Real-time Detection of Malicious PMU Data

Zeyu Mao, Ti Xu
Department of Electrical and Computer Engineering
University of Illinois at Urbana Champaign
Urbana, IL, USA

Thomas J. Overbye
Department of Electrical and Computer Engineering
Texas A&M University
College Station, TX, USA

***Abstract*—The growing installation of phasor measurement units (PMUs) provide grid operators wide-area situational awareness while introducing additional vulnerabilities to power systems from the cyber security point of view. This paper presents an online method to detect ongoing contingencies in the system and bad data injection on its PMU network. To do so, the principal component analysis is applied to leverage the spatial and temporal correlations among the synchrophasor data. Pattern match and data reconstruction are proposed to identify incident types and find their most possible locations. Case studies are carried out on a 150-bus system to demonstrate the effectiveness of the proposed scheme.**

Keywords—phasor measurement unit, principal componenet analysis, bad data injection, online detection

I. INTRODUCTION

The development of smart grids facilitates the deployment of phasor measurement unit (PMUs) to improve the system stability and reliability. Featured with precise time synchronization and high sampling rate, PMU data bring great opportunity in increasing the wide-area situational awareness of grid operators and regional reliability coordinators [1]. Additionally, the availability of PMU data enables novel solutions in many power system fields, such as state estimation, optimal power flow, and dynamic security assessment [2]. As more PMU data are collected and more applications are developed, its influence on the current and future smart grids has become greater. However, the critical infrastructures are usually targeted by malicious attackers and terrorists. Especially in recent years, there is a trend that more attackers attempt to hack power grids and their control systems. As a result of high importance in the power system monitoring and control system, PMU and its data bring additional vulnerabilities for those malicious attackers to interrupt operators' awareness and judgement, such as to decrease the reliability of the power system, and even to cause damage to equipment and economic losses. For example, if malicious data are injected into one operating PMU or phasor data concentrator (PDC) by hackers, the malicious data will be collected by the regional PDC/EMS and potentially be spread over many subsystems, like EMS and control systems. Thus, there is an urgent need to improve the cyber security in power systems, by detecting the malicious attack on PMU data and preventing attackers from disrupting the critical infrastructure.

This paper was presented in the 19th International Conference on Intelligent System Application to Power Systems (ISAP), San Antonio, Texas, 2017.

There are many studies on PMU data security in the literature. Attackers with information about the grid configuration have been proved to be able to inject arbitrary errors into certain state variables without being detected by the bad data processing techniques embedded in the phasor devices [3, 4]. A detection mechanism using the estimated transmission line parameters as the discriminant was proposed in [3]. This mechanism applies PMU data to estimate the line parameters in the grid, and then those estimated parameter values are compared against their nominal values to find any significant, unusual statistical variation(s), which may indicate a malicious data injection. Authors in [5] [6] utilize the characteristics of state estimation to detect the malicious PMU data. The cyber attack behavior is modeled inside the system estimation using the Expectation-Maximization algorithm to find missing data and to optimize intractable likelihood function in [6]. An analytical model for the cumulative sum algorithm is developed in [7], which has a shorter decision delay and more accurate decision compared to the conventional state-estimation-based bad data detection method. Some machine learning techniques are also proposed to detect anomalies in PMU data [8] [9]. In this paper, we focus on the computational efficiency of the detection method and its capability to distinguish the malicious data from the contingency data.

This paper assumes that attackers may exploit information about the PMU data format to modify the data in such a way that it has the standard structure and passes the cyclic redundancy check (CRC). According to PMU industry standard [10], all frames transmitted from PMUs follow the same structure as shown in Fig. 1. CRC-CCITT is used in these frames to verify whether each message has been corrupted or not. Though CRC-CCITT has proved to perform extremely well in the error pattern coverage, the burst error detection capability and in decreasing the probability of an undetected error occurring [10], attackers can easily generate the two-byte cyclic redundancy codes by following the associated encoding rules, which enables the corrupted data to pass the CRC.

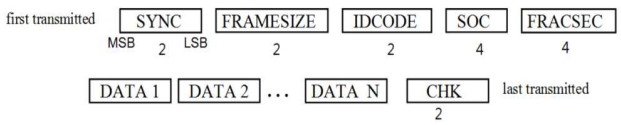

Fig. 1 Example of frame transmission order

In references [11] and [12], the concept of a time delay of the malicious data is introduced, and the specific algorithms are developed to find the desynchronization pattern. PMU errors like the time-skew and the mislabeling of flagged bits are presented in reference [13], which may introduce the similar desynchronization pattern in phasors. However, as shown in Figure 1, the second of century (SOC) and the fraction-of-second can be constant while only measurement data are changed. In this paper, we assume that the bad data injection did not modify the measurement time tags from synchrophasors.

This paper addresses the problem of detecting bad data injection from PMUs by applying a principal component analysis (PCA) based method. An online detection strategy is proposed to detect the anomalies in the PMU data with capability to distinguish the malicious data from either event or contingency data. The PCA-based method is utilized to find the patterns underlying the system-wise dynamic behaviors and consequently identify the anomaly behaviors. The proposed scheme is able to determine and locate the existence of an adversary as well as contingencies with fast response time and low computational complexity. After being trained by extensive experiment results, a classifier is then applied to enable the method to distinguish between the malicious data and contingency data with high accuracy.

The rest of this paper is organized as follows: In Section II, we present an overview of the bad data injection model and its experiment testbed environment that was built in our previous work. The PCA processing procedure is discussed in detail in Section III. Section IV presents the proposed mechanism for detecting bad data injection and verifies it through case studies using a 150-bus system. We conclude and present future work direction in Section V.

II. Bad Data Injection Simulation Environment

By leveraging the real-time data output feature of a coupled transient stability package, a synchrophasor network simulation environment is built for the online method experiment and test with capabilities to inject bad data into the measurement streams.

A. Bad Data Injection

As described in [14], a PMU measures phasors and frequency and packs the measurement with an accurate time stamp, which is synchronized using the Global Positioning System (GPS). With PMUs installed over the grid, all measurements are obtained in the same sampling rate. Those grid-wide time-aligned data are collected by the regional PDC and are available for the state estimator. Compared to the classical state estimation methods that use active and reactive power measurements as input, state estimation using the time-aligned PMU data can provide accurate snapshots of the power system conditions in a higher frequency.

With the importance of state estimation, malicious data (or fake data) could result in serious mistakes, like erroneous operation decision, or even blackout. PMU data can be corrupted if the PMU is attacked or any component (like routers) of the underlying communication network is hacked [15]. We denote $\boldsymbol{X} \in \mathbb{R}^{M \times N}$ as the set of PMU measurements with N to be number of PMU channels (i.e. voltage, current or frequency) and M to be the number of time instants considered. For $\boldsymbol{X}$, we also define each column by $\boldsymbol{c_n} = [x_{1,n}, \dots, x_{m,n}, \dots, x_{M,n}]^T$ and each row by $\boldsymbol{r_m} = [x_{m,1}, \dots, x_{m,n}, \dots, x_{m,N}]$, with each index $\{m, n\}$ indicating that the data are measured by PMU channel n at time instant m.

The bad data injection can be formed in the following equation:

$$\boldsymbol{P} = \boldsymbol{X} + \boldsymbol{D} \tag{1}$$

Where $\boldsymbol{D}$ denotes the injected data matrix, which has the same row and column size as $\boldsymbol{X}$, and $\boldsymbol{P}$ denotes the corrupted data matrix that will be used in state estimation. For any nonzero $d_{ij} \in \boldsymbol{D}$, it represents the malicious data were injected into PMU channel i at time instant j.

B. Simulation Environment

In order to simulate the bad data injection behavior on the PMU network and test the detection scheme, a synchrophasor network simulator is built [16]. The simulator utilizes a commercial transient stability package as its real-time data server, connects each component via the IEEE standard protocol C37.118.2 and contains "hackable" simulators of PMU, PDC and control center as shown in Fig. 2:

- **PMU Simulator:** This simulator complies with the IEEE standard C37.118.1-2011 [17] and works in multi-threads. As shown in Fig. 3, data are transmitted from the data server into the simulator where it is decoded and dispatched to each single PMU thread, it is then re-packed with the time tag and the cyclic redundancy codes, and finally transmitted via each individual port. A bad data injection module is integrated into each single PMU thread, so that only selected unit can be corrupted at a given time.
- **PDC Simulator:** Data streams from PMU Simulator are concentrated in this unit. Based on the multi-threaded design, the PDC buffers the streams from the connected PMUs and waits for a certain time (σ) to receive and decode the frames. When the PDC is ready to transmit, it aggregates all the measurements into a single data frame, generates a new time tag and transmits out the frame at rates up to 120 messages/second. The hack module is also embedded into the simulator, which enables the attacker to modify any value in the frame, with re-generated cyclic redundancy codes to pass the CRC.
- **Control Center Simulator:** The control center simulator is designed to receive streams from multiple PDCs, and provide visualization and analysis functions to help operators detect anomalous behaviors in the power system and/or its associated synchrophasor cyber infrastructure. With the inherent interactive

feature of the data source server, operators are able to use command functions to control the underlying transient stability simulation. In addition, a real-time PCA-based visualization block is integrated into the simulator, which is discussed in details in the next section.

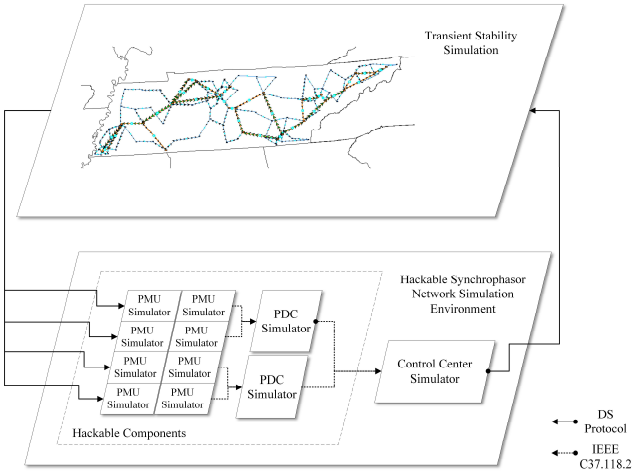

Fig. 2 The synchrophasor network simulation framework

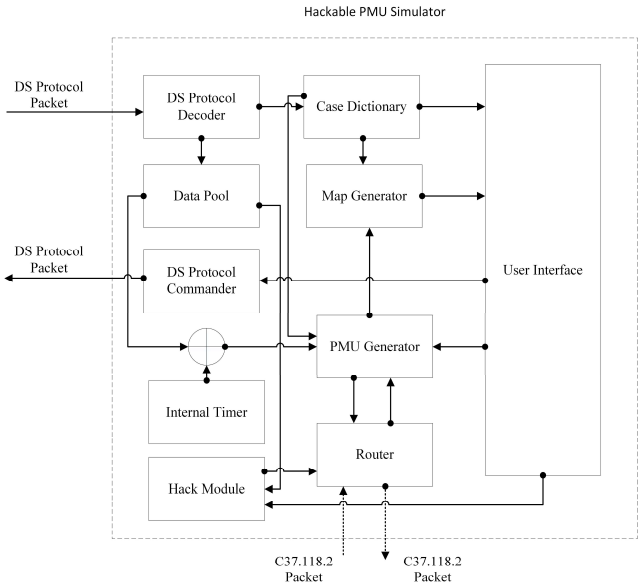

Fig. 3 The PMU Simulator architecture

III. PCA Based Analytical Scheme

The spatial and temporal correlation among the synchrophasor measurements $\boldsymbol{X}$ makes it tractable, while the injected data matrix alters the correlation resulting in variation in $\boldsymbol{P}$. However, for a dramatically large amount of data, the dynamic response behavior at any individual location might not be detectable. As a result, few sign changes of the data injection could be neglected by the grid operators.

A. PCA Procedure

In order to capture a large amount of the variation in the data as possible, PCA is used to process the aggregated data. First, $\boldsymbol{P}$ is normalized using (2) and (3):

$$\mu = \frac{1}{N}\sum_{i=1}^{N} p_{m,n} \tag{2}$$

$$z_{m,n} = p_{m,n} - \mu \tag{3}$$

Then we rescale each coordinate to make sure that different attributes (includes data at different time instants) are treated on the same scale:

$$\sigma_m^2 = \frac{1}{M}\sum_{i} (z_{m,n})^2 \tag{4}$$

$$s_{m,n} = z_{m,n}/\sigma_m \tag{5}$$

After normalization, we choose a direction $\boldsymbol{u}$ so that when the data are projected onto the direction corresponding to $\boldsymbol{u}$, where the variances of the projected data are maximized. For a given unit vector $\boldsymbol{u}$ and a point $\boldsymbol{s_n}$, the projected point on $\boldsymbol{u}$ is given by $\boldsymbol{s_n^T u}$. To maximize the variance of the projections, we choose a unit-length $\boldsymbol{u}$ so as to maximize:

$$\begin{aligned}\frac{1}{N}\sum_{i=1}^{N} (\boldsymbol{s_n^T u})^2 &= \frac{1}{N}\sum_{i=1}^{N} \boldsymbol{u}^T \mathbf{s_n} \boldsymbol{s_n^T u} \\ &= \boldsymbol{u}^T (\tfrac{1}{N}\textstyle\sum_{i=1}^{N} \mathbf{s_n} \boldsymbol{s_n^T}) \boldsymbol{u}\end{aligned} \tag{6}$$

Thus, to project the data into a k-dimensional subspace (k<n), we choose $\boldsymbol{u_1}, \ldots, \boldsymbol{u_k}$ to be the top k eigenvectors of $\sum = \frac{1}{N}\sum_{i=1}^{N} \boldsymbol{s_n s_n^T}$. To reconstruct the data in the new basis, we need to compute the corresponding vector:

$$\boldsymbol{Y^{(n)}} = \begin{bmatrix} \boldsymbol{u_1^T s_n} \\ \boldsymbol{u_2^T s_n} \\ \vdots \\ \boldsymbol{u_k^T s_n} \end{bmatrix} \in \mathbb{R}^k \tag{7}$$

B. Scheme Design

As illustrated in [18], PCA obtains the new, orthogonal direction, onto which the data set projection has the largest distribution in the remaining subspace. This results in the elimination of redundancy, thus preserving only the unique variations. In other words, if several data sets share the same scaled dynamics, only one projection can be found after the PCA process. Here we could anticipate the PCA result under three different conditions:

- For the case without bad data injection and contingencies, there is a strong spatial-temporal correlation in the measurement matrix, so that the first eigenvalue λ_1 should be significantly larger than the rest, indicating that the corresponding eigenvector $\boldsymbol{v_1}$ represents the most significant dynamic pattern.
- For the case without bad data injection but contingencies, other patterns may be triggered and unveiled by PCA due to the existence of the contingencies. The eigenvalues should have

significant and representative changes when different contingencies occur in the system.

- For the case with bad data injection but without contingencies, new patterns may be introduced into the measurements. The changes in the eigenvalues may be less significant compared to the ones in contingency cases if a few PMU/PDCs are under attack. The attack on any types of measurement data (voltage magnitude, angle or frequency) will not affect the eigenvalues of the uncorrupted measurement(s).

The three cases follow the basic spatial and temporal correlations, while the introduction of contingencies and bad data injection also generates new patterns into the measurements. Thus, to determine whether the system is having contingencies or experiencing data attack, we obtain and analyze the PCA results from several pre-defined cases. Based on the pattern found in each type of cases, a classifier is set up to determine whether the system is experiencing actual bad data injection.

Furthermore, the new projection provided by PCA shows the dynamic behavior of each observed bus. Buses with anomalous dynamic behaviors will be highlighted if the system is determined to have contingencies or data attack. In order to find these anomalous buses, a 1-D clustering is integrated into the method. Figure 4 shows the procedures of the entire PCA-based scheme.

IV. Implementation and Case Study

In this section, the proposed scheme is implemented in the synchrophasor network simulation environment, and it is tested online with different cases either having bad data, contingencies or both. To demonstrate the capability of the proposed method, we use the IEEE-118 network [19] to build the study samples, and test it with a synthetic 150-bus case [20]. Several cases are discussed in detail for illustrations.

A. Pattern Extraction

The eigenvalues obtained in the training cases (without any system event) are small and indistinguishable. Hence, we use the logarithmic values of each eigenvalue to better distinguish the pattern differences.

1) Base Case

This is the IEEE 118-bus system without contingencies and data attack. The measurement data series in this base case have some tiny fluctuations, but generally the system is running smoothly. By computing the voltage magnitude matrix, voltage angle matrix and frequency matrix using 40-instant window size and a PMU reporting rate of 30 frames per second, the range of the change of $log\lambda$ are shown in Table I.

TABLE I RANGE OF $\boldsymbol{\Delta log\lambda}$ IN THE BASE CASE

	$\Delta\log(\lambda_1)$	$\Delta\log(\lambda_2)$	$\Delta\log(\lambda_3)$
Vpu*	(-0.038, 0.051)	(-0.082, 0.105)	(0, 0.013)
Angle*	(-0.212, 0.009)	(-0.096, 0.109)	(-0.217, 0.216)
Freq*	(-0.054, 0.024)	(-0.029, 0.141)	(-0.16, 0.045)

Vpu: Voltage magnitude; Angle: Voltage angle; Freq: Frequency

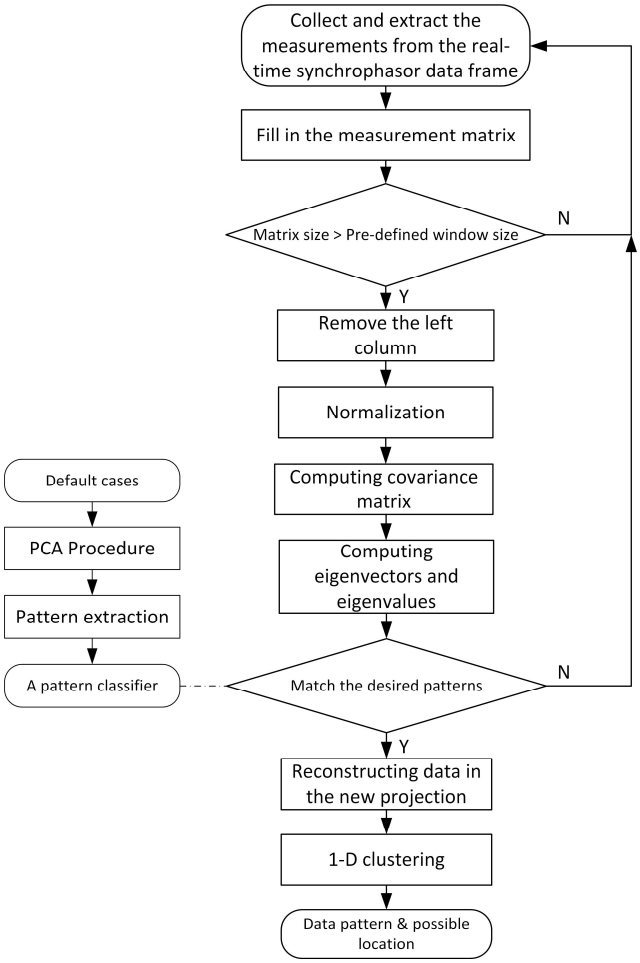

Fig. 4 Flowchart of the PCA-based scheme

2) Contingency Case

Different contingency scenarios are defined for the 118-bus case. Here we use a case with a transmission line fault to illustrate how we find the patterns.

As shown in Figure 4, few eigenvalues change significantly when the pre-defined contingency occurs in the system. Note that when the synchrophasor data from PDCs are received, the client computes the eigenvectors and eigenvalues, and compares with the results from last instant. The eigenvalues λ_1 and λ_3 increases significantly in the voltage angle matrix, however they remain relatively constant in the voltage magnitude matrix. The three eigenvalues in the frequency matrix are increasing gently compared to the other two matrixes. When focusing on the instance when contingency occurred, we found that all significant eigenvalues $\lambda_1, \lambda_2, \lambda_3$ of the angle matrix and the ${\lambda_2}^*$ of the voltage magnitude matrix are rising at that time instant, and all of them are out of the normal range, which is given in the Table 1, thus this pattern is considered to be a contingency signal when performing the proposed detection method.

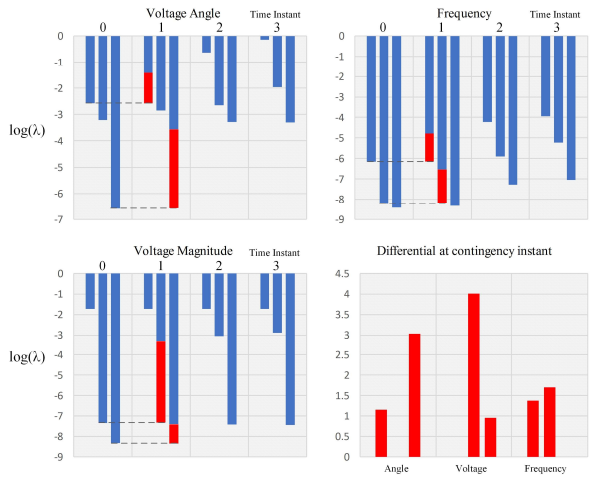

Fig. 5 Histogram of the eigenvalues

3) Bad Data Injection Case

Bad data injection exists with unusual behaviors, and is illustrated in [21]. Figure 5 shows the changing of the eigenvalues when a five-instant (0.1667s) bad data are injected into the frequency data of the PMU data packet during instant 41 to 45. As a result, the first significant eigenvalue of the frequency matrix is increased from -3.73 to -2.23 at the instant when bad data are introduced, while the third eigenvalue changes from -7.60 to -4.50.

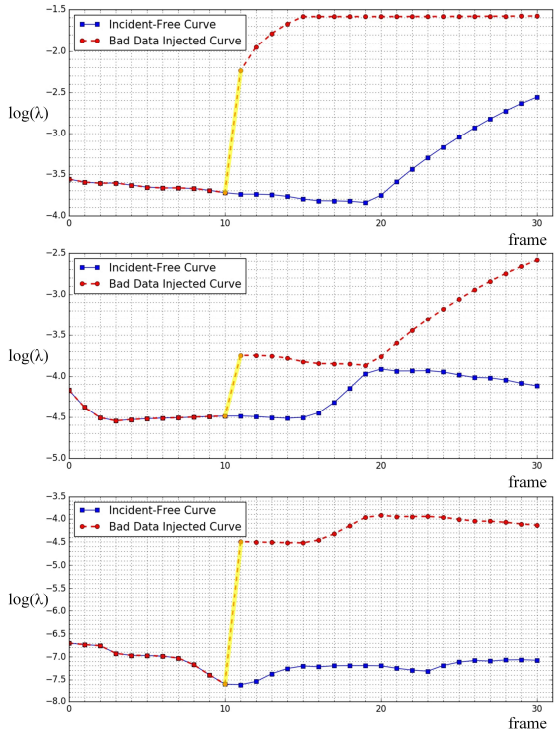

Fig. 6 Comparison between first three eigenvalues with and without bad data injection

These significant changes are considered as patterns for the bad data injection on frequency data. The patterns from other bad data injection cases are collected and a classifier based on these patterns are utilized to detect the anomalous behaviors in the synchrophasor data stream.

B. Finding Possible Incident Location(s)

After recognizing the incident type which occurs in the system, the incident location is always desired to be found. Assume $\boldsymbol{M_1}$ is an incident-free measurement matrix at time instant t_1 and from $\boldsymbol{M_1}$ we obtain the partial eigenvector matrix $\boldsymbol{K_1}^*$. Then we can reconstruct the data in the new projection (sub-space) if n eigenvectors corresponding to the n principal eigenvalues are selected:

$$\boldsymbol{r_1} = \boldsymbol{M_1} * \boldsymbol{K_1^*} * \boldsymbol{K_1^{*T}} \tag{8}$$

The n significant eigenvectors reflect the dominant of the patterns in $\boldsymbol{M_1}$. As shown in Figure 6(a), the difference between the original matrix and the reconstructed matrix is relatively small, implying that the eigenvectors extract the most dominant variances of the data matrix. At time instance t_2 ($t_2 > t_1$), $\boldsymbol{M_2}$ is updated with the bad data. The bad data pattern is not included in the eigenvalues of $\boldsymbol{M_1}$, consequently the reconstruction data $\boldsymbol{r_2}$ cannot perfectly represent the last update data $\boldsymbol{m_2}$ in $\boldsymbol{M_2}$. In Figure 6(b), the distance between $\boldsymbol{m_2}$ and $\boldsymbol{r_2}$ shows that the unit 50 is likely being corrupted at that time instant, because point 50 is far away from other points.

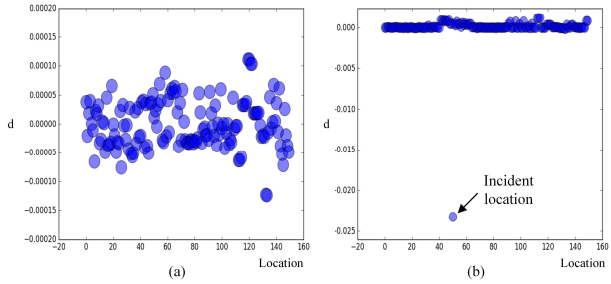

Fig. 7 Difference between reconstructed and original matrixes

C. Case Study

The proposed approach is tested using the real-time data from the synchrophasor network simulation environment. Two contingency cases (a transmission line fault and a three-phase fault) and malicious data injection on three measurements (voltage magnitude, angle and frequency) in a PMU data stream are used to test the performance of the method. The test results are shown in Table II. Contingencies and bad data injections are successfully detected, with the average response time 0.0124s, which satisfies the online detection requirement for a 30-60 fps data reporting rate. All incident locations are found after the incident type is recognized.

TABLE II TEST RESULTS WITH DIFFERENT INCIDENTS

	Eigenvalues										
Incident	$\Delta\log(\lambda_{v1})$	$\Delta\log(\lambda_{v2})$	$\Delta\log(\lambda_{v3})$	$\Delta\log(\lambda_{\alpha1})$	$\Delta\log(\lambda_{\alpha2})$	$\Delta\log(\lambda_{\alpha3})$	$\Delta\log(\lambda_{f1})$	$\Delta\log(\lambda_{f2})$	$\Delta\log(\lambda_{f3})$	Window	Detected
TLF*	4.0966	0.9402	0.1399	1.2984	0.4406	2.5119	0.4085	0.9865	1.8159	40	Yes (0.0126s)
TPF*	-0.0616	-2.1458	-0.7343	1.6729	0.6236	2.6122	1.3737	1.0849	1.9697	40	Yes (0.0120s)
BDV*	0.1007	0.166	0.5228	0	0	0	0	0	0	40	Yes (0.0123s)
BDA*	0	0	0	0.0011	-0.0515	0.1707	0	0	0	40	Yes (0.0128s)
BDF*	0	0	0	0	0	0	1.14	0.9123	2.7633	40	Yes (0.0121s)

*TLF: transmission line fault; TPF: three phase fault; BDV/A/F: bad data injection on voltage/angle/frequency

V. CONCLUSION AND FUTURE WORK

In this work, we present an online PCA-based method for processing the synchrophasor data to detect the anomaly behaviors of power systems including contingency and bad data injection. The proposed method is able to effectively recognize the incident type by pattern match and find the most possible incident location by comparing the reconstruction data with the original data, with a fast response time to satisfy the requirement for the real-time detection.

In future work, we further investigate the capability of this method with a partial observable system. When the system has limited number of PMUs, the placement of these observing points should play a big role in maximizing the observability of the system and guaranteeing that the attack on these points can be detected. More scenarios are being considered to explore the potential of this proposed method.

ACKNOWLEDGMENT

This paper is based upon work supported by the Department of Energy under Award Number DE-OE0000780.

REFERENCES

[1] T. Xu and T. Overbye, "Real-time event detection and feature extraction using PMU measurement data," *2015 IEEE International Conference on Smart Grid Communications (SmartGridComm)*, Miami, FL, 2015, pp. 265-270.

[2] Y.-F. Huang, S. Werner, J. Huang, N. Kashyap and V. Gupta, "State Estimation in Electric Power Grids: Meeting New Challenges Presented by the Requirements of the Future Grid," *IEEE Signal Processing Magazine,* vol. 29, no. 5, pp. 33-43, Sept. 2012.

[3] S. Pal and B. Sikdar, "A mechanism for detecting data manipulation attacks on PMU data," *2014 IEEE International Conference on Communication Systems*, Macau, 2014, pp. 253-257.

[4] Y. Liu, P. Ning and M. Reiter, "False data injection attacks against state estimation in electric power grids," *ACM Transactions on Computational Logic*, Chicago, Illinois, USA, Nov. 2009.

[5] A. Teixeira, S. Amin, H. Sandberg, K. H. Johansson and S. S. Sastry, "Cyber security analysis of state estimators in electric power systems," *49th IEEE Conference on Decision and Control (CDC)*, Atlanta, GA, 2010, pp. 5991-5998.

[6] D. Lee and D. Kundur, "Cyber attack detection in PMU measurements via the expectation-maximization algorithm," *2014 IEEE Global Conference on Signal and Information Processing (GlobalSIP)*, Atlanta, GA, 2014, pp. 223-227.

[7] Y. Huang, J. Tang, Y. Cheng, H. Li, K. A. Campbell and Z. Han, "Real-Time Detection of False Data Injection in Smart Grid Networks: An Adaptive CUSUM Method and Analysis," *IEEE Systems Journal,* vol. 10, no. 2, pp. 532-543, June 2016.

[8] H. Sedghi and E. Jonckheere, "Statistical structure learning of smart grid for detection of false data injection," *2013 IEEE Power & Energy Society General Meeting*, Vancouver, BC, 2013, pp. 1-5.

[9] D. Nguyen, R. Barella, S. A. Wallace, X. Zhao and X. Liang, "Smart grid line event classification using supervised learning over PMU data streams," *2015 Sixth International Green and Sustainable Computing Conference (IGSC)*, Las Vegas, NV, 2015.

[10] "C37.118.2-2011 - IEEE Standard for Synchrophasor Data Transfer for Power Systems," IEEE.

[11] D. Shi, D. J. Tylavsky and N. Logic, "An Adaptive Method for Detection and Correction of Errors in PMU Measurements," *IEEE Transactions on Smart Grid,* vol. 3, no. 4, pp. 1575-1583, Dec. 2012.

[12] C. Kumar and K. Lakshmi, "Monitoring and Detection of Fault Using Phasor Measurement Units," *International Journal of Electrical, Electronics and Mechanical Controls,* vol. 3, no. 2, May 2014.

[13] I. Idehen, Z. Mao and T. Overbye, "An emulation environment for prototyping PMU data errors," *2016 North American Power Symposium (NAPS)*, Denver, CO, 2016, pp. 1-6.

[14] A. Phadke, "Synchronized phasor measurements-a historical overview," *IEEE/PES Transmission and Distribution Conference and Exhibition*, 2002.

[15] H. Sandberg, A. Teixeira and K. Johansson, "On Security Indices for State Estimators in Power Networks," *First Workshop on Secure Control Systems*, Stockholm, Sweden, Dec. 2010.

[16] T. J. Overbye, Z. Mao, K. S. Shetye and J. D. Weber, "An interactive, extensible environment for power system simulation on the PMU time frame with a cyber security application," *2017 IEEE Texas Power and Energy Conference (TPEC)*, College Station, TX, 2017, pp. 1-6.

[17] "IEEE Std C37.118.1-2011 (Revision of IEEE Std C37.118-2005)," Dec. 28 2011.

[18] A. H. and L. Williams, "Principal component analysis," *Wiley Interdisciplinary Reviews: Computational Statistics,* vol. 4, no. 2, p. 433–459, June 2010.

[19] "IEEE 118-Bus System," Illinois Center for a Smarter Electric Grid (ICSEG), [Online]. Available: http://icseg.iti.illinois.edu/ieee-118-bus-system/.

[20] A. Birchfield, K. Gegner, T. Xu, K. Shetye and T. Overbye, "Statistical Considerations in the Creation of Realistic Synthetic Power Grids for Geomagnetic Disturbance Studies," *IEEE Transactions on Power Systems,* vol. 32, pp. 1502-1510, March 2017.

[21] M. Wu and L. Xie, "Online Detection of False Data Injection Attacks to Synchrophasor Measurements: A Data-Driven Approach," *50th Hawaii International Conference on System Sciences*, Hawaii, USA, 2017.