IEEE Open Access Journal of Power and Energy

Received 9 July 2022; revised 1 November 2022; accepted 3 December 2022.
Date of publication 19 December 2022; date of current version 13 January 2023.

Digital Object Identifier 10.1109/OAJPE.2022.3230905

Analysis of Targeted Coordinated Attacks on Decomposition-Based Robust State Estimation

NAIME AHMADI[1] (Student Member, IEEE), YACINE CHAKHCHOUKH[2] (Senior Member, IEEE), AND HIDEAKI ISHII[1] (Fellow, IEEE)

[1]Department of Computer Science, Tokyo Institute of Technology, Yokohama 226-8502, Japan
[2]Department of Electrical and Computer Engineering, University of Idaho, Moscow, ID 83843 USA

CORRESPONDING AUTHOR: N. AHMADI (ahmadi@sc.dis.titech.ac.jp)

This work was supported in part by JSPS under Grant-in-Aid for Scientific Research under Grant 22H01508, in part by JST-Mirai Program under Grant 18077648, and in part by a Grant-in-aid of the Tokyo Tech Academy of Energy and Informatics. The work of Yacine Chakhchoukh was supported in part by the Idaho Global Entrepreneurial Mission (IGEM) Grant for Security Management of Cyber-Physical Control Systems, in 2016, under Grant IGEM 17-001.

ABSTRACT The impact of false data injection (FDI) attacks on static state estimation of power systems has been actively studied in the past decade. In this paper, we consider an estimation method that first decomposes the system into islands and then implements robust regression estimators at the island level as well as the system level. We carry out an analysis to establish its advantages in terms of state estimation accuracy and attack detections. In particular, we focus on highly adversarial cases where the attacker can attack both the measurement vector and the regressor matrix and attempts to manipulate the states to targeted values. Our estimation approach employs a system decomposition method capable to generate islands small in their sizes and applies the robust estimation method of least trimmed squares. We make comparisons with methods using other decompositions and other robust estimators. To this end, we analyze the structure of the system topology and measurements and perform extensive simulations using the IEEE 14- and 118-bus systems. Furthermore, we investigate robustness improvement when phasor measurement units (PMUs) are available and hybrid state estimation can be employed.

INDEX TERMS Cyber-physical security, false data injection attacks, cycle detection methods, coordinated leverage point attacks, robust state estimation, phasor measurement units.

I. INTRODUCTION

FOR the safe and efficient operation of the power grid, the system is constantly monitored and operated at the control center. In practice, the operators use a static state estimator (SE), which provides the state of the grid [1] and permits the online security analysis. The static SE gives the optimal state consisting of bus voltage phasors estimated from redundant measurements commonly provided by supervisory control and data acquisition (SCADA) units at remote terminal units and intelligent electronic devices, including active and reactive power flows and injections, and bus voltage magnitudes. More recently, the availability of phasor measurement units (PMUs) has enabled hybrid state estimation combining both PMUs and SCADA measurements in the observation set [2] to improve SE accuracy and performance. Placing a PMU at a bus can provide the voltage phasor at that bus, and the phasor currents on several or all lines incident to that bus [3].

Recently, the increase in cyber attack incidents has raised concerns for the problem of SE security [4]. Under nominal operations, measurement errors could be present due to noise, equipment failures, and modeling errors and are detected by analyzing the residuals of the weighted least squares AC static SE. However, when an attacker launches malicious false data injection (FDI) attacks in the measurements with the knowledge on the system parameters and grid topology, the estimated states may be manipulated to targeted values without being detected as the residuals may remain small or unchanged [5], [6], [7], [8]. Recent works deal with FDI attack strategies which can be generated even if the attacker

has only limited information such as data of a subnetwork [9] and limited PMU data [10]. In the literature, various FDI attack detection methods have been proposed; see the survey paper [11] and the references therein.

On the other hand, different FDI attack scenarios against the SE have been considered. One class of adversarial attacks known to be hard to detect is that of leverage point attacks, which target the entries in the Jacobian matrix of the regression model of SE, e.g., [8], [12], [13], [14], [15]. Such attacks can be generated by introducing changes in the network parameters and topology data stored at the system operators. Recently, it is shown in [16] that modifying network parameters can reduce the necessary number of FDI attacks. In the abovementioned works, it has been established that to obtain accurate state estimates under adversarial environments, robust estimation techniques (e.g., [17]) can be especially useful, including the least trimmed squares (LTS) [8], [13], [14], [18], [19], [20] and the robust Huber M-estimator [12]. Difficulties in SE when the data in the regressor model may contain uncertainties and the importance of robust methods have been recognized in the early works of [20], [21], [22] from the 1990s. In [13], it has been proposed to use multiple robust estimators in parallel to enhance the capability of attack detections.

In this context, to deal with large-scale systems, decomposition of the grid is also found effective in [8] and [20], where in each island the SE can be performed. This approach enables robust SE algorithms to increase the number of outliers in the data that the estimator can tolerate, or the so-called breakdown points [17]. In our previous work [15], we have developed a graph-based method to automatically decompose power systems and, specifically, found that in increasing the breakdown points of the islands, the planar face traversal (PFT) algorithm [24] is useful. This feature is due to its capability to identify islands having small sizes.

In this paper, we consider the robust SE approach of [8] and [15] against adversarial attacks especially when the attacks are more targeted and coordinated. The robust SE approach is based on two techniques: (i) Decomposition of the grid into islands and (ii) use of the LTS estimator at the island/subsystem level. The LTS is known as a particularly robust SE method; it ignores a fixed number of measurements corresponding to residuals with large magnitudes. In [15], we demonstrated the superiority of our PFT-based decomposition method over other decomposition approaches. Comparisons were made in terms of breakdown points for various IEEE systems with 14, 30, 57, 118, 145, and 300 buses. However, the SE performance was verified only through simulations using random FDI attacks.

Here, we aim to further improve our PFT-based robust SE method and expose its strength and limitations under FDI cyber-attacks of various degrees and placements. First, we analyze the properties of the decomposed grid from the viewpoint of the local state estimation executed at the islands. Its advantages are highlighted in comparison to islands obtained by a simpler graph-theoretic cycle detection based on the minimum spanning tree (MST) method. Then, through simulation studies, we will demonstrate the difference between the decomposition methods and the robust SE methods. The following two developments are critical in our study:

(i) One is the enhanced version of the SE algorithm from [8] and [15] consisting of three steps as follows: It first runs the LTS decentrally at each island level and then centrally at the entire system level; its robustness is enhanced by the residual analysis carried out as the third step.

(ii) We construct adversarial coordinated FDI attacks against certain targeted buses in the system. Specifically, we attack the power injections at those targeted buses and their adjacent buses in both their measurements and the corresponding rows of the regressor matrix. By increasing the number of attack points, the attacker can eventually manipulate the state values of the targeted buses. In general, even by robust SE methods, the attacks on the regressor matrix are hard to resist and detect.

These techniques will be thoroughly tested by simulations on the IEEE 14- and 118-bus systems, and the impact of both randomly generated and targeted coordinated FDI attacks will be examined. For comparison reasons, we equip our algorithm with several robust SE schemes including the LTS, the Huber M-estimation, and the least absolute value (LAV). Furthermore, some of them as well as the conventional largest normalized residual (LNR) with a bad data detection (BDD) module will be implemented in a fully centralized fashion. Under three classes of attacks, we will demonstrate that our SE scheme clearly outperforms when equipped with the PFT-based decomposition in terms of accuracy on SE and attack detection probabilities especially when the regressor matrix is under coordinated attacks. We will moreover show that introducing PMUs can increase the SE performance.

The paper is organized as follows. Section II reviews static state estimation, bad data detection, and the attack models. Section III introduces robust estimation techniques and also the decomposition methods of power systems. Section IV analyzes the targeted attacks on decomposition-based SE. Section V presents the simulation results under several attack scenarios. Finally, in Section VI, we conclude the paper.

II. PROBLEM FORMULATION

A. STATIC STATE ESTIMATION PROBLEM

State estimation uses three kinds of data as inputs: (i) The network topology data, consisting of the on/off status of power network switches and circuit breakers between buses; (ii) the measurement data, including voltage magnitudes, power injections and flows; and (iii) the parameter data, including the branch admittance data and the variances of measurement noises. The network topology and measurement data are communicated to the control center from SCADA units. After the system's observability is verified, the weighted least squares (WLS) AC state estimator algorithm is executed to obtain the estimates of the state variables x, which

are the voltage magnitudes and phase angles at all buses of interest.

The measurement equation is expressed as $z = h(x) + e$, where $x \in R^n$ and $z \in R^m$ denote the state vector and the measurement vector, respectively, with $n \leq m$. Further, $e \in R^m$ denotes the error vector, which is assumed to follow the normal distribution with zero mean and covariance matrix R, i.e., $e \sim \mathcal{N}(0, R)$. The state variables are related to the measurements by the nonlinear measurement function $h(\cdot)$ [1].

To execute the state estimation in real time, a simplified model based on linearization is commonly used [1]. The optimal estimate of the state can be obtained as $\hat{x} = \arg\min_{\hat{x}} \left[z - h(\hat{x})\right]^T R^{-1} \left[z - h(\hat{x})\right]$. This can be computed by the iterations as $\hat{x}^{k+1} = \hat{x}^k + \Delta x^k$, where $\Delta x^k = \left[H^T R^{-1} H^T\right]^{-1} H^T R^{-1} \left(z - h(\hat{x}^k)\right)$, where $H \in R^{m \times n}$ is the regressor matrix and k is the index of the iteration. The matrix H is the Jacobian of the measurement function $h(\cdot)$ with respect to the state x. The state increment Δx^k is obtained by regressing $z - h(\hat{x}^k)$ on H. The algorithm terminates once the norm of Δx^k becomes smaller than a given threshold. Afterwards, bad data detection (BDD) is applied.

B. BAD DATA DETECTION

The BDD module is essential to protect state estimation from outliers' effects. The measurement data is checked to remove any abnormal values. After the state estimation process converges, the residuals are calculated as $r^k = z - h(\hat{x}^k)$. If any entries of r^k are large in magnitude, the corresponding measurements are eliminated, and the SE is re-executed with the remaining data. The estimation and BDD are re-iterated until such large residuals do not appear.

In practical SE, the largest normalized residual (LNR) is used with the chi-square test in the BDD [1]. This is based on the normalized residual given by $r_i^N = \frac{|r_i|}{\sqrt{S_{ii} R_{ii}}}$, where r_i is the ith element of the residual r and S is the residual sensitivity matrix given by $S = I - H(H^T H)^{-1} H^T$. If the largest normalized residual is larger than a pre-determined threshold, e.g., $|r_i^N| > 3$, it is eliminated from the measurements in the next state estimation. The estimation is re-executed until no outlier is detected.

C. MODEL OF FALSE DATA INJECTION ATTACKS

The attacker is assumed to be capable of launching FDI attacks on SE inputs corresponding to a limited number of buses, including the measurement, topology, and parameter data. We consider the more adversarial scenario where the attacker has the information about elements in the regressor matrix H. In such a case, the following two classes of attacks are particularly effective:

(i) One consists of those against the measurements. The attacker may generate stealthy attacks of the form $z_c = z + Hc$, where c is a sparse vector with nonzero values at entries corresponding to the targeted buses [5]. The attack is stealthy in the sense that the residuals are not modified, and conventional detection schemes based on analyzing the residuals cannot detect the attacks.

(ii) The other consists of those against the regressor matrix. Such attacks are called leverage point attacks [23], [25], and the matrix is modified in the form $H_c = H + \delta H$, where δH contains nonzero columns corresponding to the targeted buses. If a column in H is multiplied by a chosen scalar in an attack, the attack will control the corresponding state, and the residuals will be kept unchanged. The attack becomes stealthy, and the estimated state will be manipulated and becomes the corrupted value targeted by the attacker. To generate such attacks, the attacker needs access to the line connections, parameters, and sensors adjacent to the targeted buses.

III. ROBUST ESTIMATION VIA GRID DECOMPOSITION

In this section, we outline a robust estimation technique from our previous work [15] and its modified version based on topology decomposition and robust estimation methods designed to resist FDI attacks discussed above.

A. ROBUST ESTIMATORS

Robust estimators are designed to reduce the influence of bad data on state estimation. One key feature of such estimators is to reduce the weights given to bad data. This is in contrast to the WLS, where large residuals have more influence on the objective function. Here, we summarize the LTS estimator that we mainly use in our simulation studies later. Other robust estimators that we employ there are the least absolute value (LAV) method and Huber M-based SE.

The LTS minimizes a trimmed percentage of the regression squared residuals [17]. We use the notation $\underline{r}$ to express the sorted version of the residual r in its entries from the smallest to the largest in magnitude as $\underline{r}_1^2 \leq \underline{r}_2^2 \leq \cdots \leq \underline{r}_m^2$. Then, the LTS finds the estimate x that minimizes the cost function

$$J(x) = \sum_{i=1}^{m_T} \underline{r}_i^2, \tag{1}$$

where $m_T = \lfloor (1 - \alpha)m \rfloor + 1$ is the number of measurements used after trimming, α corresponds to the trimming fraction, and $\lfloor \cdot \rfloor$ is the floor function.

For any of the robust estimators mentioned above, its capability when FDI attacks are present in the measurements and topology data can be represented by their (finite-sample) breakdown points [17]. This is the maximum fraction of outliers in the measurements that the estimator can resist while offering reliable estimates before breaking down. The LTS is known to be one of the most robust methods and, specifically, its maximum breakdown point can be expressed as $\epsilon_{\max,m} = \frac{1}{m} \lfloor \frac{s^*}{2} \rfloor$, where s^* is the minimum number of measurements whose removal make at least one measurement critical for performing state estimation [22]. The challenging part for its calculation is that when the system is large, the computation of s^* can be expensive as it involves combinatorial aspects.

B. DECOMPOSITION INTO ISLANDS

In the power system, we might encounter buses with a low number of measurements and connections, which would impose a constraint on the breakdown point for the entire system. To keep the influence of such buses limited, it is effective to decompose the grid into several islands [8], [15], [20], [22]. Islands can be categorized into two types, radial and cyclic. In particular, finding small cycles is important for raising the cyber-security level of state estimation [15].

In this paper, we follow the approach of [15] and decompose the system into islands with three properties: (i) Each bus belongs to at least one island. (ii) The number of buses in each island is small. (iii) The total number of islands is small. As mentioned earlier, these properties help in general the robust estimation method based on LTS employed in this paper. We must note however that the level of benefits resulting from these properties may depend on the specific structures and the parts in the system where the individual islands are. For the detection of cycles, we compare two methods, namely, one based on the minimum spanning tree (MST) [26] and the other based on the planer face traversal (PFT) algorithm employed in [15]. We summarize each method below.

The MST method is simple. It finds a spanning tree in the graph representing the grid and then by adding an edge not part of the spanning tree, we can find a cycle. This however may not result in islands of small sizes nor those with high breakdown points. In contrast, in the PFT-based method, if a *planar graph* (i.e., a graph written on a plane without any intersections of edges) is given, it will find all the faces (i.e., the subgraphs of minimal cycles) and there will be no overlap among the subgraphs. This is based on the PFT algorithm [24]. In [15], details on how to efficiently deal with intersections in graphs to extend the approach are provided.

To enhance robustness in static SE based on islanding and robust techniques from [8] and [15] as discussed above, we provide a modified version of the procedure. Specifically, we follow the three-step algorithm outlined as follows:

(i) As the first step, robust estimation is performed at each island. After its convergence, normalized residuals are calculated for the estimates. Then, the residuals larger than a specified threshold will be chosen as outliers and leverage points in each island.

(ii) In the second step, the corresponding outlier entries are removed from the measurement vector z and the regressor matrix H of the entire system. The SE for the entire system is then performed based on the WLS. Afterwards, the outliers and leverage points detected in the first step are put back, and we calculate the normalized residuals for the second time. The normalized residuals larger than a threshold are chosen as the final outliers and leverage points.

(iii) The third step is for ensuring the accuracy level of estimation and reducing unobservability. After removing detected outliers from the second step, we make the state estimate for the last time.

The difference from the original approach in [8] and [15] lies in the second round of outlier detection and state estimate for the entire system in the second and third steps. This takes account of the chances that the residual-based outlier detections at the island level can be erroneous. To keep the number of false detections low, the choices of thresholds in these steps are important especially when the attacks are adversarial.

IV. TARGETED ATTACKS ON DECOMPOSITION-BASED SE

In this section, we demonstrate the effectiveness of the robust estimation method discussed above by analyzing it against a class of coordinated attacks targeting certain buses and their adjacent buses in the system. Here, we describe the system setting and the attack strategies using the IEEE 14-bus system shown in Fig. 1. Later in the paper, we extend our analysis to a larger-scale case with the IEEE 118-bus system.

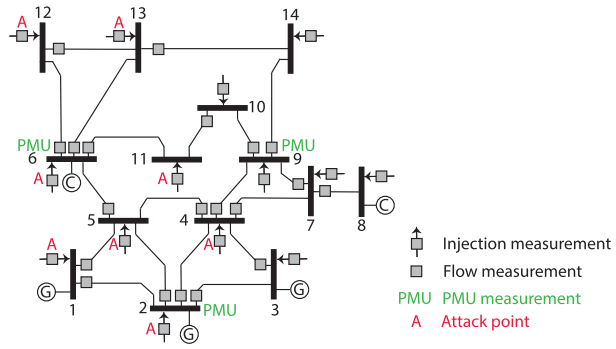


FIGURE 1. IEEE 14-bus system and the placement of measurements and attacks.

A. IEEE 14-BUS SYSTEM: DECOMPOSITION AND ITS RESILIENCY

In the power system, each bus is assumed to have measurements for voltage magnitude and both active and reactive power injections; each line has measurements for one active and one reactive power flows at its ends. For the case of the IEEE 14-bus system, there are 27 states (excluding the phase angle of the slack bus) and 82 measurements in total.

First, we decompose the system based on the PFT-based and the MST-based methods. Table 1 gives the summary of the numbers of islands, the average number of buses in each island, the numbers of buses in the largest islands, and the computation times. We notice that the PFT-based method is capable to find islands of smaller sizes. The details of the decomposition are presented in Table 2.[1] The islands are denoted as I_i, $i = 1, \ldots, 10$. Those common in both PFT- and MST-based methods are $I_1 = \{1, 2, 5\}$, $I_2 = \{2, 3, 4\}$, $I_3 = \{4, 9, 7\}$, and $I_4 = \{6, 12, 13\}$. The additional islands for the PFT-based method are $I_5 = \{2, 4, 5\}$,

[1]Note that there is one radial island, $\{7, 8\}$. This island is vulnerable to attacks due to the small number of measurements. Hence, it is assumed to be equipped with secure measurements and is not subject to attacks.

TABLE 1. Decomposition of the IEEE 14- and 118-bus system by two methods.

	14-bus		118-bus	
Decomposition method	PFT-based	MST-based	PFT-based	MST-based
Number of islands	8	8	68	71
Average number of buses in each island	3.62	4.25	4.41	6.49
Number of buses in the largest island	6	8	13	20
Computation time (sec)	0.516	0.212	4.36	0.09

TABLE 2. Islands obtained from the two decomposition methods and active power measurements linked to buses 2 and 6 in each island.

	Islands in both methods				Islands in PFT-based method			Islands in MST-based method		
Island indices	I_1	I_2	I_3	I_4	I_5	I_6	I_7	I_8	I_9	I_{10}
Buses	1,2,5	2,3,4	4,7,9	6,12,13	2,4,5	4,5,6, 9,10,11	4,5,6, 9,13,14	1,2,4,5	1,2,4,5, 6,9,10,11	1,2,4,5, 6,9,13,14
Breakdown point	1/3	1/3	1/3	1/3	1/3	1/6	1/6	1/4	1/8	1/8
# all active power meas.	6	6	6	6	6	12	12	8	16	16
# attacks to produce masked attacks	3	3	3	3	3	3	3	3	3	3
# attacks to produce targeted attacks	4	4	4	4	4	10	10	6	14	14
Active power measurements linked to bus 2										
P_{1-2}	1	0	0	0	0	0	0	1	1	1
P_{2-3}	0	1	0	0	0	0	0	0	0	0
P_{2-4}	0	1	0	0	1	0	0	1	1	1
P_{2-5}	1	0	0	0	1	0	0	0	0	0
$\underline{P_1}$	**1**	0	0	0	0	0	0	**1**	**1**	**1**
$\underline{P_2}$	**1**	**1**	0	0	**1**	0	0	**1**	**1**	**1**
P_3	0	1	0	0	0	0	0	0	0	0
$\underline{P_4}$	0	**1**	**1**	0	**1**	**1**	**1**	**1**	**1**	**1**
$\underline{P_5}$	**1**	0	0	0	**1**	**1**	**1**	**1**	**1**	**1**
Active power measurements linked to bus 6										
P_{5-6}	0	0	0	0	0	1	1	0	1	1
P_{6-11}	0	0	0	0	0	1	0	0	1	0
P_{6-12}	0	0	0	1	0	0	0	0	0	0
P_{6-13}	0	0	0	1	0	0	1	0	0	1
P_5	1	0	0	0	1	1	1	1	1	1
$\underline{P_6}$	0	0	0	**1**	0	**1**	**1**	0	**1**	**1**
$\underline{P_{11}}$	0	0	0	0	0	**1**	0	0	**1**	0
$\underline{P_{12}}$	0	0	0	**1**	0	0	0	0	0	0
$\underline{P_{13}}$	0	0	0	**1**	0	0	**1**	0	0	**1**

The underlined entries correspond to those attacked based on the attack strategy given in Table III.

$I_6 = \{4, 5, 6, 11, 10, 9\}$, and $I_7 = \{4, 5, 6, 9, 13, 14\}$ while those for the MST-based method are $I_8 = \{1, 2, 4, 5\}$, $I_9 = \{1, 2, 4, 5, 6, 9, 10, 11\}$, and $I_{10} = \{1, 2, 4, 5, 6, 9, 13, 14\}$. For these islands, their breakdown points for the LTS were calculated as shown in Table 2. Here, we observe that PFT-based islands take larger values than the MST-based ones. More specifically, it was found that for this measurement configuration, each island can tolerate up to 2 attacks regardless of its size. This means that smaller islands have larger breakdown points, indicating the advantages of the PFT-based islands. In calculating the breakdown points, we took a decoupled approach to reduce the burden of computation. In particular, we considered only active power measurements for the phase angle estimation. It is known that reactive power and voltage magnitude measurements are only weakly linked to phase angles [1].

B. TWO CLASSES OF FDI ATTACKS AGAINST THE LTS

In our simulations using the LTS, in every island, we set the number of measurements discarded to be 2 in estimation against attacks. Under this setting, the LTS may produce false state estimations depending on the number of attacks and there are two scenarios:

(i) In an island, when the number of attacks is greater than the number of trimmed measurements (i.e., 2 in all islands), the local state estimate in that island may become inaccurate; such attacks are called *masked attacks*.

TABLE 3. Attacked measurements in the IEEE 14-bus system simulations.

Number of attacks N_s	1	2	3	4	5	6	7	8
Measurements under falsification	P_2	P_6	P_1	P_4	P_{11}	P_{13}	P_{12}	P_5
Islands unable to estimate phase 2	–	–	–	I_8,I_9,I_{10}	I_8,I_9,I_{10}	I_8,I_9,I_{10}	I_8,I_9,I_{10}	I_1,I_5, I_8,I_9,I_{10}
Islands unable to estimate phase 6	–	–	–	–	–	–	I_4	I_4

(ii) In an island, when the number of coordinated attacks is greater than or equal to the total number of measurements minus the number of trimmed measurements (given as m_T in (1)), the LTS might detect the remaining clean data as outlying. Such attacks can result in estimates at values chosen by the attacker, and hence can be much more harmful to the system. Such attacks are referred to as *targeted attacks* [8].

Table 2 indicates the number of FDIs necessary to create such attacks for each island.

C. RESILIENCE ANALYSIS OF THE TWO DECOMPOSITION METHODS

In the scenario considered here, the attacker aims to modify the phases of the target buses 2 and 6. Here, the attacks will be limited to FDIs against the active power injections at these buses and their neighboring buses. To this end, the attacker attempts to gain access to the active power measurements linked to these buses and then to inject false data there. In our experiment, we demonstrate the effects of attacks by gradually increasing the number of attack points, denoted by N_s, from 1 to 8. In particular, the order of the attacked buses (in their active power injections) is shown in Table 3. Note that when we say N_s attacks are made, measurements shown under 1 to N_s in the second row of this table will be under falsification. The attacker falsifies the measurements as well as the rows of the Jacobian matrix related to these attacked buses. By increasing the number of attacks, islands failing to generate accurate estimation will increase even by using the LTS.

At this point, we would like to discuss that when FDI attacks are launched on buses 2 and 6 and their neighbors, the islands from the PFT-based method have advantages over those from the MST-based method. To this end, we make a more careful inspection of the islands obtained from both methods. By the topology of the system shown in Fig. 1, we see that the two target buses have multiple neighboring buses. The neighbors of bus 2 are buses 1, 3, 4, and 5 while those of bus 6 are buses 5, 11, 12, and 13.

First, we notice that more MST-based islands contain bus 2 than the PFT-based ones, which may already indicate that attacking bus 2 can have more impact on MST-based state estimation. In fact, as shown in Table 2, among the seven PFT-based islands, only three of them contain bus 2. In contrast, among the seven MST-based islands, five of them have bus 2. On the other hand, the number of islands containing bus 6 are six for both decomposition cases; the attack impact for this case needs further analysis.

Second, there is a certain inclusion relation among the islands from the two methods. For example, the PFT-based island $I_5 = \{2, 4, 5\}$ is fully contained in the MST-based island $I_8 = \{1, 2, 4, 5\}$ as $I_5 \subset I_8$. Similarly, it holds $I_6 \subset I_9$ and $I_7 \subset I_{10}$. These relations indicate that in general, the impact of attacks can be greater on the MST-based islands than that on the PFT-based islands as they form a superset.

Third, among the PFT-based islands I_5, I_6, and I_7, the common buses can be found to be $I_5 \cap I_6 \cap I_7 = \{4, 5\}$ whereas among the MST-based islands I_8, I_9, and I_{10}, the common buses are $I_8 \cap I_9 \cap I_{10} = \{1, 2, 4, 5\}$. This indicates that targeting not only bus 2 but also bus 1 can be problematic in the local SE at MST-based islands. Having overlaps in the islands can create vulnerabilities because when buses contained in many islands are attacked, all of those islands can be affected in the SE performance.

Finally, among the PFT-based islands, bus 6 is contained in two islands, namely, I_6 and I_7. However, these islands do not contain bus 2. Hence, for PFT-based SE, the FDI attacks on the two target buses may have more independent effects. This is clearly different for MST-based SE, since the two islands I_9 and I_{10} contain both of the target buses 2 and 6; hence, attacking these buses may have more combined effects.

To make a more detailed analysis, from the attack pattern shown in Table 3, we can generate the lower part of Table 2, where the relations between active power measurements and their connections to islands are shown with entries 1 (linked) and 0 (not linked). Now, let's consider the case when the attacker attacks four measurements with N_4 and manipulates P_1, P_2, P_4, and P_6. From the table, we confirm that at least three of these measurements are linked to all three islands given by the MST-based method, i.e., I_8, I_9, and I_{10}. Consequently, the LTS may not be capable to make precise estimates of states or to correctly find the outliers because the number of trimmed measurements is set to 2. In Table 3, the third and fourth rows show the indices of the islands for which the numbers of attacks N_s exceed their breakdown points.

On the other hand, in all remaining islands, at most two measurements are linked. Islands I_1, I_2, and I_5 have three measurements linked to bus 2 which are not attacked and thus the chance of producing correct results is higher. We note that in our robust scheme, each state is estimated in multiple islands; even if some islands fail to make accurate estimation of some states, they may be recovered by other islands. This is the reason for adding the third step in our robust SE algorithm discussed in Section III-B.

In conclusion, from the analysis and discussion so far, it is evident that the PFT-based islands should be more resilient

compared to the MST-based ones in general but especially under attacks targeting certain buses. We will confirm this aspect through simulations in the next section.

D. DISCUSSION ON DETECTION OF RANDOM ERRORS AND ATTACKS

How to distinguish between real events and FDI attacks is an important question in the context of ensuring a reliable and secure grid monitoring. Real events that can be potentially detected through our method include sensor failures, sensor noises, topology errors such as wrong states of circuit breakers and lines (open/close), and parameter errors. Sensor failures and noises occur sporadically in a limited number of sensors, mostly without much correlation. Such events can be detected by our method but may be difficult to be distinguished from attacks. If attack/failure detection continues over time at some sensors, they must be checked.

Opening lines in the system is a much more serious real event regardless of whether they are caused by faults and resulting protection actions, operator controls, or physical attacks. If one line is made open, measurements near this line will change at once. If it is a normal topology change or a fault, then the measurement changes will be consistent in the system, and this can be detected or known to the operator by other means. The proposed approach may not detect such changes by making one estimate run, partly because the least trimmed squares estimation depends on the majority of data. Moreover, under coordinated cyber-physical attacks that open a line and change all the measurements linked to this line in a consistent manner, detection would be difficult by any method using a single time snapshot. These attacks require extensive access and knowledge by the attacker and are known as stealthy attacks. These stealthy attacks could be detected, for example, by monitoring the time series in the measurements and state estimates or by securing specific sensors. For more on the subject of detection of random errors and attacks, we refer to the survey paper [11] and the references therein.

V. SIMULATION RESULTS

In the simulations, we compare the performance of state estimation as well as detection of outliers in the measurement data for seven different schemes. First of all, as estimation algorithms, we employ the following four: The conventional LNR and the robust estimators using LTS, Huber M, and LAV. Four schemes are based on the robust algorithms applied to the decomposed islands obtained from the PFT- and MST-based methods; these are denoted LTS_{PFT}, LTS_{MST}, M_{PFT}, and LAV_{PST}. Further, for comparison purposes, three schemes apply the LNR, Huber M, and LAV to the entire system in a centralized fashion, without decomposition; these are denoted with the subscript C as LNR_{C}, M_{C}, and LAV_{C}.

A. SIMULATION SETUP FOR THE IEEE 14-BUS SYSTEM

For the IEEE 14-bus system, we import the MATPOWER data from [27]. The slack bus is taken to be bus 1, whose voltage angle is fixed to zero. The error in each SCADA measurement follows the normal distribution with zero mean and standard deviation of 0.66% of the original value plus a fixed value of 0.0017. The LTS algorithm proposed in [28] is adapted to handle the sparsity in the AC SE. For the Huber M-estimator, the threshold parameter was taken as 1.345. For the detection of attacks, several thresholds are used. For the conventional LNR_{C}, the threshold is chosen to be 3 while for M_{C} and LAV_{C}, we have chosen the threshold to be 7. In the robust estimation schemes LTS_{PFT}, LTS_{MST}, M_{PFT}, and LAV_{PFT}, at each island, the threshold of 5 is used in the first step; then, in the second step, where we apply additional post-estimation processing to the whole system, we use the threshold of 7. These specific values for the thresholds were chosen after some trial runs so as to minimize the false detection alarm rates in the clean case (without attacks). (In the simulation results, the false detection alarm rates are shown in Fig. 4 (b), where the no attack case corresponds to the first row.)

For each attack case, we make Monte Carlo simulations of 100 times ($M_c = 100$). To compare the estimation accuracy of the different schemes, we evaluate the average estimation error for voltage angles in degrees as $x_e = \frac{1}{n_b M_c} \sum_{k=1}^{M_c} \left\| \hat{x}^k - x_T \right\|$, where n_b is the number of buses, $\hat{x}^k$ is the estimate from the kth Monte Carlo run, and x_T is the true state (i.e., the power flow solution). As the base case under the described conditions, without any attacks, the LNR for the centralized scheme results in the average error 0.1142.

B. ATTACKS ON MEASUREMENTS

In this part, we apply two types of attacks on the measurements and compare the seven estimation schemes.

(a) First, we generate random attacks according to Table 3, where each attacked measurement is falsified by adding a uniformly random number between 20 to 60 percent of the original measurement value. Specifically, in the case when N_s points are attacked, the attack values are set as $\delta z_i = b_i z_i$ with $b_i \sim \mathcal{U}(0.2, 0.6)$ for $i = i_1, \ldots, i_{N_s}$, where i_j is the index of the jth attacked measurement in Table 3. Then, the attacked measurement vector z_c is generated as

$$z_{c,i} = \begin{cases} z_i + \delta z_i & \text{if } i = i_1, \ldots, i_{N_s}, \\ z_i & \text{otherwise.} \end{cases} \tag{2}$$

The results of the average estimation errors in phase angles (in degrees) are shown in Fig. 2 (a) in heatmap format. We observe that all schemes are capable to achieve good estimation at least up to seven attacks. It is notable that the centralized schemes perform quite well.

(b) As a more adversarial case, we consider measurement attacks in a more coordinated fashion. Specifically, the attack vector is set as $\delta z = Hc$, where c is a sparse vector with $c_i = 0.12$ rad for the entries corresponding to the phases of the targeted buses 2 and 6 and zero otherwise. Then, in the case when N_s points are attacked, the falsified measurements are generated by (2). The results of the average estimation

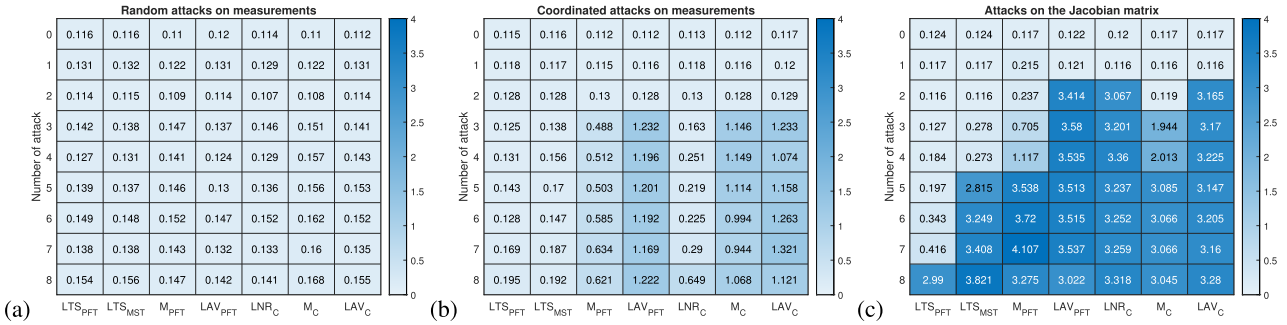


FIGURE 2. **Average estimation errors in degrees under (a) random attacks on measurements, (b) coordinated attacks on measurements, and (c) attacks on the Jacobian matrix.**

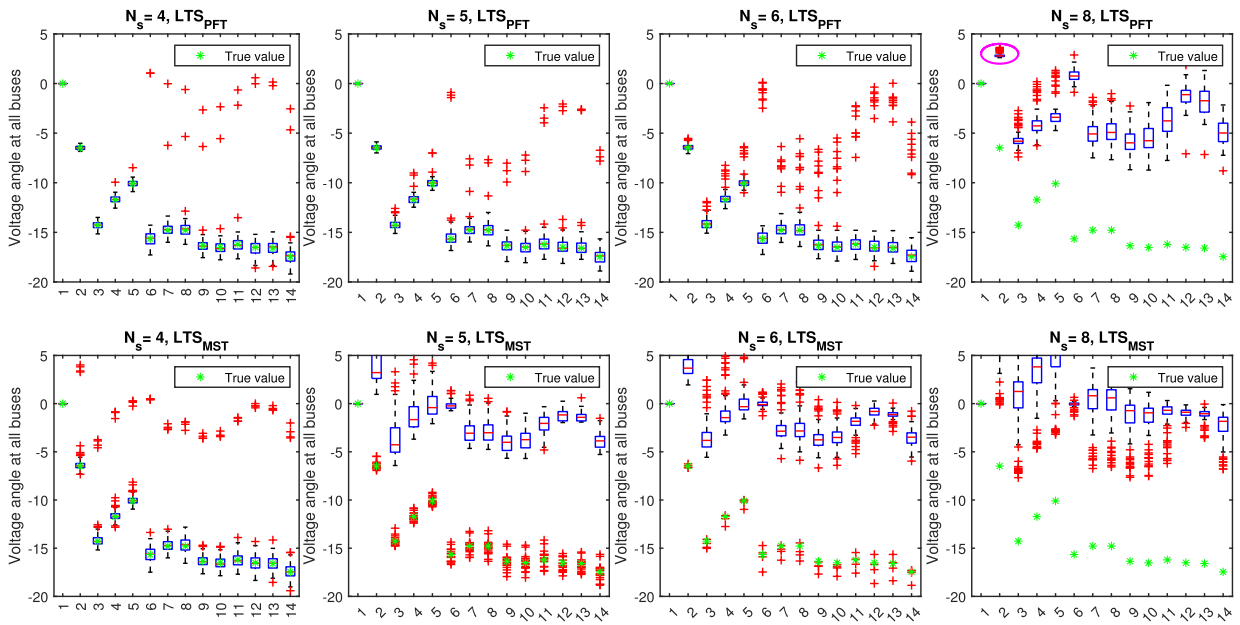


FIGURE 3. **Estimated phase angles of 14 buses by LTS-PFT (top) and LTS-MST (bottom) under attacks on the Jacobian matrix for $N_s = 4, 5, 6, 8$.**

errors are shown in Fig. 2 (b). In this case, the two LTS-based schemes demonstrate to be the most robust, tolerating up to seven attacks. Other methods quickly become unreliable. The Huber M and LAV for both centralized and decomposition-based schemes can handle only up to two attacks while the conventional centralized LNR manages up to three attacks.

C. ATTACKS ON THE JACOBIAN MATRIX

Next, we examine the effects of attacks on the Jacobian matrix, resulting in leverage points. Here, we also follow the attack strategy in Table 3 and gradually increase the number N_s. To this end, the attack values on H are generated by first setting the matrix $\delta H \in R^{m\times n}$ as

$$[\delta H]_{i,j} = \begin{cases} (\eta - 1)[H]_{i,j} & \text{if } j \text{ corresponds to phase} \\ & \text{angle of bus 2 or 6,} \\ 0 & \text{otherwise,} \end{cases}$$

for $i = 1, \ldots, m$ with $\eta = -3$. Then, the attacked Jacobian matrix H_c is set as

$$[H_c]_{i,j} = \begin{cases} [H]_{i,j} + [\delta H]_{i,j} & \text{if } i = i_1, \ldots, i_{N_s}, \\ [H]_{i,j} & \text{otherwise,} \end{cases}$$

for $j = 1, \ldots, n$. Under this attack, the estimated phases of the targeted buses 2 and 6 will become one third of the true estimate values. In the current setting, the true phase of bus 2 is -6.48 deg, and hence, after the modification by the intruder, it becomes $-6.48/\eta = 2.16$ deg.

Fig. 2 (c) shows the average estimation errors for the seven estimation schemes. Under this attack scenario, we clearly see the advantage of LTS based on the PFT decomposition method. In particular, the difference from the LTS-MST method becomes more evident as we increase the number of attacks to more than four points. Fig. 3 shows the phase angle estimations of all buses for LTS-PFT and LTS-MST in detail in box plots obtained from the Monte Carlo simulations. The green asterisks in the plots are the (true) power flow values.

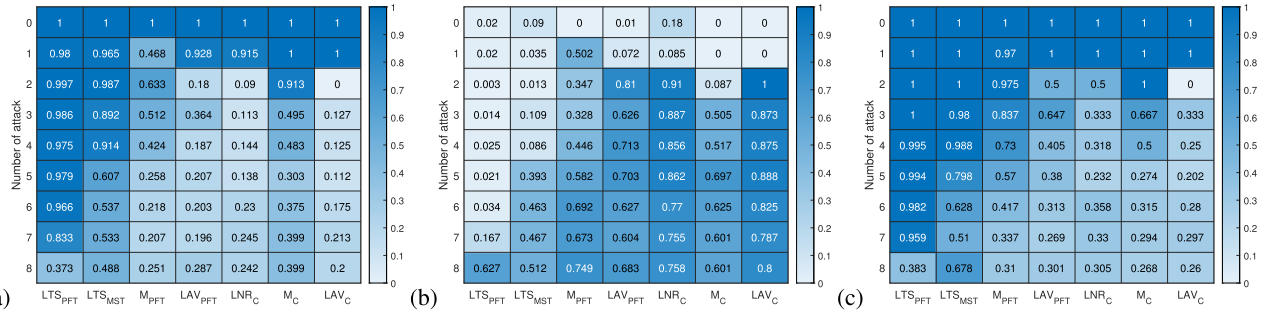


FIGURE 4. **(a) The estimated probability of detection, (b) the estimated probability of false detection, and (c) the true probability of detection of leverage points.**

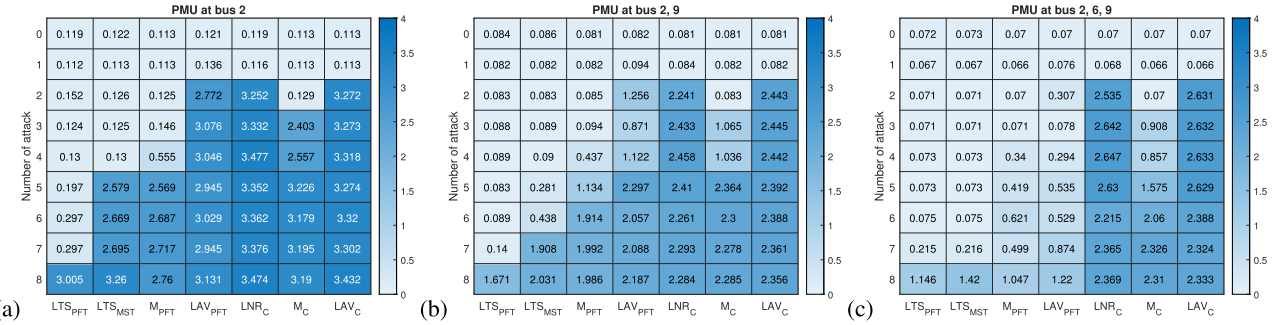


FIGURE 5. **Average estimation errors in degrees with PMUs at (a) bus 2, (b) buses 2 and 9, and (c) buses 2, 6, and 9 under coordinated attacks on the Jacobian matrix.**

When the number of attacks is $N_s = 4$, the difference between the two methods can be found in erroneous estimations in the MST-based results, indicated by the red pluses; this difference is not visible from the average estimation error data in Fig. 2 (c). Here the attack points are P_1, P_2, P_4, and P_6, and these make the estimation of the large-sized islands I_8, I_9, and I_{10} for the MST-based method vulnerable as it goes beyond the breakdown points in these islands (see Table 2). As a consequence, the estimation in these islands fails to properly detect the attack points. In contrast, under the PFT-based method, all islands remain functional in estimation. Moreover, when we increase the attacks to five points, the MST-based method totally breaks down as shown in both Fig. 2 (c) and Fig. 3. Finally, by increasing the attacks up to eight points for the PFT-based method, the phase angle at bus 2 moves to the targeted value of 2.16 deg (shown with a magenta circle in Fig. 3 for LTS_{PFT} with $N_s = 8$). This occurs even though for some islands, the number of attacks may not be enough for realizing targeted attacks (as shown in Table 2). This is because the Jacobian matrix is sparse.

As demonstrated above, the LTS based on the PFT method well outperforms other estimation schemes, especially in comparison to the conventional LNR_{C}, which is popular in practice. We would like to highlight now that even when the estimation accuracy starts to degrade after the number of attacks goes beyond 4 or so, our approach can provide good performance in terms of detection of the attacked measurements. To show this, we introduce three performance measures as follows: (a) The estimated probability of leverage point detection given by $P_l = \frac{1}{M_c}\sum_{k=1}^{M_c} \frac{n^l_{T,k}}{n^l_{T,k}+n_{F,k}}$, where $n^l_{T,k}$ is the number of detected leverage points truly present in the attack for each run k and $n_{F,k}$ is the number of falsely detected leverage points. (b) The estimated probability of false detection given by $P_f = \frac{1}{M_c}\sum_{k=1}^{M_c} \frac{n_{F,k}}{n^l_{T,k}+n_{F,k}}$. (c) The true probability of leverage point detection $d_l = \frac{1}{M_c}\sum_{k=1}^{M_c} \frac{n^l_{T,k}}{n_l}$, where n_l is the number of the leverage points introduced.

The results for these three measures (a)–(c) are shown in Fig. 4. In general, we observe that the LTS-PFT outperforms all other schemes in all three detection measures. In particular, the difference from the LTS-MST method becomes evident after N_s becomes larger than 5. Moreover, the measures for LTS-PFT indicate its high reliability in attack detection up to $N_s = 7$. Other schemes may be considered reliable in detecting only 1 leverage point except for M_{C}, which exhibits good performance when $N_s = 2$ also. In the robust statistics literature, it is known that the Huber M, LAV, and LNR are vulnerable to leverage points [17], [29], [30].

D. HYBRID ESTIMATION UNDER ATTACKS ON THE JACOBIAN

In this last part, we would like to see the effectiveness of introducing more measurements to the system and in particular use PMUs under attacks on the Jacobian as in the previous subsection. Following [31], we place PMUs at buses 2, 6, and 9 for phasor measurements. We use the errors from MATPOWER with the normal distribution of zero mean and standard deviation of 0.2 deg [27]. Here, PMUs are considered to be secure and will not be affected by FDI attacks.

TABLE 4. The numbers of islands containing different numbers of buses for the IEEE 118-bus system by the two decomposition methods.

# of buses in an island	2	3	4	5	6	7	8	9	10	11	12	13	15	16	17	20
PFT-based	9	22	15	10	1	2	3	2	2	1	0	1	0	0	0	0
MST-based	9	14	12	7	3	4	0	7	2	3	1	3	1	1	2	1

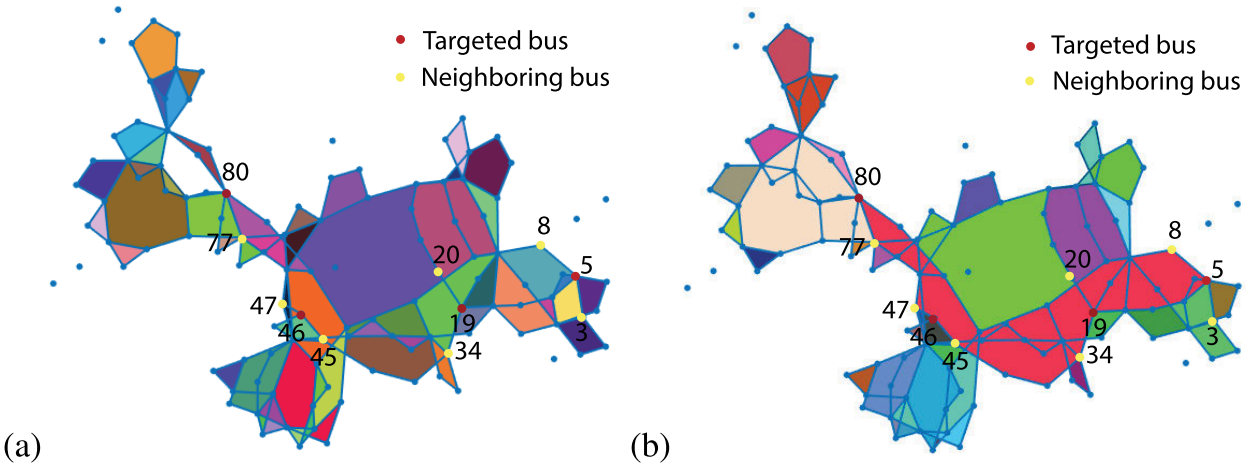


FIGURE 6. IEEE 118-bus system decomposed by (a) PFT-based and (b) MST-based methods and attacked buses.

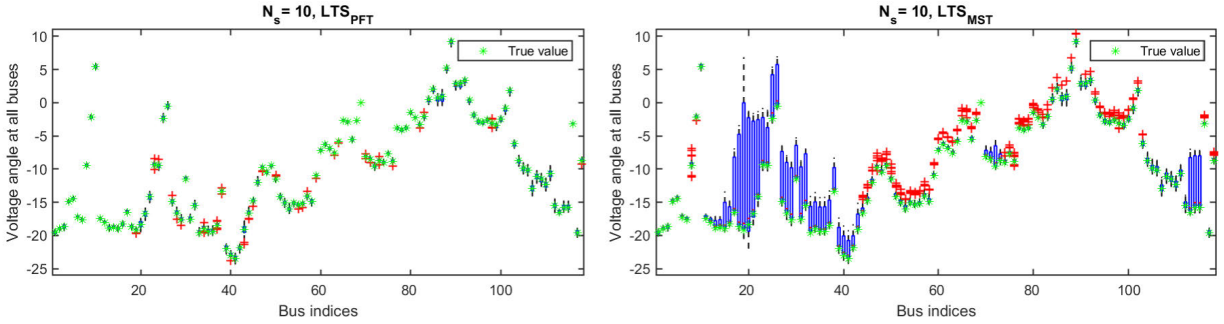


FIGURE 7. Estimated phase angles of 118 buses by LTS-PFT (left) and LTS-MST (right) under attacks on the Jacobian matrix for $N_S = 10$.

It turns out that by increasing the number of PMUs, performance enhancement can be observed especially for the decomposition-based estimations. The average estimation errors in voltage angles (in degrees) are summarized in Fig. 5 for three cases: (a) PMU at bus 2, (b) PMUs at buses 2 and 9, and (c) PMUs at buses 2, 6, and 9. Without any FDI attacks, the average errors are 0.108 for (a), 0.081 for (b), and 0.064 for (c). In comparison with the results in Fig. 2 (c) without any PMU, we see that adding PMUs has immediate effects for all schemes except for the conventional LNR and LAV under centralized computation. Here, again, the LTS-PFT method performs best: While without PMU, it tolerated 4 attacks, adding one PMU does show a clear difference in the estimation accuracy. Moreover, with two PMUs, it increases the number of tolerable attack points to 7. It takes three PMUs for the performance of LTS-MST to become similar to that of LTS-PFT. We also computed the detection probabilities for the case with PMUs. Though we do not show the results, performance enhancement was evident.

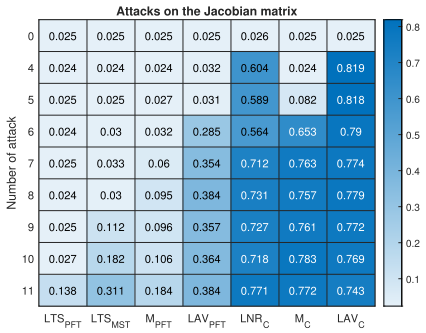


FIGURE 8. Average estimation errors under attacks on the Jacobian matrix for the IEEE 118-bus system.

E. IEEE 118-BUS SYSTEM AND ATTACKS ON ITS JACOBIAN MATRIX

We now extend our study to the IEEE 118-bus system. Compared to the small-scale 14-bus case, the two decomposition methods result in quite different sets of islands. The numbers of islands with different numbers of buses for

TABLE 5. Attacked measurements in the IEEE 118-bus system simulations.

Number of attacks N_s	4	5	6	7	8	9	10	11
Measurements under falsification	$P_5, P_{19}, P_{46}, P_{80}$	P_3	P_{20}	P_{47}	P_{77}	P_8	P_{34}	P_{45}

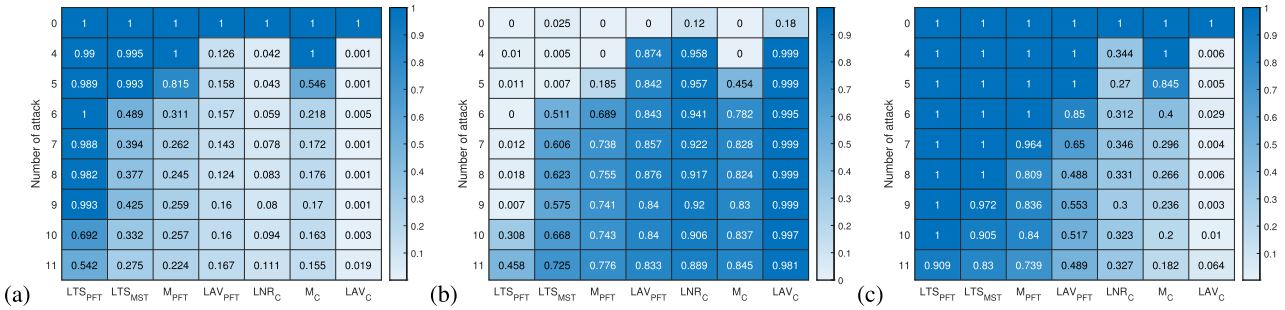


FIGURE 9. (a) The estimated probability of detection, (b) the estimated probability of false detection, and (c) the true probability of detection of leverage points for the IEEE 118-bus system.

PFT- and MST-based methods are shown in Table 4 for the IEEE 118-bus system. For example, for islands containing 5 buses, the PFT-based method resulted in a decomposition with 10 such islands while the MST-based method generated 7 such islands. We see that in general, PFT-based islands are smaller in their sizes, which should help their robustness according to our discussion so far. In particular, the maximum number of buses in an island for PFT is 13 while that for MST is 20. Also, recall that the average numbers are shown in Table 1. It is 4.41 buses per island for PST and 6.49 for MST. In Figs. 6 (a) and 6 (b), the islands obtained by the PFT- and MST-based methods are, respectively, shown by different colors. The MST-based decomposition has a particularly large island with 20 buses indicated in pink. The attack scenario studied here centers around this island. Note that the measurement configuration is as explained in Section IV-A, and the total number of measurements is 726.

To this end, four target buses are selected to be buses 5, 19, 46, and 80. In Fig. 6 (a) and (b), these buses are indicated by the red dots. They are far from each other and are clearly contained in different islands. However, notice in Fig. 6 (b) that these buses are in fact all part of the largest island (in pink color). Attacks will be generated on these buses first and then on neighboring buses indicated by the yellow dots in Figs. 6 (a) and 6 (b). We demonstrate the effects of attacks by increasing the number N_s of attack points from 4 to 11 and following the order shown in Table 5.

The slack bus is taken to be bus 69, whose voltage angle is fixed to zero. For the detection of attacks, the thresholds are set to 10 for all steps and methods. Similarly to the IEEE 14-bus system case, these values were chosen after some trial runs so that in the clean case (without attacks), the false detection alarm rates are minimized. For each attack case, we make Monte Carlo simulations of 40 times ($M_c = 40$). Without any attacks, the LNR for the centralized scheme results in the average error 0.0241.

Fig. 7 shows the phase angle estimations (in degrees) of all buses for LTS-PFT (left) and LTS-MST (right) in box plots when $N_s = 10$ obtained from the Monte Carlo simulations. Obviously, the MST-based estimations vary more in their values and the error propagates much faster in the system (especially in the largest island). Fig. 8 shows the average estimation errors for the seven estimation schemes. We clearly see the advantage of the LTS-PFT method, especially over the LTS-MST method for $N_s = 9, 10$.

The results for estimated probabilities are shown in Fig. 9. In general, we have the same pattern as that for the 14-bus system. We observe that the LTS-PFT outperforms all other schemes in all three detection measures. In particular, the difference from the LTS-MST method becomes evident after $N_s = 6$. Moreover, the measures for LTS-PFT indicate its high reliability up to $N_s = 10$. Other schemes may be considered unreliable after $N_s = 3$. Finally, we examined the average times of state estimation. For the LTS-PFT and LTS-MST methods, the running times for the SE at the largest islands (step 1 of Section III-B, based on LTS executed in parallel) became 1.12 and 7.84 sec, respectively, whereas those for the SE of the whole system after removing outliers (steps 2 and 3, based on the common WLS) were 0.24 and 0.17 sec, respectively. The LTS-PFT method is faster since the islands are overall smaller than those of the LTS-MST.

VI. CONCLUSION

In this paper, we have considered robust techniques for static SE of power systems in the presence of FDI cyber-attacks on the measurement vectors and the Jacobian matrix. Our approach is to first apply the LTS at islands obtained from PFT-based decomposition and then execute state estimation for the entire system to verify the islands' detection results. We analyzed the PFT-based and MST-based decomposition methods and demonstrated the superior performance of the proposed method with the PFT-based method through extensive simulations on the IEEE 14- and 118-bus systems. Under coordinated attacks in the Jacobian matrix, the difference between the two decomposition methods has been shown in both state estimation and attack detection accuracies. For comparison, we have implemented other robust SE schemes and have further introduced PMUs providing more secure and accurate measurements.

REFERENCES

[1] A. Abur and A. G. Exposito, *Power System State Estimation: Theory and Implementation*. Boca Raton, FL, USA: CRC Press, 2004.

[2] M. Göl, "A decentralization method for hybrid state estimators," *IEEE Trans. Power Syst.*, vol. 33, no. 2, pp. 2070–2077, Mar. 2018.

[3] J. Chen and A. Abur, "Placement of PMUs to enable bad data detection in state estimation," *IEEE Trans. Power Syst.*, vol. 21, no. 4, pp. 1608–1615, Nov. 2006.

[4] C.-C. Sun, A. Hahn, and C.-C. Liu, "Cyber security of a power grid: State-of-the-art," *Int. J. Elect. Power Energy Syst.*, vol. 99, pp. 45–56, Jul. 2018.

[5] Y. Liu, P. Ning, and M. K. Reiter, "False data injection attacks against state estimation in electric power grids," *ACM Trans. Inf. Syst. Secur.*, vol. 14, no. 13, pp. 1–33, May 2011.

[6] O. Kosut, L. Jia, R. J. Thomas, and L. Tong, "Malicious data attacks on the smart grid," *IEEE Trans. Smart Grid*, vol. 2, no. 4, pp. 645–658, Dec. 2011.

[7] J. Kim and L. Tong, "On topology attack of a smart grid: Undetectable attacks and countermeasures," *IEEE J. Sel. Areas Commun.*, vol. 31, no. 7, pp. 1294–1305, Jul. 2013.

[8] Y. Chakhchoukh and H. Ishii, "Coordinated cyber-attacks on the measurement function in hybrid state estimation," *IEEE Trans. Power Syst.*, vol. 30, no. 5, pp. 2487–2497, Sep. 2015.

[9] J. Zhang, Z. Chu, L. Sankar, and O. Kosut, "Can attackers with limited information exploit historical data to mount successful false data injection attacks on power systems?" *IEEE Trans. Power Syst.*, vol. 33, no. 5, pp. 4775–4786, Sep. 2018.

[10] M. Du, G. Pierrou, X. Wang, and M. Kassouf, "Targeted false data injection attacks against AC state estimation without network parameters," *IEEE Trans. Smart Grid*, vol. 12, no. 6, pp. 5349–5361, Nov. 2021.

[11] A. S. Musleh, G. Chen, and Z. Y. Dong, "A survey on the detection algorithms for false data injection attacks in smart grids," *IEEE Trans. Smart Grid*, vol. 11, no. 3, pp. 2218–2234, May 2020.

[12] J. Zhao, L. Mili, and M. Wang, "A generalized false data injection attacks against power system nonlinear state estimator and countermeasures," *IEEE Trans. Power Syst.*, vol. 33, no. 5, pp. 4868–4877, Sep. 2018.

[13] Y. Chakhchoukh and H. Ishii, "Enhancing robustness to cyber-attacks in power systems through multiple least trimmed squares state estimations," *IEEE Trans. Power Syst.*, vol. 31, no. 6, pp. 4395–4405, Nov. 2016.

[14] Y. Weng, R. Negi, Q. Liu, and M. D. Ilić, "Robust state-estimation procedure using a least trimmed squares pre-processor," in *Proc. IEEE PES Innovative Smart Grid Technol.*, Jan. 2011, pp. 1–6.

[15] N. Ahmadi, Y. Chakhchoukh, and H. Ishii, "Power systems decomposition for robustifying state estimation under cyber attacks," *IEEE Trans. Power Syst.*, vol. 36, no. 3, pp. 1922–1933, May 2021.

[16] C. Liu, H. Liang, and T. Chen, "Network parameter coordinated false data injection attacks against power system AC state estimation," *IEEE Trans. Smart Grid*, vol. 12, no. 2, pp. 1626–1639, Mar. 2021.

[17] R. A. Maronna, R. D. Martin, and V. J. Yohai, *Robust Statistics: Theory and Methods*. Hoboken, NJ, USA: Wiley, 2006.

[18] Y. Chakhchoukh, V. Vittal, G. T. Heydt, and H. Ishii, "LTS-based robust hybrid SE integrating correlation," *IEEE Trans. Power Syst.*, vol. 32, no. 4, pp. 3127–3135, Jul. 2017.

[19] A. A. Aljabrine, A. A. Smadi, Y. Chakhchoukh, B. K. Johnson, and H. Lei, "Resiliency improvement of an AC/DC power grid with embedded LCC-HVDC using robust power system state estimation," *Energies*, vol. 14, no. 23, p. 7847, Nov. 2021.

[20] L. Mili, M. Cheniae, N. Vichare, and P. Rousseeuw, "Robust state estimation of electric power systems," *IEEE Trans. Circuits Syst. I, Fundam. Theory Appl.*, vol. 41, no. 5, pp. 349–358, May 1994.

[21] L. Mili, V. Phaniraj, and P. J. Rousseeuw, "Least median of squares estimation in power systems," *IEEE Trans. Power Syst.*, vol. 6, no. 2, pp. 511–523, May 1991.

[22] M. G. Cheniae, L. Mili, and P. J. Rousseeuw, "Identification of multiple interacting bad data via power system decomposition," *IEEE Trans. Power Syst.*, vol. 11, no. 3, pp. 1555–1563, Aug. 1996.

[23] A. Majumdar and B. C. Pal, "Bad data detection in the context of leverage point attacks in modern power networks," *IEEE Trans. Smart Grid*, vol. 9, no. 3, pp. 2042–2054, May 2018.

[24] A. Windsor. (2015). *Planar Face Traversal, Boost C++ Libraries*. Accessed: Dec. 8, 2021. [Online]. Available: https://www.boost.org/doc/libs/1_36_0/libs/graph/doc/planar_face_traversal.html

[25] S. Tan, W.-Z. Song, M. Stewart, and L. Long, "LPAttack: Leverage point attacks against state estimation in smart grid," in *Proc. IEEE Global Commun. Conf.*, Dec. 2014, pp. 643–648.

[26] T. H. Cormen, C. E. Leiserson, R. Rivest, and C. Stein, *Introduction to Algorithms*, 2nd ed. Cambridge, MA, USA: MIT Press, 2001.

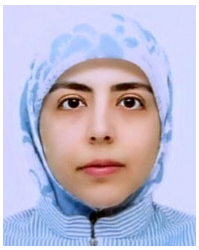
[27] R. D. Zimmerman and C. E. Murillo-Sánchez. (2019). *MATPOWER Version 6.0*. Accessed: Dec. 8, 2021. [Online]. Available: https://matpower.org

[28] J. Agulló, C. Croux, and S. Van Aelst, "The multivariate least-trimmed squares estimator," *J. Multivariate Anal.*, vol. 99, no. 3, pp. 311–338, Mar. 2008.

[29] J. Zhao and L. Mili, "Vulnerability of the largest normalized residual statistical test to leverage points," *IEEE Trans. Power Syst.*, vol. 33, no. 4, pp. 4643–4646, Jul. 2018.

[30] M. Dorier, G. Frigo, A. Abur, and M. Paolone, "Leverage point identification method for LAV-based state estimation," *IEEE Trans. Instrum. Meas.*, vol. 70, pp. 1–10, 2021.

[31] S. Chakrabarti and E. Kyriakides, "Optimal placement of phasor measurement units for power system observability," *IEEE Trans. Power Syst.*, vol. 23, no. 3, pp. 1433–1440, Aug. 2008.



NAIME AHMADI (Student Member, IEEE) received the B.Sc. degree in electrical engineering power system and the M.Sc. degree in electrical engineering power system protection from the Amirkabir University of Technology (Tehran Polytechnic), Tehran, Iran, in 2012, and 2014, respectively. She is currently pursuing the Ph.D. degree with the Department of Computer Science, Tokyo Institute of Technology, Tokyo, Japan. Her research interests include power state estimation and power system cyber security.

YACINE CHAKHCHOUKH (Senior Member, IEEE) received the Ph.D. degree in electrical engineering from Paris-Sud XI University, Paris, France, in 2010. His industrial experience was with the French Electrical Transmission System Operator (RTE-EDF, France). He is currently an Associate Professor with the University of Idaho, Moscow, ID, USA. His research interests include cyber and physical security for the smart grid and power systems control and analysis. In 2017, he was a recipient of the *IEEE SPS Signal Processing Magazine* Best Paper Award.

HIDEAKI ISHII (Fellow, IEEE) received the M.Eng. degree in applied systems science from Kyoto University, Kyoto, Japan, in 1998, and the Ph.D. degree in electrical and computer engineering from the University of Toronto, Toronto, ON, Canada, in 2002.

He was a Post-Doctoral Research Associate at the Coordinated Science Laboratory, University of Illinois at Urbana–Champaign, Urbana, IL, USA, from 2001 to 2004, and a Research Associate at the Department of Information Physics and Computing, The University of Tokyo, Tokyo, Japan, from 2004 to 2007. Since 2007, he has been with the Tokyo Institute of Technology, Yokohama, Japan, where he is currently a Professor with the Department of Computer Science. He was a Humboldt Research Fellow at the University of Stuttgart, from 2014 to 2015. His research interests include networked control systems, multi-agent systems, distributed algorithms, hybrid systems, and cyber security of power systems. He has been the Chair of the IFAC Coordinating Committee on Systems and Signals, since 2017. He received the IEEE Control Systems Magazine Outstanding Paper Award, in 2015. He has served as an Associate Editor for the IEEE Transactions on Control of Network Systems, IEEE Control Systems Letters, *Mathematics of Control, Signals, and Systems*, *Automatica*, and the IEEE Transactions on Automatic Control.