






Article

A Novel Technique to Detect False Data Injection Attacks on Phasor Measurement Units

Saleh Almasabi ^{1,*}, Turki Alsuwian ¹, Ehtasham Javed ², Muhammad Irfan ¹, Mohammed Jalalah ^{1,3}, Belqasem Aljafari ¹ and Farid A. Harraz ^{3,4}

¹ Electrical Engineering Department, College of Engineering, Najran University, Najran 11001, Saudi Arabia; tmalsuwian@nu.edu.sa (T.A.); miditta@nu.edu.sa (M.I.); msjalalah@nu.edu.sa (M.J.); bhaljafari@nu.edu.sa (B.A.)

² Neuroscience Center, Helsinki Institute for Life Sciences, University of Helsinki, 00014 Helsinki, Finland; ehtasham.javed@helsinki.fi

³ Promising Centre for Sensors and Electronic Devices (PCSED), Advanced Materials and Nano-Research Centre, Najran University, P.O. Box 1988, Najran 11001, Saudi Arabia; faharraz@nu.edu.sa

⁴ Nanomaterials and Nanotechnology Department, Central Metallurgical Research and Development Institute (CMRDI), P.O. Box 87 Helwan, Cairo 11421, Egypt

* Correspondence: ssalmasabi@nu.edu.sa

Abstract: The power industry is in the process of grid modernization with the introduction of phasor measurement units (PMUs), advanced metering infrastructure (AMI), and other technologies. Although these technologies enable more reliable and efficient operation, the risk of cyber threats has increased, as evidenced by the recent blackouts in Ukraine and New York. One of these threats is false data injection attacks (FDIAs). Most of the FDIA literature focuses on the vulnerability of DC estimators and AC estimators to such attacks. This paper investigates FDIAs for PMU-based state estimation, where the PMUs are comparable. Several states can be manipulated by compromising one PMU through the channels of that PMU. A Phase Locking Value (PLV) technique was developed to detect FDIAs. The proposed approach is tested on the IEEE 14-bus and the IEEE 30-bus test systems under different scenarios using a Monte Carlo simulation where the PLV demonstrated an efficient performance.

Keywords: cyber-physical security; false data injection attacks; state estimation; phase lock value; phasor measurement units; smart grids



Citation: Almasabi, S.; Alsuwian, T.; Javed, E.; Irfan, M.; Jalalah, M.; Aljafari, B.; Harraz, F.A. A Novel Technique to Detect False Data Injection Attacks on Phasor Measurement Units. *Sensors* **2021**, *21*, 5791. <https://doi.org/10.3390/s21175791>

Academic Editors: Rafael Pastor Vargas, Llanos Tobarra and Antonio Robles-Gómez

Received: 15 July 2021

Accepted: 23 August 2021

Published: 28 August 2021

Publisher's Note: MDPI stays neutral with regard to jurisdictional claims in published maps and institutional affiliations.



Copyright: © 2021 by the authors. Licensee MDPI, Basel, Switzerland. This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license (<https://creativecommons.org/licenses/by/4.0/>).

1. Introduction

In recent years, numerous cyber-attacks were launched against electric power systems, which caused power outages, such as the Ukraine blackout on 23 December 2015 and Manhattan, New York blackout on 13 July 2019 [1,2]. Cyber-attacks are aimed to either damage the power grid or to manipulate the grid markets to gain a financial advantage. Such attacks can lead to many wrong decisions to be taken by the control engineers of the electric power grid. Therefore, it is important to investigate, study and analyze such attacks and data manipulation through the techniques of state estimation (SE) to identify those data that has been attacked and manipulated.

The SE is an essential part of the Supervisory Control and Data Acquisition (SCADA) system, where the SCADA uses state estimators to find the actual states of the power grid. These state estimates are then, utilized by the energy management system (EMS) to perform different system operations, such as contingency analysis and optimal power flow.

Traditionally, state estimators obtain grid measurements from remote terminal units (RTUs), which measure the voltage magnitudes, power injections, and power flows. These measurements are used by the state estimator to obtain the voltage magnitudes and angles for the buses in the grid [3].

The recent advancements of smart meters, such as phasor measurement units (PMUs) and advanced meter infrastructure (AMI), have enhanced the situational awareness and enabled a more secure grid operation. However, these new technologies introduced new vulnerabilities and raised the risk of cyber-threats, as shown in Figure 1. One of these risks is data manipulation, where the adversaries manipulate the measured data to change the system operating conditions, thereby, damaging the grid operations. Such cyber-attacks are known as false data injection attacks (FDIAs).

The FDIA poses are a real threat due to its ability to bypass bad data detection (BDD), thereby changing the system operations without being detected [4]. The BDD is used to detect outliers by using residual-based methods [3]. However, FDIAs utilize the power grid topology to mask the false data and bypass BDD [5].

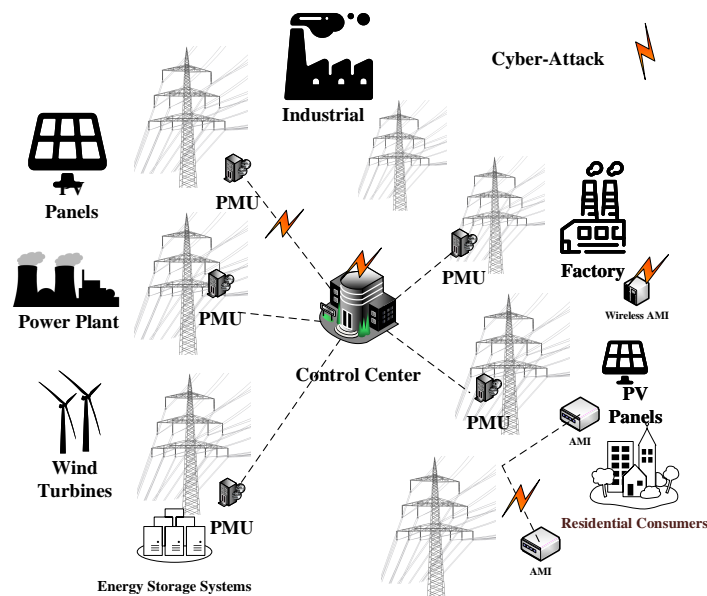


Figure 1. Cyber threats in a smart grid.

Most of the FDIA literature focuses on RTU measurements and the DC estimator framework. Teixeira et al. [6] used random FDIAs to evaluate the performance of the BDD in state estimators. Protecting a minimum subset of measurements to guard against FDIAs was proposed by [7,8]. Wang et al. [9] proposed a systematic topology switch of the network for detecting FDIAs.

FDIAs can also be used on AC-estimators, although it is harder to bypass the BDD due to the nonlinearity of these estimators [10,11]. Masking FDIAs with Line outages was investigated in [12], where the adversaries require limited knowledge of the grid topology. Based on the signal processing technique, wavelet singular entropy (WSE) is employed for the detection of any false data injection in the AC systems [13]. Wireless sensor networks (WSNs), including cyber-physical systems (CPSs), were implemented for detection of the distributed attacks of false data injection and jamming attacks [14]. Theoretical analysis for an imperfect FDIA model based on a forecasting-aided method was introduced in [15]. The above-mentioned references are considered RTU-based FDIA in an AC system setting.

Over the last decade, the PMUs started emerging as a better option for grid monitoring over the legacy RTUs, due to their precise measurements, ability to measure phasors and high refresh rate [16]. As a result, several researchers have investigated PMUs vulnerability to FDIAs. The ability to spoof the global positioning system (GPS) signal of PMUs was assessed by [17,18] where several techniques were introduced. The Low Rank Matrix (LRM) factorization method was introduced by [19], to identify false data injection attacks on PMUs. It is shown that the proposed method was able to identify proper power system operation states as well as detect the malicious attacks.

However, later research on LRM [20] demonstrated that a more sophisticated attacker that understands the temporal correlation of PMU data can exploit it to design unobservable FDIA attacks that cannot be detected by the LRM detector. The authors of [21] proposed an optimal placement approach where, by securing a minimum number of PMUs, FDIA attacks are infeasible. Ding et al. [22] developed a probabilistic model for cyber-threats on PMUs and used an optimal PMU placement to enhance the observability under such a threat.

The optimal placement of PMUs (OPP) using an integrated linear programming (ILP) algorithm to prevent the FDIA attacks was presented by [23]. It was discovered that a weak power grid can be transformed into a robust power grid by adding a few PMUs at vulnerable locations.

By looking at the literature of FDIA attacks, most studies are considering RTU-based FDIA attacks. These studies were performed in either a DC estimator or AC estimator setting. The PMUs were typically used as redundant units to secure the RTU measurements against FDIA attacks [21]. PMUs have also been used as a source of online data to forecast and develop FDIA detection techniques under an RTU-based estimator [24]. In [25], a detector for FDIA attacks on hybrid estimators contingent upon the absence of outliers in PMU data.

As discussed earlier PMUs were considered as a backup or a secure platform against FDIA, and the impact of compromising PMUs has not been considered before. In this paper, the effect of attacking state estimators via PMUs data is considered. The strategy for attacking via PMUs and its impact on the state estimators is investigated.

The paper also proposes a detection mechanism for the FDIA attacks based on a synchronization metric named the phase lock value (PLV) [26]. The PLV was originally proposed in the field of neuroscience to investigate the signals from two or more distinct brain regions whether they are functionally connected or not [27,28]. The PLV quantifies the synchronicity present between two signals based on phase changes [29–31], where the underlying assumption is that, for a certain time-period, if the phase changes of two signals are consistent, they are said to be connected/synchronized, and PLV will result in a value closer or equal to 'one'.

Whereas, if phase changes do not show consistency, two signals are not connected and for such PLV will have a value closer or equal to 'zero'. With this background in mind, PLV can be utilized to study unwanted randomness between signals/data. For example, consider two connected signals resulting in a consistent phase change, but when randomness is added to one of the signals, then the differences in phases are no longer constant, and thus two signals are no longer connected to each other. On similar lines, Patrick Celka [31] showed that different types of noise processes affect PLV differently and the strength of noise enhances between-processes effects. However, common among noise processes, it could be noticed that, with the introduction of noise, the PLV tends toward zero implying that the underlying signals deviate from being synchronized.

This motivated us to utilize this concept in the identification of FDIA, and we hypothesized that under normal circumstances, when there is no data manipulation, the buses in the grid will have consistent phase changes between them, whereas, in the case of manipulated data, the differences between phases will no longer be constant. The proposed approach is tested on the IEEE 14-bus and the IEEE 30-bus test systems under different conditions using Monte Carlo simulation.

The main contributions of this article can be summarized as follows:

- Most of the existing FDIA attacks assume DC model associated with RTUs. In RTU-based attacks, the adversaries need to compromise several RTUs, where PMU-based attacks compromising one PMU are sufficient for a successful attack. This paper addresses PMU-based FDIA attacks.
- This presents an effective approach for detecting FDIA attacks using PLV.
- The proposed approach requires no training to build a model, and can be used online to detect FDIA attacks.

The rest of the paper is organized as follows. Section 2 describes state estimation in the presence of PMUs. Section 3 discusses the attack strategy for FDIA. Section 4 presents

the proposed PLV detection mechanism. Section 5 presents the simulation results, and Section 6 concludes the paper.

2. State Estimation

State estimators use the measurements obtained for the RTUs or the PMUs to find the voltage magnitudes and angles for the buses (\hat{x}). If the grid is completely observable by the PMUs, the state estimation becomes a linear process [3,32]. For the process to be linear, the state and measurements vectors (\hat{x} , z) in (1) are considered to be in the rectangular form (real and imaginary). State estimators use the data from either RTUs or PMUs, then, based on the acquired data, the state estimation process becomes linear or nonlinear. The RTUs measure the voltage magnitudes, power flows, and power injections. The PMUs on the other hand, measure the voltages of the buses and current flows in phasor form. The measurement model can be described as follows

$$z_p(t) = \mathbf{H}\hat{x}(t) + v(t), \quad (1)$$

where $z_p(t)$ is the measurement vector at time t ; the t is dropped for convenience. \mathbf{H} is the transition matrix, $\hat{x}(t)$ is the state vector, and v is the measurement noise [3].

In PMU-based state estimation, the measurement vector z_p is arranged in a rectangular form to enable a linear estimation process, $z_p = [V_1^{real} V_1^{imag} \dots I_m^{real} I_m^{imag}]^T$ [3,32]. The same arrangement is applied to the state vector \hat{x} as follows

$$\hat{x} = [V_1^{real}, V_1^{imag} \dots V_n^{real}, V_n^{imag}]^T. \quad (2)$$

By using this arrangement the transition matrix \mathbf{H} becomes an m by $2n$ constant matrix with two parts, where m and n are the number of measurements and buses, respectively. The first part is the identity matrix \mathbf{I} corresponding to the direct measurements of bus voltages by the PMUs. The second part is a sub-matrix corresponding to the current measurements as in (3).

$$\begin{bmatrix} \mathbf{I}_{m_v \times 2n} \\ \mathbf{H}_{\alpha_{m_i}, \beta_{m_i} \times 2n} \end{bmatrix}. \quad (3)$$

where, m_v and m_i are the number of voltage and current measurements respectively. h_α and h_β are the matrices of the branch admittance Y_{ij} decomposed such that h_α produces the real part of the branch current I_{ij} , and h_β produces the imaginary part of the branch current I_{ij} . Therefore, h_α and h_β for the current I_{ij} can be expressed as follows

$$h_{\alpha_{ij}} = [0 \dots G_{ij} \quad -G_{ij} \quad 0 \dots -B_{ij} - B_{ii} \quad B_{ij} \quad 0 \dots]; \quad (4)$$

$$h_{\beta_{ij}} = [0 \dots -B_{ij} + B_{ii} \quad B_{ij} \quad 0 \dots G_{ij} \quad G_{ij} \quad 0 \dots]; \quad (5)$$

By using the model described above the states \hat{x} can be determined using weighted least squares as follows:

$$\hat{x} = (\mathbf{H}^T \mathbf{R}^{-1} \mathbf{H})^{-1} \mathbf{H}^T \mathbf{R}^{-1} z_p; \quad (6)$$

where \mathbf{R} is the covariance matrix of the noise.

3. Attack Model

This section describes FDIAs for RTU-based and PMU-based state estimators. Different notations will be used for both estimators, as they differ in terms of the type of measurements and transition matrices. For the RTU-based attacks, z_R and H will be used to refer to the measurement and transition matrix. As for the PMU-based attacks, z_p and \mathbf{H} will be used to refer to the measurement and transition matrix.

3.1. RTU-Based Attack Models

In DC-estimators, the voltage magnitude of all the buses in the grid is assumed to be equal to one p.u., and the angle difference between the buses is assumed to be less than five degrees. Therefore, the measurement model for DC-estimators becomes

$$z_R = Hx_{DC} + v; \quad (7)$$

where z_R and v are the measurement and noise vectors, respectively, with a size of m by one. In DC-estimators, z_R is an n by one vector whose elements are the power flow and power injection described in (8). x_{DC} is the vector of bus angles θ with a size equals to the number of buses n . H is constructed to correspond to the following model:

$$P_{ij} = \frac{\theta_i - \theta_j}{\text{Reactance of line } ij}; \quad (8)$$

$$P_i = \sum P_{ij}.$$

Under the DC-estimators paradigm, the adversaries try to manipulate the measurement vector z_R in (7) while avoiding detection by the BDD in (9). This manipulation should be less than the tolerance (τ) of the residual to avoid detection. Therefore, the sparse attack vector (a) in (10) should be $a = c \times h$, where $h \in H$ and c is the desired manipulation by the adversaries. By using a the residual for the BDD remains the same as shown in (11).

$$\|z_R - Hx_{DC}\| \leq \tau \quad (9)$$

$$z_{R,comp.} = z_R + a \quad (10)$$

As seen in (11), by using such a vector the regular BDD can no longer detect the FDIA [7–9]. However, the adversaries need to have partial knowledge of the grid topology to use such a vector.

$$\begin{aligned} \|z_{R,comp.} - Hx_{comp.}\| &= \|z_R + a - H(x_{DC} + c)\| \\ &= \|z_R + H \times c - H \times x_{DC} - H \times c\| \\ &= \|z_R - H \times x_{DC}\| \leq \tau. \end{aligned} \quad (11)$$

In AC-estimators, the voltage magnitudes are no longer assumed as in the DC-estimator but estimated. The measurement vector z consists of voltage magnitudes, power flows, and power injections. These measurements make the state estimation a nonlinear process since (H) becomes a nonlinear function of the states (x) as in (12). Solving for the states x is done iteratively, in a similar process to that of the power flow by using the Jacobian matrix J and updating both the vector of the states x and J .

$$z = H(x) + v. \quad (12)$$

The AC-estimators uses the normalized residual for BDD in (9). However, since the states are not linearly dependent on H , the attack vector (a) needs to be a function of H to avoid detection. The FDIA can be implemented by making a as follows

$$z_{comp.} = z_{true} + a; \quad (13)$$

where

$$a = h(x_{comp.}) + H(x_{true}),$$

true subscript indicates true (uncompromised) state or measurement,
comp. subscript indicates compromised state or measurement.

As a result, the attack vector compromises the states without being detected as in (14) [11].

$$\begin{aligned} \|z_{comp.} - H(x_{comp.})\| &= \|z_{true} + a - H(x_{comp.})\| = \\ &= \|z_{true} + H(x_{comp.}) - H(x_{true}) - H(x_{comp.}) - 2H(x_{true})\| \\ &= \|z_{true} - Hx\| \leq \tau. \end{aligned} \quad (14)$$

3.2. PMU-Based Attack Model

The previous section describes FDIAs for RTUs where several units need to be manipulated for a successful attack. PMUs, on the other hand, have several channels where a single PMU can measure the bus voltage and all adjacent bus currents in phasor form. This feature enables linear state estimation. However, in the context of FDIAs compromising one PMU is sufficient for launching successful attacks. As for RTU-based attacks, the adversaries need to compromise/manipulate several RTUs. The measurement model for the PMUs can be described as follows:

$$z_p = \mathbf{H}x + v. \quad (15)$$

To launch such attacks, the measurements vector z_p in (15), which consists of the bus voltages and current flows can be changed using the same approach described in Section 3.1. By using the grid topology, the attack vector can be masked, thereby, bypassing the BDD. The grid topology (\mathbf{H}) can be estimated by monitoring the measurements of the targeted PMUs, and there is no need for estimating the whole grid topology. Only local topology ($h \in \mathbf{H}$), is needed for launching successful FDIAs. The attack vector can be constructed as follows

$$z_{comp.} = z_{true} + a; \quad (16)$$

where

$$\begin{aligned} a &= c \times [0 \dots h_1 h_2 \dots h_i 0 \dots 0]^T, \\ z_{comp.} &= [z_{true_1} z_{true_2} \dots z_{comp_1} z_{comp_2} \dots z_{comp_i} z_{true_{i+1}} \dots]^T, \\ h_i &\text{ is a subset of } \mathbf{H}. \end{aligned}$$

By using this vector the residual in (17) remains unchanged.

$$\begin{aligned} \|z_{comp.} - Hx_{comp.}\| &= \|z_{true} + a - H(x + c)\| \\ &= \|z_{true} + hc - Hx - hc\| = \|z_{true} - Hx\| \leq \tau. \end{aligned} \quad (17)$$

Therefore, as long as the adversaries adhere to the vector in (16), the FDIA will be successful. One common factor between RTU-based and PMU-based attacks is the reliance on the network topology. This information can be obtained through disgruntled employees or through monitoring the data stream. The differences between RTU-based and PMU-based attacks are as follows: 1. RTUs are easier to compromise; however, the adversaries need to compromise several RTUs depending on the network topology. As for the PMUs, they are harder to compromise but compromising one PMU is sufficient. 2. In RTU-based attacks, the aim is to change the bus angles, as the voltage magnitudes are assumed to be constant. In the PMU-based attack, on the other hand, both the voltage magnitudes and angles can be targeted.

4. Detection of FDIAs

This section presents the PLV approach for detecting FDIAs. Numerous studies in the field of neuroscience have studied synchronization between two signals from distinct brain regions, and the commonly used measure is PLV [26]. It measures the phase interaction between complex signals using the following:

$$PLV(t) = |E(e^{j\varphi_{12}(t)})| \quad (18)$$

where $\varphi(t)$ is the phase difference $\varphi_{12}(t) = \theta_1(t) - \theta_2(t)$, $E[\cdot]$ denotes the expected value, and the PLV is estimated at time t . The phase θ_1 and θ_2 are the phases of the following signals:

$$\begin{aligned} x_1(t) &= A_1(t)e^{j\theta_1(t)} \\ x_2(t) &= A_2(t)e^{j\theta_2(t)}. \end{aligned} \quad (19)$$

The PLV ranges [0 1] where 0 represents huge variability between phases or in other words no synchrony, and 1 describes identical phases, i.e., synchrony. See Figures 2 and 3 for a visual description. Figure 2 is an example of correlated signals and corresponding PLV, where: (i) phases of a single trial of two complex-value signals at t_0 , (ii) difference between phases for multiple trials is presented, and (iii) resulting in complex PLV, whereas its magnitude, $abs()$, gives the resulting PLV. The same is repeated in Figure 3 to show the resulting small PLV for uncorrelated signals. In this article, Equation (18) is utilized to develop an analytical detection procedure of FDIA. Algorithm 1 describes the steps involved.

Algorithm 1: PLV-based FDIA detection

Input: complex data from PM,U including the attacked data
Initialize: $t = 1$, $T =$ total samples, $Win = 2$, $\tau_p = 0$;
while $t < T$ **do**
 calculate $\theta_n(t)$, where n goes to N , i.e., the total number of buses
 while $n \leq N$ **do**
 while $m \leq N$ **do**
 compute $\varphi_{m,n}(t) = \theta_n(t) - \theta_m(t)$;
 estimate PLV for every t with window size of Win using ;
 $PLV_{m,n}(t) = | E(e^{j\varphi_{m,n}(t)}) |$;
 $\mathcal{Z}(t) = \frac{1}{m \times n} \sum_{m,n} [PLV_{m,n}(t)]$;
 compute $\tau_p = 2\sigma_{\mathcal{Z}(t)}$;
 create binary vector $g(t)$ i.e. ;
 if $\mathcal{Z}(t) < \tau_p$ **then**
 | $g(t) = 0$
 else
 | $g(t) = 1$
 To differentiate transients in $g(t)$ due to load variation from attacked data, check ;
 if $\mathcal{A}_0 > \tau_p$ and $\mathcal{A}_1 > \tau_p$ **then**
 | $g(t) = 0$
 else
 | $g(t) = 1$
 return $g(t)$;
Output $g(t)$, 0 indicating indices of attacked data and 1 representing true data.;

The proposed algorithm makes certain assumptions for the detection of FDIA. It includes: (i) at least the first three time-samples of input data are not attacked, (ii) since the PLV is calculated at each time-sample with a window of size '2 time-samples', the attacked segments should be separated by a segment of three true data samples. Otherwise, if there are one or two true data samples between two attacked segments, the proposed method will consider them as attacked also.

Here, it is also important to highlight that we tested different window sizes for the PLV calculation, and the best results were found for the window size = 2 samples as shown in Figure 4. We used the 'True Positive rate' to show how variable window sizes affect the predicted outcome. These assumptions are not substantial compared to the requirements in existing studies, such as a large amount of non-attacked historical data to train classifiers [8,9].

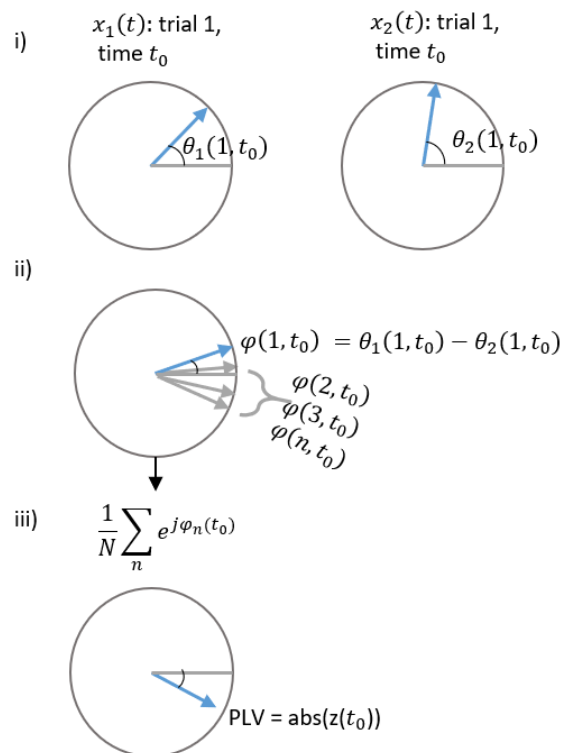


Figure 2. Correlated signals and corresponding PLV. (i) phases of a single trial of two complex-value signals at t_0 , (ii) difference between phases for multiple trials is presented (iii) The resulting in complex PLV for the correlated signals.

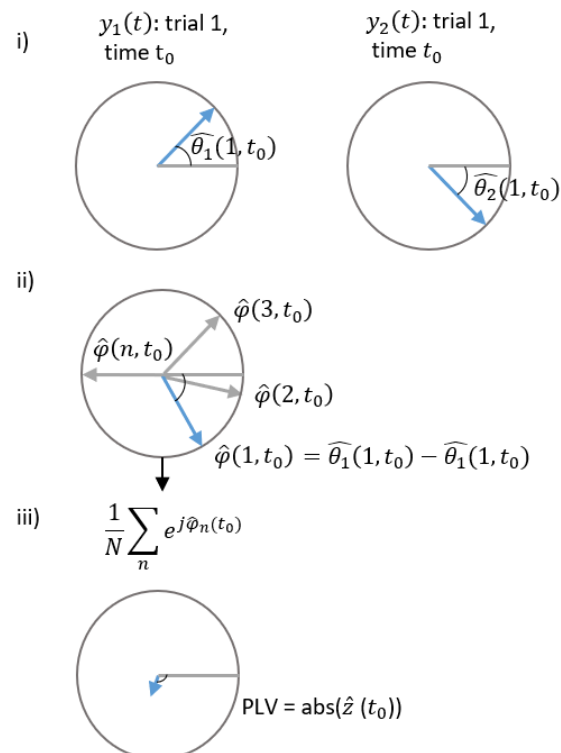


Figure 3. Uncorrelated signals and corresponding PLV. (i) phases of a single trial of two complex-value signals at t_0 , (ii) difference between phases for multiple trials is presented (iii) The resulting in complex PLV for the uncorrelated signals.

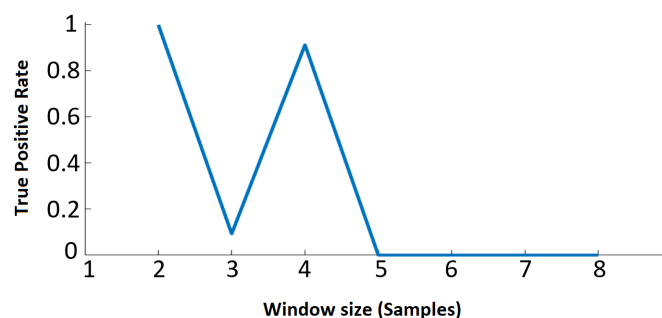


Figure 4. True positive rate by varying window sizes for the calculation of PLV.

Figure 5 shows an example of false data detection using the proposed method over a simulated data of two buses from above mention the network topology: (a) instantaneous phases $\theta_1(t)$ for the first signal having sudden changes due to load variations, (b) instantaneous phases $\theta_2(t)$ for the second signal that has attacked samples and changes in phases due to load variation between attacked samples.

This is to show that the proposed method is capable of differentiating between attacked samples and samples with phase changes due to load variations. (c) The absolute values of PLV for each sample between (a) and (b) are shown along with the threshold τ_p , which is calculated as $2 \times$ the standard deviation present in $z_p(t)$. (d) The predicted flag $g(t)$ i.e., samples that are not attacked and samples that are attacked, estimated using proposed method is provided (e) for ground truth, the Flag with true labeling of samples is presented.

$$g(t) = \begin{cases} 0, & \text{if } \mathcal{A}_0 > \tau_p \ \& \ \mathcal{A}_1 > \tau_p \\ 1, & \text{else} \end{cases} \quad (20)$$

where $\mathcal{A}_0 = \mathcal{Z}(t_{i-1}) - \mathcal{Z}(t_i)$; $\mathcal{A}_1 = \mathcal{Z}(t_{i+2}) - \mathcal{Z}(t_{i+1})$.

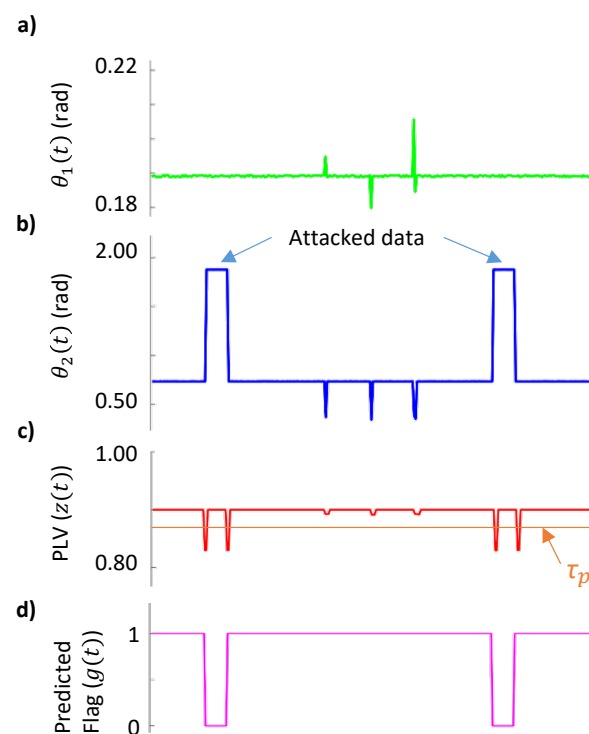


Figure 5. Cont.

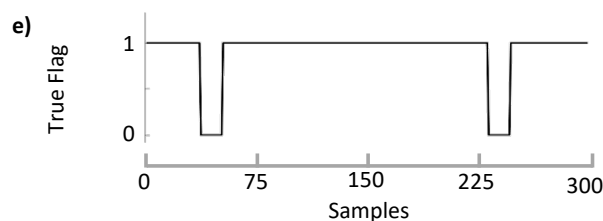


Figure 5. Example of false data detection using PLV. (a,b) are instantaneous phases $\theta_1(t)$, $\theta_2(t)$ over a time-length of 300 samples. (c) Phase lock value between two signals, spikes appear when there is a change in phases of a given signal. (d) Based on the proposed method, false data injected in (b) are predicted (Flag value '0' highlights attacked samples). (e) A waveform representing the ground truth is shown as a reference.

5. Simulation and Results

This section presents the PLV approach for detecting PMU-based FDIAs. The approach is carried out on the IEEE 14-bus and the IEEE 30-bus test systems. The FDIAs are tested on both systems using the approach mentioned in Section 3.2. The test systems and PMU locations are shown in Figures 6 and 7. The PMU locations were chosen to achieve complete observability under normal conditions [33–35], where each PMU measures the currents of all adjacent buses and the voltage of the bus of the PMU. Zero injection buses are not considered in PMU placement.

In the proposed approach, only the current data are processed to detect FDIAs. By ignoring the voltage data, the computation efficacy is enhanced, without affecting the accuracy of the detection. The adversaries need to use the attack vector a in (16), otherwise the BDD in (17) will catch this manipulation as outlier data. Therefore, processing the current data is sufficient as no successful attacks can be launched without compromising this data.

Each PMU can generate up to 50 samples per second. In this paper, the PMUs are assumed to be sending the data at a 30 Hz rate, and the state estimation is done every second. This assumption means that the state estimator has a measurement matrix z of size m by 30 available for evaluation.

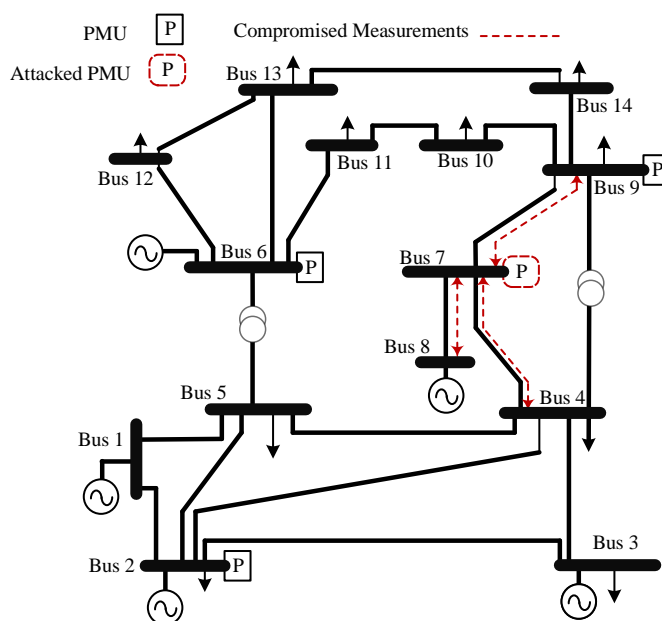


Figure 6. IEEE 14-bus with PMU locations.

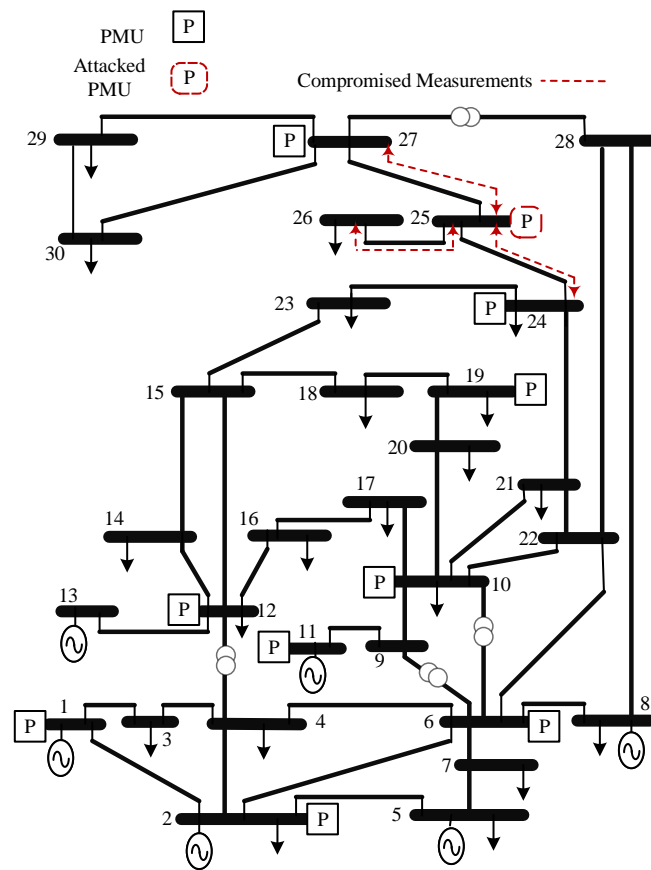


Figure 7. IEEE 30-bus with PMU locations.

5.1. Performance Metrics

The efficacy of the PLV approach is evaluated using performance metrics resulting from the confusion matrix. As the confusion matrix demonstrates the efficiency of any given method in predicting classes of test data where the ground truth is also known. The confusion matrix is defined as shown in Table 1.

The derivatives from the confusion matrix, which provides quantitative analysis of goodness of the proposed method, are:

$$Accuracy(Acc) = \frac{TP + TN}{TP + FN + FP + TN} \quad (21)$$

Acc refers to the term that provides a ratio of correctly predicted samples to total samples.

$$Specificity(Spec) = \frac{TN}{TN + FP} \quad (22)$$

Spec or true negative rate, provides the ratio of correctly identified negatives.

$$Sensitivity(Sen) = \frac{TP}{TP + FN} \quad (23)$$

Sen or true positive rate, provides the ratio of correctly identified positives.

$$F_1score = \frac{2TP}{2TP + FP + FN} \quad (24)$$

where

TP normal samples identified correctly (true positive)

FP attacked samples identified incorrectly (false positive)

TN attacked samples identified correctly (true negative)

FN normal samples identified incorrectly (false negative)

F_1 score is a harmonic mean of the recall and precision, where the recall is the same as *Sen*, and the precision is the ratio of the number of true positive samples to the number of true plus false positives.

Table 1. Confusion matrix.

Predicted Class \ Actual Class	Positive	Negative
	Positive	True Positive (TP)
Negative	False Positive (FP)	True Negative (TN)

5.2. Case Studies

Each PMU is assumed to measure the voltage of bus where the PMU is located, and the currents of all adjacent buses. Each PMU is sending the measurements at a speed of 30 samples per second. The meter errors of PMU measurements follow the normal distribution with a zero mean and standard deviation of 10^{-3} . The tests are performed on the IEEE 14-bus and IEEE 30-bus test systems. The load of each test system is varied for all scenarios and all Monte Carlo simulations.

- **Scenario I:** In this scenario, the PMU located at bus 7 is attacked by the adversaries, and fifty Monte Carlo simulations are carried out. The attack vector a is kept constant for all fifty cases, however, the instant and duration of the attack are random.
- **Scenario II:** In this scenario, the attacked PMU is random, and fifty Monte Carlo simulations are carried out. The attack vector a is kept constant for all fifty cases, however, the instant and duration of the attack are random.
- **Scenario III:** In this scenario, the attack vector a changes randomly for each Monte Carlo simulation. The attacked PMU is chosen randomly, and the duration of the attack is random.

The results for the IEEE 14-bus test system are shown in Table 2, where the PLV shows consistent results regardless of the scenario complications. As mentioned earlier, each scenario had a total of fifty Monte Carlo simulations, and the results for each case were evaluated using the metrics in Section 5.1. Therefore, Table 2 shows the mean and the standard deviation for all scenarios based on the Monte Carlo simulations. Table 3 shows a sample of the results for **Scenario III** where different PMUs are attacked at random.

Table 2. The mean and standard deviation of the PLV performance for the IEEE-14 bus system.

Case	Metric	Attack Vector	Attacked PMU	Acc (mean \pm std)	Spec (mean \pm std)	Sen (mean \pm std)	F1-Score (mean \pm std)
Scenario I:		constant	7	99.973 \pm 0.1155	99.996 \pm 0.0165	99.976 \pm 0.1155	0.999 \pm 0.0090
Scenario II:		constant	random	99.992 \pm 0.0022	99.992 \pm 0.0022	100 \pm 0.0000	0.999 \pm 0.0011
Scenario III:		variable	random	99.972 \pm 0.0045	99.973 \pm 0.0047	99.999 \pm 0.0000	0.998 \pm 0.0023

Table 3. Scenario III: Sample results for the IEEE-14 bus system.

Case Number	Attacked PMU	Acc %	Spec %	Sen %	F1-Score
7	7	99.96806	99.96453	99.67929	0.99839
19	9	99.97685	99.97429	99.76812	0.99884
41	6	99.98101	99.97894	99.80815	0.99904
2	2	99.9686	\approx 100	99.96864	0.99984

For the IEEE 30-bus test system, **Scenario III**: is used to test the validity of the PLV approach. In addition to the increased number of measurements due to the increased number of buses and number of PMUs as shown in Figure 7, the system presents interesting cases where PMUs are located at radial buses, such as bus 10. Therefore, if this particular

PMU is attacked, the adversaries will manipulate two signals, which are non-redundant. However, the proposed approach achieved good results as shown in Tables 4 and 5.

The receiver operating characteristic (ROC) shown in Figure 8, indicates the effectiveness of the PLV as a detection tool for FDIAs. Even in cases where there is a low redundancy the PLV performance is effective—for instance, the case of attacking the PMU of bus 10 where there is one current measurement and one voltage measurement. The window size for the PLV in the above results is two as this is the most effective size. Figure 9 shows the ROC for different window sizes, which indicates that the performance deteriorates as the window size becomes larger. Moreover, the even number window size performances are better than the odd ones. Incidentally, this performance and window size relationship benefits the computation burden as smaller window sizes lead to lesser processing times.

Table 4. Scenario III: Sample results for the IEEE-30 bus system.

Case Number	Attacked PMU	Acc %	Spec %	Sen %	F1-Score
1	1	99.98333	100	99.98177	0.99991
2	12	99.97685	100	99.97453	0.99987
3	2	99.98143	100	99.97958	0.99989
4	8	99.98380	100	99.98219	0.99991
5	10	99.97917	100	99.97705	0.99988
6	19	99.97731	100	99.80815	0.99988
7	24	99.98148	100	99.97970	0.99989
8	27	99.98333	100	99.98163	0.99991
9	11	99.98287	100	99.98106	0.99991

Table 5. The mean and standard deviation of the PLV performance for the IEEE-30 bus system.

Case	Metric	Attack Vector	Attacked PMU	Acc (mean \pm std)	Spec (mean \pm std)	Sen (mean \pm std)	F1-Score (mean \pm std)
Scenario III:		variable	random	99.9814 \pm 0.0029	100 \pm 0.000	99.9795 \pm 0.0032	0.9897 \pm 0.00160

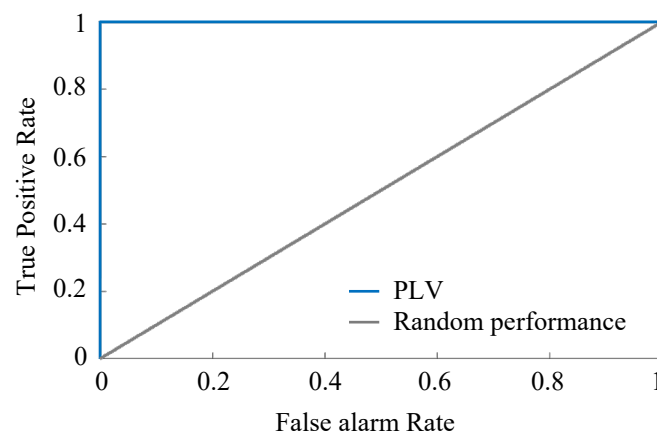


Figure 8. Performance for IEEE-14 system, Scenario III and case number 19 (randomly chosen): ROC curve of the proposed method along with reference ROC curve representing 50% sensitivity and 50% specificity.

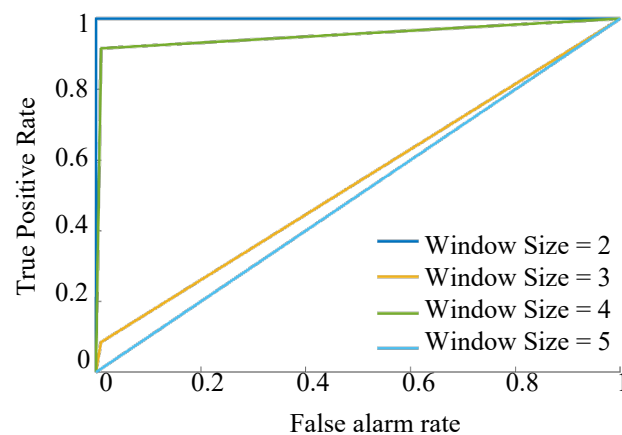


Figure 9. Receiver operating characteristic curve of PLV for different window sizes.

6. Conclusions

In this paper, we introduced PMU-based FDIAs where compromising one PMU is sufficient to launch successful attacks and bypass BDD. The paper also introduces a new approach for detecting FDIA where PLV is used to measure the correlation between the measured signals and detect abnormalities. The proposed approach requires no training to build a model and can be used online along with existing BDD. The PLV approach as a detection mechanism was tested on the IEEE 14-bus and IEEE 30-bus test systems using a Monte Carlo simulation with several scenarios where PLV was proven to be an efficient detection tool for FDIAs.

The PLV was used on the current data to decrease the computation burden, and the results demonstrated that using current data was sufficient. In cases where the adversaries change the voltage data without manipulating the current data, the BDD will flag such values as outliers. In the proposed approach, a window size of two was shown to be the best choice as the accuracy of the PLV drops significantly with the larger window sizes. The load change was considered as part of normal operations as such changes are expected during the day. In the PLV approach, the load conditions were varied randomly, and the intensity of the attacks varied to test the robustness of the PLV approach.

As the goal of the adversaries is to change some elements in the state vector by launching FDIAs, which can be done in steady state measurement data. The type of measurements and state estimator plays a significant role in launching and detecting FDIAs. One of the future directions is to investigate FDIAs in hybrid estimators where there is a mix of RTU and PMU measurements and the lack of synchronization between RTUs and PMUs adds complexity to the problem.

Author Contributions: S.A. and T.A. performed funding acquisition, project management, literature review, data collection, data visualization and manuscript writing. M.I. and E.J. performed algorithm design, data analysis and paper editing. M.J., B.A. and F.A.H. performed funding acquisition, project management, resource management and paper editing. All authors have read and agreed to the published version of the manuscript.

Funding: This research was supported by the Deputyship for Research and Innovation-Ministry of Education, Kingdom of Saudi Arabia.

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: Not applicable.

Acknowledgments: The authors would like to acknowledge the support of the Deputyship for Research and Innovation-Ministry of Education, Kingdom of Saudi Arabia for this research through

a grant (NU/IFC/ENT/01/004) under the Institutional Funding Committee at Najran University, Kingdom of Saudi Arabia.

Conflicts of Interest: The funders had no role in the design of the study; in the collection, analyses, or interpretation of data; in the writing of the manuscript, or in the decision to publish the results.

References

- Liang, G.; Weller, S.R.; Zhao, J.; Luo, F.; Dong, Z.Y. The 2015 Ukraine Blackout: Implications for False Data Injection Attacks. *IEEE Trans. Power Syst.* **2017**, *32*, 3317–3318. [[CrossRef](#)]
- Yuan, P.; Zhang, Q.; Zhang, T.; Chi, C.; Zhang, X.; Li, P.; Gong, X. Analysis and Enlightenment of the Blackouts in Argentina and New York. In Proceedings of the 2019 Chinese Automation Congress (CAC), Hangzhou, China, 22–24 November 2019; pp. 5879–5884. [[CrossRef](#)]
- Abur, A.; Exposito, A.G. *Power System State Estimation: Theory And Implementation*; CRC Press: Boca Raton, FL, USA, 2004.
- Liu, Y.; Ning, P.; Reiter, M.K. False data injection attacks against state estimation in electric power grids. *ACM Trans. Inf. Syst. Secur.* **2011**, *14*, 13. [[CrossRef](#)]
- Li, S.W.; Wu, F.; Zhang, J.; Zhu, C.Q. Selecting the Shortest One from Multi-Source and Multi-Channel Paths. *J. Geomat. Sci. Tech.* **2010**, *5*, 018.
- Teixeira, A.; Amin, S.; Sandberg, H.; Johansson, K.H.; Sastry, S.S. Cyber security analysis of state estimators in electric power systems. In Proceedings of the 2010 49th IEEE Conference on Decision and Control (CDC), Atlanta, GA, USA, 15–17 December 2010; pp. 5991–5998.
- Bi, S.; Zhang, Y.J. Defending mechanisms against false-data injection attacks in the power system state estimation. In Proceedings of the 2011 IEEE GLOBECOM Workshops (GC Wkshps), Houston, TX, USA, 5–9 December 2011; pp. 1162–1167.
- Bi, S.; Zhang, Y.J. Graphical methods for defense against false-data injection attacks on power system state estimation. *IEEE Trans. Smart Grid* **2014**, *5*, 1216–1227. [[CrossRef](#)]
- Wang, S.; Ren, W. Stealthy false data injection attacks against state estimation in power systems: Switching network topologies. In Proceedings of the 2014 American Control Conference (ACC), Portland, OR, USA, 4–6 June 2014; pp. 1572–1577.
- Liang, G.; Zhao, J.; Luo, F.; Weller, S.R.; Dong, Z.Y. A review of false data injection attacks against modern power systems. *IEEE Trans. Smart Grid* **2017**, *8*, 1630–1638. [[CrossRef](#)]
- Rahman, M.A.; Mohsenian-Rad, H. False data injection attacks against nonlinear state estimation in smart power grids. In Proceedings of the Power and Energy Society General Meeting (PES), Vancouver, BC, Canada, 21–25 July 2013; pp. 1–5.
- Liu, X.; Li, Z.; Liu, X.; Li, Z. Masking transmission line outages via false data injection attacks. *IEEE Trans. Inf. Forensics Secur.* **2016**, *11*, 1592–1602. [[CrossRef](#)]
- Dehghani, M.; Ghiasi, M.; Niknam, T.; Kavousi-Fard, A.; Tajik, E.; Padmanaban, S.; Aliev, H. Cyber Attack Detection Based on Wavelet Singular Entropy in AC Smart Islands: False Data Injection Attack. *IEEE Access* **2021**, *9*, 16488–16507. [[CrossRef](#)]
- Guan, Y.; Ge, X. Distributed Attack Detection and Secure Estimation of Networked Cyber-Physical Systems Against False Data Injection Attacks and Jamming Attacks. *IEEE Trans. Signal Inf. Process. Over Netw.* **2018**, *4*, 48–59. [[CrossRef](#)]
- Zhao, J.; Zhang, G.; Dong, Z.Y.; Wong, K.P. Forecasting-Aided Imperfect False Data Injection Attacks Against Power System Nonlinear State Estimation. *IEEE Transactions on Smart Grid* **2016**, *7*, 6–8. [[CrossRef](#)]
- Phadke, A.G.; Thorp, J.S. *Synchronized Phasor Measurements and Their Applications*; Springer Science & Business Media: New York, NY, USA, 2008.
- Xie, J.; Meliopoulos, A.S. Sensitive detection of GPS spoofing attack in phasor measurement units via quasi-dynamic state estimation. *Computer* **2020**, *53*, 63–72. [[CrossRef](#)]
- Schmidt, E.; Gatsis, N.; Akopian, D. A GPS spoofing detection and classification correlator-based technique using the LASSO. *IEEE Trans. Aerosp. Electron. Syst.* **2020**, *56*, 4224–4237. [[CrossRef](#)]
- Liu, L.; Esmalifalak, M.; Ding, Q.; Emesih, V.A.; Han, Z. Detecting false data injection attacks on power grid by sparse optimization. *IEEE Trans. Smart Grid* **2014**, *5*, 612–621. [[CrossRef](#)]
- Zhang, J.; Chu, Z.; Sankar, L.; Kosut, O. False data injection attacks on phasor measurements that bypass low-rank decomposition. In Proceedings of the 2017 IEEE International Conference on Smart Grid Communications (SmartGridComm), Dresden, Germany, 23–27 October 2017; pp. 96–101.
- Kim, T.T.; Poor, H.V. Strategic protection against data injection attacks on power grids. *IEEE Trans. Smart Grid* **2011**, *2*, 326–333. [[CrossRef](#)]
- Ding, W.; Xu, M.; Huang, Y.; Zhao, P.; Song, F. Cyber attacks on PMU placement in a smart grid: Characterization and optimization. *Reliab. Eng. Syst. Saf.* **2021**, *212*, 107586. [[CrossRef](#)]
- Bae, J. Cost-Effective Placement of Phasor Measurement Units to Defend against False Data Injection Attacks on Power Grid. *Energies* **2020**, *13*, 3862. [[CrossRef](#)]
- Ashok, A.; Govindarasu, M.; Ajarapu, V. Online detection of stealthy false data injection attacks in power system state estimation. *IEEE Trans. Smart Grid* **2016**, *9*, 1636–1646. [[CrossRef](#)]
- Zhao, J.; Mili, L.; Wang, M. A generalized false data injection attacks against power system nonlinear state estimator and countermeasures. *IEEE Trans. Power Systems* **2018**, *33*, 4868–4877. [[CrossRef](#)]

26. Lachaux, J.P.; Rodriguez, E.; Martinerie, J.; Varela, F. Measuring phase synchrony in brain signals. *Hum. Brain Mapp.* **1999**, *8*, 194–208. [[CrossRef](#)]
27. Schmidt, B.T.; Ghuman, A.S.; Huppert, T.J. Whole brain functional connectivity using phase locking measures of resting state magnetoencephalography. *Front. Neurosci.* **2014**, *8*, 141. [[CrossRef](#)]
28. Yoshinaga, K.; Matsuhashi, M.; Mima, T.; Fukuyama, H.; Takahashi, R.; Hanakawa, T.; Ikeda, A. Comparison of Phase Synchronization Measures for Identifying Stimulus-Induced Functional Connectivity in Human Magnetoencephalographic and Simulated Data. *Front. Neurosci.* **2020**, *14*, 648. [[CrossRef](#)] [[PubMed](#)]
29. Wang, Z.; Tong, Y.; Heng, X. Phase-locking value based graph convolutional neural networks for emotion recognition. *IEEE Access* **2019**, *7*, 93711–93722. [[CrossRef](#)]
30. Wang, Z.M.; Zhou, R.; He, Y.; Guo, X.M. Functional Integration and Separation of Brain Network Based on Phase Locking Value During Emotion Processing. *IEEE Trans. Cogn. Dev. Syst.* **2020**. [[CrossRef](#)]
31. Celka, P. Statistical Analysis of the Phase-Locking Value. *IEEE Signal Process. Lett.* **2007**, *14*, 577–580. [[CrossRef](#)]
32. Göl, M.; Abur, A. A fast decoupled state estimator for systems measured by PMUs. *IEEE Trans. Power Sys.* **2015**, *30*, 2766–2771. [[CrossRef](#)]
33. Almasabi, S.; Mitra, J. Multi-Stage Optimal PMU Placement Considering Substation Infrastructure. *IEEE Trans. Ind. Appl.* **2018**, *54*, 6519–6528. [[CrossRef](#)]
34. Almasabi, S.; Mitra, J. A Fault-Tolerance Based Approach to Optimal PMU Placement. *IEEE Trans. Smart Grid* **2019**. Accepted. [[CrossRef](#)]
35. Khajeh, K.G.; Bashar, E.; Rad, A.M.; Gharehpetian, G.B. Integrated Model Considering Effects of Zero Injection Buses and Conventional Measurements on Optimal PMU Placement. *IEEE Trans. Smart Grid* **2017**, *8*, 1006–1013. [[CrossRef](#)]