Enhancing Cyber-Security of Distributed Robust State Estimation

Identification of Data Integrity Attacks in Multi-Operator Power System

Shefaei, Alireza ; Mohammadpourfard, Mostafa ; Lakshminarayana, Subhash ; Mohammadi-Ivatloo, Behnam ; Anvari-Moghaddam, Amjad ; Roshan Milani, Karim

Published in:
2020 28th Iranian Conference on Electrical Engineering (ICEE)

DOI (link to publication from Publisher):
10.1109/ICEE50131.2020.9260709

Publication date:
2020

Document Version
Accepted author manuscript, peer reviewed version

Enhancing Cyber-Security of Distributed Robust State Estimation: Identification of Data Integrity Attacks in Multi-Operator Power System

Alireza Shefaei
Faculty of Electrical
and Computer Engineering
University of Tabriz
Tabriz, Iran
a.shefaei94@ms.tabrizu.ac.ir

Mostafa Mohammadpourfard
Department of Electrical
and Computer Engineering
Sahand University of Technology
Tabriz, Iran
mohammadpourfard@sut.ac.ir

Subhash Lakshminarayana
School of Engineering
University of Warwick
Coventry, United Kingdom
subhash.Lakshminarayana@warwick.ac.uk

Behnam Mohammadi-ivatloo
Faculty of Electrical
and Computer Engineering
University of Tabriz
Tabriz, Iran
bmohammadi@tabrizu.ac.ir

Amjad Anvari-Moghaddam
Department of Energy Technology
Aalborg University
Aalborg, Denmark
aam@et.aau.dk

Karim Roshan Milani
Deputy of Engineering and Planning Department
East Azerbaijan Electricity Distribution Company
Tabriz, Iran
kr_milani@yahoo.com

***Abstract*—State estimation (SE) has a crucial role to play in the monitoring and control of power grids. Although currently the SE is typically done in a centralized or hierarchical manner, distributed SE will become a significant alternative to centralized and hierarchical approaches in the future smart grids. This is because the power grids will be increasingly interconnected in future smart grids and the complexity scale of an interconnection will render centralized SE computationally formidable. Performing distributed SE requires leveraging advanced communication and computation technology. Nevertheless, relying on communication networks raises its susceptibility to data integrity attacks, such as false data injection (FDI) attacks. In this paper, we demonstrate that the attacker who compromises the communication infrastructure can launch an FDI attack on distributed SE which could circumvent present robust estimators and bad data detectors. Afterwards, to effectively defense against the proposed FDI attack, , two detection methods are proposed for two different modes of an interconnected power system. A detector is developed that validates the error of estimates of the state variables relative to their actual value as an index using a threshold value for different areas when the network is being run by an operator. A controlled information dissemination strategy is utilized to securely notify all areas of each other's proposed index when the network is being run by multiple operators. The proposed algorithms are validated on the IEEE 14-bus test system.**

I. Introduction

The geographical expansion of the power system along with its restructuring make distributed methods the primary option for executing power system functions. State estimation as one of the most important of these functions was also not excluded. By breaking the central energy management unit into several units distributed over the power system, it was no longer necessary to send measurements to a single center. This, in addition to removing many communication constraints, also significantly reduced the computational burden of executing the state estimation function. In this case, two modes can be used to operate the distributed system. One is the operation of the whole system by one operator but in distributed manner for some reasons such as reducing the computational burden. Another is the operation of each area by a single operator in the form of a restructured power system. Implementing distributed functions require the use of modern communication and information technologies (ICTs) [4]. However, the use of ICTs also poses challenges, including cyber attacks. False data injection attack (FDIA) is one of these attacks that has been extensively investigated in power systems [6]. In this attack the attacker by injecting a certain amount in measurements causes an error in the estimates made by the operator. The attack can even cause system-wide physical damage [7]. Hence its identification and the appropriate response to it, are the requirements for the safe operation of the distributed power system. For example, visualization [8], machine learning [9], sparse optimization [10], and moving target defense [11] can be numerated as attack detection methods. In distributed manner also can be mentioned to generalized cumulative sum [12] and statistical decision theoretic framework [13] as instances of detection methods. In this paper, first, the robust distributed state estimation was proposed in [1] is briefly explained. So, a distributed FDIA is introduced that in which the measurements corresponding to boundary buses in neighboring areas are used to falsify the distributed state estimation (DSE) in converging to true estimation. Then it is proved that the proposed attack can bypass the robust (RDSE) by showing no change of bad data vector after the attack. After explaining how the

interconnected power system can be operated by one operator or number of operators by number of areas, an attack detection method is presented for both modes. In the first mode, the operator calculates the error of areas and compares them with a threshold value and then finds the attacked area. In the latter mode, after receiving the approximate error of the different areas in a stepwise process, the operators of each area compare them and find out whether his area is under attack or not.

The rest of the paper is as follows. Section II describes the RDSE in power system. In Section III it is explained that how the proposed attack can get through the RDSE. Two detection and localization methods is presented in Section IV, and the numerical results is brought in Section V. Finally, Section VI concludes the paper.

II. The RDSE in Power System

Suppose an interconnected power system consists of K areas, which each one has M_k measurements ordered in vector $\mathbf{z}_k$ and N_k states ordered in vector $\mathbf{x}_k$. The measurements are the bus voltages and line currents measured by PMUs in rectangular form and the states are the voltage of all buses in the same form. An unknown vector $\mathbf{o}_k$ corresponding to measurements vector is defined to represent the bad data. Its entries are non-zero when bad data exist. There is a linear relation between measurements and states in each area $k \in \mathcal{K}$ as the following:

$$\mathbf{z}_k = \mathbf{H}_k \mathbf{x}_k + \mathbf{o}_k + \mathbf{w}_k, \tag{1}$$

in which $\mathbf{H}_k$ is the Jacobian matrix of area k and $\mathbf{w}_k$ is measurement error vector of this area. If $f_k(\mathbf{x}_k, \mathbf{o}_k; \mathbf{z}_k, \mathbf{H}_k)$ be the estimation function of area k, the states and bad data of each area can be estimated and identified by solving the optimization problem

$$\min_{\mathbf{x}_k, \mathbf{o}_k} \quad f_k(\mathbf{x}_k, \mathbf{o}_k; \mathbf{z}_k, \mathbf{H}_k) \tag{2a}$$

$$\text{s.t.} \quad \|\mathbf{o}_k\|_0 \leq \tau_0, \tag{2b}$$

that the constraint points that τ_0 bad data can be expected. Since the l_0-norm of (2b), which counts up the number of non-zero elements in the vector, makes the problem NP-hard, it is replaced with its l_1-norm in the subsequent equations. (2) can be extended as the following to estimate the all states of power system and identify all bad data in it in a centralized manner.

$$\min_{\mathbf{x}, \mathbf{o}} \quad \sum_{k=1}^{K} f_k(\mathbf{x}, \mathbf{o}) \tag{3a}$$

$$\text{s.t.} \quad \|\mathbf{o}\|_1 \leq \tau_1 \tag{3b}$$

The state of boundary buses in the state vector $\mathbf{x}$ of (3) is included as many neighboring areas as those buses have. For reaching to a decentralized state estimation, neighboring areas' dependence upon the boundary buses must be obviated. For this purpose, neighboring areas should share state variable of their boundary buses. So by introducing a constraint for boundary buses of each one of the two neighboring areas and making the state variables of both neighboring areas equivalent, we have

$$\min_{\mathbf{x}_k, \mathbf{o}_k} \quad \sum_{k=1}^{K} f_k(\mathbf{x}_k) + \lambda \|\mathbf{o}_k\|_1 \tag{4a}$$

$$\text{s.t.} \quad \mathbf{x}_{k,k'} = \mathbf{x}_{k',k}, \quad \forall k' \in \mathcal{N}_k, \forall k, \tag{4b}$$

where λ is a positive parameter to represent the (3) in the Lagrangian form and $\mathbf{x}_{k,k'}$ (and its equivalent, $\mathbf{x}_{k',k}$) is the vector of shared state variables between area k and k' and $\mathcal{N}_k$ is the set of neighboring areas of area k. Also vector $\mathbf{x}_{k,b}$ is defined as the vector of shared state variables between area k and its all neighboring areas. Moreover, since $\mathbf{o}_k$ belongs to a single area, it does not need to be shared. With the purpose of having a fully DSE, optimization problem (4) must be prepared for using methods for distributing optimization problems such as alternating direction method of multipliers (ADMM) [2]. To this end, Lagrange multipliers $\mathbf{v}_{k,k'}$ are introduced for each constraint of (3) [1]. The resulting iterative solution scheme is

$$\mathbf{x}_k^{(t+1)} = (\mathbf{H}_k^T \mathbf{H}_k + c\mathbf{D}_k)^{-1} (\mathbf{H}_k^T (\mathbf{z}_k - \mathbf{o}_k^{(t)}) + c\mathbf{D}_k \mathbf{p}_k^{(t)}) \tag{5a}$$

$$\mathbf{s}_k^{(t+1)} = \mathbf{U}_{\mathbf{x}_k} . \sum_{\forall k' \in \mathcal{N}_k} \mathbf{Y}_{k,k'} . \mathbf{x}_{k',k}^{(t+1)} \tag{5b}$$

$$\mathbf{p}_k^{(t+1)} = \mathbf{p}_k^{(t)} + \mathbf{s}_k^{(t+1)} - \frac{1}{2} (\mathbf{Y}_{k,b} . \mathbf{Y}_{k,b}^T . \mathbf{x}_k^{(t)} - \mathbf{s}_k^{(t)}) \tag{5c}$$

$$\mathbf{o}_k^{(t+1)} = \begin{cases} x + \lambda & x < -\lambda \\ 0 & |\, x \,| \leq \lambda \\ x - \lambda & x > \lambda \end{cases}, \tag{5d}$$

where $c > 0$ is a predefined constant, $\mathbf{D}_k$ is a diagonal matrix whose element $d_{i,i}$ equals the number of areas sharing the ith state variable of the vector $\mathbf{x}_k$, $\mathbf{U}_{\mathbf{x}_k}$ is a diagonal matrix whose diagonal element $u_{i,i}$ equals to the inverse of the number of areas (if greater than 0) sharing the ith state variable of the vector $\mathbf{x}_k$, and non-diagonal elements equal zero, and $\mathbf{Y}_{k,k'}$ is a matrix that determines the connection between vector $\mathbf{x}_k$ and vector $\mathbf{x}_{k,k'}$, and its elements $y_{i,j}$ equal one if the ith element (state variable) in $\mathbf{x}_k$ corresponds to the jth element (state variable) in $\mathbf{x}_{k,k'}$, and zero otherwise. Similar to the latter, matrix $\mathbf{Y}_{k,b}$ ($\mathbf{Y}_{b,k}$) determines the connection between vector $\mathbf{x}_k$ and vector $\mathbf{x}_{k,b}$ ($\mathbf{x}_{b,k}$), and its elements is determined as it was done for $\mathbf{Y}_{k,k'}$. Also x in (5d) is equal to $\mathbf{z}_k - \mathbf{H}_k \mathbf{x}_k^{(t+1)}$. When difference between the estimated value of one of ADMM's iterations and its previous iteration be less than a predefined value, it is said the DSE has been converged. If $t^* + 1$ be the mentioned iteration and ϵ be the *convergence threshold*, then $\forall k \in \mathcal{K}$, $\|\mathbf{x}_k^{(t^*+1)} - \mathbf{x}_k^{(t^*)}\|_\infty \leq \epsilon$. From the identification view, during the iterations, the procedure adjusts the measurements whose error exceeds the threshold λ by approaching their error to zero in order to provide a robust estimation.

III. Attack on the RDSE

The distributed FDIA and how it can get through the RDSE is described and proved in this section. The proposed distributed FDIA is theoretically explained in this subsection with a view to the purpose and manner of attack. The aim of attack is to disrupt the DSE from converging to its true estimations. This aim is achieved by means of boundary buses of neighboring areas. The proposed FDIA is conducted in such a way that it passes decentralized bad data detectors (BDDs) in addition to the centralized ones. Suppose the attacker has a complete information about the interconnected power system, i.e. measurements vector $\mathbf{z}_k$ and the Jacobian matrix $\mathbf{H}_k$ for all of the $k \in \mathcal{K}$ areas. Also she or he has access to all system's measurements for manipulation purpose. Consider a set of target boundary buses denoted by $\mathcal{B}_a$ which are common to a set of neighboring areas denoted by $\mathcal{K}_a$. If attacker wants to inject a value to the state of the target buses, she or he must launch FDIA in each one of the $K_a = |\mathcal{K}_a|$ areas separately but simultaneously. In more details, give $\mathbf{c}_i$ as injected vector to the state vector of attacked boundary buses $\mathbf{x}_a$ through area $i \in \mathcal{K}_a$, and $\mathbf{a}_i$ as attack vector of area i which is added to that area's measurements vector. So, the proposed distributed FDIA can be conducted as the form of adapted from FDIA's base paper [6] as the following

$$\mathbf{a}_i = \mathbf{H}_i \mathbf{c}_i, \qquad \forall i \in \mathcal{K}_a \tag{6}$$

$$\mathbf{z}_{a_i} = \mathbf{z}_i + \mathbf{a}_i, \qquad \forall i \in \mathcal{K}_a. \tag{7}$$

It should be noted that although the vectors $\mathbf{a}_i$ are independently injected to the measurements vector $\mathbf{z}_i$ of each area i, but this injection is occurred in the same time and on a unified samples of measurements. By following the instructions of [6], it is provable that the proposed attack can get through the BDDs. Give the RDSE as a prominent instance of BDDs. Since the role of measurement residual in DSE is performed by $\mathbf{o}_k$ vectors in RDSE, hence instead of using the method of [6], remaining the $\mathbf{o}_k$ vectors without change before and after the attack is used to prove bypassing the RDSE. Suppose (1) is solved using the least square error estimator as the following

$$\mathbf{x}_k = (\mathbf{H}_k^T \mathbf{H}_k)^{-1} \mathbf{H}_k^T (\mathbf{z}_k - \mathbf{o}_k). \tag{8}$$

To keep the value of vector $\mathbf{o}_i$ for the area $i \in \mathcal{K}_a$ unchanged after attack we must have:

$$|\mathbf{z}_i - \mathbf{H}_i \mathbf{x}_i| = |\mathbf{z}_{a_i} - \mathbf{H}_i \mathbf{x}_{a_i}|. \tag{9}$$

So, by substituting (6) and (7) in (9) and simplification, we can simply get $|\mathbf{o}_i| = |\mathbf{o}_{a_i}|$, which $\mathbf{o}_{a_i}$ denotes $\mathbf{o}_i$ under attack. This indicates that the vector $\mathbf{o}_k$ does not change after the attack and the proposed attack bypasses the RDSE.

Illustrative Example. Suppose the original measurements z_1 and z_2 of area 1 and 2, respectively, can pass the decentralized bad data detection (robust DSE) of [1]. The malicious measurements $z_{a1} = z_1 + a_1$ and $z_{a2} = z_2 + a_2$ of areas 1 and 2, respectively, can pass the decentralized bad data detection if a_1 and a_2 are a linear combination of the column vectors of H_1 and H_2, respectively, that is, $a_1 = H_1 c_1$ and $a_2 = H_2 c_2$. This definition is extendable to a boundary bus with more than two neighboring areas.

For bus 5 of the IEEE 14-bus test system (Fig. 1) and with an attack size of 0.05, c_1 and c_1 are 6×1 and 12×1 vectors that those non-zero arrays related to bus 5 are equal to 0.05. Vector a_1 is a 10×1 vector which its elements corresponding to the voltage magnitude of bus 5, line current (1,5), and (2,5) are non-zero and a_2 is a 14×1 vector which its element corresponding to the line current (4,5) is non-zero (all of parameters and variables have been expressed in rectangular coordinates). By considering 0.01 and 0.02 as standard deviation per real component of voltages and currents measurements, respectively, we run robust DSE [1] for 100 times and get the average of the obtained estimated states. It should be noted that the estimated value of magnitude and phase angle of bus voltage 5 in the normal condition are about 1.0118 and -0.1595 , respectively, that Represent the size of attack. Also, the o vector of robust DSE algorithm [1] indicates that the bad data is remained unchanged after the attack.

IV. Detection Methods

This section presents two detection methods for the attack described in the previous section on the DSE. One of these methods is when the power system is operated by an operator but in a distributed state. Another is for a situation where the power system is operated in a distributed manner by several independent operators working together. Before explaining these two methods, it is necessary to establish a criterion for measuring the accuracy of the estimates. Here, the estimated error of the state variables in the DSE relative to their actual value as (10) is used.

$$e_{o_k}^{(t)} = \frac{\|\mathbf{x}_k - \mathbf{x}_k^{(t)}\|_2}{N_k} \tag{10}$$

In this equation, $e_{o_k}^{(t)}$ is the per area error to the true state and $\mathbf{x}_k$ is vector of area k's true states.

A. A Visualization Method

The proposed method in this section assumes that an individual has measurements, parameters, and system status information and estimates for all areas of the distributed system. In this case, the operator can only detect the attack by computing the error of estimation of the areas and comparing their difference with a threshold value. For this propose, they calculate the per area error (10) of K areas and so compare the difference of the obtained values with each other. In this case, the biggest difference relates to the area that was attacked. In an equivalent and simpler way, the operator can draw and compare the per area error diagram of all areas on a single page. In this way, the area with the most error is the area under attack. In the method of this operation mode, when the difference between the error of areas is not exceeded the threshold, or when drawing all the areas overlapped (or very close to each other), it can be seen that no attack on the system has occurred. Detecting an attack by either measuring

the error of the areas or drawing an error diagram simply results in identifying its location. Detecting the location of the attack is partial, and given the commonality of boundary buses between neighboring areas, the proposed method helps identify the buses under attack by determining the neighboring areas.

B. A Distributed Method

The general model of operation of the restructured power system at present is its operation by several independent operators. In this case, since the estimation errors are not available to one person, it is not possible to use the previous subsection attack detection method. Hence, a new distributed attack detection method is presented in this section. The proposed method is based on the propagation of the error rates data of the areas with their neighboring areas in a way that does not compromise their privacy. The operator should not be trapped in the economic repercussions of exposing their estimation data while fleeing the attack. For this purpose, each area sends a message to the neighboring area by adding a bit of error to the error rate of its estimations, via a communication link intended to share the boundary bus estimates. The neighboring area does the same for the mentioned area. In the next step, each area reports its neighbor's error rate (obtained in the previous step) to its other neighboring areas. By repeating this method over and over again, all areas will find out the error rate of the other areas. At this point, all areas notice an area that has been attacked. The proposed detection procedure is explained in the following algorithm: Given that

Algorithm 1 Distributed Detection Method

1: **procedure**
2: **for all** $k \in \mathcal{K}$ **do**
3: add a value to its error
4: send its error to neighboring areas and receive their error
5: **end for**
6: **if** each area has the error of all areas **then**
7: compare the errors and localize the attacked area
8: **else**
9: **for all** $k \in \mathcal{K}$ **do**
10: send its neighboring areas' error to other neighboring areas and receive the error of neighbors of neighboring areas
11: **end for**
12: **if** each area has the error of all areas **then**
13: compare the errors and localize the attacked area
14: **else**
15: And so on ...
16: **end if**
17: **end if**
18: **end procedure**

the time required to send error rates to neighbors is equal to the time required to send boundary bus state estimates, it is not expected that the time required to detect an attack exceeds the time needed to execute the DSE. However, this depends on the arrangement and how the areas are connected in the distributed system.

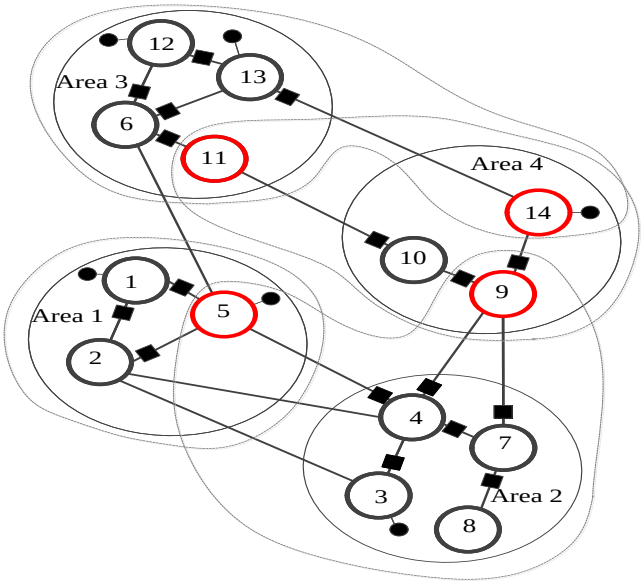

Fig. 1. The IEEE 14-bus system partitioned into four areas [1]. Dashed lassos show the buses belonging to area state vectors $\mathbf{x}_k$. PMU bus voltage (line current) measurements depicted by circles (squares). Boundary buses are distinguished by red circles.

V. Numerical Results

The numerical results of DSE, attack, and detection and localization methods are bought and discussed. The implementation environment is MATLAB 2015 and hardware is Intel Duo Core @ 2.6 GHz (2GB RAM). At first the DSE is run on the IEEE 14-bus system which is partitioned into four area as shown in Fig. 1. The numerical results of DSE and RDSE can be found in [1] in details, however the per area error curve for all of areas in normal condition is shown as in Fig. 2. As it can be seen from the Fig. 2, the error curve of all the areas is close and overlaps in the last iterations of the ADMM algorithm. Numerically speaking, the mean of per area error of area 1 to 4 for 100 run are 0.000280195, 0.00021197, 0.000116829, and 0.000175132, respectively, that their difference is less than 10^{-4}.

1) First Operation Mode: In this case, the whole system is operated in a distributed manner by one person, the attack on each of the areas as well as the simultaneous attack on the two boundary buses is investigated. Suppose the attacker inject 0.1 attack to the state of each one of the boundary buses using the manipulation of corresponding measurements of each buses.After run 100 times of RDSE and get the average, the Table I is obtained. The non-superscript error symbols in

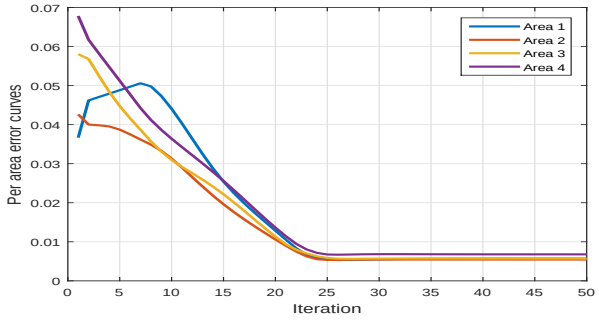

Fig. 2. Per area error curves.

TABLE I
THE AVERAGE OF 100 RUN RESULTS FOR ATTACK TO BOUNDARY BUSES

Attacked Area(s):	1	2	3	4	1&3
e_{o_1}	0.015487395	0.001834562	0.001692615	0.003982198	0.000860611
e_{o_2}	0.007845573	0.009115612	0.001288792	0.002881257	0.000913118
e_{o_3}	0.001812915	0.001105559	0.0105333375	0.009987055	0.001744574
e_{o_4}	0.00248189	0.013622524	0.013143816	0.01229558	0.001721832
Min Diff Error	0.007641822	0.004506912	0.002610441	0.002308525	0.000022742

the first column of the table correspond to the last iteration of the ADMM algorithm. The last row of the table shows the least error difference of the area with the maximum error with the nearest error. As is clear, this value is much larger for attack to an area than the threshold value 10^{-4} specified in the previous section. In the case of the fifth column, because the two areas are attacked, those two areas should compare their error with the areas that were not attacked.

The system operator can also easily detect an attack by drawing per area error curves. As shown in Fig. 3 and 4, the area under attack has substantially more error value, which is quite distinct when compared to Fig. 2. Regarding the Fig. 3(c) and Fig. 3(d), it should also be noted that the detection of the attack bus by the proposed method is approximate, yet the attack areas are accurately detectable.

2) Second Operation Mode: In this mode of operation, the results are exactly the same as those obtained in the previous section. However, because all four areas are operated by four different operators, not all of this information is available to a person who can detect and locate the attack. Therefore, the method described in Sec. IV-B is used. By applying Alg. 1 to the test system, a table like the following is created to share the error rate between the areas. It should be noted that this table is fixed for any type of attack and is only related to the system arrangement and how the areas are connected. As it is

TABLE II
THE PROCEDURE OF SHARING THE ERROR RATES BETWEEN AREAS

	Areas			
Steps	1	2	3	4
1	$1 \rightarrow 2$	$2 \rightarrow 1\&2 \rightarrow 4$	$3 \rightarrow 4$	$4 \rightarrow 2\&4 \rightarrow 3$
2	No Action	$4 \rightarrow 1\&1 \rightarrow 4$	No Action	$3 \rightarrow 2\&2 \rightarrow 3$
3	No Action	$3 \rightarrow 1$	No Action	$1 \rightarrow 3$

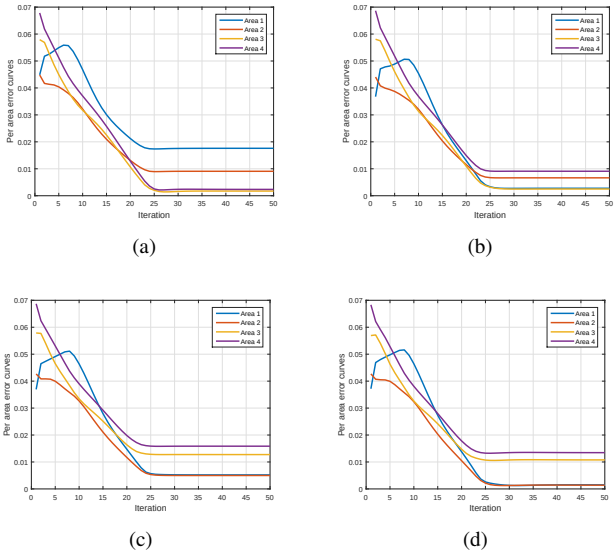

Fig. 3. Per area error of four areas estimation for attack to buses: (a) 5, (b) 9, (c) 14, and (d) 11.

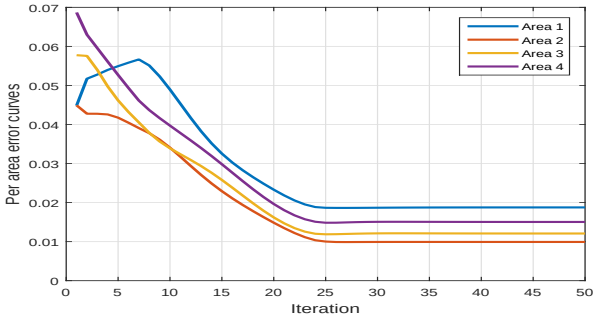

Fig. 4. Per area error of four areas estimation for attack to buses 5 and 11.

clear, after doing three repetitions, all the areas are aware of the error rates of the other areas. Consider the values in Table I by adding a random value of 0.1 of their values to preserve the privacy of the areas'information. In the meanwhile, if each area compares the error difference of the areas for each types of attacks, it will find the attacked area by comparing the values obtained with the threshold value 10^{-4}.

The time required to execute this algorithm is less than the time needed to execute the DSE program, since the execution time of each step of this algorithm is equal to the time of transferring the boundary buses' estimates between areas.

VI. CONCLUSION

A FDIA on DSE is proposed and it is proved that this attack can get through the distributed bad data detection methods with emphasis on RDSE. Two operation modes of an interconnected power system are described and for both of them an attack detection and localization method is provided. Per area error of estimation of distributed estimator to the true underlying state is defined as a measure to be used in

both detection methods. Comparison of the measure with a threshold value is used for operating the whole system by one person, and for operating each area by one person, the stepwise error dissemination is privately used. The simulations were done on IEEE 14-bus test system and the results indicate the applicability of the detection methods.

REFERENCES

[1] V. Kekatos and G. B. Giannakis, "Distributed robust power system state estimation," *IEEE Transactions on Power Systems*, vol. 28, no. 2, pp. 16171626, 2013.

[2] S. Boyd, N. Parikh, E. Chu, B. Peleato, J. Eckstein *et al.*, "Distributed optimization and statistical learning via the alternating direction method of multipliers," *Foundations and Trends® in Machine learning*, vol. 3, no. 1, pp. 1122, 2011.

[3] O. Vuković and G. Dán, "Security of fully distributed power system state estimation: Detection and mitigation of data integrity attacks," *IEEE Journal on Selected Areas in Communications*, vol. 32, no. 7, pp. 15001508, 2014.

[4] M. Shahidehpour and Y. Wang, *Communication and control in electric power systems: applications of parallel and distributed processing.* John Wiley & Sons, 2004.

[5] M. Mohammadpourfard, Y. Weng, and M. Tajdinian, "Benchmark of machine learning algorithms on capturing future distribution network anomalies," *IET Generation, Transmission& Distribution*, vol. 13, no. 8, pp. 1441-1455, Apr 2019.

[6] Y. Liu, P. Ning, and M. K. Reiter, "False data injection attacks against state estimation in electric power grids," *ACM Transactions on Information and System Security (TISSEC)*, vol. 14, no. 1, p. 13, 2011.

[7] J. Liang, L. Sankar, and O. Kosut, "Vulnerability analysis and consequences of false data injection attack on power system state estimation," *IEEE Transactions on Power Systems*, vol. 31, no. 5, pp. 3864–3872, 2015.

[8] M. Mohammadpourfard, A. Sami, A. R. Seifi, "A statistical unsupervised method against false data injection attacks: A visualization-based approach", *Expert Systems with Applications*, vol. 84, pp. 242-261, Oct. 2017.

[9] M. Mohammadpourfard, A. Sami, Y. Weng, "Identification of false data injection attacks with considering the impact of wind generation and topology reconfigurations", *IEEE Transactions Sustainable Energy*, vol. 9, no. 3, pp. 1349-1364, Jul. 2018.

[10] L. Liu, M. Esmalifalak, Q. Ding, V. A. Emesih, and Z. Han "Detecting false data injection attacks on power grid by sparse optimization." *IEEE Transactions Smart Grid*, vol. 5, no. 2, pp. 612-621, Mar. 2014.

[11] Z. Zhang, R. Deng, D. Yau, P. Cheng, and J. Chen, "On effectiveness of detecting fdi attacks on power grid using moving target defense," in *2019 IEEE Power & Energy Society Innovative Smart Grid Technologies Conference (ISGT)*. IEEE, 2019, pp. 15.

[12] S. Li, Y. Yilmaz, X. Wang, "Quickest detection of false data injection attack in wide-area smart grids", *IEEE Transactions Smart Grid*, vol. 6, no. 6, pp. 2725-2735, Nov. 2015. 2014.

[13] R. Anguluri, V. Katewa, and F. Pasqualetti, "Centralized versus decentralized detection of attacks in stochastic interconnected systems," *arXiv preprint arXiv:1903.10109*, 2019.