814 Japan.

*This work was partly supported by JSPS KAKENHI Grant Numbers JP19H02158, JP21H04558, JP22K04163.

a) E-mail: k-kobaya@ssi.ist.hokudai.ac.jp

DOI: 10.1587/transfun.2022MAP0010

Copyright © 2023 The Institute of Electronics, Information and Communication Engineers

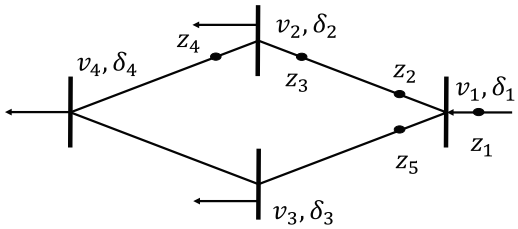

Fig. 1 An example of a power network.

in the steady-state. The bus phase angles are denoted by δ_i, $i = 1, 2, \ldots, n+1$. One (arbitrary) bus phase angle is fixed as a reference angle. In this paper, we fix δ_1 as $\delta_1 := 0$, and consider estimating only n angles. Let z_i, $i = 1, 2, \ldots, m$ denote the m active power flow measurements. Assume that the phase differences $\delta_i - \delta_j$ in the power network are sufficiently small. The following linear approximation is therefore accurate:

$$z = Hx,$$

where $z = [z_1, z_2, \ldots, z_m]^\top \in \mathcal{R}^m$ and $x = [\delta_2, \delta_3, \ldots, \delta_{n+1}]^\top \in \mathcal{R}^n$. For simplicity of discussion, we consider the noise-free case.

The matrix H can be derived from a given power network (see, e.g., [10]). For example, the matrix H of the power network shown in Fig. 1 can be obtained as

$$H = \begin{bmatrix} -1 & -1 & 0 \\ -1 & 0 & 0 \\ 1 & 0 & 0 \\ 1 & 0 & -1 \\ 0 & -1 & 0 \end{bmatrix}.$$

We also assume that $\mathrm{rank}(H) = n$. A solution $\hat{x}$ (i.e., the estimated value) minimizing $\frac{1}{2}\|Hx - z\|^2$ can be derived as

$$\hat{x} = (H^\top H)^{-1} H^\top z. \tag{1}$$

In this paper, the estimation method using (1) is called a centralized state estimation.

2.2 Distributed State Estimation

We summarize distributed state estimation using ADMM. Consider decomposing a power network into K subsystems. The matrix H and the vector z are decomposed into

$$H = \begin{bmatrix} H_1 \\ H_2 \\ \vdots \\ H_K \end{bmatrix}, \quad z = \begin{bmatrix} z_1 \\ z_2 \\ \vdots \\ z_K \end{bmatrix},$$

respectively. For simplicity of discussion, we assume that the size of H_i is the same (i.e., the size of z_i is also the same).

In the conventional ADMM, we consider the system consisting of K slave nodes and one master node (see Fig. 2). The slave node i has both H_i and z_i of the subsystem i. Using H_i and z_i, the slave node i calculates the estimated state $\hat{x}_i$,

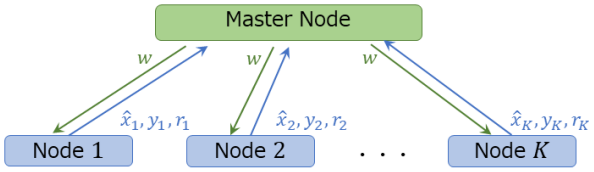

Fig. 2 A master node and slave nodes in ADMM.

Algorithm 1: Distributed state estimation using ADMM

Given $\varepsilon > 0, \gamma > 0, r_i^{(0)}, \hat{x}_i^{(0)}$, and $y_i^{(0)}$. Set $k = 0$.
while the stopping criterion ($\sum_i^K r_i^{(k)} < \varepsilon$) is not satisfied **do**
  $w^{(k+1)} = \frac{1}{K}\sum_{i=1}^K (\hat{x}_i^{(k)} - y_i^{(k)})$.
  Broadcast $w^{(k+1)}$ to all the local nodes.
  for $i = 1, 2, \ldots, K$ in parallel **do**
    $\hat{x}_i^{(k+1)} = \arg\min_z \frac{1}{2}\|H_i x - z_i\|^2 + \frac{1}{2\gamma}\|w^{(k+1)} + y_i^{(k)} - x\|^2$.
    $y_i^{(k+1)} = y_i^{(k)} + w^{(k+1)} - \hat{x}_i^{(k+1)}$.
    Send $\hat{x}_i^{(k+1)}$, $y_i^{(k+1)}$, and $r_i^{(k+1)} := \|H_i \hat{x}_i^{(k+1)} - z_i\|$ to the master node.
  end for
  $k \leftarrow k + 1$.
end while

the dual variables y_i, and the residual r_i as follows:

$$\begin{aligned} \hat{x}_i^{(k+1)} &= \arg\min_x \frac{1}{2}\|H_i x - z_i\|^2 \\ &\qquad + \frac{1}{2\gamma}\|w^{(k+1)} + y_i^{(k)} - x\|^2 \\ &= (\gamma I_N - \gamma^2 H_i^\top (I_{\frac{m}{K}} + \gamma H_i H_i^\top)^{-1} H_i) \\ &\qquad \times (H_i^\top z_i + \frac{1}{\gamma}(w^{(k+1)} + y_i^{(k)})), \end{aligned} \tag{2}$$

$$y_i^{(k+1)} = y_i^{(k)} + w^{(k+1)} - \hat{x}_i^{(k+1)}, \tag{3}$$

$$r_i^{(k+1)} := \|H_i \hat{x}_i^{(k+1)} - z_i\|.$$

The master node aggregates the computation result, and calculates the average as follows:

$$w^{(k+1)} = \frac{1}{K}\sum_{i=1}^K (\hat{x}_i^{(k)} - y_i^{(k)}),$$

which is sent to all the local nodes. A solution (i.e., the estimated state) minimizing the objective function $\frac{1}{2}\|Hx - z\|^2 (= \frac{1}{2}\sum_{i=1}^K \|H_i x_i - z\|^2)$ can be derived by Algorithm 1. Since the stopping criterion is checked in the master node, the estimated state can be obtained in this node. It is guaranteed that $\lim_{k\to\infty} \hat{x}_i^{(k)} = \hat{x}$ holds (see, e.g., [1] for further details).

Remark 1: One of the weak points in the conventional ADMM is to use a master node. A fully distributed ADMM method in which a master node is not required has been proposed (see, e.g., [2], [7]). For simplicity of discussion, we use the conventional ADMM. Depending on the computational environment, we may choose an appropriate ADMM method.

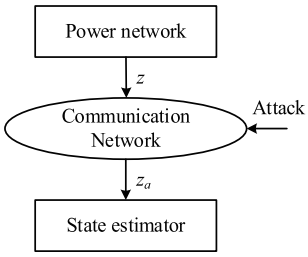

Fig. 3 Cyber attack in centralized state estimation.

2.3 False Data Injection Attack in Centralized State Estimation

In the centralized state estimation, as a method for detecting false data, we consider calculating the residual (i.e., the difference between the measured value z and the estimated value $H\hat{x}$). It is said that false data is injected if the following condition holds:

$$r := \|H\hat{x} - z\| > \tau, \tag{4}$$

where τ is a given threshold, and is determined from the tolerated error.

We suppose that a cyber attack through a communication network is detected by the state estimator (see Fig. 3). Here, we assume that an attacker knows the matrix H (i.e., the structure of the power network). Although an attacker can then change the state $\hat{x}$, the state estimator cannot detect this change from the value of the residual r. Such a cyber attack is called an FDI attack. In FDI attacks, we suppose that an attacker can change the measured value z to $z_a = z + a$, where $a = [a_1, a_2, \ldots, a_m]^\top$ is called an attack vector. We assume that the attack vector a is generated by $a = Hc$, where c is an arbitrary vector. The estimated state $\hat{x}_a$ after a cyber attack can be calculated by

$$\begin{aligned}\hat{x}_a &= (H^\top WH)^{-1}H^\top W z_a \\ &= \hat{x} + (H^\top WH)^{-1}H^\top WHc \\ &= \hat{x} + c.\end{aligned}$$

That is, $\hat{x}$ can be changed to $\hat{x} + c$ if an attacker utilizes $a = Hc$. However, in this case, the residual r is not changed as follows:

$$\begin{aligned}\|H\hat{x}_a - z_a\| &= \|H(\hat{x} + c) - (z + Hc)\| \\ &= \|H\hat{x} - z\|.\end{aligned}$$

Thus, by attacking multiple sensors, an attacker can achieve a tampering that cannot be detected by the state estimator.

3. Proposed Detection Method

3.1 Effect Analysis of FDI Attacks in ADMM

Now, we consider analyzing the effect of FDI attacks in ADMM. In this paper, we suppose the system configuration

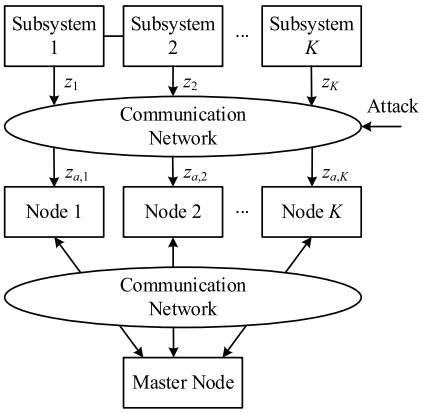

Fig. 4 Cyber attack in distributed state estimation.

shown in Fig. 4, where $z_{a,i}$ is the measured value of the subsystem i after a cyber attack. We assume that cyber attacks occur simultaneously in all subsystems. The master node judges whether an FDI attack has occurred. We remark that cyber attacks through a communication network between the master node and slave nodes are not considered. This is because this technical issue can be overcome by using, e.g., fully distributed ADMM methods [2], [7] and Blockchain technologies [8]. Since $\hat{x}_i^{(k)}$, $k = 0, 1, 2, \ldots$ converges to $\hat{x}$ in (1), elimination of FDI attacks occurs, where k is the number of turns. Hence, FDI attacks cannot be detected from the estimated state obtained by Algorithm 1.

We consider why ADMM eliminates FDI attacks. When an FDI attack does not occur, $\hat{x}_i^{(k+1)}$ and $y_i^{(k+1)}$ in Algorithm 1 can be expressed as (2) and (3), respectively. Using (2) and (3), the residual $r_i^{(k+1)}$ can be expressed as

$$\begin{aligned}r_i^{(k+1)} &= \|H_i\hat{x}_i^{(k+1)} - z_i\| \\ &= \|H_i(\gamma I_N - \gamma^2 H_i^\top (I_{\frac{m}{K}} + \gamma H_i H_i^\top)^{-1} H_i) \\ &\quad \times (H_i^\top z_i + \frac{1}{\gamma}(w^{(k+1)} + y_i^{(k)})) - z_i\| \\ &= \|(I_{\frac{m}{K}} + \gamma H_i H_i^\top)^{-1}\gamma H_i H_i^\top z_i \\ &\quad + (I_{\frac{m}{K}} + \gamma H_i H_i^\top)^{-1} H_i(w^{(k+1)} + y_i^{(k)})) - z_i\| \\ &= \|(I_{\frac{m}{K}} + \gamma H_i H_i^\top)^{-1} H_i(w^{(k+1)} + y_i^{(k)})) \\ &\quad - (I_{\frac{m}{K}} + \gamma H_i H_i^\top)^{-1} z_i\| \\ &= \|(I_{\frac{m}{K}} + \gamma H_i H_i^\top)^{-1}(H_i(w^{(k+1)} + y_i^{(k)}) - z_i)\|.\end{aligned}$$

Consider FDI attack detection using the residual after convergence. When an FDI attack does not occur, we have $w^{(k+1)} \to \hat{x}$, $y_i^{(k)} \to 0$ $(k \to \infty)$. Then, the converged residual r_i is expressed as

$$\begin{aligned}r_i &:= \lim_{k\to\infty} r_i^{(k+1)} \\ &= \lim_{k\to\infty} \|(I_{\frac{m}{K}} + \gamma H_i H_i^\top)^{-1} \\ &\quad \times (H_i(w^{(k+1)} + y_i^{(k)}) - z_i)\|\end{aligned}$$

$$= \|(I_{\frac{m}{K}} + \gamma H_i H_i^\top)^{-1}(H_i\hat{x} - z_i)\|.$$

Next, consider the case of the FDI attack. For each subsystem i, the measured value z_i is changed to $z_{a,i} = z_i + a_i$. The attack vector a_i is defined by $a_i = H_i c$. The values of w and y converge $w^{(k+1)} \to \hat{x} + c$, $y_i^{(k)} \to 0$ $(k \to \infty)$. Let $r_{a,i}^{(k+1)}$ denote the residual in subsystem i when an FDI attack occurs. The converged residual is expressed as

$$\begin{aligned}
\lim_{k\to\infty} r_{a,i}^{(k+1)} &= \lim_{k\to\infty} \|(I_{\frac{m}{K}} + \gamma H_i H_i^\top)^{-1} \\
&\quad \times (H_i(w^{(k+1)} + y_i^{(k)})) - (z_i + H_i c))\| \\
&= \|(I_{\frac{m}{K}} + \gamma H_i H_i^\top)^{-1}(H_i(\hat{x} + c) \\
&\quad - (z_i + H_i c))\| \\
&= \|(I_{\frac{m}{K}} + \gamma H_i H_i^\top)^{-1} \\
&\quad \times (H_i\hat{x} + H_i c - z_i - H_i c)\| \\
&= r_i,
\end{aligned}$$

which implies that also in the distributed state estimation, the residual in no attack case is the same as that in an attack case. In other words, the elimination of an FDI attack occurs.

Based on the above discussion, we consider using the residuals before convergence to detect the FDI attack. For some $T \ll \infty$, we can obtain

$$\begin{aligned}
r_{a,i}^{(T+1)} &= \|(I_{\frac{m}{K}} + \gamma H_i H_i^\top)^{-1}(H_i(w^{(T+1)} + y_i^{(T)}) \\
&\quad - (z_i + H_i c))\| \\
&\neq r_i^{(T+1)}.
\end{aligned}$$

In this case, the elimination of the FDI attack does not occur. Hence, the FDI attack appears in the residual, and can be detected.

3.2 Attack Detection in ADMM

Based on the results described in Sect. 3.1, we propose a detection method using tentative state estimation. Consider calculating the residual from tentative state estimation for each subsystem. Here, we use the residual $r_i^{(k)}$, $i = 1, 2, \ldots, K$, $k = 0, 1, \ldots, T$, where T is given in advance. We define the detection parameter for the subsystem i as

$$s_i := \sum_{k=0}^{T} r_i^{(k)}. \tag{5}$$

The value of the detection parameter s_i may increase or decrease due to FDI attacks. It is therefore necessary to set the upper and lower thresholds for the detection parameter. For some steady-state candidates, the value of the detection parameter s_i is estimated from numerical experiments of normal cases. The upper and lower thresholds are set using the estimation result and the tolerated error. From such preliminary experiments, the interval for the subsystem i in the normal condition, i.e.,

$$\underline{s}_i \le s_i \le \overline{s}_i \tag{6}$$

is estimated. State estimation using Algorithm 1 is applied at a certain time interval, and s_i can be then calculated. Let $s_i(t)$ denote the detection parameter s_i at time t. We then determine that an FDI attack occurs in the subsystem i at time t, if $s_i(t)$ does not satisfy (6). This condition can be judged in each slave node. Since s_i can also be calculated by the master node, this condition can also be judged in this node.

4. Numerical Example

4.1 Problem Setting

We explain the problem setting. Consider the IEEE 14-bus system [16], where n and m are given by $n = 13$ and $m = 20$, respectively. The matrix H is given by

$$H = \begin{bmatrix}
-1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & -1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
1 & -1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
1 & 0 & -1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
1 & 0 & 0 & -1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 1 & -1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 1 & -1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 1 & 0 & 0 & -1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 1 & 0 & 0 & 0 & 0 & -1 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 1 & -1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & -1 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & -1 & 0 & 0 \\
0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & -1 & 0 \\
0 & 0 & 0 & 0 & 0 & 1 & -1 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 1 & 0 & -1 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & -1 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & -1 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & -1 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & -1 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & -1
\end{bmatrix}.$$

The matrix H is decomposed into four matrices (i.e., $K = 4$ and $H_i \in \mathcal{R}^{5\times 13}$). We suppose that z and $\hat{x}^{(0)}$ are given by

$$\begin{aligned}
z = [&25.0, 34.9, 5.0, 10.0, 9.9, 5.0, 0.0, 15.0, 20.0, 24.9, \\
&11.7, 4.3, 8.7, 10.0, 5.0, 8.2, 16.8, 8.2, 4.3, 3.1]^\top
\end{aligned}$$

and $\hat{x}^{(0)} = -50 \times 1_{13\times 1}$, respectively. The vector c in the attack vector $a = Hc$ is given by $c = [0_{1\times 12}, 10]^\top$. In this example, we suppose that an attack to only the subsystem 4 represented by H_4 occurs.

4.2 Simple Solution Method

Based on the least squares method, we consider a simple method for distributed state estimation in which ADMM is not used. In the least squares method, a solution minimizing the sum of the squares of the residual is used as the estimated value. (1) is one of the typical examples. First, consider the attack-free case. In each subsystem, a quadratic programming (QP) problem is solved. First, the subsystem 1 solves the following QP problem:

Table 1 The results of distributed state estimation calculated by each subsystem.

Bus	State estimation			
	$\hat{x}_1$	$\hat{x}_2$	$\hat{x}_3$	$\hat{x}_4$
No.1	-25.01	-25.01	-25.01	-25.01
No.2	-30.02	-30.02	-30.02	-30.02
No.3	-35.03	-35.03	-35.03	-35.03
No.4	-34.99	-34.99	-34.99	-34.99
No.5	0	-59.91	-59.91	-59.91
No.6	0	-50.06	-50.06	-50.06
No.7	0	0	-60.06	-60.06
No.8	0	-55.09	-55.09	-55.09
No.9	0	0	0	-63.36
No.10	0	0	-71.63	-71.63
No.11	0	0	-64.31	-64.31
No.12	0	0	-68.70	-68.70
No.13	0	0	0	-71.90

$$\hat{x}_1 = \arg\min_x \frac{1}{2}\|H_1 x - z_1\|.$$

Non-zero elements in $\hat{x}_1$ are taken from $\hat{x}_1$, and are given by $L_1\hat{x}_1$, where L_1 is a binary matrix with appropriate size. The subsystem 2 solves the following QP problem:

$$\min_x \frac{1}{2}\|H_2 x - z_2\| \text{ subject to } L_1 x = L_1\hat{x}_1.$$

A solution for this QP problem is denoted by $\hat{x}_2$. Non-zero elements in $\hat{x}_2$ are taken from $\hat{x}_2$, and are given by $L_2\hat{x}_2$, where L_2 is a binary matrix with an appropriate size. The subsystem 3 solves the following QP problem:

$$\min_x \frac{1}{2}\|H_3 x - z_3\| \text{ subject to } L_2 x = L_2\hat{x}_2.$$

In a similar way, the subsystem 4 also solves the QP problem. A solution to the QP problem in the subsystem 4 is denoted by $\hat{x}_4$. The computation result is shown in Table 1. A solution for the QP problem solved by the subsystem 4 corresponds to (1). Thus, in this case, we can obtain a correct solution by such a simple method based on the least squares method.

Next, consider the attack case. A solution to the QP problem in the subsystem 4 is denoted by $\hat{x}_{a,4}$. In a similar way to the above method, we can obtain $\hat{x}_{a,4}$, as shown in Table 2, by sequentially solving the QP problems. From Table 2, we see that the 13th element of $\hat{x}_4$ is changed. That is, $\hat{x}_{a,4} = \hat{x}_4 + c$ holds. By validating this solution method based on some patterns of c, in this example, $\hat{x}_{a,i} = \hat{x}_i + c$ holds. From this fact, the value of the residual is expressed as

$$\begin{aligned} r_{i,a} &= \|H_i\hat{x}_{i,a} - z_{i,a}\| \\ &= \|H_i(\hat{x}_i + c) - (z_i + H_i c)\| \\ &= \|H_i\hat{x}_i - z_i\| \\ &= r_i. \end{aligned}$$

Elimination of FDI attacks occurs, and the value of the residual does not change. Therefore, we cannot detect the FDI attack using such a simple method.

Table 2 Comparison of the results of distributed state estimation in the attack case.

Bus	State estimation		
	$\hat{x}_{a,4}$	$\hat{x}_4$	c
No.1	-25.01	-25.01	0
No.2	-30.02	-30.02	0
No.3	-35.03	-35.03	0
No.4	-34.99	-34.99	0
No.5	-59.91	-59.91	0
No.6	-50.06	-50.06	0
No.7	-60.06	-60.06	0
No.8	-55.09	-55.09	0
No.9	-63.36	-63.36	0
No.10	-71.63	-71.63	0
No.11	-64.31	-64.31	0
No.12	-68.70	-68.70	0
No.13	-61.90	-71.90	10

Table 3 Detection results for each subsystem.

Subsystem	1	2	3	4
Lower Threshold	36	25	11	14
Upper Threshold	38	27	13	16
Parameter (Normal)	36.74	26.38	11.68	14.88
Parameter (Attack)	48.43	41.61	19.34	24.18

4.3 Proposed Method

Finally, we consider applying the proposed method based on ADMM. The parameters γ and ε in Algorithm 1 are given by $\gamma = 10$ and $\varepsilon = 1.0 \times 10^{-6}$, respectively. In the detection parameter s_i of (5), the parameter T is given by $T = 10$. The interval in (6) is given by

$$\begin{aligned} &36 \le s_1 \le 38, \;\; 25 \le s_2 \le 27, \\ &11 \le s_3 \le 13, \;\; 14 \le s_4 \le 16. \end{aligned}$$

The computation result is shown in Table 3. From this table, we see that the attacked values exceed the upper thresholds in all subsystems. As a result, we can detect the FDI attack in each subsystem. Although the FDI attack occurs in only the subsystem 4, the attack appears in all subsystems. This is because the master node shares the results of the state estimation of all subsystems. Figure 5 and Fig. 6 show a sequence of the residual in ADMM. From these figures, we see that the trends differ between the normal and attack cases. In the proposed method, such a difference is utilized.

5. Conclusion

In this paper, we proposed a method for detecting an FDI attack in distributed state estimation of a power network based on ADMM. The key idea is to use the residual of the tentative estimated state in the process of distributed state estimation. Furthermore, we presented the effectiveness of the proposed method on the IEEE 14-bus model.

There are several future challenges. First, in the proposed method, we focus only on a single steady state. However, depending on the operations of power networks, the

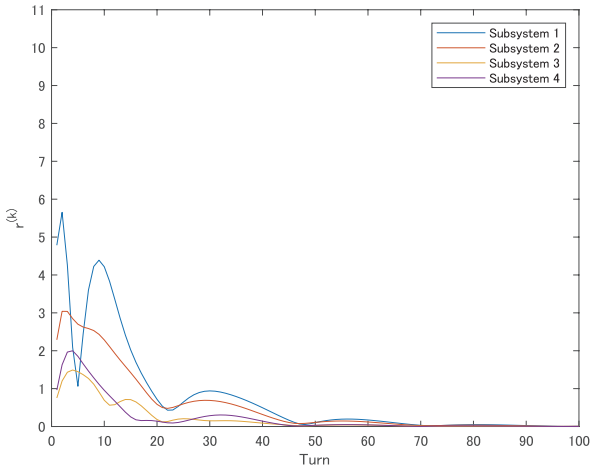

Fig. 5 Residual in the calculation process of ADMM (Normal case).

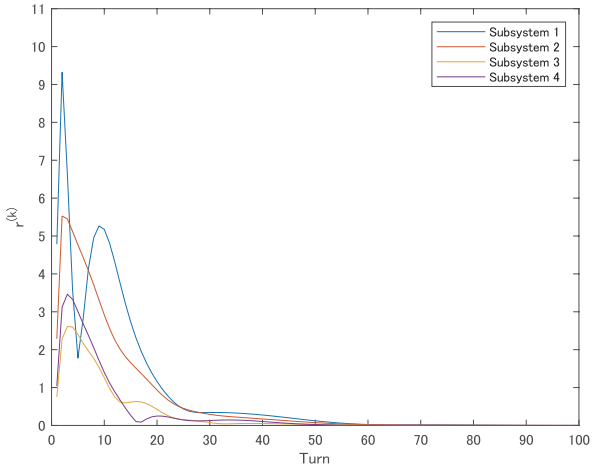

Fig. 6 Residual in the calculation process of ADMM (Attack case).

steady state is changed. In (6), the lower and upper thresholds must be also changed. In addition, these bounds also depend on the initial estimated value $\hat{x}_i^{(0)}$. It is important to develop a design method for the lower and upper thresholds based on the steady state and the initial estimated value. Next, it is also important to consider the dynamics of a power network. Finally, it is also one of the future efforts to validate the effectiveness of the proposed method under more real FDI attacks for a larger standard model of a power network.

References

[1] S. Boyd, N. Parikh, E. Chu, B. Peleato, and J. Eckstein, Distributed optimization and statistical learning via the alternating direction method of multipliers, Foundations and Trends in Machine Learning, vol.3, no.1, pp.1–122, 2011.

[2] D. Du, X. Li, W. Li, R. Chen, M. Fei, and L. Wu, "ADMM-based distributed state estimation of smart grid under data deception and denial of service attacks," IEEE Trans. Syst., Man, Cybern., Syst., vol.49, no.8, pp.1698–1711, 2019.

[3] N. Hayashi, T. Sugiura, Y. Kajiyama, and S. Takai, "Distributed event-triggered algorithm for unconstrained convex optimization over weight-balanced directed networks," IET Control Theory & Applications, vol.14, no.2, pp.253–261, 2020.

[4] B. Li, R. Lu, and G. Xiao, Detection of False Data Injection Attacks in Smart Grid Cyber-Physical Systems, Springer, 2020.

[5] H. Li, Q. Lü, Z. Wang, X. Liao, and T. Huang, Distributed Optimization: Advances in Theories, Methods, and Applications, Springer, 2020.

[6] Y. Liu, P. Ning, and M. Reiter, "False data injection attacks against state estimation in electric power grids," Proc. 16th ACM Conf. on Computer and Communications Security, pp.21–32, 2009.

[7] Y. Matsuda, Y. Wakasa, and E. Masuda, "Fully-distributed accelerated ADMM for DC optimal power flow problems with demand response," Proc. 12th Asian Control Conf., pp.740–745, 2019.

[8] D. Ogawa, K. Kobayashi, and Y. Yamashita, "Effectiveness and limitation of Blockchain in distributed optimization: Applications to energy management systems," IEICE Trans. Fundamentals, vol.E104-A, no.2, pp.423–429, Feb. 2021.

[9] F. Pasqualetti, F. Dörfler, and F. Bullo, "Control-theoretic methods for cyberphysical security: Geometric principles for optimal cross-layer resilient control systems," IEEE Control Syst. Mag., vol.35, no.1, pp.110–127, 2015.

[10] H. Sandberg, A. Teixeira, and K.H. Johansson, "On security indices for state estimators in power networks," First Workshop on Secure Control Systems, 2010.

[11] T. Shinohara and T. Namerikawa, "On the vulnerabilities due to manipulative zero-stealthy attacks in cyber-physical systems," SICE Journal of Control, Measurement, and System Integration, vol.10, no.6, pp.563–570, 2017.

[12] T. Shinohara, T. Namerikawa, and Z. Qu, "Resilient reinforcement in secure state estimation against sensor attacks with a priori information," IEEE Trans. Autom. Control, vol.64, no.12, pp.5024–5038, 2019.

[13] A. Teixeira, K.C. Sou, H. Sandberg, and K.H. Johansson, "Secure control systems: A quantitative risk management approach," IEEE Control Syst. Mag., vol.35, no.1, pp.24–45, 2015.

[14] D.B. Unsal, T.S. Ustun, S.M.S. Hussain, and A. Onen, "Enhancing cybersecurity in smart grids: False data injection and its mitigation," Energies, vol.14, no.9, article ID 2657, 2021.

[15] M. Yamashita, N. Hayashi, and S. Takai, "Dynamic regret analysis for event-triggered distributed online optimization algorithm," IEICE Trans. Fundamentals, vol.E104-A, no.2, pp.430–437, Feb. 2021.

[16] https://icseg.iti.illinois.edu/ieee-14-bus-system/

Sho Obata received the B.E. degree in 2020 and the M.I.S degree in 2022 from Hokkaido University. His research interests include cybersecurity.

Koichi Kobayashi received the B.E. degree in 1998 and the M.E. degree in 2000 from Hosei University, and the D.E. degree in 2007 from Tokyo Institute of Technology. From 2000 to 2004, he worked at Nippon Steel Corporation. From 2007 to 2015, he was an Assistant Professor at Japan Advanced Institute of Science and Technology. From 2015 to 2022, he was an Associate Professor at Hokkaido University. Since 2023, he has been a Professor at the Faculty of Information Science and Technology, Hokkaido University. His research interests include discrete event and hybrid systems. He is a member of IEEE, IEEJ, IEICE, ISCIE, and SICE.

Yuh Yamashita received his B.E., M.E., and Ph.D. degrees from Hokkaido University, Japan, in 1984, 1986, and 1993, respectively. In 1988, he joined the faculty of Hokkaido University. From 1996 to 2004, he was an Associate Professor at the Nara Institute of Science and Technology, Japan. Since 2004, he has been a Professor of the Graduate School of Information Science and Technology, at Hokkaido University. His research interests include nonlinear control and nonlinear dynamical systems. He is a member of SICE, ISCIE, IEICE, RSJ, and IEEE.