A Data Driven Detection and Locating of Cyber and Physical Stresses in Smart Grid based on State Correlations

Md Abul Hasnat and Mahshid Rahnamay-Naeini
Electrical Engineering Department, University of South Florida, Tampa, Florida, USA
hasnat@mail.usf.edu, mahshidr@usf.edu

***Abstract*—Smart grids being complex cyber-physical infrastructures demand real-time monitoring of their dynamic states. Phasor measurement units (PMUs) are smart metering devices with a high sampling rate, which facilitate visualizing the dynamics of the states with the help of time series corresponding to the system's parameters and attributes. This work shows the signatures of different cyber-attacks and some physical phenomenons on the PMU time series and their impacts on the correlation among the components' states. A technique exploiting the instantaneous state correlation matrix (associated with any electrical attribute, i.e. bus voltage angle) is proposed for providing early alerts for attacks to the control center's operators in real-time. The type of attack (cyber or physical) and the location of the component that is compromised by the attackers are also detectable by observing the instantaneous correlation matrix as an image.**

***Index Terms*—Cyber-attacks, PMU data, state correlations, time series, smart grid.**

I. Introduction

Smart grids are critical cyber-physical infrastructures that are large in size, dynamic in operation and complex in nature and therefore, a wide area monitoring system (WAMS) based real-time monitoring is necessary for the proper functioning of the system. Phasor measurement units (PMU) are very high sampling rate devices for the measurement of the electrical attributes (e.g, voltage and current phasors, and frequency) in real-time, which are deployed throughout the WAMS to obtain data to estimate the states of the system for the continuous monitoring of the system. Modern power systems are rapid-changing and more stochastic than before because of the introduction of the of smart devices, electrical vehicles, and other modern electrical devices in the load side and distributed energy resources (DER) in the generator side. For the quickest response in case of different events and stresses, on-line monitoring of the states is required. Moreover, cyber-attacks of different types can hamper and mislead the control center to take wrong decisions and operating actions. Therefore, such events and stresses should be detected by the system in real-time to have prevention against situations affecting the reliability of the system, such as, physical attacks masked by cyber attacks. Earlier detection of the anomalies in the grid and determination of its location may save the grid from further damage, for example, cascading failures followed by large blackouts.

The continuous data streams from all the PMUs can be considered as the multivariate time series. Managing large time-stamped data from the PMUs as time series enables us to apply different real-time detection techniques on the PMU data to provide alarms in the case of anomalies. Since the sampling rates of the PMUs are high, rapid estimation of the states in real-time can be possible for the control mechanism.

The power system is an interconnected system and the correlation among the component's states are governed by the physics of the power flow. Since the power flow varies with time according to load variations and other physical events, the correlations among the states vary in time. In addition to normal events that can cause variations in correlations, cyber-attacks and physical stresses can also affect the correlation among the state of the components. These correlations can be calculated and observed from the PMU time series associated with system components.

In this work, we have demonstrated that the changes in the correlation pattern among the states (i.e. PMU time series) with time can be used as a useful visualization tool for monitoring the condition of the grid. By visualizing the instantaneous state correlation matrix as an image, we observe that both the cyber-attacks and physical phenomena have certain signatures, which can be used for identifying various types of stresses. The correlation matrices can be both visually and algorithmically be analyzed to extract the signature of stresses and locate them in the system. Real-time analyzing of the instantaneous correlation matrix as an image can provide earlier alarm about the cyber and physical anomalies and can locate them as well. In this paper, we present examples of such correlation matrix images and a simple image processing method for detecting and locating cyber and physical stresses on the system.

II. Literature Review

Although the real-time detecting and locating of the cyber or physical events in smart grid are newer topics to address by researchers, various methods for the detection of anomalies in the power grids have already emerged. For instance, Chen et. al. [1] proposed determining a lower-dimensional model for data by using the historical data. In real-time, this lower-dimensional model of the data is used to predict data one step ahead. If the mismatch between the predicted data and the actual data exceeds a certain threshold, the data is considered to be anomalous. Wu et. al. [2] also proposed a robust online detection method of the anomaly in power systems in which an alternative feature selection method has been used to determine the lower-dimensional representation of the PMU data. The authors proposed iForest algorithm for the detection of the anomalies. Cai et. al. [3] proposed detecting and locating anomalies in the grid by considering the PMU data stream as multivariate time series and obtaining the principal components of the data. The real-time detection technique involved applying the k-nearest neighbor (kNN) method on the T^2 and Q statistics of the Principle Component Analysis (PCA) represented data and comparison with those of historical data.

Kurt et. al. [4] proposed a cumulative sum (CUSUM) based algorithm for the real-time detection of cyber and hybrid attacks in smart grids. Chu et. al. [5] used three sample quadratic prediction algorithm (TSQPA) based filter to predict a sample from its previous three samples and proposed a false data detection algorithm on the basis of the mismatch between the predicted sample and the measured sample. This latter paper shows that the false data detection method works quite accurately on the suddenly applied false data, but fails to perform in the case of gradually changing false values.

Some neural network based methods have also been presented in the literature for detecting cyber-attacks in power systems in real-time. For example, Ganjkhani et. al. [6] proposed nonlinear auto-regressive exogenous neural network (NARXNN) to detect false data injection attacks in real-time. NARXNN is a robust recurrent neural network architecture specially designed for time series. This method exploits the highly correlated states for predicting the states one-step ahead using measurement values along with historical data. Comparing the predicted state values with the original measurements, the technique identifies injected false data. In our work, we also considered the PMU data as time series and proposed a simple and fast method for the real-monitoring of the cyber and physical anomalies in smart grids based on state correlations, which works better than existing methods particularly for gradually changing events such as ramp attacks.

III. Correlation among the States of the Components

Since the power system is an interconnected structure, the electrical attributes measured at different PMUs have a significant amount of correlation based on the geographical distance, nature of the power flow, physical and structural properties of the system including connectivities, line impedance, etc. In our study, on the IEEE 118 bus system, we have assumed that there are PMUs at each of the 118 buses. However, in today's power system the assumption is not entirely realistic, nevertheless, the technique developed in this paper can be extended for real-life power systems with a limited number of PMUs by incorporating any of the optimal PMU placement algorithms [7]. Fig. 1 illustrates the correlation among the PMUs in terms of one of the electrical attributes. The correlations illustrated in Fig. 1 have been calculated from the day long PMU data considered as time series. We notice that on average there are high correlations among the PMU data.

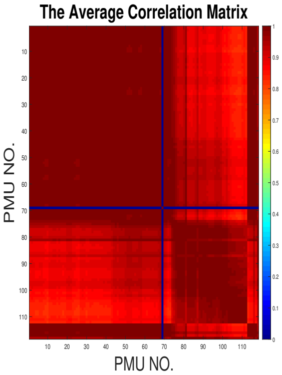


Fig. 1. Average correlations among PMU data in IEEE 118 bus system (calculated over day-long time series).

For the simulation of the PMU data time series, we have used MATPOWER 6.0 [8] to run the power flow solution with time-varying loads in all the load buses to generate the time series. The daily load profiles from the NYISO [9] are collected and normalized to add to the MATPOWER's default load to generate the time series. Standard PMU data consists of continuous (at a sampling rate of a few kHz) measurements of voltage phasor, current phasor, and frequency at a bus. However, PMUs send data to the control center to at a much lower rate (a few Hz). In our simulation, we have considered 0.033Hz as the sampling rate, however, the method can be easily extended to higher sampling rates by increasing computational resources.

The correlation pattern shown in Fig. 1 changes in time based on the influence of various changes in the power grid, for example, load demand variation, topology changes, generation variation, tripping of the transmission line, etc. Also, if any of the PMUs is compromised by cyber-attacks the observed correlation among the PMUs will change. Our goal is to characterize the changes in the correlation among the PMU time series to detect whether there is a cyber attack, to distinguish it from other probable physical events and to determine the location of the PMU which is under attack. In this section, we will illustrate the effects of typical physical phenomena and cyber attacks on the PMU time series and will study the effects on the correlation pattern among the PMU data by observing the instantaneous correlation matrix in real-time.

A. *Effects of Physical Events on PMU Time Series*

We have investigated the effects of different physical events on the time series from the nearest PMU as well as nearby PMUs to the event. In this paper, we define nearby as buses, which are one hop away from the main bus. Fig. 2 illustrates the effects of a few physical events (line tripping, abrupt load change, and load power factor change) on the voltage angle time series of the PMU installed on the bus in which these events occurred. In this case, we have simulated all the events on BUS No. 85 of IEEE 118 bus system. For all the events, sharp changes can be observed in the time series at the onset of the events. Similar behavior can be observed if the event occur at other buses in the system.

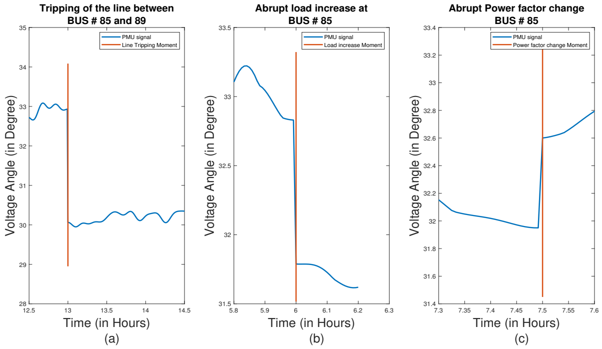


Fig. 2. Effects of physical events on the nearest PMU time series.

Most of the physical events influence the nearby buses in addition to the buses where the incident occurred. For example, we observe the effect of single tripping. Fig. 3 illustrates the effect of tripping of the transmission line between Bus no. 85 and BUS No. 89 of IEEE 118 bus system on the nearby PMU signals (voltage angles). We can observe that the tripping affects bus voltage angle signals of PMU No. 85, 87 & 89 but the signal in PMU No. 88 seems to be unaffected although PMU No. 88 is not geographically very distant from the tripped line.

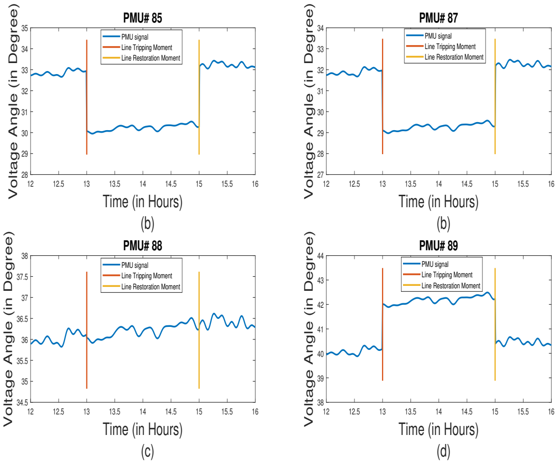


Fig. 3. The effects of a single line trip on the few PMUs nearest to the place of incidence.

B. Mathematical Formulation of the Cyber Attacks

Different types of cyber-attacks threaten smart grid security and newer types of attacks are being designed every day. In this paper, we have considered three types of cyber attacks: Denial-of-Service (DoS) attack, Data-replay attack, and Ramp attack. Among them, DoS attack and Data-replay attacks are very common for any cyber-physical system while the ramp attack is special because of the difficulties in detecting the attack due to the absence of discontinuities at the onset of the attack. In this subsection, we will try to find mathematical formulations of them and illustrate their effects on PMU time series.

Let, $\mathcal{P}$ be the set of the PMUs in IEEE 118 bus system, $\mathcal{A} \subset \mathcal{P}$ be the set of PMUs under cyber attack and $\mathcal{S} \subset \mathcal{P}$ be the set of PMUs the attackers have access to record data.

The DoS attack can be modeled as the unobservability of the PMU data during the attack duration. Let, $x_i(t)$ be the actual time series of any electrical attribute (e.g. voltage phase angle) of the bus associated with the $i-$th PMU. In the case of the $i-$th PMU to be under DoS attack, the time series from this PMU can be represented as:

$$x_{DoS_i}(t) = \begin{cases} n_i(t) & \text{if } t_{start} \leq t \leq t_{end} \\ x_i(t) + n_i(t) & \text{otherwise,} \end{cases} \tag{1}$$

where t_{start} and t_{end} are, respectively, the starting and ending of the DoS attack, and $n_i(t)$ is the Additive White Gaussian Noise signal associated with the $i-$th PMU. (Fig. 4a)

In data replay attack, the attacker records the data from some of the PMUs that they have access and replays the past data in the present time to the PMUs under attack:

$$x_{Replay_i}(t) = \begin{cases} x_k(t' + t - t_{start}) + n_i(t) & \text{if } t_{start} \leq t \leq t_{end} \\ x_i(t) + n_i(t) & \text{otherwise,} \end{cases} \tag{2}$$

where t_{start} and t_{end} are, respectively, the starting and ending of the replay attack and t' is the starting of the recording time. Here, $i \in \mathcal{A}$ and $k \in \mathcal{S}$. (Fig. 4b for $i = k$ and Fig. 4c for $i \neq k$). From hour 16 to 17, the attacker injected the past data (hour 13-14) from Bus 85 into the same bus (Fig. 4b), whereas from hour 21 to 22, the attacker injected past data form PMU of bus 102 into the PMU of bus 85 (Fig. 4c).

In the ramp false data injection, the attacker slowly introduces bad data to remain undetectable by any prediction based detector. In Fig. 4d, we observe the ramp attack at hour 18, instead of a sharp change in values at the instant 18.00 hour, false data are gradually inserted into the PMU time series as follows:

$$x_{Ramp_i}(t) = \begin{cases} x_i(t_{start}) + n_i(t) + m(t - t_{start}), & \text{if } t_{start} \leq t \leq t_{end} \\ x_i(t) + n_i(t), & \text{otherwise,} \end{cases} \tag{3}$$

where, m is the slope.

C. The Instantaneous Correlation Matrix

In our study, since we have assumed that there are PMUs in each of the buses, the time series from the nearby PMUs should have strong correlations among themselves. However, because of the changes in the load curve and other dynamics of the power system, the correlation among the PMU time series changes with time. Therefore, we are interested in the instantaneous correlation among the the PMU time series. The

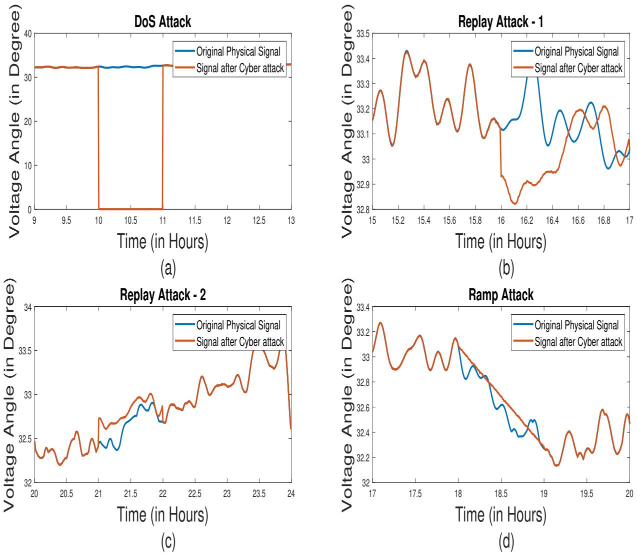


Fig. 4. The effects on the voltage angle time series associated with the PMU at Bus 85: (a): DoS Attack (Hour 10-11) (b): Replay Attack Hour (16-17) with the past data from the same bus; (c): Replay Attack (Hour 21-22) with past data from Bus 102; (d) Ramp attack at Hour (18-19).

instantaneous correlation matrix of the PMU data at any time instant t is an $N \times N$ square matrix $C(t)$. Any element of $C(t)$ is represented as:

$$r_{ij}(t) = \frac{\int_{t-t_c}^{t} x_i(\tau)x_j(\tau)d\tau}{\sqrt{\int_{t-t_c}^{t} x^2{}_i(\mu)d\mu}\sqrt{\int_{t-t_c}^{t} x^2{}_j(\nu)d\nu}}, \quad i,j \in \mathcal{P}, \quad (4)$$

In Fig. 5 the instantaneous correlation matrix $C(t)$ has been visualized as an image during various events. Since PMU at bus index 69 is the reference PMU (PMU associated with the slack bus), we can see a horizontal and vertical line corresponding to PMU No. 69 in all the cases. In case of cyber attacks, the correlation profile of the attacked PMU with all other PMUs changes are distinguishable from the horizontal and vertical lines in the correlation image. Physical events on a single bus affects nearby PMUs. We can observe distinct areas in the correlation image. The ramp attack also affects the correlation image in a similar way which is undetectable by linear predictors as was also discussed in [5].

IV. Method for Detection and Locating Events in Real-Time

In this paper, we propose a technique to provide the operator an early alert about the cyber attacks on the smart grid and to find the attack locations based on the instantaneous state correlations. An operator can have an alarm of any cyber physical anomaly by visualizing the instantaneous state correlation matrix image itself in real-time and the location of the attack is also identifiable from the image in real-time based on the horizontal and vertical lines that appear in the image. The automatic identification of the anomalies involves simple image processing technique (i .e. detecting horizontal and vertical lines for cyber-attacks.)

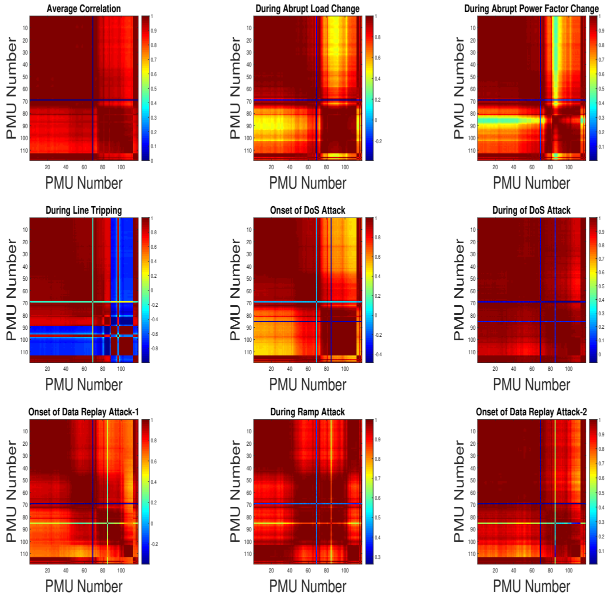


Fig. 5. Correlation matrix images for various cyber and physical events.

For detection and locating of the attack in real-time, we process the instantaneous correlation matrix image, $C(t)$ for each sample. The steps are given below:

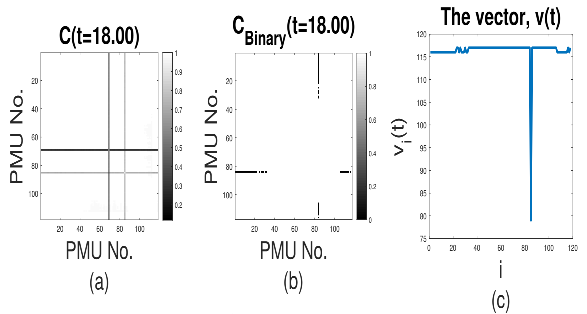


Fig. 6. (a) Instantaneous correlation matrix at the onset of the ramp attack, (b) image after removing reference PMU and thresholding, (c) the vector, $\underline{v}(t)$.

Converting $C(t)$ to binary form: At first, we remove the horizontal and vertical line for the reference (slack bus) from $C(t)$. Then we apply threshold to that image to obtain a binary image $C_{Binary}(t)$ by . Here, we have selected the threshold as the median of the intensity values of the pixels of $C(t)$. $C(t)$ and $C_{Binary}(t)$ are shown in Fig. 6(a) and Fig. 6(b), respectively.

Calculating $\underline{v}(t)$: From the binary correlation image we determine the number of PMUs with which any PMU has a significant correlation (above threshold). Let the $i-$th element of the vector $\underline{v}(t)$ represents the number of PMUs with which the time series of the $i-$th PMU has a significant correlation at time instant t, where $i \in \mathcal{P}$. We calculate the $\underline{v}(t)$ as: $\underline{v}(t) = C_{Binary}(t)\underline{u}$, where $u = [1, 1, ...1]^T$.

Detection of Cyber Attack: Let denote the $n-th$ minimum element of a vector, $\underline{x}$ as $min(\underline{x}, n)$. We detect a cyber attack if:

$$min(\underline{v}(t),2) - min(\underline{v}(t),1) > b, \tag{5}$$

where, b is a threshold selected empirically.

Locating Cyber Attack: The PMU which is compromised by the attacker can be identified as the index of the minimum element of $\underline{v}(t)$. Mathematically, the index, l of the attacked PMU is calculated from the following equation:

$$v_l(t) = min(\underline{v}(t),1). \tag{6}$$

Since some of the PMUs have significant correlations with a small number of PMUs in even in normal condition, for avoiding false positive we check for $v_l(t) < v_{hist,l}$ to declare cyber-attack, where $\underline{v}_{hist} = C_{hist}\underline{u}$. C_{hist} is the historical average correlation matrix.

The cyber-attacks can be distinguished from the physical events in this process as in the next example. Fig. 7 illustrates the effect of a physical phenomenon on the correlation matrix. From Fig. 7(c) we can observe that, a few consecutive elements of the vector $\underline{v}(t)$ are comparatively smaller than the others unlike cyber-attacks illustrated in Fig. 6, where a single element of the vector $\underline{v}(t)$ is very small compared to the others.

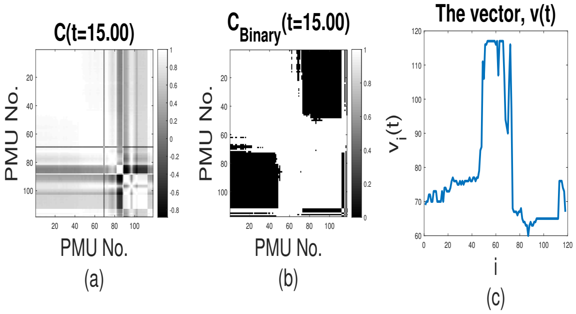


Fig. 7. (a) Instantaneous Correlation Matrix at the onset of a physical event (restoration of a tripped line), (b) Image after removing reference PMU and thresholding, (c) the vector, $\underline{v}(t)$.

V. Performance Evaluation

A. Detection of Cyber-attacks

Our evaluations show that the proposed method has a good performance for the detection of cyber-attacks. Table. I shows the detection and the correct locating rate for different types of cyber-attacks. The average detection and locating rate has been calculated by simulating cyber-attacks in all the PMUs of IEEE 118 bus system. This method performs well for the ramp attacks as well, which is difficult to detect because of the gradual injection of the falsified data.

B. Detecting and Locating Physical Stresses

Since any physical event on a single bus affects the electrical attributes of several buses, determining the exact PMU location is difficult from the correlation image. In some of the case, we can exactly detect and locate physical attacks. Fig. 8 illustrates detection of the tripping of Branch No. 87 in IEEE 118 bus system, which connects BUS No. 55 and BUS No. 59. From the correlation matrix in Fig. 8(a) we can easily identify some anomaly near PMU No. 58 to PMU No. 64. Since we can see horizontal and vertical lines within a range instead of a single PMU (as in the case of cyber attack), it can be decided that the stress is physical. The effect is also identifiable from $\underline{v}(t)$ in Fig. 8(b) and the algorithm locates PMU No. 59 as the anomalous PMU, which was in fact connected to the tripped line.

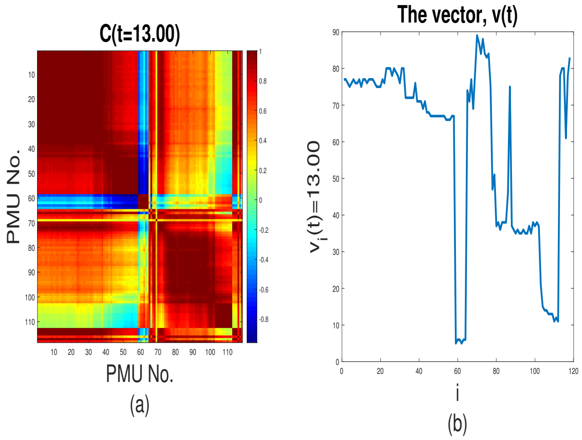


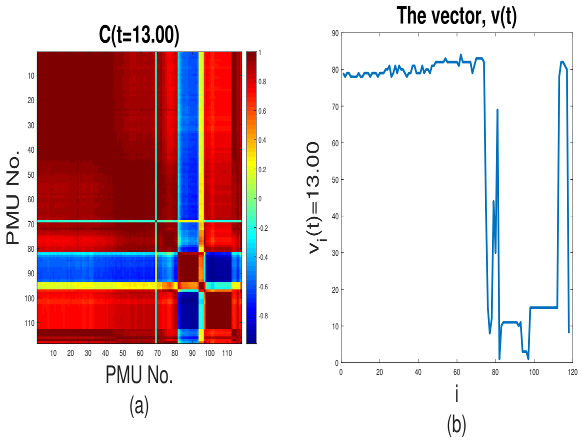
Fig. 8. (a) Instantaneous correlation matrix at the onset of a physical event (tripping line between BUS No. 55 and BUS No. 59), (b) the vector, $\underline{v}(t)$ at the onset of the event.

However, in some cases, this method detects the event correctly but fails to locate it exactly. For example, we simulated a line tripping between BUS No. 92 and BUS No. 102. From Fig. 9(a) we can easily identify that there is an event within BUS No. 82 and BUS No. 93, but the method locates the failure at BUS No. 82, which is in fact two hops away from BUS No. 92. And in some cases, the method fails to detect physical events. Fig. 10 illustrates such cases.

In summary, the proposed method based on the state correlation matrix can detect and locate cyber attacks with good performance. However, while the method can detect physical stresses and distinguish it from cyber attacks, it may not be able to accurately locate the physical stresses in the system. In future work, we will investigate and characterize the properties

TABLE I
Performance of Detecting and Locating Cyber Attacks in Terms of True Detection Rate and Rate of Locating the Exact Attacked PMU.

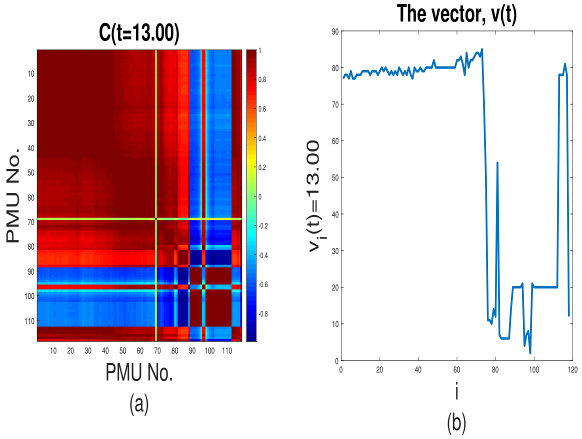
Cyber Attack	Detection Rate	Exact Locating Rate
DoS Attack	1.0000	0.9915
Replay Attack	0.9915	0.8803
Ramp Attack	0.9402	0.8454



(a)

(b)

Fig. 9. (a) Instantaneous correlation matrix at the onset of a physical event (tripping line between BUS No. 92 and BUS No. 102), (b) the vector, $\underline{v}(t)$ at the onset of the event.



(a)

(b)

Fig. 10. (a) Instantaneous correlation matrix at the onset of a physical event (tripping line between BUS No. 85 and BUS No. 89), (b) the vector, $\underline{v}(t)$ at the onset of the event.

of the system and components that may affect the performance of the method to enhance locating physical stresses.

VI. Conclusion

In this work, we introduced a real-time state correlation-based monitoring technique for early detection of anomalies in power grids using PMU time series. The state correlation matrix of the system was generated and analyzed. The visual presentation of state correlation matrices provide a simple yet effective visualization tool to detect stresses, such as cyber attacks and various physical events, in real-time. We developed a simple image processing-based technique for the detection and locating of cyber-attacks in smart grids from the instantaneous correlation image and distinguishing them from the physical anomalies. Prospective future works include detection and locating of coordinated cyber-attacks, classification among the cyber-attacks, and detecting of physical failures under unobservablities using the correlation among the PMU data.

Acknowledgment

This material is based upon work supported by the National Science Foundation under Grant No. 1761471.

References

[1] Y. Chen, L. Xie, and P. R. Kumar, ”Dimensionality reduction and early event detection using online synchrophasor data,” 2013 IEEE Power Energy Society General Meeting, Vancouver, BC, 2013, pp. 1-5.

[2] T. Wu, Y. A. Zhang, and X. Tang, ”Isolation Forest Based Method for Low-Quality Synchrophasor Measurements and Early Events Detection,” 2018 IEEE International Conference on Communications, Control, and Computing Technologies for Smart Grids (SmartGridComm), Aalborg, 2018, pp. 1-7.

[3] L. Cai, N. F. Thornhill, S. Kuenzel, and B. C. Pal, ”Wide-Area Monitoring of Power Systems Using Principal Component Analysis and k-Nearest Neighbor Analysis,” in IEEE Transactions on Power Systems, vol. 33, no. 5, pp. 4913-4923, Sept. 2018.

[4] M. N. Kurt, Y. Yilmaz, and X. Wang, ”Real-Time Detection of Hybrid and Stealthy Cyber-Attacks in Smart Grid,” in IEEE Transactions on Information Forensics and Security, vol. 14, no. 2, pp. 498-513, Feb. 2019.

[5] Z. Chu, A. Pinceti, R. Biswas, O. Kosut, A. Pal, and L. Sankar, ”Can Predictive Filters Detect Gradually Ramping False Data Injection Attacks Against PMUs?”, arXiv:1905.02271 [cs.SY], 2019.

[6] M. Ganjkhani, S. Fallah, S. Badakhshan, S. Shamshirband, and Kwok-wing Chau. ”A Novel Detection Algorithm to Identify False Data Injection Attacks on Power System State Estimation.” Energies 12, no. 11 (2019): 2209.

[7] W. Yuill, A. Edwards, and S. Chowdhury, ”Optimal PMU placement: A comprehensive literature review”, IEEE Power and Energy Society General Meeting, 2011.

[8] R. D. Zimmerman, C. E. Murillo-Snchez, and R. J. Thomas, *MATPOWER: Steady-State Operations, Planning and Analysis Tools for Power Systems Research and Education*, IEEE Transactions on Power Systems, Volume: 26, Issue:1 , Feb. 2011.

[9] The New York Independent System Operator, Inc[US], https://www.nyiso.com/.