An Improved FDIA Approach for PMU-Assisted Linear Power System State Estimation

***S. Kundu[1,2], M. Alam[1], B.K. Saha Roy[1], S.S. Thakur[1]**

1 Department of EE, NIT Durgapur, Durgapur, India

2 Department of EEE, Bharat Institute of Engineering & Technology, Hyderabad, India

***Corresponding Author**

Email addresses: sk.17ee1102@phd.nitdgp.ac.in (S. Kundu); ma.18ee1501@phd.nitdgp.ac.in (M. Alam); bk.saharoy@ee.nitdgp.ac.in (B.K. Saha Roy); sst@ee.nitdgp.ac.in (S.S. Thakur)

Phone No: +91-8359880715 (S. Kundu); +91-9002272140 (M. Alam); +91-9434789043 (B.K. Saha Roy); +91-9434788023 (S.S. Thakur)

Abstract

Power system state estimation is vulnerable to stealthy false data injection attack (FDIA) that bypasses conventional bad data detectors. In this paper, an improved FDIA detection approach has been proposed using a phasor measurement unit (PMU) assisted linear power system state estimation scheme. The proposed detection approach tracks the changes of complex PMU measurements between the current time instant of the present-day and one step previous time instant of the previous day. This variation of complex PMU measurement is then compared with the variation of forecasted measurements. Manhattan distance has been applied to calculate the distance between the distribution of two different measurement variations. In the event of an FDIA, the Manhattan distance will increase significantly from normal conditions. The proposed approach has been validated on two IEEE benchmark test systems. The produced results clearly depict the efficacy of the proposed approach.

Keywords- state estimation, FDIA, PMU, bad data, Manhattan distance.

1. Introduction

State estimation is an important tool in maintaining the secure and reliable operation of the power grid. The state estimation in power systems is generally performed with the conventional measurements obtained from various remote terminal units (RTUs). Conventional measurements typically incorporate injected real and reactive powers, real and reactive line flows, and generator buses' voltage magnitudes. Both PMU and RTU measurements in general comprise small random measurement errors which originate due to inaccurate measurement devices or noises [1-2]. However, faulty measurement equipment or defective telecommunication systems may cause the measurement noise to be large. These measurements comprising large noises are termed bad measurements. Traditional bad data detection approaches [3-4] can successfully detect these large measurement noises.

Recently, the operation of power systems is subjected to the increasing threat from cyber attackers [5-7]. The vulnerability of state estimation to stealthy attack vectors which aren't detected by conventional bad data detection approaches have been addressed by various researchers [8-30]. Liu *et al.* [8] first show that a maiden cyber-attack termed false data injection attack (FDIA) can simply get past the conventional bad data detection system. In their work, the researchers demonstrated that an attacker can exploit power system structure to instigate such attack that can infiltrate random noise into certain state variables while evading existing bad data detection approaches.

Traditional bad data detection process fails to detect the FDIA, as the measurement residual obtained during FDIA remains unchanged. Several attempts have been made to assuage the effects of FDIA. Existing mitigation approaches are mainly based on protection [9-15] and detection [16-30] based methods. In order to defend against FDIA, Yang *et al.* [9] developed both protection based and detection-based methodology. In order to provide protection-based defense, they identify the critical meters to be protected by applying a heuristic-based approach. For detection-based methodology, spatial and temporal-based detection schemes have been implemented. Bobba *et al.* [10] have shown that FDIA can be detected by protecting a strategically selected set of basic measurements. Brute force-based approach has been implemented by them to select the measurement sets to be protected. Tian *et al.* [11] proposed a TOTAL protection strategy against both perfect and imperfect

FDIA. The TOTAL protection framework reduces the attack impact of usual imperfect FDIA, while providing defense against usual perfect FDIA. The researchers constructed the meter selection problem as a linear binary programming or Integer programming based on whether the protection approach comprises of PMUs or not. Khanna *et al.* [12] developed a defense mechanism that chooses the most critical measurements to secure. For that purpose, a priority-based protection methodology has been implemented by incorporating normalized measurement Jacobian matrix instead of binary measurement Jacobian. In [13], the researchers formulated a least-budget defense approach to protect FDIA. They determined the meters to be protected and their corresponding defense budget. Das *et al.* [14] implemented a scheme that provides enhanced network resilience against FDIA. In order to select an optimal set of sensors, a computationally cheap approach based on logical analysis of data has been presented. In [15], graphical methods have been suggested to safeguard against FDIA. The authors formulate the problem of securing minimal measurements as a variant Steiner tree problem in a graph. The problem has been solved by applying approximation method based on tree pruning approach. Protection-based methods have the drawback of decreased redundancy as only a few secured and reliable measurements can be utilized. Further, the protection-based approaches don't guarantee secure protection always. Unlike protection approaches, detection techniques can identify erroneous data that has been included into the measurements.

Chaojun *et al.* [16] implemented Kullback-Leibler divergence for tracking the measurement dynamics to detect the FDIA. However, SCADA-based non-linear SE has been discussed in their paper. In [17], the researchers enhanced the accuracy of the above approach by applying a joint transformation-based technique. Some other approaches detect FDIA by implementing advanced state estimation methods like the data-driven approach [18] and least trimmed squares estimation [19]. A sequential detector that depends on the generalized likelihood ratio has been formulated in [20] for the detection of false data attacks. Further, in order to provide wide-area monitoring of the smart grid, a distributed sequential detector utilizing level-triggered sampling has been proposed in their work. In [21], Chen *et al.* detected false data attacks in smart grid by utilizing spatial-temporal relationships between grid structures. Liu *et al.* [22] developed the false data detection problem as a matrix separation problem and solved the problem by applying two approaches, i.e., the nuclear norm minimization approach and the low-rank matrix factorization technique. Ashok *et al.* [23] proposed an online detection approach to detect malicious false data. In their approach, the researchers utilized load forecasting information, generation schedules, and real-time synchro-phasor measurements to detect the injected false data. Furthermore, they have assumed that synchro-phasor data is free from data tampering as it has inherent cyber security mechanisms. However, some existing literature suggests that attackers can also inject malicious data into PMU measurements. Basumallik *et al.* [24] exhibit the vulnerability of synchro phasor measurements to cyber-attacks. However, their approach is based on adopting non-linear hybrid state estimation. In the references [25] and [26], synchro phasor data obtained from PMUs are manipulated due to the presence of a GPS spoofing attack (GSA). A highly discriminative detection approach utilizing the *k*-smallest residual similarity test is proposed in [27]. However, in their work the authors considered the FDIA to be an imperfect one. Artificial intelligence-based approaches like reinforcement learning [28], deep learning [29], and extreme learning machines [30] are also being applied for the detection of malicious data. Seemita *et al.* [31] evaluated the equivalent impedances of transmission lines for detection of data manipulation attacks in PMUs. However, they haven't explored it for a PMU-assisted linear state estimation framework. In [32], the authors suggested a novel attack vector formulation method for linear SE framework by incorporating low-rank approach. However, the detection strategy hasn't been discussed in their paper. Obata et al. [33] recently introduced a detection strategy based on distributed state estimation. In [34], the authors developed an unsupervised detection framework to detect the FDIA. Shuheng et al. [35] suggests a novel FDIA detection approach for unbalanced distribution systems. In their approach, square root unscented Kalman filter has been applied to produce SE results. Thereafter, a generalized likelihood ratio test is formulated to detect FDIAs. The authors of [36] implemented combined static and dynamic state estimation to detect FDIA. Although recently some references [37-40] have discussed cyber-attacks on PMUs, however, only few of them have concentrated on detection of FDIA. Moreover, most of those frameworks haven't considered the identification of attacked measurements and none of those methodologies have the ability to detect successive attacks.

Linear state estimation in power systems is obtained with the inclusion of measurements received from optimally placed PMUs. Therefore, determining the optimal locations of PMUs is vital in power systems.

Different techniques [41-43] have been suggested by various researchers for solving the problem of optimal PMU placement. Although all these approaches are different, they provide the same number of optimal PMUs.

The existing literature mainly discusses various detection techniques to filter out injected false data in the conventional SCADA-based non-linear state estimator. However, recent research suggests that PMU measurements are also vulnerable to cyber-attacks. Considering this vulnerability, this article focuses on detecting false data attacks in PMU-assisted linear state estimator. Furthermore, the existing literature haven't considered the detection of false data in successive time samples. The proposed framework successfully detects data manipulation in consecutive time samples. The main contributions of the article are summarized below.

- Formulation of an improved FDIA detection approach that can successfully detect malicious data in complex PMU measurements, unlike most of the previous approaches, which detect false data in traditional SCADA measurements.
- Application of Manhattan distance for obtaining the distance between the distribution of two different measurement variations to detect the injected malicious data, which traditional bad data detection (BDD) fails to detect.
- Implementation of the proposed detection approach for PMU-assisted linear state estimation framework.
- Successful detection of false data in consecutive time samples.

The rest of the article is organized as below. Section 2 gives the mathematical background of PMU-assisted linear state estimation, traditional bad data detection approach, and FDI attacks. In Section 3, the proposed detection methodology, along with the Manhattan distance, are discussed. Section 4 provides the simulation set up and in section 5, results and discussions are provided. Finally, section 6 concludes the article.

2. Mathematical Background

In this section, mathematical formulation of optimal allocation of PMU, PMU-assisted linear state estimation, along with traditional bad data detection and FDI attacks are presented.

2.1. Optimal allocation of PMU

The optimal PMU placement problem for a system that consists of n no. of buses can be mathematically expressed as

$$\min \sum_{i=1}^{n} \cos t_i x_i \qquad (1)$$
$$st\ f(x) \geq d$$

where 'd' represents a unit vector of dimension 'n' and the PMU installation cost at i^{th} bus is represented by $cost_i$.

The observability constraint function, $f(x)$, determines whether a certain bus is observable or unobservable. If a particular bus is unobservable, then the corresponding entry of $f(x)$ will be 'zero' and will be 'one' in the case of the observable bus. Assuming all the PMUs have equal and unity cost, the problem formulation of optimal PMU placement can be given as

$$\min \sum_{i=1}^{n} x_i \qquad (2)$$
$$st\ f(x) \geq d$$

2.2. PMU-assisted linear state estimation

PMU-assisted linear state estimation utilizes the linear measurement function, which is given in equation (3).

$$z_m = Hx + \xi \tag{3}$$

Where, z_m is $(m \times 1)$ dimensional vector of the complex PMU measurements, which comprises complex line currents and complex bus voltages, H is the observation matrix, which is composed of two sub-matrices, i.e., H_1 and H_2. The entries of H_1 is a function of line admittances, whereas H_2 is a unity matrix. ξ is the noise vector. The covariance matrix for ξ is given as

$$\varphi = \begin{bmatrix} \varphi_l & 0 \\ 0 & \varphi_v \end{bmatrix} \tag{4}$$

Where φ_l and φ_v are the covariance matrix for complex line currents and complex bus voltages, respectively. The gain matrix is calculated as

$$G_m = H^T \varphi^{-1} H \tag{5}$$

The estimated state can be calculated as

$$x = G_m^{-1} H^T \varphi^{-1} z_m \tag{6}$$

2.3. Bad data detection

Conventional bad data detection approach relies on the residual analysis of $r_m = z_m - Hx$. The presence of bad data is verified by comparing the residual with a threshold value. If the residual is larger than the threshold, then it is assumed that bad data is present in the measurements. Otherwise, the measurement is considered normal. The threshold is decided after performing a chi-square test considering a desired significance level.

2.4. False data injection attack

The work carried out in [8] shows that an attacker can generate stealthy false data and thereby inject if the attacker knows the network structure and can perturb several measurements at the same time. The formulated false data injection attack can circumvent the bad data detection method, if the attack vector $'a'$ satisfies the following condition, i.e., $a = Hc$. ‘ a ’ is the malicious data incorporated into the actual measurements, and $'c'$ is the injected state estimation error. The manipulated measurements after being attacked can be mathematically written as

$$z_{att} = z_m + a \tag{7}$$

After the injection of false data, the estimated state also comprises errors and can be mathematically represented as

$$x_{att} = x + c \tag{8}$$

Traditional bad data detection mechanism fails to detect false data injection attack as the measurement residuals remain unchanged. The measurement residuals after the attack can be represented as

$$r_a = z_{att} - Hx_{att} = \left(z_m + a\right) - H\left(x + c\right) = z_m - Hx = r \tag{9}$$

This shows that the measurement residual remains unaffected even after the injection of false data. Thus, conventional bad data detection mechanism fails to detect false data injection attack.

3. Proposed Methodology

The proposed detection approach is an online detection method that tracks the variation of measurements

obtained at the current time instant (k) of the present day and one step previous time instant $(k-1)$ of the previous day. This variation of complex PMU measurement is then compared with the variation of forecasted measurements. Manhattan distance has been applied to calculate the distance between the distribution of two different measurement variations. Assuming $'\alpha'$ is the distribution of measurement variation obtained from the deviation of real-time measurements whereas $'\beta'$ represents the distribution of measurement variation obtained from the historical measurements. α can be mathematically expressed as

$$\alpha = z_m^k - z_m^{pre,k-1} \tag{10}$$

The mathematical expression of β is given as

$$\beta = z_{forecasted}^k - z_{forecasted}^{pre,k-1} \tag{11}$$

z_m^k is the measurement vector at time instant k of the present day and $z_m^{pre,k-1}$ is the measurement vector at time instant $k-1$ of the previous day. $z_{forecasted}^k$ is the forecasted measurement at time instant k of the present day and $z_{forecasted}^{pre,k-1}$ is the forecasted measurement at time instant $k-1$ of the previous day. It has been assumed that there is no significant load variation occurs in between two consecutive days.

The deviation of these two different measurement variations can be mathematically given as

$$\nabla = \alpha - \beta \tag{12}$$

3.1 Manhattan Distance

The Manhattan distance calculated between two vectors is same to the one-norm of the distance between the vectors. The Manhattan distance between two points x and y can be mathematically expressed as

$$d(x, y) = \sum(x - y) \tag{13}$$

Considering the above formula, the Manhattan distance ∇ can be mathematically obtained as

$$p_{dist} = \sum_{i=1}^{m} (\alpha - \beta) \tag{14}$$

$$= \sum_{i=1}^{m} \left[\left(z_m^k - z_{forecasted}^k \right) + \left(z_{forecasted}^{pre,k-1} - z_m^{pre,k-1} \right) \right] \tag{15}$$

where $'m'$ is the total no. of measurements.

In case of any data manipulation in power systems, the p_{dist} value will become higher than that of normal conditions. Therefore, if the p_{dist} value is higher at any instant; then it is assumed that FDIA occurs.

3.2 Algorithmic steps

The algorithmic steps of the proposed approach are depicted through the flowchart provided in Figure 1. Initially, complex PMU measurements, viz. complex line currents and complex bus voltages, are obtained at the current time instant k of the present day. The next step is to compute the variation of real-time measurements α from equation (10). For calculating α, the complex PMU measurements of one step before time instant $k-1$ of the previous day is compared with the complex PMU measurements obtained at time instant k of the present day. It might be noted that in this methodology, one step before time instant of the previous day has been considered instead of the present day. This is because, by considering the one step before time instant of the previous day, the proposed methodology can successfully detect FDIA in successive time samples. The next step is to compute the distribution of measurement variation β obtained from the historical measurements.

The Manhattan distance of the deviation of two different distributions α and β is further determined to detect the occurrence of FDIA.

4. Simulation Details

The simulation study has been carried out by varying the loads as provided in Reliability test systems of IEEE [44]. The present day is chosen Thursday, which has 96% peak load of the weekly peak load, and the previous day is Wednesday, which has 98% peak load of the weekly peak load. Power factor is supposed to be constant so that the reactive power follows the active counterpart. The total load change has been distributed among the generators based on their participation factors. Consecutive load flows have been done to determine the true values of the states. Simulated measurements are produced by inclusion of Gaussian noise of zero mean and standard deviation of 0.5% to the true values. The efficacy of the proposed approach has been verified on test networks of IEEE 14 bus and IEEE 118 bus. The line diagram of the IEEE 14 bus test system, along with the allocated PMU, is shown in Figure 2. It is noticed that four PMUs have to be placed on buses 2, 6, 7, and 9 for making the system completely observable. Each PMU measures the line currents with the connected buses and the voltage of the bus where it is installed. For the IEEE 118 bus system, 32 PMUs have to be allocated for entire system observability. The optimal locations for both IEEE 14 and 118 bus test systems are provided in Table 1.

4.1 Performance Evaluation Indices

The effectiveness of the proposed approach is evaluated through various performance evaluation indices as defined below.

False positive rate: False positive represents the case when the detection technique detects an attack even if there is no attack. A false positive rate (FPR) can be mathematically given as

$$FPR = FP \Big/ \left(FP + TN \right) \tag{16}$$

where FP is the false positive and TN is the true negative.

False negative rate: False negative represents the case when the detection approach fails to detect an attack. The mathematical expression of false negative rate (FNR) is

$$FNR = FN \Big/ \left(FN + TP \right) \tag{17}$$

where FN is the false negative and TP is the true positive.

True positive rate: True positive rate (TPR) or detection rate represents the case when the detection technique successfully detects an attack. TPR is mathematically expressed as

$$TPR = TP \Big/ \left(TP + FN \right) \tag{18}$$

Table 2 provides the details of attacked state variables and the magnitude of attacks. It is noted that for IEEE 14 bus system the attacker tries to perturb the complex state variables at buses 9, 12, and 13 with an attack magnitude of 1-10%. Similarly, for IEEE 118 bus test system, the perturbed states are complex bus voltages at buses 112 and 118, and the attack magnitude is increased to 10 % from 1%.

5. Results and Discussions

The suggested detection method is tested on IEEE 14 bus and IEEE 118 bus systems. The results for both test systems are provided below.

5.1 IEEE 14 bus test system

Figure 3 depicts the calculated p_{dist} when the state variables have been perturbed by 2% of their original value. From the figure, it is noted that during k=5, 6, 7, the p_{dist} value rises from its normal conditions. The rise in p_{dist} value suggests presence of false data attacks in the system. It is worth noting here that the p_{dist} value remains high for successive time samples. Therefore, FDIA can be detected even it occurs in consecutive time samples.

Similarly, Figure 4 exhibits the p_{dist} value when the attack magnitude has been increased to 5%. From this figure, it is seen that the p_{dist} value becomes higher during the occurrence of an attack in the system. It is also noted that with the increase in attack magnitude, the p_{dist} value increases. Figure 5 gives the value of p_{dist} corresponds to a 10% increase in attack magnitude. It is worth pointing out here that even with the increase in attack magnitude, the proposed approach successfully detects the FDIA in successive time samples. Therefore, considering Figure 3-5, one can clearly detect if there is an attack in the system.

Figure 6 shows the variation of ∇ through bar chart with varying measurement no. From this figure, it is noted that measurement no. 6, 9, 10, 12, 13, and 14 which are being attacked corresponds to the higher value of ∇. The attackers perturb those measurements to corrupt the states $x_9, x_{12},$ and x_{13}. Figure 7 shows the changes of the false positive rate with the detection threshold. It is noticed that choosing of low detection threshold value increases the FPR. It is seen that with the increase in detection threshold, the FPR decreases and reduces to zero. Figure 8 depicts the variation of true positive rate with attack magnitudes for detection threshold 0.01. It is noted that when the attack magnitude is less than 0.01, the TPR is less than one. However, with the increase in attack magnitude, TPR increases and quickly becomes one.

5.2 IEEE 118 bus system

Figure 9 depicts the calculated p_{dist} value when the attackers manipulate the state variables by 1%. It is noticed that during the FDIA, the value of p_{dist} abruptly becomes higher. Increase in p_{dist} value suggests that there is a disturbance in the system which is due to a cyber-attack. Figure 10 and Figure 11 show calculated p_{dist} when the attack magnitude increased to 5% and 10% respectively. Similarly, it is noticed that during time samples k=5, 6, and 7, the distance value increases indicating the presence of a FDIA. From both figures, it is noted that the proposed approach successfully detects FDIA in consecutive time samples even when the attack intensity is increased. Figure 12 shows the variation of ∇ through bar chart with varying measurement no. It is noticed that measurement no. 93, 95, and 139 have higher values of ∇ which indicates that those measurements are being manipulated by the attackers to perturb the complex bus voltages at bus 112 and bus 118.

Figure 13 exhibits the variation of FPR with changes in detection thresholds. It is noticed that when the detection threshold is low, the FPR is a little high. However, as the detection threshold increases the FPR reduces and finally settles to zero when the threshold equals to 0.01. The variation of TPR i.e., detection rate with the increase in attack magnitudes for detection threshold 0.01 is depicted in Figure 14. It shows that the proposed detection approach provides 100% successful detection rate irrespective of the attack magnitudes. From the above-discussed results, it can be easily inferred that the FPR depends on the detection thresholds. Choosing of high detection threshold eliminates the false positives case which yields an improved detection rate.

5.3 Comparative discussions with other approaches

In the existing literature, many approaches have been introduced by various researchers for detection of false data. However, most of the existing detection methodologies have concentrated on detecting false data in SCADA measurements based non-linear state estimator. Therefore, the existing literature lacks detection strategies for detection of false data in complex PMU measurements. Although the authors of [24] have studied

the impact of false data in PMU devices, they haven't suggested a detection strategy to detect malicious false data. The authors of [25] have studied the impact of GPS spoofing attack in PMU assisted forecasting aided state estimation (FASE). However, GPS spoofing attack is different from stealthy FDIA. Also, the authors have considered FASE framework in their approach. This is to be noted that only a handful of researchers [37-40] have concentrated on detecting cyber-attacks in PMUs. Further, only few of them [38-40] have discussed false data type intrusion detection. Comparison of proposed approach with the methods discussed in [37-40] is provided in Table 3. For comparison, three parameters have been considered, viz. if the detected attack is FDIA or not, identification of attacked measurements, and lastly capability to detect FDIA in consecutive time samples.

From Table 3, it is observed that only the authors of reference [38] has discussed on identification of attacked measurements. Furthermore, none of the references have focused on detecting FDIA in consecutive time samples.
The proposed framework not only identifies the attacked measurements but also has the ability to detect attack in successive time samples.

6. Conclusions

In this paper, an improved FDIA detection approach has been suggested for linear power system state estimation which utilizes complex PMU measurements. The proposed detection framework is based on calculating the deviation of complex PMU measurements between the current time instant of the present day and one step before time instant of the previous day. Thereafter, the Manhattan distance has been applied to obtain the distance between the distributions of these two different measurement variations. The proposed approach has been implemented on IEEE 14 bus and IEEE 118 bus test systems. Provided results depict that the proposed framework has a high detection rate and low false positives. It is observed that the proposed detection approach successfully detects FDIA even if it occurs in subsequent time samples.

REFERENCES

[1] Abur, A., and Exposito A.G., *Power System State Estimation: Theory and Implementation* 1st ed. New York, NY, USA: Marcel Dekker, (2004).

[2] Monticelli, A., *State Estimation in Electric Power Systems: A Generalized Approach*. New York, NY, USA: Springer, (1999).

[3] Martínez-Parrales, R., Fuerte-Esquivel, CR., and Alcaide-Moreno, BA. "Analysis of bad data in power system state estimation under non-gaussian measurement noise", *Electr. Power Syst. Res.*, **186,** p: 106424 (2020).

[4] Lin, Y., and Abur, A. "A highly efficient bad data identification approach for very large-scale power systems", *IEEE Trans Power Syst.*, **33**(6), pp .5979-5989 (2018).

[5] Ten, C.W., Liu, C.C., and Manimaran, G. "Vulnerability assessment of cybersecurity for SCADA systems", *IEEE Trans Power Syst.*, **23**(4), pp. 1836-1846 (2008).

[6] Sridhar, S., Hahn, A., and Govindarasu, M. "Cyber–physical system security for the electric power grid," In *Proceedings of the IEEE*, **100** (1):210-224 (2011).

[7] Liu, C.C., Stefanov, A., Hong, J., et al. "Intruders in the grid", *IEEE Pow and Energ mag*., **10**(1), pp. 58-66 (2011).

[8] Liu, Y., Ning, P., and Reiter, M.K. "False data injection attacks against state estimation in electric power grids", In *proc. 16th ACM Conf. Comput. Commun. Security (CCS)*, Chicago, IL, USA, pp. 21-32, (2009).

[9] Yang, Q., Yang, J., Yu, W., et al. "On false data-injection attacks against power system state estimation: modeling and countermeasures", *IEEE Trans. Parallel and Dist. Sys.*,**25**(3), pp.717-729, (2014).

[10] Bobba, R.B., Rogers, K.M., Wang, Q., et al. "Detecting false data injection attacks on dc state estimation", In *Preprints of the First Workshop on Secure Control Systems, CPSWEEK* (2010).

[11] Tian, J., Wang, B., Li, T., et al. "Total: optimal protection strategy against perfect and imperfect false data injection attacks on power grid cyber–physical systems", *IEEE Int. of Things J.*, **8**(2), pp.1001-1015, (2021).

[12] Khanna, K., Panigrahi, B.K., and Joshi, A. "Priority-based protection against the malicious data injection attacks on state estimation", *IEEE Syst. J.*, **14**(2), pp.1945-1952, (2020).
[13] Deng, R., Xiao, G., and Lu, R. "Defending against false data injection attacks on power system state estimation", *IEEE Trans. Ind Inf.*, **13** (1), pp.198-207, (2017).
[14] Das, T.K., Ghosh, S., and Koley, E. "Prevention and detection of FDIA on power-network protection scheme using multiple support set", *J of Inf Sec App.*, **63**, p. 103054, (2021).
[15] Bi, S., Zhang, Y.J. "Graphical methods for defense against false-data injection attacks on power system state estimation", *IEEE Trans. Smart Grid*, **5**(3), pp. 1216-1227, (2014).
[16] Chaojun, G., Jirutitijaroen, P., Motani, M. "Detecting false data injection attacks in ac state estimation", *IEEE Trans. Smart Grid*., **6**(5), pp. 2476-2483, (2015).
[17] Singh, S.K., Khanna, K., Bose, R., et al. "Joint-transformation-based detection of false data injection attacks in smart grid", *IEEE Trans on Ind Inf.*, **14**(1), pp. 89-97, (2018).
[18] Weng, Y., Negi, R., Faloutsos, C., et al. "Robust data-driven state estimation for smart grid", *IEEE Trans. Smart Grid*. **8**(4), pp. 1956-1967, (2017).
[19] Chakhchoukh, Y., and Ishii, H. "Enhancing robustness to cyber-attacks in power systems through multiple least trimmed squares state estimations", *IEEE Trans. Pow Syst.* **31**(6), pp. 4395-4405 (2016).
[20] Li, S., Yılmaz, Y., Wang, X. "Quickest detection of false data injection attack in wide-area smart grids", *IEEE Trans. Smart Grid*, **6**(6), pp. 2725-2735, (2015).
[21] Chen, P.Y., Yang, S., McCann, J.A., et al. "Detection of false data injection attacks in smart-grid systems", *IEEE Comm Mag.*, **53**(2), pp. 206-213, (2015).
[22] Liu, L., Esmalifalak, M., Ding, Q., et al. "Detecting false data injection attacks on power grid by sparse optimization", *IEEE Trans. Smart Grid*, **5**(2), pp. 612-621, (2014).
[23] Ashok, A., Govindarasu, M., and Ajjarapu, V. "Online detection of stealthy false data injection attacks in power system state estimation", *IEEE Trans. Smart Grid*, **9**(3), pp.1636-1646, (2018).
[24] Basumallik, S., Eftekharnejad, S., Davis, N., et al. "Impact of false data injection attacks on PMU-based state estimation" *2017 North American Power Symposium (NAPS)*, pp. 1-6, (2017).
[25] Geetha, S. J., Meghwani, A., Chakrabarti, S., et al. "Spoofing attack on synchrophasor gps clock: impact and detection in power system state estimation", *Int J of Elect Pow & Ener Syst.* **134**, p. 107396, (2022).
[26] Fan, X., Du, L., and Duan, D. "Synchrophasor data correction under gps spoofing attack: a state estimation-based approach" *IEEE Trans. Smart Grid*, **9**(5), pp. 4538-4546, (2018).
[27] Cheng, G., Lin, Y., Zhao, J., et al. "A highly discriminative detector against false data injection attacks in ac state estimation", *IEEE Trans. Smart Grid*, **1**(1), (2022).
[28] Kurt, M.N., Ogundijo, O., Li, C., et al. "Online cyber-attack detection in smart grid: a reinforcement learning approach", *IEEE Trans. Smart Grid*, **10**(5), pp.5174-5185, (2019).
[29] He, Y., Mendis, G.J., and Wei, J. "Real-time detection of false data injection attacks in smart grid: a deep learning-based intelligent mechanism", *IEEE Trans. Smart Grid*, **8**(5), pp. 2505-2516, (2017).
[30] Xue, D., Jing, X., and Liu, H. "Detection of false data injection attacks in smart grid utilizing elm-based ocon framework", *IEEE Acc.*, **7**, pp. 31762-31773, (2019).
[31] Pal, S., Sikdar, B., and Chow, J.H. "Classification and detection of PMU data manipulation attacks using transmission line parameters", *IEEE Trans. Smart Grid*, **9**(5), pp. 5057-5066, (2018).
[32] Mukherjee, D. "Data-driven false data injection attack: a low-rank approach", *IEEE Trans Smart Grid*, **13**(3), pp. 2479-2482, (2022).
[33] Obata, S., Kobayashim, K., and Yamashita, Y. "On detection of false data injection attacks in distributed state estimation of power networks", *2021 IEEE 10th Global Conference on Consumer Electronics (GCCE)*, Kyoto, Japan, pp. 472-473, (2021).
[34] Chen, C., Wang, Y., Cui, M., et al. "Data-driven detection of stealthy false data injection attack against power system state estimation", *IEEE Trans. Industrial Informatics*, **18**(12), pp. 8467-8476, (2022).
[35] Wei, S., Xu. J., Wu, Z., et al. "A false data injection attack detection strategy for unbalanced distribution networks state estimation", *IEEE Trans Smart Grid*, **14**(5), pp. 3992-4006, (2023).
[36] Hu, P., Gao, W., Li, Y., et al. "Detection of false data injection attacks in smart grid based on joint dynamic and static state estimation", *IEEE Acc.*, **11**, pp. 45028-45038, (2023).
[37] Wang, X., Shi, D., Wang, J., et al. "Online identification and data recovery for PMU data manipulation attack", *IEEE Trans Smart Grid*, **10**(6), pp. 5889-5898, (2019).
[38] Khalafi, Z.S., Dehghani, M., Khalili, A., et al. "Intrusion detection, measurement correction, and attack localization of PMU networks", *IEEE Trans Ind Electr*, **69**(5), pp. 4697-4706, (2022).
[39] Almasabi, S., Alsuwian, T., Javed, E., et al. "A novel technique to detect false data injection attacks on phasor measurement units", *Sensors*, **21**(17), p. 5791, (2021).

[40] Khare, G., Mohapatra, A., and Singh, S.N. "A real-time approach for detection and correction of false data in PMU measurements", *Elec Pow Syst Res*, **191**, p. 106866, (2021).
[41] Kundu, S., Alam, M., Saha Roy, B.K., et al. "Allocation of optimal PMUS for power system observability using promethee approach", *Int Trans. Elec Ener Syst.*, **2022**; pp. 1–16, (2022).
[42] Meenakshi Devi, and M., Geethanjali, M. "Hybrid of genetic algorithm and minimum spanning tree method for optimal PMU placements", *Meas.*, **154,** p. 107476, (2020).
[43] Babu, R., and Bhattacharyya, B. "Strategic placements of PMUs for power network observability considering redundancy measurement", *Meas.*, **134**, pp. 606–623, (2019).
[44] Grigg C et al. "The ieee reliability test system-1996. a report prepared by the reliability test system task force of the application of probability methods subcommittee", *IEEE Trans. Pow Syst.*, **14**(3), pp. 1010–1020, (1999).

List of Figures

List of Tables

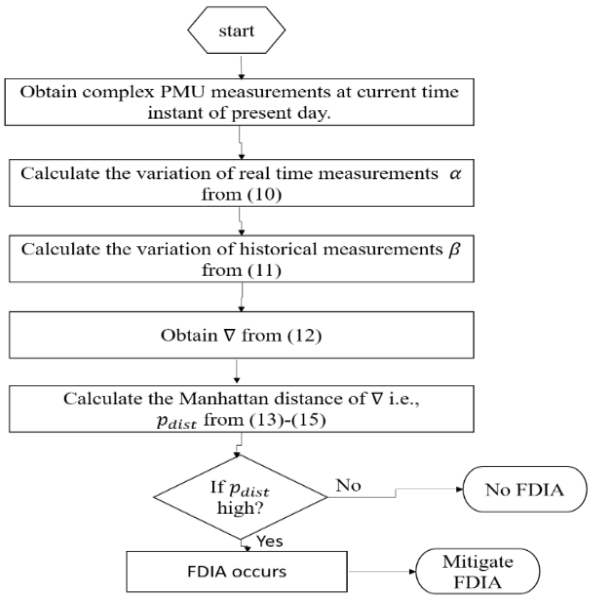

Figure 1 Flowchart of the proposed detection approach

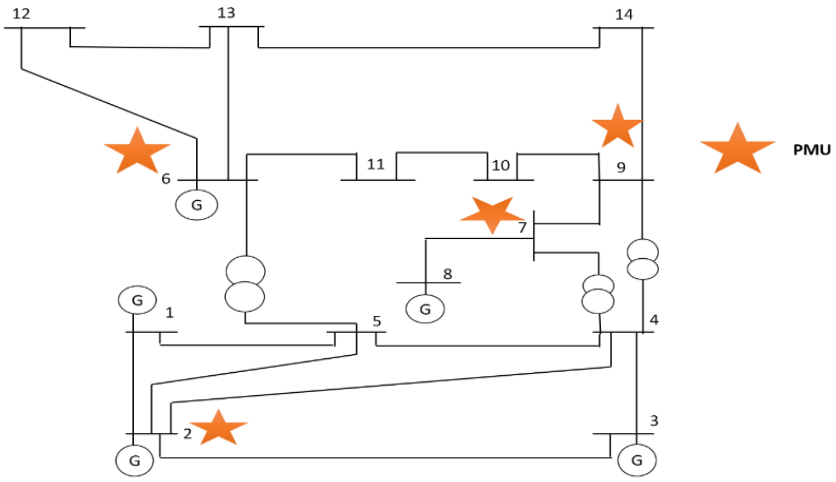

Figure 2 Single line diagram of IEEE 14 bus test system with allocated PMUs

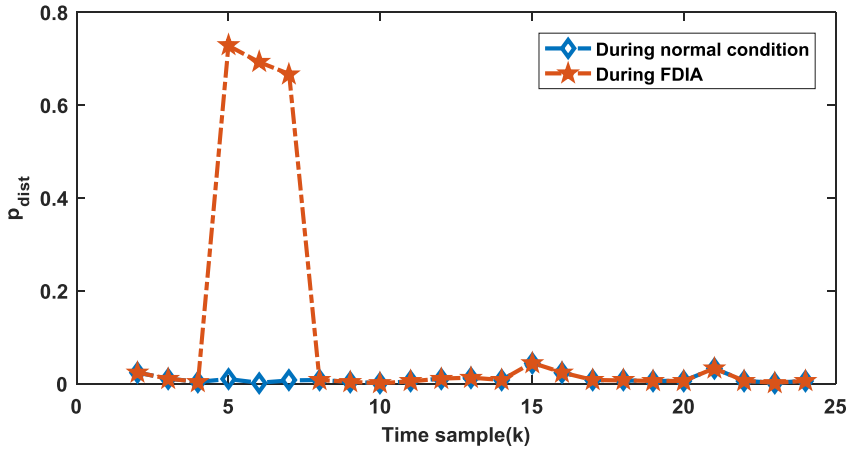

Figure 3 Calculated p_{dist} when the attack magnitude increased to 2%

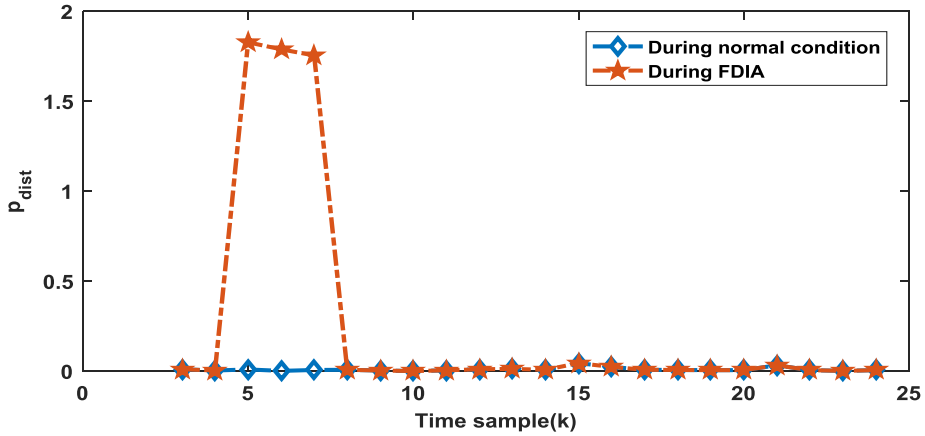

Figure 4 Calculated p_{dist} when the attack magnitude increased to 5%

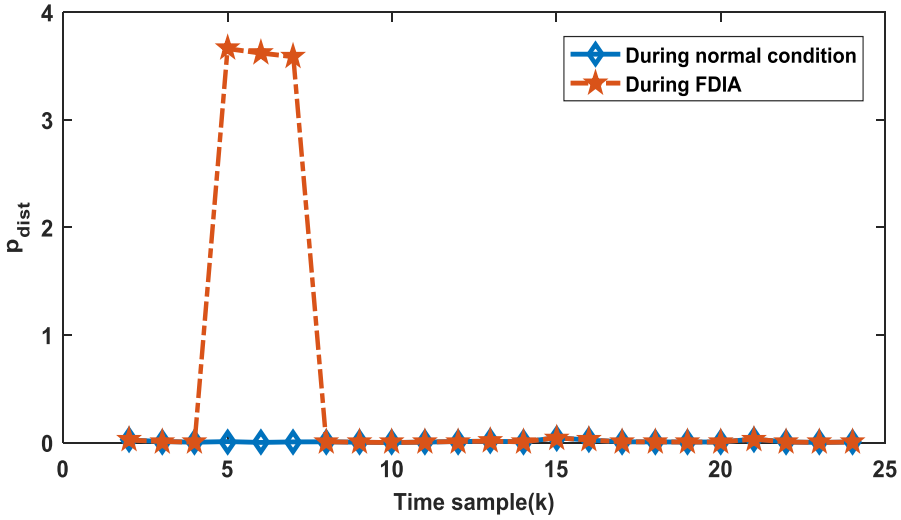

Figure 5 Calculated p_{dist} when the attack magnitude increased to 10%

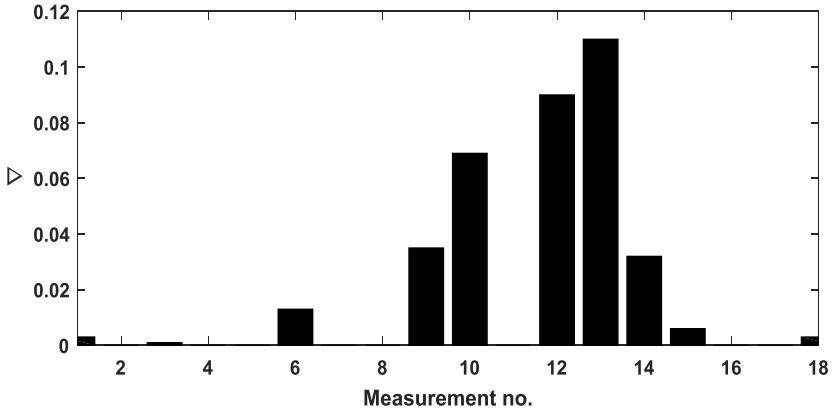

Figure 6 Depiction of the variation of ∇ through bar chart with varying measurement numbers

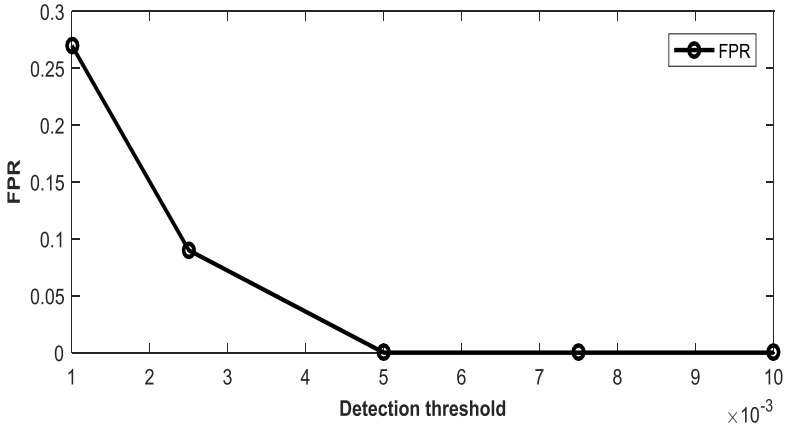

Figure 7 Variation of false positive rate with a detection threshold

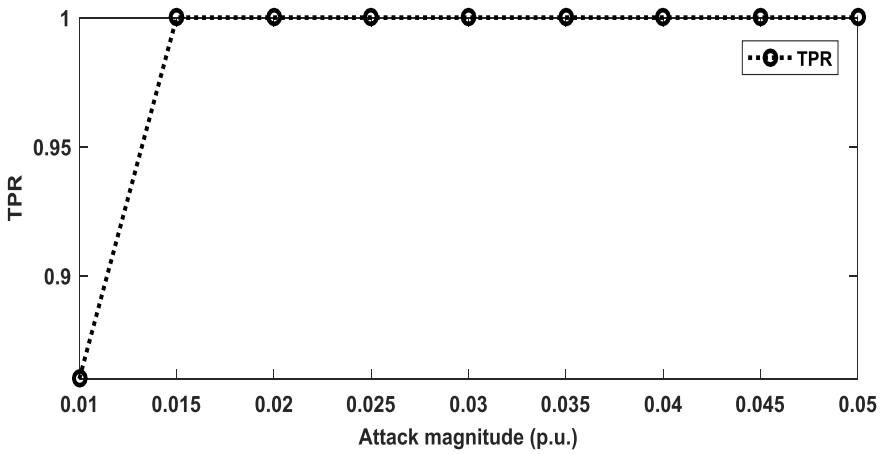

Figure 8 Variation of true positive rate with attack magnitudes for detection threshold 0.01

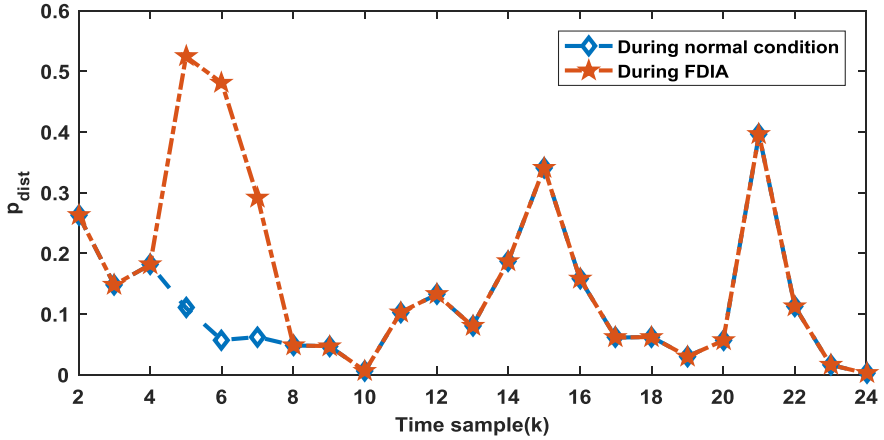

Figure 9 Calculated p_{dist} when the attack magnitude increased to 1%

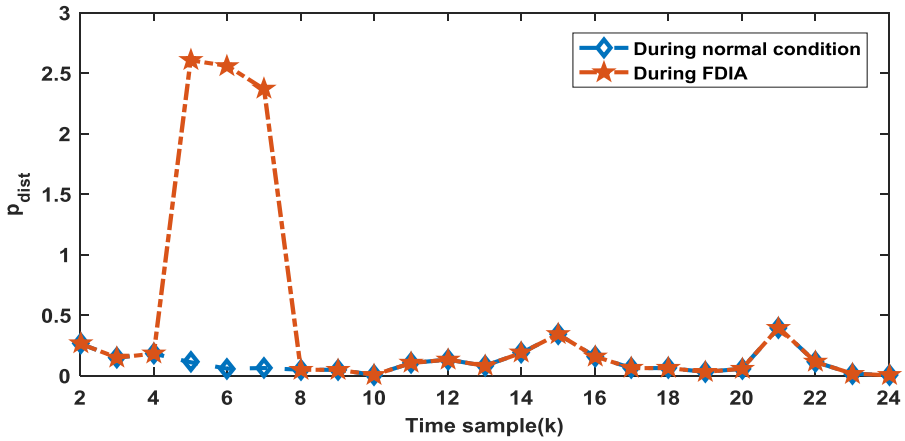

Figure 10 Calculated p_{dist} when the attack magnitude increased to 5%

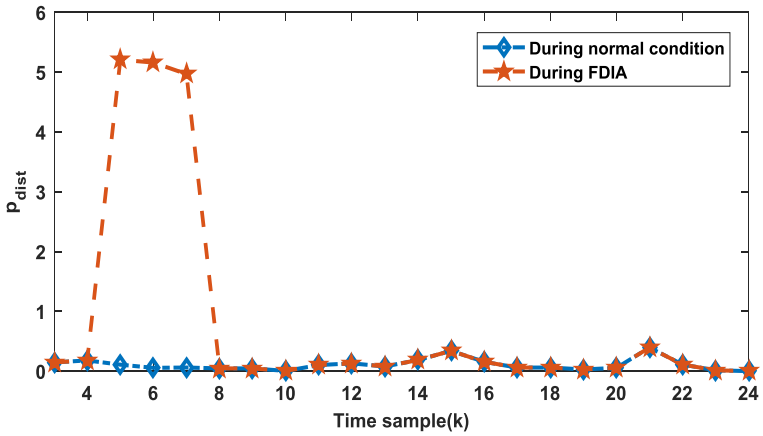

Figure 11 Calculated p_{dist} when the attack magnitude increased to 10%

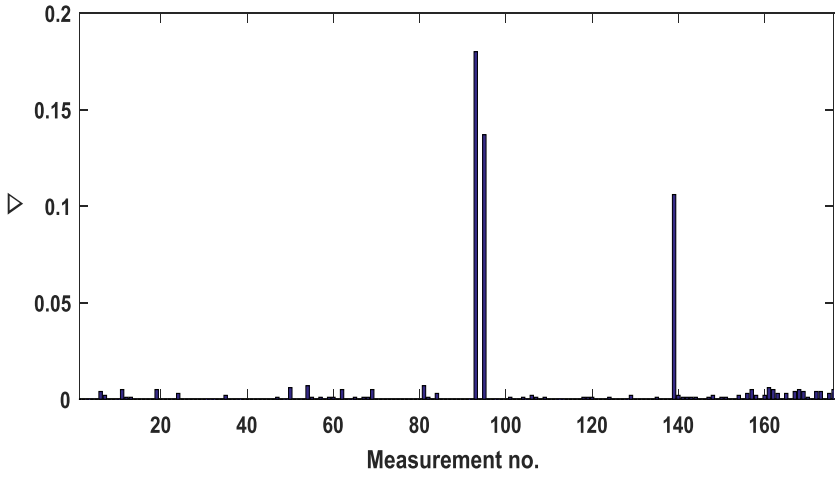

Figure 12 Depiction of the variation of ∇ through bar chart with varying measurement numbers

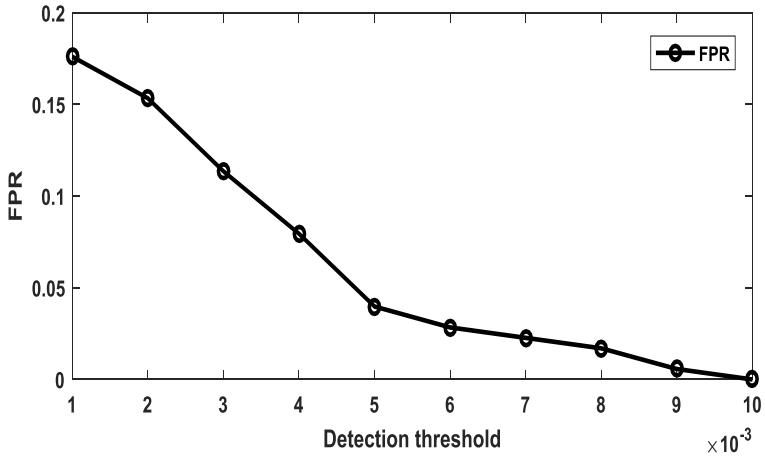

Figure 13 Variation of false positive rate with detection threshold

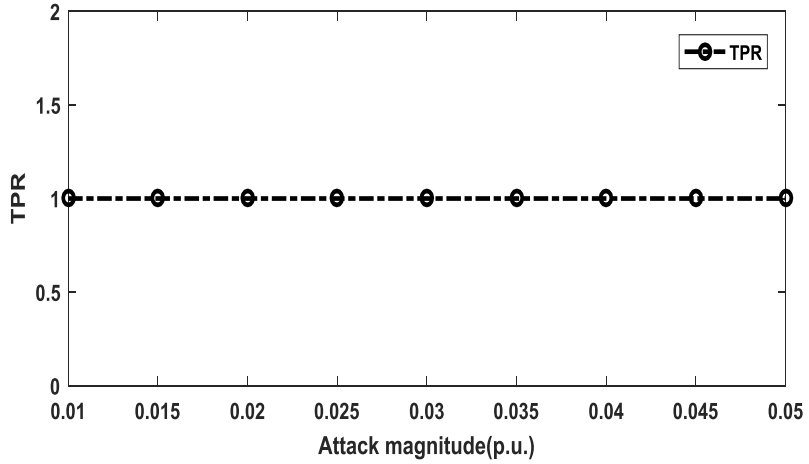

Figure 14 Variation of true positive rate with attack magnitude for detection threshold 0.01

Table 1 Optimal No. and Locations of PMUs

Bus test system	Optimal No.	Locations of PMUs
IEEE 14	4	2, 6, 7, 9
IEEE 118	32	1,5,9,12,15,17,21,24,25,28,34,37,41, 45,49,53,56,62,64,68,71,75,77,80,85, 86,90,94,101,105,110,114

Table 2 Attacked state variables and their magnitude of attacks

Bus test system	Attacked states	Magnitude of attack (%)
IEEE 14	x_9, x_{12}, and x_{13}	1-10
IEEE 118	x_{112} and x_{118}	1-10

Table 3 Comparison with other methods

Reference	*Detection of FDIA?*	*Identification of attacked measurements?*	*Capability to detect FDIA in successive time samples?*
[37]	No	No	No
[38]	Yes	Yes	No
[39]	Yes	No	No
[40]	Yes	No	No
Proposed	Yes	Yes	Yes

Biographies

Shubhrajyoti Kundu is presently working as an Assistant Professor in the Dept. of Electrical and Electronics Engineering, Bharat Institute of Engineering and Technology, Hyderabad. He has done his B. Tech in Electrical Engineering from West Bengal University of Technology, West Bengal, India in the year 2012, and has completed M.E in Industrial System and Drives from RGPV, Bhopal, India in the year 2015. Presently, He is working towards his PhD degree from National Institute of Technology, Durgapur, India. His research interest includes Optimal PMU placement, State Estimation in power systems, False data injection attack in power systems etc.

Mehebub Alam has done his B. Tech in Electrical Engineering from West Bengal University of Technology, West Bengal, India in the year 2012, and has completed his M. Tech and PhD from National Institute of Technology Durgapur, India in the year 2018 and 2023 respectively. His research interest includes line outage

identification, state estimation etc.

Biman Kumar Saha Roy received the PhD in Electrical Engineering from Indian Institute of Technology Kharagpur, India in 2013. Presently, he holds the post of Assistant Professor in Electrical Engineering Dept. at National Institute of Technology Durgapur. Before joining National Institute of Technology Durgapur, he worked as an Assistant Professor in the Dept. of Electrical Engineering, NIT Agartala, India. He has published several papers in reputed Journals and Conferences. He has active research interest on Power systems state estimation, synchro-phasor application to power system, Optimal PMU Placement, etc.

Siddhartha Sankar Thakur obtained his PhD in Electrical Engineering from Indian Institute of Technology Kharagpur in the year of 2000. He Joined National Institute of Technology (NIT) Durgapur in the year 1985 as an Assistant Professor and presently, he holds the post of Professor in the Electrical Engineering Department, NIT Durgapur, India. He has published several papers in reputed Journals and Conferences. He has active research interest on Power systems state estimation, Dynamic state estimation, synchro-phasor application to power system, Optimal PMU Placement, Identification of Line outage, Load forecasting etc.