Intrusion Detection, Measurement Correction, and Attack Localization of PMU Networks

Khalafi, Zahra sadat; Dehghani, Maryam; Khalili, Abdullah; Sami, Ashkan; Vafamand, Navid; Dragicevic, Tomislav

Published in:
IEEE Transactions on Industrial Electronics

Link to article, DOI:
10.1109/TIE.2021.3080212

Publication date:
2022

Document Version
Peer reviewed version

Intrusion Detection, Measurement Correction, and Attack Localization of PMU Networks

Zahra Khalafi, Maryam Dehghani, *Senior Member, IEEE*, Abdullah Khalili, Ashkan Sami, Navid Vafamand, and Tomislav Dragičević, *Senior Member, IEEE*

***Abstract*—Accurate state estimation is essential for correct supervision of power grids. With the existence of cyber-attacks, state estimation may become inaccurate which can eventually lead to wrong supervisory decision making. To detect cyber-attacks in power grids equipped with PMUs, a new intrusion detection system based on clustering approach (PMUIDS) is proposed in this paper. After solving the optimal PMU placement in N-1 contingency, several static state estimations are obtained by removing the measurements of one PMU in each time. The resulting state vectors are clustered in two steps: 1- Subtractive clustering is employed to obtain the number of clusters which determines the number of integrity attacks, 2- Fuzzy C-means clustering assigns the state vectors to the corresponding clusters which determines the attacked PMUs. In addition, two theorems are proved which indicate that the attacker cannot coordinate successful stealth attacks in cases that by removing attacked PMUs from state estimation, the power system still remains fully observable. Furthermore, in the case of possible stealth attacks, the attacker cannot falsify the estimation of any arbitrary state variable. The hardware-in-the-loop (HiL) results on a sample power system show that the proposed approach can detect integrity attacks, determine the number of attacks, obtain the correct state vector, and localize the attacks, even in case of multiple simultaneous attacks.**

***Index Terms*—Attack localization, intrusion detection, measurement correction, PMU network, static state estimation**

I. Introduction

Secure state estimation is a challenging issue in future smart grids equipped with PMUs [1]–[5]. The PMU network is based on Information Technology (IT) networks and protocols which are vulnerable to a variety of cyber-attacks [6]. These attacks may impose false information to the control center, which could lead to false control decisions [7]–[9].

Among the cyber-attacks, those attacks that make power system state estimation inaccurate, are especially dangerous since they can lead to wrong supervisory decision makings. Attacks in this class are usually referred to as false (bad) data injection (or integrity) attacks [10]-[11]. Such attacks are usually detected by a number of bad data detection methods [12]–[14] such as sum detector [15], χ^2 detector [16], and learning-based methods [17], [18]. However, these approaches only detect the attack and they fail to localize the attack and present correct measurements. On the other hand, invaders can orchestrate coordinated false data injection attacks (such as those in [19]–[21]) to make them unobservable by conventional detection methods. Such attacks are called stealth (or interacting) attacks.

In order to detect stealth attacks, a number of methods have been proposed in the literature [1], [22]–[25]. It should be noted that in addition to these researches, several methods are available to mitigate the stealth attacks using authentication, multi-path routing or encryption devices. However, they increase the implementation cost and complexity, and also impose additional delay [26], [27].

In this paper, a new intrusion detection system based on clustering techniques, called PMUIDS, is proposed which has some advantages over the previous researches, which are described next. In PMUIDS, first the optimal PMU placement is employed such that the network still remains full observable even if a single contingency happens (observability in *N-1* contingency). Then, in each time step, measurements of one PMU are removed and the state vector is calculated. In the next step, the resulting state vectors are clustered. For this purpose, subtractive clustering obtains the number of clusters and, fuzzy C-means clustering assigns the state vectors to the correct cluster. The number of one-member clusters indicates the number of integrity attacks. These one-member clusters are also used to determine the attacked PMUs and obtain the correct state vector.

In this paper, the most related works on stealth attack detection are also reviewed and quantitatively compared with the proposed method. For this purpose, the following properties are checked for each of the algorithms: (1) Obtaining Correct Measurement (OCM): The capability of the attack detection methods in obtaining the correct value of state vector is checked through this property. (2) Attack Localization (AL): This feature checks whether the algorithm is able to determine the location of attacks or not. (3) Concurrent Random Attacks Detection (CRAD): This property shows the capability of the algorithm in detecting several random (non-coordinated)

Z. Khalafi, M. Dehghani, A. Sami, and N. Vafamand are with the School of Electrical and Computer Engineering, Shiraz University, Shiraz, Iran (e-mails: {z.khalafi, mdehghani, sami, n.vafamand}@shirazu.ac.ir).
A. Khalili is with the Department of Electrical and Computer Engineering, University of Hormozgan, Bandar Abbas, Iran (email: khalili@hormozgan.ac.ir).
T. Dragičević is with the Center for Electric Power and Energy, Department of Electrical Engineering, Technical University of Denmark, Lyngby, Denmark (e-mail: tomdr@elektro.dtu.dk).

attacks. (4) Stealth Attack Detection (SAD): Obviously, this feature investigates the ability of detection methods in detecting stealth attacks. (5) Obtaining the Number of Attacks (ONA): The ability of attack detection methods in obtaining the number of random (or coordinated) attacks is shown through this feature. (6) Requiring Non-Electrical Information (RNEI): This feature deals with this property that whether an attack detection method requires non-electrical (e.g. cyber security) information to detect stealth attacks or not. For example, in addition to power grid information, [28] needs security information such as data collected from intrusion detection sensors or a database of firewall rules. However, this approach causes the design process to be more complicated and imposes additional delays.

By specifying the above properties in Table I, comparison between the previous researches and PMUIDS is straightforward. Results in Table I demonstrate that methods proposed in [25] and [28] are more similar to PMUIDS. However, as discussed earlier, method of [28] requires non-electrical information and the method proposed in [25] requires secure PMUs for detecting stealth attacks. Secure PMUs need security controls such as encryption and authentication which impose additional delays [25].

In summary, the PMUIDS features are as follows: (1) Detecting integrity attacks on power grids using a novel clustering approach. (2) Localizing the attacks. (3) Obtaining the correct state vector when by removing the measurements of attacked PMUs, the power system still remains full observable. (4) Requiring only electrical information (by placing additional PMUs) which does not cause additional delay. (5) Decreasing the probability of successful stealth attacks. The main contributions of this paper are the novel PMUIDS based on clustering technique with the above features, and two theorems that one mathematically proves by an appropriate PMU placement, the successful interacting attack cannot happen, and the other one proves if PMUs are not placed appropriately, then the successful interacting attack can happen. However, even in this situation, the measurements of some parts of the power system can be corrected by the PMUIDS.

The rest of the paper is organized as follows: Section II reviews the overall structure of PMU networks and static state estimation algorithm. In addition, two theorems about coordination of interacting attacks are presented in this section. Section III presents the suggested PMUIDS and the clustering-based approach. The HiL results on a sample power system is given in Section IV. Finally, conclusions of this research are given in Section V.

II. Integrity Attack Detection in PMU Networks Exploiting Static State Estimation

PMU networks are set up on the IT-based protocols. They are constituted from PMUs, Phasor Data Concentrators (PDCs) and communication networks for data transmission in a hierarchical structure which is expanded in a wide area measurement system (WAMS) and at the top level, transfers data to the control center [33], [34]. The network has two different parts; regional and backbone networks (Fig. 1). While the regional networks are responsible for transferring data from each PMU to the related PDC [3], the backbone network has the main role of communication in a higher level among PDCs and the control center. The received data in the control center can be exploited for different studies, i.e., state estimation, stability assessment, etc. [35]. The main difference between the PMU and SCADA systems is that in the PMU system, the real and imaginary parts of the voltages and currents are available and the measurement model is inherently linear. Moreover, the PMU systems are more resilient against attacks. Though, they are still vulnerable to some kinds of attacks [36].

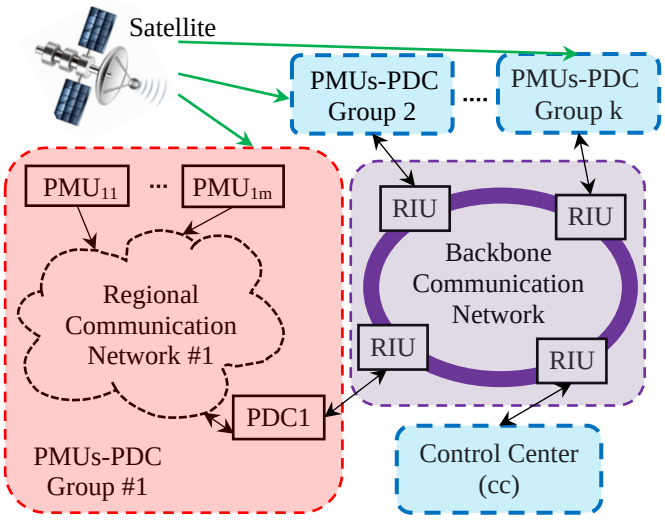

Fig. 1. Hierarchical structure of PMU networks [34].

In [36], false data injection attack (FDIA) on power systems

TABLE I. Properties of PMUIDS and Some Methods In Literature for False Data Injection Attack Detection

Method	OCM	AL	CRAD	SAD	Main idea for detecting stealth attack	ONA	RNEI
[1]	No	No	Yes (at most four attacks)	Partially	• Using Redundant PMUs	No	No
[16]	No	No	Yes	No	• Kalman Filter and χ^2 detector	No	No
[18]	No	No	Yes	Yes	• Comparing the error with pre-defined threshold	No	No
[22]	No	No	Yes	Partially	• Perturbing grid topology	No	No
[23]	No	Yes	To some extent	Partially	• Employing distributed state estimation using power system decomposition	No	No
[25]	Yes	Yes	Yes	Partially	• Optimal placement of secure PMUs (i.e. PMUs that cannot be attacked)	No	Yes
[26]	No	Partially	Yes	Partially	• Using a fully distributed algorithm for power system state estimation	No	No
[28]	Yes	Yes	Yes	Yes	• Combining cyber data with power grid information	No	Yes
[29]	No	Partially	Yes	Partially	• Distance between probability distribution function of measurement variation	No	No
[30]	Yes	No	Yes	Yes	• Adding protected meters to be sure about some measurements	No	Yes
[31]	Yes	No	Yes	Yes	• Needs some meters to be absolutely protected	No	Yes
[32]	Yes	No	Yes	Yes	• Increases the number of PMUs so that FDI cannot impact estimation	No	No
PMUIDS	Yes	Yes	Yes	Partially	• Optimal placement of PMUs in N-1 contingency	Yes	No

equipped with PMUs is studied and by exploiting static state estimation, the voltages in the power system are estimated. Then, some solutions (such as redundant PMU) are suggested to avoid load shedding in the power system. Similarly, in [32], FDIA on WAMSs is considered and an algorithmic solution is proposed to address the issue of additional PMU installation and placement with cyber security consideration. However, those approaches do not offer all properties of the suggested PMUIDS listed in Table I. For detecting integrity attacks in such networks, this paper combines the theories of static state estimation and data clustering approaches. In the static state estimation and static attack detection method, the system operating point changes slowly that the fast transient response is negligible [37]. Then, the values of currents and voltages for that operating point are used.

In the following, the theory is briefly reviewed and its capability in integrity attack detection is discussed. Furthermore, two theorems about the possibility of interacting attacks in PMU networks are presented.

A. Static State Estimation

In general, the measurement equation for an n –bus system is as follows [38]:

$$Z_n = HV + e = (H_r + jH_m).(E_v + jF_v) + e \quad (1)$$

where $(H_r + jH_m) \in C^{m\times n}$ is the Jacobian matrix of measurements, $e = (e_1, \dots, e_m)^T$ is the measurement noise vector and $V = (E_v + jF_v) \in C^{n\times 1}$ and $Z_n = (A + jB) \in C^{m\times 1}$ are the state vector and the measurements vector, respectively and $A = H_rE_v - H_mF_v$, $B = H_mE_v + H_rF_v$.

Define a new measurement vector Z as follows [38]:

$$Z = \begin{bmatrix} A \\ B \end{bmatrix} = \begin{bmatrix} H_r & -H_m \\ H_m & H_r \end{bmatrix} \begin{bmatrix} E_v \\ F_v \end{bmatrix} + e = HX + e \quad (2)$$

where $X \in \mathbb{R}^{(2n-1)\times 1}$ is the new state vector and $H \in \mathbb{R}^{2m\times(2n-1)}$ is the new linear measurement Jacobian matrix. The estimation of state vector $\hat{X}$ is procured as follows [39]:

$$\hat{X} = \begin{bmatrix} \hat{E}_v \\ \hat{F}_v \end{bmatrix} = (H^TRH)^{-1}H^TR \begin{bmatrix} A \\ B \end{bmatrix} = (H^TRH)^{-1}H^TRZ \quad (3)$$

where R is the covariance matrix and determines the weight of each array in the measurement vector Z. Without loss of generality, in the rest of this paper, it is assumed that R is equal to I. It means that we used the known least square method to find the optimal static state estimation. Additionally, the matrix H should be non-singular, so that H^TRH is inversible. This issue is treated by the so-called numerical observability [38], in which not only the system is topological observable, but also as much PMUs are allocated as needed to make the system fully observable.

B. Interacting Attack Detection

Assume that an integrity attack happens in the PMU network and some measurements are altered. The vector of observed measurements after attack is $Z_a = Z + a$ which consists of two parts; the real measurements $Z = (z_1, \dots, z_{2m})^T$ and the false data added to the real measurements $a = (a_1, \dots, a_{2m})^T$ that is called the attack vector. Assume that, $\hat{X}_a$ refers to false estimation of state vector, $\hat{X}_a = \hat{X} + W$, in which, W is the state estimation error due to the vector injected by the attacker.

In [12]–[14], for detection of bad data (such as attack) the constraint is to check $\left\|Z - H\hat{X}\right\|^2$ with a threshold and if this norm is less than the predefined threshold, it is concluded that there is no bad data in measurements. A category of attacks is interacting attacks, in which the attack vector has the specific form $a = HW$ and do not result in a large deviation from threshold and cannot be detected by these methods. This kind of attack can be organized in two ways [20]:

- The attacker's only intention is to deceive the result of state estimation. Therefore, W is assumed to be a random vector.
- The attacker aims to add specific errors to the estimation of particular state variables. Consequently, this kind of attack is called targeted false data injection attack. In other words, in targeted attacks, W is not a random vector.

Assume that the attacker wants to orchestrate random interacting attack. The matrices Q and K are defined as follows:

$$Q = H(H^TH)^{-1}H^T \quad , \quad K = Q - I \quad (4)$$

Notice that $QH = H$. Multiplying this equation and $a = HW$ by W and Q respectively, it can be concluded:

$$\left.\begin{array}{c} a = HW \rightarrow Qa = QHW \\ QH = H \rightarrow QHW = HW = a \end{array}\right\} \Rightarrow Qa = a \rightarrow (Q - I)a = Ka = 0 \quad (5)$$

Solving (5), the attack vector can be obtained.

Assume that the attacker's access is limited and he can only forge few PMU's data. Therefore, only the elements of vector a that correspond to falsified PMUs, can be non-zero. Showing the nonzero elements of a with vector a' and the corresponding columns of matrix K with matrix K', (5) results in:

$$K'a' = 0 \quad (6)$$

If K' is a full rank matrix, (6) has a unique solution $a' = 0$. Therefore, it is highly unlikely for successful interacting attacks to happen. Otherwise, the equation has infinite number of non-zero solutions with the following general form [20]:

$$a' = (I - K'^{+}K')\eta \quad (7)$$

where η is an arbitrary non-zero vector with the same length as a' and K'^{+} is pseudo inverse of matrix K'. Consequently, when the attacker only has access to the measurements of few PMUs, the interacting attack may be detectable in some cases.

In the following, two theorems are presented to determine whether or not a successful random interacting attack can be organized in PMU networks. In addition, if possible interacting attack happens, it is significant to know how the affected state variables are limited (successful targeted interacting attacks are restricted). Before mentioning the theorems, some definitions are given as follows:

- φ_1 & φ_2: The number of PMUs to guarantee full observability (topologically and numerically) in normal condition and $N-1$ contingency, respectively ($\varphi_2 > \varphi_1$)
- $L = \{l_1, \dots, l_{\varphi_2}\}$: The set of buses which define the locations of installed PMUs in $N-1$ contingency condition.
- o_i: Each subset of L, which makes power system full observable (observable set).
- $O = \{o_i | i = 1, \dots, N_o\}$: The set of observable sets.
- u_i: Each subset of L, which cannot make power system full observable (unobservable set).

- $U = \{u_i | i = 1, \dots, N_u\}$: The set of unobservable sets.
- $S = \{s_i | s_i = L - o_i, i = 1,2, \dots N_o\}$, where s_i is a set of PMUs which omitting their measurements' still makes the power system full observable.
- $\bar{S} = \{\bar{s}_i | \bar{s}_i = L - u_i, i = 1,2, \dots N_u\}$, where $\bar{s}_i$ is a set of PMUs that omitting their measurements' results in the power system not be full observable anymore.
- L_A: The set of buses that the attacker gain access to the measurements of their PMUs.
- *m:* the number of all measurements obtained from φ_2 PMUs.

Theorem 1: Assume that φ_2 PMUs are installed in the system. If the attacker only has access to a set of PMUs which belong to S (i.e. $L - L_A \in O$), the matrix K' is full rank and successful interacting attacks will not happen.

Proof: Select one observable set o_i from the set O. The number of measurements related to eliminated PMUs (s_i) is shown by m_e. These measurements are the ones that the attacker has access to them and can falsify them. The number of remaining PMU measurements which cannot be altered by the attacker is equal to $m_r = (m - m_e) \geq n$. Since, interchanging rows or columns of a matrix doesn't change the rank of matrix, without loss of generality, the matrix H can be considered as follows:

$$H_{2m \times (2n-1)} = [H_r^T \quad H_e^T]^T \tag{8}$$

where H_e is a $2m_e \times (2n-1)$ matrix and consists of the rows of H that correspond to measurements of eliminated PMUs and H_r is a $2m_r \times (2n-1)$ matrix which is related to the remaining PMUs. The full observability (topologically and numerically) of power system before and after elimination of the specified PMUs (s_i), results in:

$$\begin{gathered} rowspace(H) = rowspace(H_r) = \mathbb{R}^{2n-1} \\ rank\ (H) = rank\ (H_r) = 2n-1 \end{gathered} \tag{9}$$

In other words, any vector in $\mathbb{R}^{2n-1}$can be written as a linear combination of rows of H or H_r. Define matrix Y as follows:

$$Y = (H^T H)^{-1} = \left([H_r^T \quad H_e^T] \begin{bmatrix} H_r \\ H_e \end{bmatrix} \right)^{-1} \tag{10}$$

The matrix Q will be obtained as the following:

$$Q = H(H^T H)^{-1} H^T = \begin{bmatrix} H_r Y H_r^T & H_r Y H_e^T \\ H_e Y H_r^T & H_e Y H_e^T \end{bmatrix} \tag{11}$$

Therefore, the matrix K will be represented as follows:

$$K = Q - I = \begin{bmatrix} H_r Y H_r^T - I_{2(m-m_e)} & H_r Y H_e^T \\ H_e Y H_r^T & H_e Y H_e^T - I_{2m_e} \end{bmatrix} \tag{12}$$

Here, vector a' consists of the last $2m_e$ elements of vector a (those elements that the attacker has access to). Therefore, matrix $K'_{2m \times 2m_e}$is as follows:

$$K' = \begin{bmatrix} H_r Y H_e^T \\ H_e Y H_e^T - I_{2m_e} \end{bmatrix} \tag{13}$$

As it is mentioned before, if K' is a full rank matrix, the successful interacting attacks will not happen. If each vector in $\mathbb{R}^{2m_e}$ is presented as a linear combination of rows of matrix K', then the row space of K' is $\mathbb{R}^{2m_e}$ and this matrix is full rank. Therefore, to prove the nonexistence of successful interacting attack, we need to prove that for each vector $F \in \mathbb{R}^{2m_e}$ the equation $G^T K' = F^T$ has an appropriate solution. Partitioning vector G^Tas $G^T = [g_1^T \quad g_2^T]$, where g_1 and g_2 are $(2m_r \times 1)$ and $(2m_e \times 1)$ vectors respectively, concludes:

$$G^T K' = g_1^T H_r Y H_e^T + g_2^T H_e Y H_e^T - g_2^T \tag{14}$$

On the other hand, each arbitrary vector $F^T H_e \in \mathbb{R}^{2n-1}$ can be written as a linear combination of rows of H_r. Therefore, for each arbitrary vector F, the equation $g_1^T H_r = F^T H_e$ has a solution that is called $\bar{g}_1$. As it is shown in the following, for each arbitrary vector F, the vector $\bar{G} = \begin{bmatrix} \bar{g}_1^T & -F^T \end{bmatrix}^T$ is a solution for the equation $G^T K' = F^T$:

$$\left.\begin{gathered} \bar{G}^T K' = \bar{g}_1^T H_r Y H_e^T - F^T H_e Y H_e^T + F^T \\ \bar{g}_1^T H_r = F^T H_e \end{gathered}\right\} \Rightarrow \bar{G}^T K' = F^T \tag{15}$$

Therefore, it is shown that if the attacker has access to the measurements of a set of PMUs that belongs to S, each vector $F \in \mathbb{R}^{2m_e}$ can be presented as a linear combination of rows of K' which means that the matrix K' is full rank. Therefore, the equation $K'a' = 0$ has a unique solution $a' = 0$ and the successful interacting attacks will not happen. ■

Theorem 2: Assume that the attacker only gain access to a set of PMUs which belongs to $\bar{S}$ (i.e. $L - L_A \in U$) and can organize an interacting attack in the form of $a = HW$. In this case, the estimation error vector (W) will have a specified structure and all of its elements related to the buses that are still observable after removing the attacked PMUs (L_A), are zero. Therefore, the attacker can only falsify estimation of buses that become unobservable after omitting L_A

Proof: Consider the case that the attacker gain access to a set of PMUs that belongs to $\bar{S}$ and can manage a successful interacting attack $a = HW$. The estimation of state vector using all measurements after the attack is as follows:

$$\begin{aligned} \hat{X}_a &= (H^T H)^{-1} H^T Z_a = (H^T H)^{-1} H^T (Z + HW) \\ &= \hat{X} + W \end{aligned} \tag{16}$$

Since $L - L_A \in U$, omitting measurements of attacked PMUs, makes some buses unobservable. Those elements of vectors W, $\hat{X}$ and $\hat{X}_a$ that are related to observable buses are shown by W_o, $\hat{X}_o$ and $\hat{X}_{a_o}$. Define vector a_r by removing the elements related to L_A from a. In addition, define matrix H_r by removing the corresponding rows of H. Therefore, the equation $a_r = H_r W$ still holds.

Assume that matrix H_{rc} is obtained by removing the zero columns related to unobservable state variables from matrix H_r. Since these zero columns have no effect on the value of vector a_r, after removing them, the equation $a_r = H_{rc} W_o$ still holds. Although the power system is not full observable after omitting the measurements related to L_A, the voltages of observable buses can be estimated as follows:

$$\begin{aligned} \hat{X}_{a_o} = (H_{rc}^T H_{rc})^{-1} H_{rc}^T Z_{a_r} &= (H_{rc}^T H_{rc})^{-1} H_{rc}^T (Z_r + a_r) \\ &= (H_{rc}^T H_{rc})^{-1} H_{rc}^T (Z_r + H_{rc} W_o) \\ &= \hat{X}_o + W_o \end{aligned} \tag{17}$$

On the other hand, the remaining measurements after omitting the attacked PMUs (L_A) are correct. Therefore, the estimation of observable buses will be correct, too.

$$Z_{a_r} = Z_r \Rightarrow \hat{X}_{a_o} = (H_{rc}^T H_{rc})^{-1} H_{rc}^T Z_r = \hat{X}_o \tag{18}$$

Comparing (17) to (18), it is concluded that $W_o = 0$. Therefore, the attacker can't target any arbitrary bus and only estimation of buses that become unobservable by removing measurements of attacked PMUs may be wrong. ■

In Theorems 1 and 2, the PMUs belong to the sets S and $\bar{S}$, respectively. Depending the attacker access to the sets S and $\bar{S}$, the attack success changes. From Theorem 1, one infers that gaining access to the measurement of those PMUs that belong to S, does not result in successful interacting attacks. Based on Theorem 2, gaining access to those PMUs that belong to $\bar{S}$ may falsify the estimation of buses that become unobservable after omitting the attacked PMUs. By using these two theorems, all set of PMUs that by gaining access to their measurements, organizing a successful interacting attack might be possible (i.e. $\bar{S}$) can be determined and the buses that falsifying their estimation is much easier than other buses (i.e. buses that become unobservable in most cases) can be identified.

III. PMUIDS

In this section, the steps of PMUIDS for detecting attacks, localizing them, determining the number of attacks and obtaining the correct measurements are presented. In the suggested approach, different state estimation vectors are calculated and compared in the control center. The redundancy of PMUs is increased to make it possible to obtain several solutions for the state estimation problem. Then, clustering is employed to detect the number and location of attacks and obtain the correct estimation of state vector. Notice that in case of multiple simultaneous attacks, if by omitting measurements of falsified PMUs, the power system remains fully observable, the state vector can be estimated correctly. Otherwise, only the correct voltages of observable buses will be obtained.

The PMUIDS algorithm is as follows:

1) Perform PMU placement by taking $N-1$ contingency conditions into account.

2) Install PMUs on the buses determined in the previous step.

3) Omit the measurements received from one of the PMUs and calculate the estimation of the state vector V_1 by using the measurements of other PMUs.

4) In a row, consider each PMU data to be omitted once and exploit the other measurements for the required estimation data. After elimination of i^{th} PMU data, go to Step 3 and calculate state vector V_i and φ_2. Thus, different estimation results $(V_1, V_2 \dots, V_{\varphi_2})$ will be acquired.

5) Use the following formula to calculate the mean of all state vectors:

$$V_{Ave} = mean\left(V_1, V_2 \dots, V_{\varphi_2}\right) = \frac{1}{\varphi_2}\sum_{i=1}^{\varphi_2} V_i \tag{19}$$

6) Choose Euclidean norm as an appropriate measure to find the distance between each state and the mean.

$$Dis_i = \| V_i - V_{Ave} \|_2 \tag{20}$$

7) Find the state vector with the largest distance from the mean.

$$Dis^* = \max_i (Dis_i) \tag{21}$$

If this distance is smaller than a threshold, ε, PMUIDS ignores it and concludes that no attack has occurred. Otherwise, if the largest distance from the mean is larger than a threshold, it can be concluded that an attack has occurred. The threshold ε is considered to remove the effect of measurement noises and it is the key to identify the integrity attack from the noisy measurements.

8) In this step, the number and locations of the attacks will be detected. First, by using subtractive clustering algorithm, the number of clusters will be obtained. Then, by using fuzzy c-mean clustering, each state vector will be assigned to the right cluster. The number of single-member clusters shows the number of attacks. In addition, those PMUs that their data was omitted in calculating the state vectors associated with single-member clusters are the attacked ones.

9) For single-attack cases, the state vector with maximum distance from the mean which was found in Step 7 shows the correct measurements. For multiple simultaneous attacks, the measurements of detected attacked PMUs will be omitted and state estimation will be done based on the remaining measurements. If the remaining measurements make the power system fully observable, the correct estimation of state vector will be obtained. Otherwise, only the correct voltages of observable buses will be estimated.

To prove the capability of PMUIDS, assume that only measurements of PMU_i are forged. Implementing the above algorithm, it is obvious that when data of PMU_i is omitted, the state estimation result is correct (Estimation_1). All the other cases contain the forged data and will lead to wrong estimations. Since the forged data affect all these estimated state vectors similarly, their results will be very close to each other, but different from Estimation_1. In other words, the state estimation results will form two clusters, where one of them is a single member cluster (Estimation_1). This scheme can be extended to the cases that measurements of more PMUs are altered by attackers.

It should be noted that the proposed algorithm does not have any limitation for $N-2$ or further assumption. Furthermore, the algorithm does not have any limitation for large-scale systems. It is just needed to have enough measurement to be sure that the matrix H of (3) is nonsingular. Thereby, it is required to install as much PMUs as they guarantee the matrix non-singularity, which is the limitation of all static state estimation approaches.

IV. HiL Results

The approach proposed in Section III is applied on the known IEEE 14-bus test system though the OPAL-RT HiL environment, shown in Fig. 2. The structure of the HiL setup consists of an OPAL-RT as a Real-Time Simulator (RTS) which simulates the IEEE 14-bus grid, seven virtual Phasor PMUs, and the static attack detection; a PC as the programming host; an amplifier that generates the current and voltage for the PMUs; two real PMU devices; and a satellite-synchronized clock. The optimal PMU locations are found by the method introduced in [40]–[41]. The optimal numbers of PMUs in normal and $N-1$ contingency conditions are equal to 4 and 9, respectively. The locations of PMUs in $N-1$ contingency condition is shown with $S_2 = \{2,4,5,6,7,8,9,11,13\}$. In Fig. 3, the modified version of the IEEE 14-bus system benchmark with the assumption of no connection between the buses 5 and 6 is shown. The PMU network is designed and 9 PMUs (PMU_A,

PMU_B, … , PMU_I) are allocated. Additionally, the network for transferring data from PMU to PDC and the CC are selected. It is assumed that the network requires 3 PDCs, corresponding regional networks (R1, R2, & R3) and Ring Interface Units (RIU) and a back-bone network.

In the part of the static attack detection, initially an integrity attack is generated and added to data of the attacked real/virtual PMU devices to falsify the measurements. Then, the static attack detection method is performed.

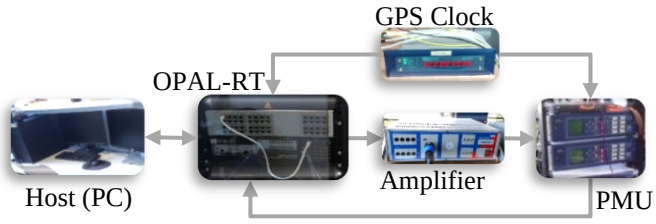

Fig. 2. The OPAL-RT HiL setup for testing the attack detection method on an IEEE 14-bus system.

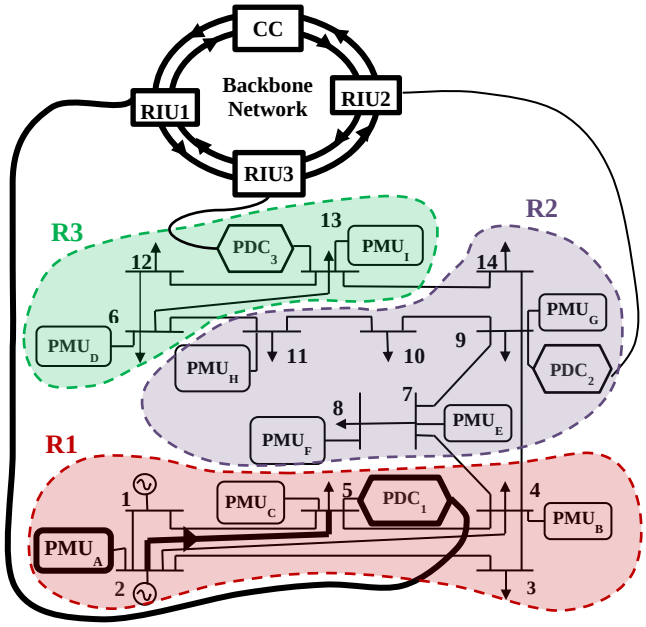

Fig. 3. PMU-PDC-CC network of IEEE 14- bus test system

A. *Analyzing the results of Theorems 1 and 2*

In this part, it is considered that the proposed PMUIDS detects the attacked PMUs and the applicability of Theorems 1 and 2 is investigated. These theorems facilitate analyzing the feasibility of successful interacting attacks. To do this, the sets S (or O) and $\bar{S}$ (or U) are required and can be obtained based on the topology of IEEE 14-bus and the places of PMUs and PDC. Table II shows the number of observable and unobservable sets for different PMU numbers $4 \leq \gamma \leq 9$.

TABLE II. THE NUMBER OF OBSERVABLE AND UNOBSERVABLE SETS

PMU Numbers (γ)	Number of u_i	Number of o_i
9	0	1
8	0	9
7	7	29
6	45	39
5	106	20
4	125	1

These sets are utilized in Theorems 1 and 2 to analyze the possible attacks. The results are as follows:

- **(Single attack):** Since 9 PMUs are placed in the grid, if one random PMU is attacked, (and detected by the PMUIDS), still 8 PMUs measurements are available. Based on Table II, there is no set of unobservable set (i.e. $U \in \emptyset$) and all possible sets are observable. Thereby, based on Theorem 1, the system is fully observable; and no successful attack can be performed.
- **(Two attacks):** If two random PMUs are attacked, they are detected and the power system still has 7 available PMUs. In this case, 29 sets out of 36 sets are fully observable and based on Theorem 1, system states are fully observable; and, 7 sets out of 36 sets are unobservable and based on Theorem 2, their corresponding states are lost, meanwhile the other states are observable. This shows that only 7 out of 36 possible sets of two simultaneous attacks can be a successful interacting attack, which results into the loss of some buses' states. Consequently, the probability of organizing targeted false data injection attack is highly unlikely. The possible interacting attacks on two PMUs and the buses that their estimation could be wrong are shown in Table III. Moreover:
  1) No one can deceive the estimation of buses (2, 4, 5, 6, 7, and 9) without being detected.
  2) To deceive the estimation of bus 10 without being detected, the attacker should have access to the measurements of buses 9 and 11, otherwise successful interacting attack is impossible.

TABLE III. POSSIBLE INTERACTING ATTACK ON TWO PMUS

u_i	Falsified PMUs	Buses with wrong estimation (unobservable buses)
{5,6,7,8,9,11,13}	{2,4}	3
{4,6,7,8,9,11,13}	{2 ,5}	1
{2,4,5,7,8,9,13}	{6,11}	11
{2,4,5,7,8,9,11}	{6,13}	{12,13}
{2,4,5,6,9,11,13}	{7,8}	8
{2,4,5,6,7,8,13}	{9,11}	10
{2,4,5,6,7,8,11}	{9,13}	14

- **(Three attacks):** In this case, 6 available PMUs' measurements are available. Based on Table II, this means that only 45 out of 83 possible sets of three simultaneous attacks can be a successful interacting attack. Furthermore:
  1) No one can falsify the estimation of buses (4, 5, 6, and 7) without being detected.
  2) To falsify the estimation of bus 9 without being detected, the attacker should have access to the data of buses 4, 7 and 9, otherwise successful interacting attack is impossible.

B. *Evaluating the proposed PMUIDS*

In this part, three scenarios are considered for evaluating PMUIDS on IEEE 14-bus system. In the first Scenario, the power system is working normal and no attack is carried out. This scenario indicates whether PMUIDS produces any false results or not. In the second scenario, one integrity attack is carried out. Results of this scenario show whether PMUIDS can successfully detect the attack, obtain the correct measurements, and localize the attack in case of one attack at a time or not.

Finally, in the third scenario, three attacks are simultaneously orchestrated on the IEEE 14-bus system. This test investigates whether PMUIDS can still detect intrusion, determine the number and location of attacks and correct estimation in case of simultaneous attacks or not. It should be noted that since PMUIDS employs mathematically proven techniques, in similar scenarios, similar results will be obtained.

B.1. Scenario 1: No Attack

First, consider the case that no attack happened in the PMU network. At each step, 8 out of 9 PMUs are selected and the state vector is estimated based on the method described in section III.A. Therefore, for calculating V_A, all measurements except information gathered from PMU_A is used. Similarly, this procedure is repeated for all PMUs. Therefore, nine solutions (V_A, V_B…., V_I) are obtained for different state estimation problems which are shown in Fig. 4. It is obvious that all solutions are very close to each other. The small differences between the state vectors in this case is due to measurement noises. The Euclidean distance of each state vector to the V_{ave} is presented in Table IV.

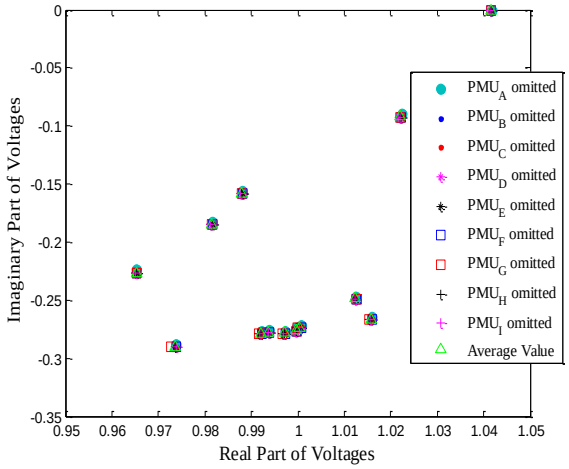

Fig. 4. The estimation results prior to experiencing any attack

B.2. Scenario 2: One Attack

Assume that the measurements of PMU_A (shown in Fig. 3) are falsified to simulate an integrity attack. This PMU transfers the information to PDC_1. Here, a series of actions are needed to check whether integrity attack (Man-in-the-Middle (MitM)) modified the PMU data. A similar procedure to Section IV.B.1 is repeated to find 9 state vectors while data from one of the PMUs is eliminated. The Euclidean distance of computed state vectors to V_{ave} are presented in Table IV.

According to the Results, V_A has the largest Euclidean distance to V_{ave} which is greater than ε = 0.05. Therefore, PMUIDS can effectively detect the attack. The subtractive and fuzzy c-means clustering methods are exploited to determine the clustering information which is useful in attack determination.

The number of clusters that is calculated by subtractive clustering algorithm equals to 2. One of these clusters consists of 8 vectors (V_B, V_C…., V_I) and the second one, is a single-member cluster (V_A) shown in Fig. 5. Thus, there is only one attack and PMU_A that wasn't used in calculation of V_A contains the falsified data and its data is compromised. Since only one attack is happened in the network, state vector V_A represents the accurate estimations.

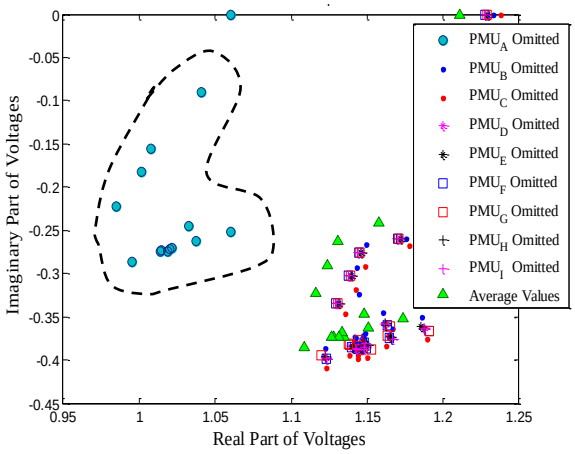

Fig. 5. All solutions for the state estimation problem after one attack

B.3. Scenario 3: Three Attacks

Assume that the measurements of PMU_A, PMU_D and PMU_G are altered to simulate three integrity attacks. The same detection procedure is used here. The estimation results (V_A ,V_B, V_C…., V_I) are presented in Fig. 6 and the corresponding Euclidean distance is presented in Table IV. The results show that the norm of difference between V_D and V_{ave} is the largest value, equal to 0.84103. Therefore, the attack is detected properly. The number of clusters in this case equals to 4. Three of these clusters, which are marked with dashed lines in Fig. 6, only consist of one state vector. Other state vectors (V_B, V_C, V_E, V_F, V_H, V_I) form a cluster together. Therefore, the number of attacks is identified correctly. The PMUs, whose data were omitted in calculating the state vectors associated with single-member clusters, will be effectively determined as the location of attacks. Since after removing the detected forged PMUs, the power system remains full observable, the true values of bus voltages can be obtained.

By using the proposed PMUIDS, the system state vector is estimated and clustered via the approach presented in the Appendix. If one gets no specific cluster, it shows that all solutions are very close to each other and no attack does happen, which is evident in Scenario A. However, if more clusters are achieved, an attack is detected. Based on the number of clusters, it is possible to determine the number of simultaneous attacks. As can be seen in Scenarios B and C, one and three clusters are obtained, respectively which is in consistent with the number of

TABLE IV. NORM OF THE DIFFERENCE BETWEEN ESTIMATED VECTORS AND THE MEAN VALUE

	Dis1	Dis2	Dis3	Dis4	Dis5	Dis6	Dis7	Dis8	Dis9
Before Attack	0.00349	0.00045	0.00048	0.00058	0.00049	0.00079	0.00108	0.00092	0.00084
One Attack	0.58452	0.0599	0.10686	0.07179	0.06906	0.07292	0.07069	0.07576	0.07542
Three Attacks	0.49932	0.14472	0.1602	0.84103	0.13346	0.1371	0.39936	0.15263	0.15551

the simultaneous attacks.

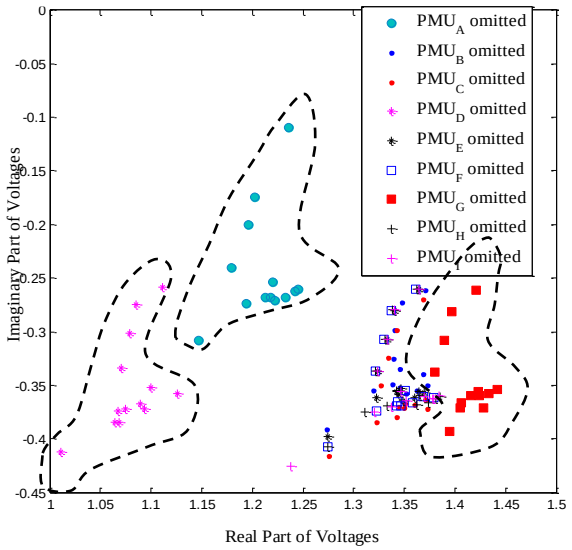

Fig. 6. All solutions for the state estimation problem after three attacks

V. Conclusion

In this paper, integrity attack on power systems was studied and a procedure based on the static state estimation and data clustering algorithms was presented to accurately detect the number and location of attacks and determine which PMU in the network contained malicious data. This detection can be done in the control center by comparing different state estimation results and data clustering approaches and it was called PMUIDS. The theory of detecting attacks by PMUIDS is proved by two theorems. The theorems show that in most cases, the successful interacting attacks cannot happen and PMUIDS can effectively detect any arbitrary false data that is added to the measurements. However, in some special cases that many PMUs are forged and the remained ones cannot make the whole power system observable, the successful interacting attacks can happen. Even in such a case, the algorithm is still able to provide correct measurements for some parts of the system based on the number of unfalsified PMUs. The HiL results on a sample power system prove the PMUIDS capability in finding the forged PMU data. For future work, considering more complex large-scale systems is suggested. Further, considering the issue of PMU faulty measurements and distinguishing it from the attacked PMUs can be an interesting work.

Appendix: Data Clustering Algorithm

Each clustering analysis has two pre-requisites; determining the number of clusters and the clustering method. Here, for determining the number of clusters, subtractive clustering technique is utilized [42]. In each step of this iterative algorithm, the potential to be a cluster center is evaluated for all points in the data set and the point with the highest potential value, which has more data in its neighborhood, will be found. Then, by using some criteria, it is determined whether that point is a new cluster center or not. After obtaining a new cluster center, the potential values of the remaining data points will be modified and the process repeats for the remaining points till no new cluster center can be found. Based on subtractive clustering, the number of clusters and a good initial guess for cluster centers are obtained. However, data points of each cluster cannot be found in this method. This information can be derived by utilizing fuzzy c-mean (FCM) clustering. The FCM algorithm iteratively minimizes the following objective function [43]:

$$J = \sum_{j=1}^{n_d}\sum_{i=1}^{n_c} \mu_{ij}^2 \left\| d_j - c_i \right\|^2 \tag{22}$$

where n_d refers to the number of data samples, n_c refers to number of clusters determined by subtracting clustering method, d_j is the j-th data point, c_i is the i-th cluster center, μ_{ij} refers to the membership degree of j-th data in the i-th cluster and is computed as follows:

$$\mu_{ij} = \frac{1}{\sum_{l=1}^{n_c} \left(\frac{\left\| d_j - c_i \right\|}{\left\| d_j - c_l \right\|} \right)^2} \tag{23}$$

In the initial step of FCM algorithm, pre-fixed n_c and initial values for cluster centers are determined. Then, the optimum value of the cluster centers and membership degrees are procured iteratively by minimizing the objective function.

References

[1] A. Giani, E. Bitar, M. Garcia, M. McQueen, P. Khargonekar, and K. Poolla, "Smart Grid Data Integrity Attacks," *IEEE Trans. Smart Grid*, vol. 4, no. 3, pp. 1244–1253, Sep. 2013, doi: 10.1109/TSG.2013.2245155.

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

[3] M. Dehghani, Z. Khalafi, A. Khalili, and A. Sami, "Integrity attack detection in PMU networks using static state estimation algorithm," in *2015 IEEE Eindhoven PowerTech*, 2015, pp. 1–6.

[4] X. Wang, D. Shi, J. Wang, Z. Yu, and Z. Wang, "Online Identification and Data Recovery for PMU Data Manipulation Attack," *IEEE Trans. Smart Grid*, vol. 10, no. 6, pp. 5889–5898, Nov. 2019, doi: 10.1109/TSG.2019.2892423.

[5] Y. Chakhchoukh, H. Lei, and B. K. Johnson, "Diagnosis of Outliers and Cyber Attacks in Dynamic PMU-Based Power State Estimation," *IEEE Trans. Power Syst.*, vol. 35, no. 2, pp. 1188–1197, Mar. 2020, doi: 10.1109/TPWRS.2019.2939192.

[6] S. Siamak, M. Dehghani, and M. Mohammadi, "Dynamic GPS Spoofing Attack Detection, Localization, and Measurement Correction Exploiting PMU and SCADA," *IEEE Syst. J.*, pp. 1–10, 2020, doi: 10.1109/JSYST.2020.3001016.

[7] A. S. Musleh, H. M. Khalid, S. M. Muyeen, and A. Al-Durra, "A Prediction Algorithm to Enhance Grid Resilience Toward Cyber Attacks in WAMCS Applications," *IEEE Syst. J.*, vol. 13, no. 1, pp. 710–719, Mar. 2019, doi: 10.1109/JSYST.2017.2741483.

[8] S. Sahoo, T. Dragicevic, and F. Blaabjerg, "Cyber Security in Control of Grid-Tied Power Electronic Converters–Challenges and Vulnerabilities," *IEEE J. Emerg. Sel. Top. Power Electron.*, pp. 1–1, 2019, doi: 10.1109/JESTPE.2019.2953480.

[9] S. Sahoo, J. C.-H. Peng, S. Mishra, and T. Dragicevic, "Distributed Screening of Hijacking Attacks in DC Microgrids," *IEEE Trans. Power Electron.*, pp. 1–1, 2019, doi: 10.1109/TPEL.2019.2957071.

[10] D. Wang, X. Guan, T. Liu, Y. Gu, Y. Sun, and Y. Liu, "A survey on bad data injection attack in smart grid," in *2013 IEEE PES Asia-Pacific Power and Energy Engineering Conference (APPEEC)*, Kowloon, Hong Kong, Dec. 2013, pp. 1–6, doi: 10.1109/APPEEC.2013.6837157.

[11] H. Javanmardi, M. Dehghani, M. Mohammadi, S. Siamak, and M.R. Hesamzadeh, "BMI-based Load Frequency Control in Microgrids Under False Data Injection Attacks," *IEEE Syst. J.*, 2021, doi: 10.1109/JSYST.2021.3054947.

[12] 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, doi: 10.1109/TPWRS.2006.881149.

[13] J. Zhu and A. Abur, "Bad Data Identification When Using Phasor Measurements," in *2007 IEEE Lausanne Power Tech*, Lausanne, Switzerland, Jul. 2007, pp. 1676–1681, doi: 10.1109/PCT.2007.4538567.

[14] J. l. Duran-Paz, F. Perez-Hidalgo, and M. J. Duran-Martinez, "Bad Data Detection of Unequal Magnitudes in State Estimation of Power Systems [Power Engineering Letters]," *IEEE Power Eng. Rev.*, vol. 22, no. 4, pp. 57–60, Apr. 2002, doi: 10.1109/MPER.2002.4312111.

[15] D. Ye and T.-Y. Zhang, "Summation Detector for False Data-Injection Attack in Cyber-Physical Systems," *IEEE Trans. Cybern.*, pp. 1–8, 2019, doi: 10.1109/TCYB.2019.2915124.

[16] K. Manandhar, X. Cao, F. Hu, and Y. Liu, "Detection of Faults and Attacks Including False Data Injection Attack in Smart Grid Using Kalman Filter," *IEEE Trans. Control Netw. Syst.*, vol. 1, no. 4, pp. 370–379, Dec. 2014, doi: 10.1109/TCNS.2014.2357531.

[17] Y. He, G. J. Mendis, and J. Wei, "Real-Time Detection of False Data Injection Attacks in Smart Grid: A Deep Learning-Based Intelligent Mechanism," *IEEE Trans. Smart Grid*, vol. 8, no. 5, pp. 2505–2516, Sep. 2017, doi: 10.1109/TSG.2017.2703842.

[18] M. Ganjkhani, S. N. Fallah, S. Badakhshan, S. Shamshirband, and K. Chau, "A Novel Detection Algorithm to Identify False Data Injection Attacks on Power System State Estimation," *Energies*, vol. 12, no. 11, p. 2209, Jun. 2019, doi: 10.3390/en12112209.

[19] L. Xie, Y. Mo, and B. Sinopoli, "False Data Injection Attacks in Electricity Markets," in *2010 First IEEE International Conference on Smart Grid Communications*, Gaithersburg, MD, USA, Oct. 2010, pp. 226–231, doi: 10.1109/SMARTGRID.2010.5622048.

[20] 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. 1, pp. 1–33, May 2011, doi: 10.1145/1952982.1952995.

[21] Z.-H. Yu and W.-L. Chin, "Blind False Data Injection Attack Using PCA Approximation Method in Smart Grid," *IEEE Trans. Smart Grid*, vol. 6, no. 3, pp. 1219–1226, May 2015, doi: 10.1109/TSG.2014.2382714.

[22] W. Niemira, R. B. Bobba, P. Sauer, and W. H. Sanders, "Malicious data detection in state estimation leveraging system losses & estimation of perturbed parameters," in *2013 IEEE International Conference on Smart Grid Communications (SmartGridComm)*, Vancouver, BC, Canada, Oct. 2013, pp. 402–407, doi: 10.1109/SmartGridComm.2013.6687991.

[23] Y. Gu, T. Liu, D. Wang, X. Guan, and Z. Xu, "Bad data detection method for smart grids based on distributed state estimation," in *2013 IEEE International Conference on Communications (ICC)*, Budapest, Hungary, Jun. 2013, pp. 4483–4487, doi: 10.1109/ICC.2013.6655273.

[24] H. Varmaziari and M. Dehghani, "Cyber-attack detection system of large-scale power systems using decentralized unknown input observer," in *2017 Iranian Conference on Electrical Engineering (ICEE)*, Tehran, Iran, May 2017, pp. 621–626, doi: 10.1109/IranianCEE.2017.7985114.

[25] J. Kim and L. Tong, "On phasor measurement unit placement against state and topology attacks," in *2013 IEEE International Conference on Smart Grid Communications (SmartGridComm)*, Vancouver, BC, Canada, Oct. 2013, pp. 396–401, doi: 10.1109/SmartGridComm.2013.6687990.

[26] O. Vukovic and G. Dan, "Security of Fully Distributed Power System State Estimation: Detection and Mitigation of Data Integrity Attacks," *IEEE J. Sel. Areas Commun.*, vol. 32, no. 7, pp. 1500–1508, Jul. 2014, doi: 10.1109/JSAC.2014.2332106.

[27] O. Vukovic, K. C. Sou, G. Dan, and H. Sandberg, "Network-Aware Mitigation of Data Integrity Attacks on Power System State Estimation," *IEEE J. Sel. Areas Commun.*, vol. 30, no. 6, pp. 1108–1118, Jul. 2012, doi: 10.1109/JSAC.2012.120709.

[28] S. Zonouz, K. M. Rogers, R. Berthier, R. B. Bobba, W. H. Sanders, and T. J. Overbye, "SCPSE: Security-Oriented Cyber-Physical State Estimation for Power Grid Critical Infrastructures," *IEEE Trans. Smart Grid*, vol. 3, no. 4, pp. 1790–1799, Dec. 2012, doi: 10.1109/TSG.2012.2217762.

[29] H. Margossian, M. A. Sayed, W. Fawaz, and Z. Nakad, "Partial grid false data injection attacks against state estimation," *Int. J. Electr. Power Energy Syst.*, vol. 110, pp. 623–629, Sep. 2019, doi: 10.1016/j.ijepes.2019.03.039.

[30] G. Liang, S. R. Weller, J. Zhao, F. Luo, and Z. Y. Dong, "False data injection attacks targeting DC model-based state estimation," in *2017 IEEE Power & Energy Society General Meeting*, Chicago, IL, Jul. 2017, pp. 1–5, doi: 10.1109/PESGM.2017.8273918.

[31] R. Deng, G. Xiao, and R. Lu, "Defending Against False Data Injection Attacks on Power System State Estimation," *IEEE Trans. Ind. Inform.*, vol. 13, no. 1, pp. 198–207, Feb. 2017, doi: 10.1109/TII.2015.2470218.

[32] Q. Yang, L. Jiang, W. Hao, B. Zhou, P. Yang, and Z. Lv, "PMU Placement in Electric Transmission Networks for Reliable State Estimation Against False Data Injection Attacks," *IEEE Internet Things J.*, vol. 4, no. 6, pp. 1978–1986, Dec. 2017, doi: 10.1109/JIOT.2017.2769134.

[33] A. G. Phadke and J. S. Thorp, *Synchronized phasor measurements and their applications*, vol. 1. Springer, 2008.

[34] Y. Wang, W. Li, J. Lu, and H. Liu, "Evaluating multiple reliability indices of regional networks in wide area measurement system," *Electr. Power Syst. Res.*, vol. 79, no. 10, pp. 1353–1359, Oct. 2009, doi: 10.1016/j.epsr.2009.04.005.

[35] J. De La Ree, V. Centeno, J. S. Thorp, and A. G. Phadke, "Synchronized Phasor Measurement Applications in Power Systems," *IEEE Trans. Smart Grid*, vol. 1, no. 1, pp. 20–27, Jun. 2010, doi: 10.1109/TSG.2010.2044815.

[36] Q. Wang, W. Tai, Y. Tang, M. Ni, and S. You, "A two-layer game theoretical attack-defense model for a false data injection attack against power systems," *Int. J. Electr. Power Energy Syst.*, vol. 104, pp. 169–177, Jan. 2019, doi: 10.1016/j.ijepes.2018.07.007.

[37] 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. on Smart Grid*, vol. 11, no. 3, pp.2218-2234, Oct. 2019, doi: 10.1109/TSG.2019.2949998.

[38] R. Sodhi, S. C. Srivastava, and S. N. Singh, "Optimal PMU placement method for complete topological and numerical observability of power system," *Electr. Power Syst. Res.*, vol. 80, no. 9, pp. 1154–1159, Sep. 2010, doi: 10.1016/j.epsr.2010.03.005.

[39] "Praviraj PG (2020). Power System State Estimation with PMU (Phasor Measurement Unit), MATLAB Central File Exchange, (https://www.mathworks.com/matlabcentral/fileexchange/65621-power-system-state-estimation-with-pmu-phasor-measurement-unit), Retrieved May 24, 2020.

[40] M. Dehghani, B. Shayanfard, and A. R. Khayatian, "PMU Ranking Based on Singular Value Decomposition of Dynamic Stability Matrix," *IEEE Trans. Power Syst.*, vol. 28, no. 3, pp. 2263–2270, Aug. 2013, doi: 10.1109/TPWRS.2013.2246196.

[41] M. Dehghani, L. Goel, and W. Li, "PMU based observability reliability evaluation in electric power systems," *Electr. Power Syst. Res.*, vol. 116, pp. 347–354, Nov. 2014, doi: 10.1016/j.epsr.2014.07.008.

[42] Q. Ren, L. Baron, and M. Balazinski, "Fuzzy identification of cutting acoustic emission with extended subtractive cluster analysis," *Nonlinear Dyn.*, vol. 67, no. 4, pp. 2599–2608, Mar. 2012, doi: 10.1007/s11071-011-0173-5.

[43] H. Izakian and A. Abraham, "Fuzzy C-means and fuzzy swarm for fuzzy clustering problem," *Expert Syst. Appl.*, vol. 38, no. 3, pp. 1835–1838, Mar. 2011, doi: 10.1016/j.eswa.2010.07.112.

Zahra Sadat Khalafi received her B.Sc. degree in Electronic engineering from the Electrical engineering department of Yazd University, Yazd, Iran, in 2003. She then received her M.Sc. degree in Control engineering from the Power and Control Engineering department of Shiraz University, Shiraz, Iran in 2014. Currently she works as an education export and instructor at school of E-Learning in Shiraz University. Her areas of interest include: Smart Grid, PMU Networks, Reliability Analysis, Machine Learning, Linear Matrix Inequalities in Control, Model Predictive Control.

Maryam Dehghani (M'10-SM'18) received her B. Sc. and M. Sc. degrees in electrical engineering from Shiraz university, Shiraz, Iran, in 1999 and 2002, respectively and her PhD from Amirkabir University of Technology, Tehran, Iran in 2008. She is currently an associate professor in the school of electrical and computer engineering, Shiraz university, Shiraz, Iran. Her research interests include Linear Matrix Inequalities (LMI) and Bilinear Matrix Inequalities (BMI) applications in control, Linear Parameter Varying (LPV) systems, and Control applications in Biomedical and Power systems.

Navid Vafamand received his B.Sc. degree in electrical engineering and M.Sc. degree in control engineering form Shiraz University of Technology, Iran, in 2012 and 2014, respectively, and Ph. D. in control engineering at Shiraz University, Shiraz, Iran, in 2019. Currently, he serves as a research assistance at Shiraz University. He was a Ph.D. Visiting student with the Department of Energy Technology, Aalborg University, Denmark, from 2017 to 2018. Dr. Vafamand is the co-author of more than 80 international conference and journal papers and four chapter-books and an active reviewer in several journals. His main research interests include Takagi-Sugeno (TS) fuzzy systems, linear parameter varying (LPV) models, predictive control, and DC microgrids.

Abdullah Khalili received his M.S.C. in Software Engineering (in 2011) from Iran University of Science and Technology where he worked on Dynamic Malware Detection as his thesis title. He received his Ph.D. from CSE and IT department of Shiraz University in 2016. Title of his Ph.D. thesis was "A Multi-Tier Intrusion Detection for Industrial Control Systems". He is currently an assistant professor at the department of Electrical and Computer Engineering in University of Hormozgan. His research interests include CPS Security, ICS and SCADA Security, Power System Security, Machine Learning, and Pattern Recognition.

Ashkan Sami is an Associate Professor of Computer Science and Software Engineering at Shiraz University and National Elite's Foundation Professor since 2019. Ashkan teaches and conducts multidisciplinary research on Data Science, Applied AI, Cyber Security and Software Engineering. He obtained his B.S.E.E. from Virginia Tech; U.S.A. and PhD in 2006 from Tohoku University, where his PhD became a Japanese national project and earned him a tenured faculty position at Tohoku University; Japan. His current work on AI-based system design. Dr. Sami has been graduated more than 100 M.S. and Ph.D. students under his supervision.

Tomislav Dragičević (S'09-M'13-SM'17) received the M.Sc. degree and the industrial Ph.D. degrees in electrical engineering from the Faculty of Electrical Engineering, University of Zagreb, Zagreb, Croatia, in 2009 and 2013, respectively.,From 2013 to 2016, he was a Postdoctoral Research Associate with Aalborg University, Denmark, where he was an Associate Professor from 2016 to 2020. He was a Guest Professor at Nottingham University, U.K., during Spring/Summer of 2018. Since 2020, he has been a Professor with the Technical University of Denmark. His research interests include design and control of microgrids, and application of advanced modeling and control concepts to power electronic systems. He has authored and coauthored more than 200 technical papers (more than 100 of them are published in international journals, mostly in IEEE), eight book chapters, and a book in the field.,Dr. Dragičević is an Associate Editor of the IEEE Transactions on Industrial Electronics, IEEE Transactions on Power Electronics, IEEE Journal of Emerging and Selected Topics in Power Electronics, and IEEE Industrial Electronics Magazine. He was a recipient of the Končar Prize for the Best Industrial Ph.D. thesis in Croatia, and a Robert Mayer Energy Conservation Award. He is a winner of Alexander van Humboldt fellowship for experienced researchers.