Detection of False Data Injection Attacks in Smart Grids: A Real-Time Principle Component Analysis

Ahmed S. Musleh[1], Mahdi Debouza[2], Haris M. Khalid[3], and Ahmed Al-Durra[2]
[1]School of Electrical Engineering and Telecommunications, *The University of New South Wales*, Sydney, Australia
[2]Department of Electrical & Computer Engineering, *Khalifa University of Science & Technology*, Abu Dhabi, UAE
[3]Department of Electrical and Electronics Engineering, *Higher Colleges of Technology*, Sharjah, UAE
ahmed.aldurra@ku.ac.ae

***Abstract*—False Data Injection (FDI) is one of the most dangerous attacks on cyber-physical systems as it could lead to disastrous consequences in the operation of the power grids. In this paper, a comprehensive investigation of the (FDI) attacks in smart grids is presented. A detection algorithm is utilized in analyzing the FDI attacks in real-time environment based on the Principle Component Analysis (PCA). It provides an adequate solution to the FDI problem for its ability to extract information about the correlation of the collected measurements. This provides a more accurate and sensitive response than the previous FDI detection techniques. Furthermore, the light computations associated with this algorithm make it a very good candidate for real-time environment testing. The results concluded in the paper illustrate a very promising future for the PCA-based real-time FDI attack detection schemes.**

Keywords—Cyber-physical systems, cyber security, false data injection attack (FDIA), phasor measurement units (PMU), principle component analysis (PCA), real-time implementation, smart grid

I. INTRODUCTION

The recent years have witnessed the introduction of various smart grid technologies which aim to 1) improve the assets of the grid, 2) increase its utilization, 3) raise its capability to react to and resolve the problems of the grid in a faster and a more efficient manner. Though these continually evolving technologies have opened the door to huge advantages to the power grid operations, they have also created different challenges to the operation of power grids. The complicated smart grid's functionalities and structures necessitate advanced, decentralized, and sophisticated monitoring and control schemes. These schemes must be employed to ensure a coherent, smooth, and stable grid operation [1]. To address these concerns, different information technologies and communication systems have been integrated with the operation of the smart grid. This digital integration has changed the smart grid into a cyber-physical system, thereby making it prone to vulnerabilities of data injection attacks. The impacts of these attacks are deeply investigated in [2], where it can be concluded that cyber and physical attacks are deeply connected and shall be addressed as one entity.

Cyber-physical attacks vary in their type, form, and impact. Some of these attacks are: time synchronization attacks [3], GPS spoofing attacks [4], and Denial-of-Service (DOS) attacks [5]. Another very important cyber-physical systems attack is the false data injection (FDI) attack, where the attacker manipulates or injects false data either in the measurements or the control signals to alter the dynamics of the power grid [6]. This type of attacks could be very hazardous to the operation of the power grid as they are very difficult to detect.

Countermeasures against FDI attacks are classified in literature into 1) protection-based schemes, and 2) detection-based schemes. Protection-based schemes rely on protecting the measurements of the power grid from being manipulated. This is obtained by increasing the redundancy of the power grid measurements [7]. However, the major drawbacks of the protection-based schemes are the unguaranteed effectiveness with the different operating conditions of the power grid and the extreme need for the measurements' redundancy [8]. On the other hand, detection-based schemes utilize the Bayesian framework in detecting FDI attacks that would look like an anomaly among the set of measurements [9]. The main drawback of these schemes is the incapability of detecting FDI attacks that closely imitate the normal distribution of the measurements of the power grid. These attacks are also known as stealthy attacks [8].

To address the detection of FDI attacks, several studies have been carried out using different algorithms and techniques. Most of these techniques utilize estimation and probability theories as presented in [10]. The authors proposed a state estimation-based prediction technique to address the FDI attacks in [11]. Graphical methods have been introduced in [12] to study defending mechanisms against FDI attacks on power system state estimation. An integration between historical and forecasted measurements is presented in [13] in order to enhance the resiliency of smart grids against FDI attacks. Various other techniques have been adopted to detect FDI attacks, such as Kalman filter [14], sparse optimization [15], and machine learning [16]. However, there is still a research gap in the area of real-time implementation of the proposed methods in the current FDI attack detection techniques. This is due to the massive computations involved in these techniques as well as the need for the full and accurate power grid model parameters.

To bridge the research gap, this paper proposes a new detection technique built on the Principle Component Analysis (PCA). This technique illustrates the covariance structure of a set of measurements through straightforward linear combinations. The main features of PCA are: 1) dimension reduction, and 2) pattern identification of association among the measurements of a network [17]. PCA has been involved deeply in anomaly detection problems in many fields such as: Data Mining [18] and Internet of things (IoT) [19]. Through the reduction of the dimension of the measurements, PCA provides a fast and efficient method for detecting anomalies (FDI attacks) in an online real-time environment [20]. This attribute makes PCA a very attractive method for detecting FDI attacks. The main contributions that differentiate this paper from previously published works are stated as:

- This work demonstrates, to the best of the authors' knowledge, the first study that employs the PCA method in real-time FDI attacks detection.
- It provides key insights into the framework of a real-time environment for testing the proposed PCA-based FDI attack detection.

The rest of the paper is organized as follows: Section II presents a background of the FDI attack and the proposed PCA-based detection method. Section III demonstrates the implementation and the evaluation of the proposed method. The concluding remarks are stated in section IV.

II. PCA METHOD FOR FDI ATTACK DETECTION

This section describes the problem formation, which is built by describing a power system model, followed by the convention-based and PCA-based FDI attack detection representations respectively.

A. Power System Model

In this paper, the voltage measurements are being collected via Phasor Measurement Units (PMU). These PMUs are installed at each node of the grid. It is initially considered that there is no measurement loss from the PMU nodes, and all PMUs operate at the same sampling frequency. Therefore, for every time instant t a new set of measurements is obtained. Consequently, the PMUs within the grid have the capability to collect voltage measurements as [11]:

$$x_i^{t+1} = f(x_i^t) + v_i^t, \quad t = 0,1,\dots,T \tag{1}$$

$$z_i^t = H_i^t x_i^t + \omega_i^t, \quad i = 0,1,\dots,N \tag{2}$$

where $x_i^0 \in \mathbb{R}^n$ is the initial state, n is the state vector dimension in the subspace $\mathbb{R}$, $f(x_i^t)$ is a nonlinear function which describes the state transition of the model, t represents the time step, $v_t^i \in \mathbb{R}^n$ is the process noise, and T is the overall time steps considered. In (2), $z_i^t \in \mathbb{R}^m$ is the measurements vector at the i^{th} node, m is the measurements vector dimension in the subspace $\mathbb{R}$, $H_i^t \in \mathbb{R}^{m\times n}$ is the measurements Jacobian matrix which maps the states to the measurements, $\omega_i^t \in \mathbb{R}^m$ is the measurements noise, and N is the total number of measurements that are collected from the PMUs installed at the grid.

Equations (1) and (2) represent the main power grid model which is concluded by most of the state estimation algorithms. It is also the model utilized for the state estimation based FDI detection.

B. Conventional State Estimation based FDI Detection

Most of the state estimation algorithms depend on the residual evaluation to detect and declare FDI attacks. The residual (also known as L_2-norm) is realized as:

$$r_i^t = \|z_i^t - H_i^t x_i^t\| \tag{3}$$

Here, the residual evaluation r_i^t is basically the amount of error between the state and the measurement. From this error, the conclusion of a FDI attack is drawn by comparing this error to a predefined threshold value τ ; thus, if $r_i^t = \|z_i^t - H_i^t x_i^t\| \geq \tau$, then a FDI attack is noticed. The main drawback of the residual based FDI attack detection is the case where stealthy attacks are present in all measurements collected as shown in [21]. With this attack, the measurements shall have the same dynamics as the normal behavior of the grid; therefore, it will not be detected via the normal residual test as $\|z_i^t - H_i^t x_i^t\| < \tau$. An important alarm was triggered from the results drawn from [21]. This alarm emphasizes on the necessity of revisiting the conventional state estimation techniques used to detect possible cyber-physical attacks in the power grids.

C. PCA-based FDI Attack Detection

PCA is an orthogonal transformation based statistical method that transforms a set of measurements of likely correlated variables (PMUs in this study) into a set of values of linearly-uncorrelated variables called the principal components. PCA is also known as the true eigenvector analyses. This method could be a technique that reveals the internal, hidden, and complex structure of the measurements set in a way that best highlights the variance distribution among the measurements set. The main advantage of PCA is the reduction of the dimension of the measurements sets without compromising the variance among the measurement points. Thus, PCA can produce a lower dimensional picture of the higher dimensional data space where each variable corresponds to an axis. This lower dimensional picture is basically the projection of measurement points as viewed from its most informative point of view that are also known as the principle components directions. These principle component directions are the dominant eigenvectors of the measurement covariance matrix. These dominant eigenvectors are the most informative vectors in the original measurements space; therefore, they are taken as the principal directions. To find these principle components direction, we first need to consider the measurements set as shown below:

$$\boldsymbol{Z} = [z_i^T;\ z_i^T;\ \dots;\ z_i^T] \in \mathbb{R}^{m\times n} \tag{4}$$

where each row of z_i represents a measurement instance in an n dimensional space, and m is the overall number of the measurement samples collected. From these measurement samples, the principle components is deduced as follows [20]:

$$max \sum_{i=1}^{n} \boldsymbol{V}^T(\boldsymbol{z}_i - \mu)(\boldsymbol{z}_i - \mu)^T\boldsymbol{V}, \tag{5}$$

where $\boldsymbol{V} \in \mathbb{R}^{n\times k}$ is a k dominant eigenvector matrix, and μ is the global mean. From here, we can easily figure out that the PCA technique is basically a task of finding a subspace where the projected measurements points have the largest possible variation. The problem in (5) can be solved by deriving the singular value decomposition (SVD) of the covariance matrix of the measurements which is basically finding the eigenvector and the eigenvalues of the covariance matrix as follows:

$$\boldsymbol{\Sigma_Z V} = \boldsymbol{V\Lambda}, \tag{6}$$

where

$$\boldsymbol{\Sigma_Z} = \frac{1}{n}\sum_{i=1}^{n}(\boldsymbol{z}_i - \mu)(\boldsymbol{z}_i - \mu)^T, \tag{7}$$

represents the measurements covariance matrix. Every single column of $\boldsymbol{V}$ is an eigenvector of $\boldsymbol{\Sigma_Z}$, and $\boldsymbol{\Lambda}$ is the diagonal matrix that represents the associated eigenvalues. As the SVD theorem states, only the first few eigenvectors will have the main contribution to the measurements' distribution; thus, the rest eigenvectors shall be neglected for their insignificant contribution to the measurements' distribution. Once the principle directions are found, the next step is to utilize them

ALGORITHM 1: *PCA-BASED FDI ATTACK DETECTION*

Input: *Measurements Z*

Output: *Score of anomalies* ψ

Initialization: *covariance matrix* $\boldsymbol{\Sigma_Z}$

1. **While** *new measurements set received,* **do**
2. *Calculate the mean* μ
3. **for** $i = 0 - n$, **do**
4. *Calculate* $(\boldsymbol{z_i} - \boldsymbol{\mu})(\boldsymbol{z_i} - \boldsymbol{\mu})^T/\boldsymbol{n}$
5. *Add* $(\boldsymbol{z_i} - \boldsymbol{\mu})(\boldsymbol{z_i} - \boldsymbol{\mu})^T/\boldsymbol{n}$ *to covariance matrix* $\boldsymbol{\Sigma_Z}$
6. **end for**
7. *Return covariance matrix* $\boldsymbol{\Sigma_Z}$
8. *Calculate eigenvectors* V *from* $\boldsymbol{\Sigma_Z V = V\Lambda}$
9. *Find the score of anomalies* ψ
10. **end While**
11. *Return score of anomalies* ψ

in detecting FDI attacks. For this purpose, the absolute value of the cosine similarity is employed to measure the variations in the principle directions of each measurement point $\boldsymbol{v}_i$ and the global principle direction of the whole measurements $\widetilde{\boldsymbol{v}}$ as shown next:

$$\psi = 1 - \left| \frac{\langle \boldsymbol{v}_i, \widetilde{\boldsymbol{v}} \rangle}{\|\boldsymbol{v}_i\| \|\widetilde{\boldsymbol{v}}\|} \right|, \tag{8}$$

where ψ represents the score of anomaly which indicates the possibility of a potential attack into that specific measurement point. In other word, the higher the value of ψ the more likely that the measurement sample is attacked. By comparing the scores of anomaly with a threshold value τ, we can decide the possibility of an FDI attack. The value of τ is determined based on the range of the score of anomaly of the normal clean measurement points. The full algorithm of the PCA based FDI attack detection is demonstrated in Algorithm 1.

III. Implementation and Evaluation

To test the proposed PCA-based FDI attacks detection, a real-time experiment environment is adopted. Several test cases to investigate the effectiveness of the proposed method as employed as follows.

A. Testbed Description

The testbed utilized in this study is based on the one introduced in [22, 23]. In this testbed, an IEEE 14-bus multi-machine power grid is employed. It consists of 2 generators (G), 3 synchronous condensers (C), 20 transmission lines, 11 dynamic loads, and 4 transformers. The system operates at a base voltage of 138 kV, and the overall complex powers are around few hundreds of MVA. Voltage measurements are collected from the grid using Phasor Measurement Units (PMU) operating with a sampling rate of 5 samples/second. This system is simulated in a real-time environment using Real Time Digital Simulator (RTDS). PMUs are built within RTDS according to IEEE PMU standard C37.118.1-2011 [24]. However, since the RTDS is designed specifically for power systems modeling, it is extremely challenging to have the PCA mathematical operations; thus, a MATLAB program is employed as a software in the loop (SIL) scheme. This program begins with establishing a TCP/IP connection for the PMUs within RTDS. Then, it starts receiving the PMU measurement messages according to the IEEE PMU standard

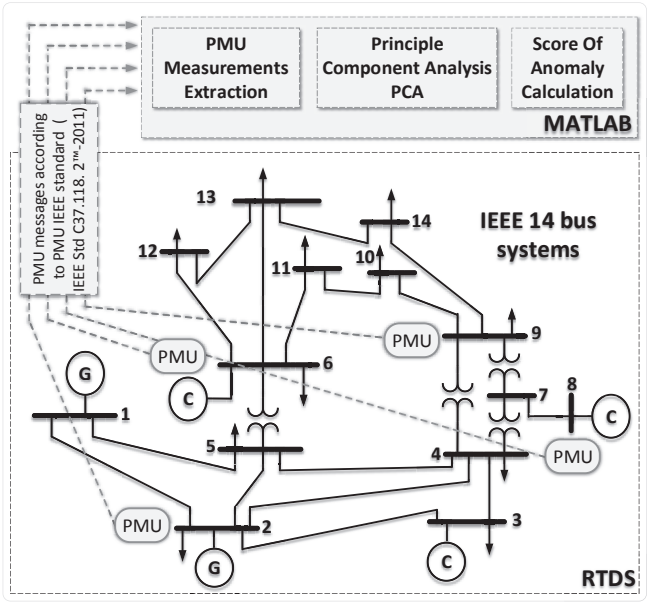


Fig. 1. Setup of the proposed testbed. All the busses have PMUs installed, but the figure only shows only 4 to simplify the figure.

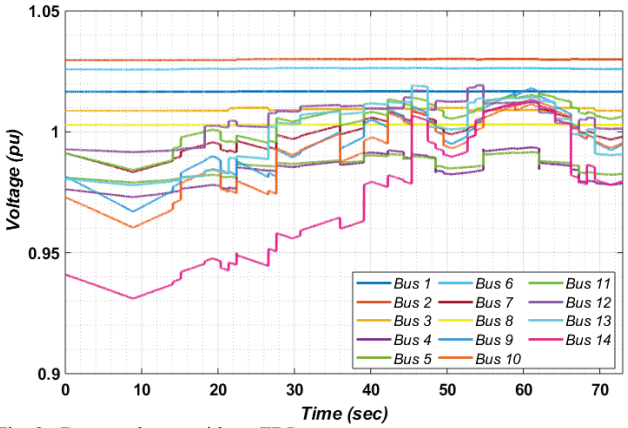
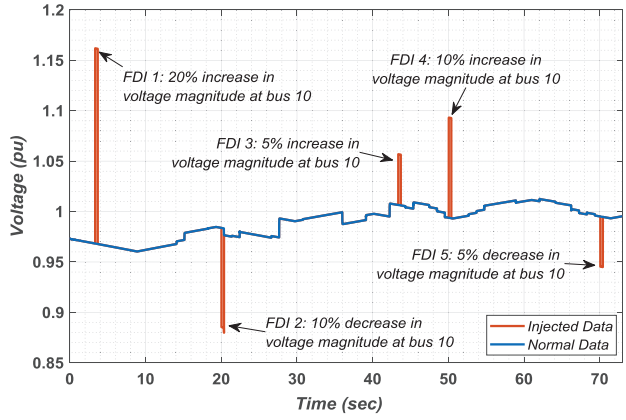


Fig. 2. Buses voltages with no FDI

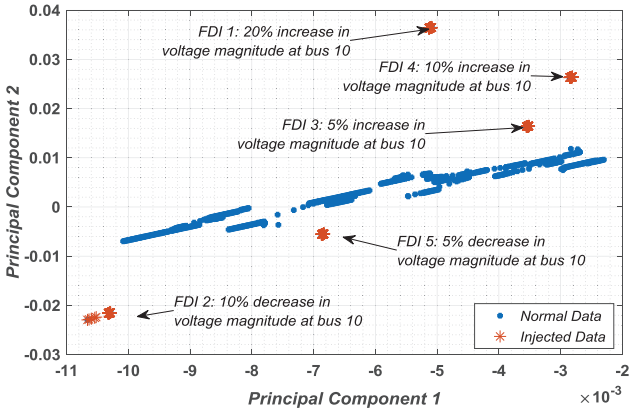
C37.118.1- 2011. PCA-based FDI detection is then carried out. Two special RTDS cards which are GTSYNC and GTNETx2 are utilized in the SIL implementation. GTSYNC utilizes a 1PPS GPS signal to synchronize the PMUs, and GTNETx2 carries out the network communication through via GTNET_PMU protocol for PMU data transmission according to the IEEE C37.118.1-2011. Figure 1 illustrates the full testbed setup.

B. Test Cases

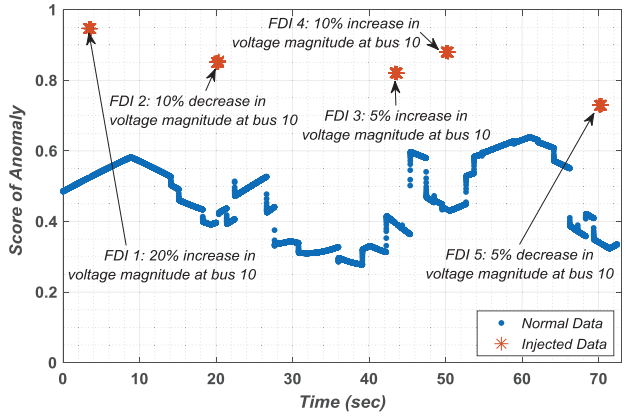
To evaluate the effectiveness of the proposed scheme, several test cases have been designed and implemented. These test cases include several FDI attacks in the collected PMU measurements. Each one of them has a specific purpose and importance. Several changes in the loads are made to create a dynamic behavior of the power grid to imitate normal operations. Figure 2 illustrates the PMU voltage magnitude measurements of the power grid dynamics. It is noted that all load busses vary in their voltage levels from 0.93pu to 1.03pu. In each of the following cases, FDI attacks are illustrated along with the PCA analysis using two principle components and the score of anomaly. It must be noted that the period for each FDI attack is assumed to be 0.2 seconds or 10 samples of the system operating at 50Hz.



(a)

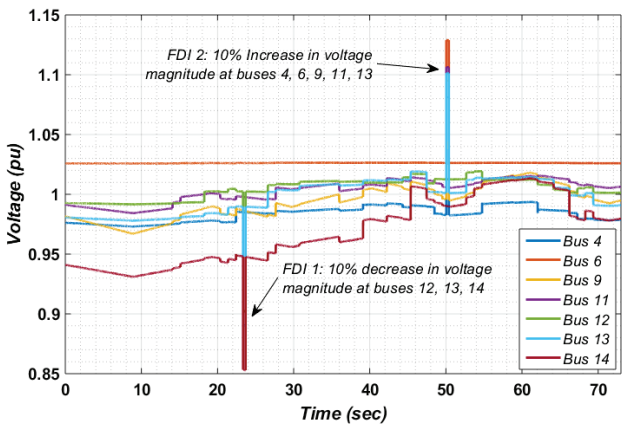


(b)

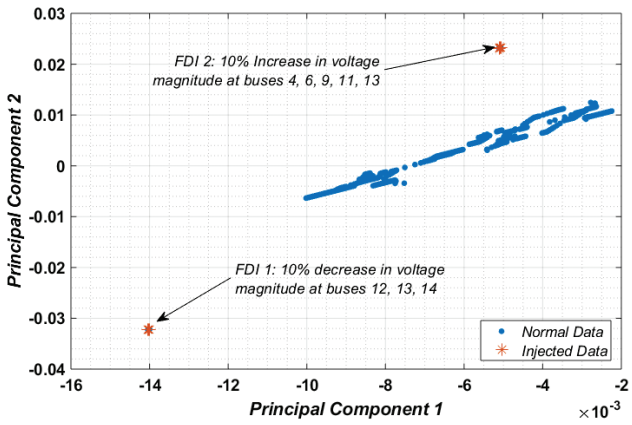


(c)

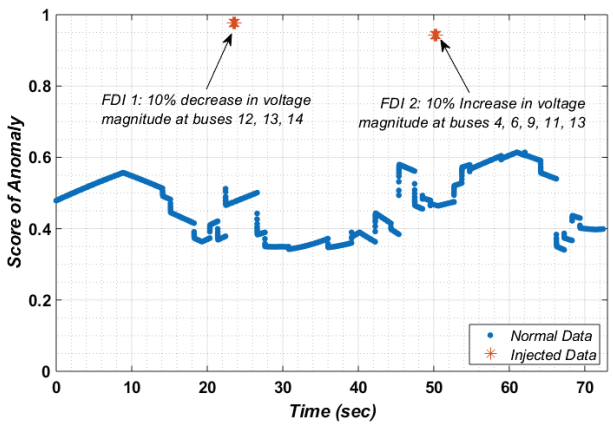
Fig. 3. Case-I results: (a) Voltage magnitude-based FDI profile, (b) 2-D principle components representation, (c) Score of anomaly illustration



(a)



(b)



(c)

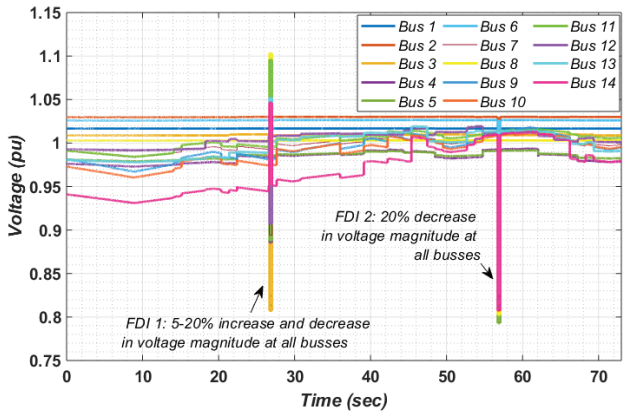
Fig. 4. Case-II results: (a) Voltage magnitude-based FDI profile, (b) 2-D principle components representation, (c) Score of anomaly illustration

1) Case I: FDI in one PMU with different magnitudes:

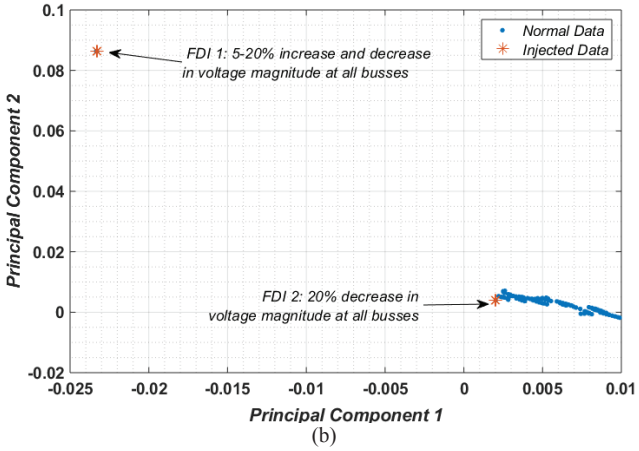
This case aims at finding the sensitivity of the PCA-based FDI attack detection towards the different magnitudes of FDI attacks. The case introduces 5 FDI attacks at different time steps of voltage magnitude readings of bus 10. The attacks are: 20% increase starting at 4s, 10% decrease starting at 20s, 5% increase starting at 43s, 10% increase starting at 50s, and 5% decrease starting at 70s. These attacks are illustrated in Fig. 3 (a). Fig. 3 (b) illustrates the PCA results of the FDI attacks in two principle components space where it is shown that the attacks are situated far from the normal measurement points. In Fig. 3 (c), the scores of anomaly are illustrated. The score of anomaly shows that higher magnitude FDI attacks are easily separated from the normal measurement points. The results, in this case, show that PCA can be a very effective method in detecting even a slight change in the measurement such as 5%.

2) Case II: Two 10% FDI attacks in adjacent PMUs:

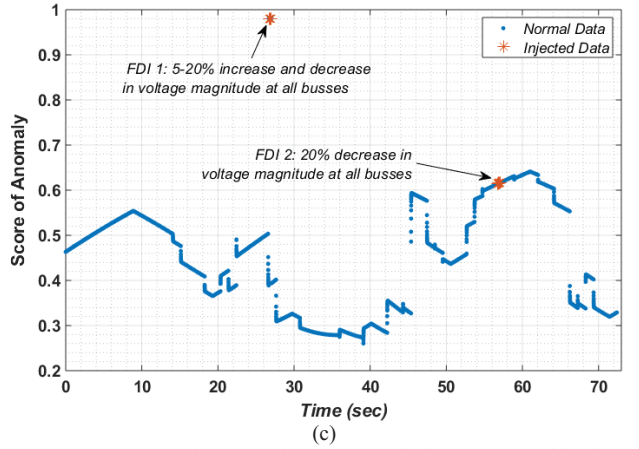
The objective of this case is to investigate the response of the PCA detection method when multiple adjacent PMUs are manipulated. This represents a form of stealthy attacks where the attacker manipulates adjacent PMUs' readings which shall make it harder to detect. To illustrate this, we conducted two attacks: the first attack decreases the voltage magnitude by 10% at busses 12, 13, and 14 starting at 22s. The second attack injects a 10% increase in voltage magnitudes at busses 4, 6, 9, 11, and 13 starting at 50s. These attacks are illustrated in Fig. 4 (a). Fig. 4 (b) illustrates the PCA results of these two FDI attacks in two principle components space where it is



(a)



(b)



(c)

Fig. 5. Case-III Results: (a) Voltage magnitude-based FDI profile, (b) 2-D principle components representation, (c) Score of anomaly illustration

clearly shown that the attacks are situated far from the normal measurements points. In Fig. 4 (c), the scores of anomaly are illustrated. It is clear that both of the attacks were pinpointed successfully as they have a much higher score of anomaly than the normal measurement points. This illustrates the satisfying response of PCA in detecting these kinds of stealthy attacks. This represents an advantage of PCA based detection method.

3) Case III: 10% FDI in all PMUs:

This case illustrates the situation when the whole measurements are being manipulated with FDI attacks. This hints a very high vulnerability of the system as the attacker needs to have a full access to the grid and its parameters. Note the test case is designed to analyze an alarming situation. Else, an attacker having access to full measurement is a problem of national security. To illustrate this type of attacks, two FDI attacks are designed: 5-20% random increase and decrease in voltage magnitude at all busses starting at 27s and 20% decrease in voltage magnitude at all busses starting at 57s. These attacks are illustrated in Fig. 5 (a). The first FDI attacks represent the case when the attacker has access to the whole measurements of the grid, yet he or she does not have the knowledge of the grid topology; thus, he or she just changes the measurements randomly. The second FDI attack illustrates the case when the attacker has the full knowledge of the grid, and thus he or she creates an attack that mimics the dynamics of the power grid. Figure 5 (b) illustrates the PCA results of these two FDI attacks in two principle components space, and the scores of anomaly are illustrated in Fig 5 (c). While the first attack is clearly pinpointed, the second one is not separable from the normal measurement points. This result is since PCA detection algorithm depends on the correlation between the measurements points. Thus, if the whole system's measurements are changed with the same associated magnitude, then the correlation between the measurements will be the same as the normal measurements points, and the attack will not be separable. This case is the most severe case where the full power grid is breached.

C. Relative Comparison

In order to compare the performance of the PCA-based FDI attacks detection method with other methods, several relative comparison points are considered as follows:

- Detection of stealthy attacks:

PCA-based FDI attacks detection has shown a great performance in detection such attacks. This makes it one of the few algorithms that can pinpoint smart stealthy attacks. Other form of algorithms such as [14] and [15] are not able to do such work as they do not consider the correlation information of the measurements collected. Thus, this cannot be feasible for them. On the other hand, machine learning based algorithms such as [16] show similar behavior to the PCA algorithm in detection stealthy attacks.

- Detection of full system breach:

Full system breach remains the main challenge for almost all the FDI attack detection algorithms including PCA based method. However, the main difference here is that PCA method can identify full system attack if the correlation between the measurements is not the same as the normal measurement points even if the whole measurements are change. Other algorithms fail fully when it comes to detection any type of full system breaches.

- Scalability:

This means the ability to perform the detection algorithm in large systems. Unlike most of the detection algorithms, PCA provides a light computational border which makes it scalable.

- Real-time compatibility:

This is the most important attribute because it indicates the possibility of conducting the detection algorithm in real time. In literature, this is possible only with the machine learning based algorithms. However, these algorithms require extensive training to be conducted prior to employment. This is not the case with the PCA method. Table 1 illustrates a brief relative comparison of the main FDI attack detection algorithms along with the PCA algorithm.

TABLE 1. BRIEF RELATIVE COMPARISON OF DIFFERENT BAD DATA DETECTION ALGORITHMS

Reference	Algorithm	Detection of Stealthy Attacks	Detection of full system breach	Scalability	Real-Time Compatibility
[14]	Kalman Filter	Not possible	Not possible	Not Scalable	Not Compatible
[15]	Sparse Optimization	NA	Not possible	Not Scalable	Not Compatible
[16]	Machine Learning	Possible	Not possible	Scalable	Compatible with exhaustive training
The proposed work	**PCA**	**Possible**	**Possible when the system dynamics are unknown**	**Scalable**	**Compatible**

IV. Conclusion

A PCA method for detecting FDI attacks in smart grids is presented in this paper. This technique utilizes the covariance structure of a set of measurements through straight forward linear combinations of these measurements. The proposed scheme is implemented for the first time, to the best of the authors' knowledge, in a real-time environment. The method efficacy is investigated using different case studies. The results presented in case studies show the effectiveness of this method in FDI detection. Nevertheless, the method has a limitation in detecting attacks when all measurements are affected at the same time. Future studies will focus on finding solutions to overcome this drawback possibly by integrating both voltage magnitude and angle in the PCA based FDI attacks detection which shall increase the effectiveness of the PCA algorithm.

References

[1] S. M. Muyeen and S. Rahman, Communication, control and security challenges for the smart grid, IET, 2017.

[2] Y. Mo, T. H.-J. Kim, K. Brancik, D. Dickinson, H. Lee, A. Perrig and B. Sinopoli, "Cyber–physical security of a smart grid infrastructure," *Proceedings of the IEEE,* vol. 100, no. 1, pp. 195 - 209, 2011.

[3] Z. Zhang, S. Gong, A. D. Dimitrovski and H. Li, "Time synchronization attack in smart grid: impact and analysis," *IEEE Transactions on Smart Grid,* vol. 4, no. 1, pp. 87 - 98, 2013.

[4] C. Konstantinou, M. Sazos, A. S. Musleh, A. Keliris, A. Al-Durra and M. Maniatakos, "GPS spoofing effect on phase angle monitoring and control in a real-time digital simulator-based hardware-in-the-loop environment," *IET Cyber-Physical Systems: Theory & Applications,* vol. 2, no. 4, pp. 180-187, 2017.

[5] S. Liu, X. P. Liu and Abdulmotaleb El Saddik, "Denial-of-Service (dos) attacks on load frequency control in smart grids," in *2013 IEEE PES Innovative Smart Grid Technologies Conference (ISGT)*, Washington, 2013.

[6] G. Liang, J. Zhao, F. Luo, S. R. Weller and Z. Y. Dong, "A review of false data injection attacks against modern power systems," *IEEE Transactions on Smart Grid,* vol. 8, no. 4, pp. 1630 - 1638, 2017.

[7] Q. Yang, J. Yang, W. Yu, D. An, N. Zhang and W. Zhao, "On false data-injection attacks against power system state estimation: modeling and countermeasures," *IEEE Transactions on Parallel and Distributed Systems,* vol. 25, no. 3, pp. 717 - 729, 2014.

[8] G. Chaojun, P. Jirutitijaroen and M. Motani, "Detecting false data injection attacks in AC state estimation," *IEEE Transactions on Smart Grid,* vol. 6, no. 5, pp. 2476 - 2483, 2015.

[9] H. M. Khalid and J. C.-H. Peng, "A bayesian algorithm to enhance the resilience of WAMS applications against cyber attacks," *IEEE Transactions on Smart Grid,* vol. 7, no. 4, pp. 2026 - 2037, 2016.

[10] H. M. Khalid and J. C.-H. Peng, "Immunity toward data-injection attacks using multisensor track fusion-based model prediction," *IEEE Transactions on Smart Grid,* vol. 8, no. 2, pp. 697 - 707, 2017.

[11] 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 Systems Journal,* vol. 13, no. 1, pp. 710-719, 2019.

[12] S. Bi and Y. J. Zhang, "Graphical methods for defense against false-data injection attacks on power system state estimation," *IEEE Transactions on Smart Grid,* vol. 5, no. 3, pp. 1216 - 1227, 2014.

[13] A. Ashok, M. Govindarasu and J. Wang, "Cyber-physical attack-resilient wide-area monitoring, protection, and control for the power grid," *Proceedings of the IEEE,* vol. 105, no. 7, pp. 1389 - 1407, 2017.

[14] 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 Transactions on Control of Network Systems,* vol. 1, no. 4, pp. 370 - 379, 2014.

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

[16] M. Esmalifalak, L. Liu, N. Nguyen, R. Zheng and Z. Han, "Detecting stealthy false data injection using machine learning in smart grid," *IEEE Systems Journal,* vol. 11, no. 3, pp. 1644 - 1652, 2017.

[17] C. Mei and J. Fan, Data Analysis Methods, Higher Education Press, 2006.

[18] B. Liu, Y. Xiao, P. S. Yu, Z. Hao and L. Cao, "An efficient approach for outlier detection with imperfect data labels," *IEEE Transactions on Knowledge and Data Engineering,* vol. 26, no. 7, pp. 1602 - 1616, 2014.

[19] D. H. Hoang and H. D. Nguyen, "A PCA-based method for IoT network traffic anomaly detection," in *2018 20th International Conference on Advanced Communication Technology (ICACT)*, 2018.

[20] Y.-J. Lee, Y.-R. Yeh and Y.-C. F. Wang, "Anomaly detection via online oversampling principal component analysis," *IEEE Transactions on Knowledge and Data Engineering,* vol. 25, no. 7, pp. 1460 - 1470, 2013.

[21] Y. Liu, P. Ning and M. K. Reiter, "False data injection attacks against state estimation in electric power grids," *ACM Transactions on Information and System Security ,* vol. 14, no. 1, pp. 1-33, 2011.

[22] A. S. Musleh, S. Muyeen, A. Al-Durra, I. Kamwa, M. A. Masoum and S. Islam, "Time-delay analysis of wide-area voltage control considering smart grid contingences in a real-time environment," *IEEE Transactions on Industrial Informatics,* vol. 14, no. 3, pp. 1242-1252, 2018.

[23] A. S. Musleh, S. Muyeen, A. Al-Durra and I. Kamwa, "Testing and validation of wide-area control of STATCOM using real-time digital simulator with hybrid HIL–SIL configuration," *IET Generation, Transmission & Distribution,* vol. 11, no. 12, pp. 3039-3049, 2017.

[24] "IEEE Standard for Synchrophasors for Power Systems, IEEE C37.118-2011," IEEE Power and Energy Soc., 2011.