Realistic Synchrophasor Data Generation for Anomaly Detection and Event Classification

K. S. Sajan, M. Bariya, S. Basak, *Member, IEEE*, A. Srivastava, *Senior Member, IEEE*,
A. Dubey, *Senior Member, IEEE*, A. von Meier, *Member, IEEE* and G. Biswas, *Fellow, IEEE*

***Abstract*—The push to automate and digitize the electric grid has led to widespread installation of Phasor Measurement Units (PMUs) for improved real-time wide-area system monitoring and control. Nevertheless, transforming large volumes of high-resolution PMU measurements into actionable insights remains challenging. A central challenge is creating flexible and scalable online anomaly detection in PMU data streams. PMU data can hold multiple types of anomalies arising in the physical system or the cyber system (measurements and communication networks). Increasing the grid situational awareness for noisy measurement data and Bad Data (BD) anomalies has become more and more significant. Number of machine learning, data analytics and physics based algorithms have been developed for anomaly detection, but need to be validated with realistic synchophasor data. Access to field data is very challenging due to confidentiality and security reasons. This paper presents a method for generating realistic synchrophasor data for the given synthetic network as well as event and bad data detection and classification algorithms. The developed algorithms include Bayesian and change-point techniques to identify anomalies, a statistical approach for event localization and multi-step clustering approach for event classification. Developed algorithms have been validated with satisfactory results for multiple examples of power system events including faults and load/generator/capacitor variations/switching for an IEEE test system. Set of synchrophasor data will be available publicly for other researchers.**

***Index Terms*—Phasor Measurement Units, Synthetic data, Wide-area Monitoring, Anomaly Detection, Event Detection and classification.**

I. Introduction

THE growing complexity of electricity generation and consumption, along with more frequent natural and man-made disruptions, are threatening the nation's electric grid. Efforts to build a smart grid aim to address these issues to improve the reliability and resilience of the system. The envisioned smart grid has real-time, wide-area system visualizations for operators to better inform their decision making and reduce the system's susceptibility to large outages [1], [2]. The basis for this improved system visibility are measurement devices, such as Phasor Measurement Units (PMUs), which produce GPS time-stamped, high resolution, high frequency measurements of phasor quantities. The proliferation of sensor data brings its own challenges, including handling data anomalies, enabling real time processing and cyber-security management [3]. Overall, converting high resolution PMU measurements into actionable system insights in real-time remains a largely open challenge, reflected in the limited control room applications of PMU measurements [4]–[6]. Multiple work have been reported to utilize these data but validation requires realistic data with given anomalies and events. Field data is difficult to acquire and not labeled for anomalies and events.

This work aims to generate realistic but synthetic synchrophasor data. Enhanced situational awareness utilizing synchrophasor data are developed for anomaly detection and event classification. The design of the tool integrates principles from machine learning, data science, cyber-security, and power engineering. The vision for the tool is that it will supplement Energy Management Systems (EMS) to enhance the decision making capabilities of power grid operators especially under challenging and extreme events [7]. One fundamental component of this decision support tool is detecting and classifying *anomalies* in the measurement streams, which is critical for reliable grid operation. These anomalies may arise from physical changes in the system (in which case they are termed *events*), or issues in the cyber infrastructure that handles the measurements (in which case they are termed *bad data*). For example, a voltage sag is an event anomaly, while a missing data packet is a bad data anomaly. Awareness and differentiation of both anomaly types is essential for full cyber-physical situational awareness.

A variety of techniques are described for anomaly detection. They can broadly be categorized as graph-based [8], model-based [9], density based [10] and clustering based [11]. Graph-based methods detect outliers by estimating joint distributions over data streams, but can face a dimensionality problem as the number of streams grows. Model-based approaches are generally efficient, but developing accurate models of streaming measurements is challenging. Clustering based models may detect an evolving behavior of the underlying process as an outlier. Density-based approaches such as local outlier factor (LOF) may also fail due to the curse of dimensionality. For detecting anomalies over a PMU data stream, A. Ahmed et al. [12] use an deep autoencoder, Pan et al. [13] use data mining techniques to monitor PMU measurements. Chen et al. [14] [15] use linear basis expansion on PMU data. Paul et al. [16] use machine learning on PMU data via Hadoop and openPDC. In [17] Y. Zhou et al. use kernel based PCA to build up statistical models for nominal state and then detect anomalies on abnormal behavior. Moreover, research presented in [18] uses a threshold based method for detecting outliers from reconstructed output values of the autoencoder model. Research presented in [19] uses z-score method for detecting outliers. In [20], the authors have presented threaded ensemble autoencoder for anomaly detection.

To accurately assess the real-world performance of our tools, we must test them on *realistic* synchrophasor data. However, obtaining real measurements and metadata from

K.S. Sajan and A. Srivastava are with the Washington State University. M. Bariya and A. von Meier are with the University of California Berkeley. S. Basak, A. Dubey and G. Biswas are with the Vanderbilt University. Authors would like to acknowledge financial support from NSF 1840192 and 1840052 for this work.

operational systems is difficult due to strict security and confidentiality regulations protecting most data sets. Instead, we aim to generate highly realistic *simulated* PMU data by adding realistic noise and bad data effects to noiseless simulated measurements. Our choice of realistic noise is based on studies of field deployed PMUs in [21] and [22].

The main contributions of this paper can be summarized as:

1) We present a method for creating realistic but synthetic PMU measurements.
2) We introduce two techniques for event and bad data detection. These are applied separately to current and voltage measurements, which allows for redundancy in the detection.
3) The detection methods associate a certainty or probability measure with the flagged events or bad data which reflects the certainty in the flagging.
4) Identification of key PMUs 'seeing' events based on a statistical technique.
5) A multi-step clustering approach is introduced to classify the detected events into five event categories: fault event, load event, capacitor event, generation change event, and generator switching event.

II. Extracting noise and features from field PMUs and integration with synthetic data

Due to the inaccessibility of real measurement datasets, most proposed PMU applications are not tested on real or even realistic data. Therefore, there is limited confidence in their ability to succeed in the real world. To overcome this, we aim to generate realistic simulated PMU measurements by adding realistic noise and bad data effects to ideal, noiseless simulated measurements. Our choice of noise level and model is based on [21] and [22], which use two different approaches to estimate the noise level from PMUs deployed on operational power networks. In [21], noise in transmission PMU measurements is found to be about 45 dB and follow a Gaussian model. In [22], noise in higher accuracy distribution PMU measurements is found to be about 55 dB. Based on these results, we generate realistic measurements by adding Gaussian noise at two levels: 30 dB (a conservatively high noise level) and 45 dB (a realistic noise level). We also generate measurements with Laplacian noise to assess algorithm performance under a different noise distribution.

The PMU communication network is vulnerable to malfunctions such as response time, time delay or actual communication link failures thus resulting in bad data injection, dropped data packets, and missing data samples. To address issues in the cyber infrastructure, we also injected bad data, missing data and missing packet cases to the simulated PMU data to assess algorithm performance of the proposed method.

III. Anomaly Detection and Classification in Synchrophasor Data

To convert high-resolution PMU measurements into useful information and insight for operators, we must detect, localize, and categorize anomalies, including physical events and data anomalies. Anomaly detection is the problem of differentiating anomalous measurements from normal data. Note that the capability to distinguish between these categories is not only important for common operations, but critical for reducing vulnerability to malicious cyber-attacks. For those anomalies that are physical events, event localization consists of identifying the bus or line where the event occurred. Finally, event categorization consists of determining the event type to the highest level of specificity. Figure-1 shows the complete architecture of the proposed methodology for anomaly detection and event classification.

A. Anomaly Detection

Statistical approaches are well suited to the problem of generic anomaly detection. Their premise is that anomalies always produce a change in the *statistics* of the measurements. Therefore, these techniques are general and do not assume a specific anomaly type or measurement signature. Statistical approaches also associate a probability measure with detected anomalies, which captures how far from normal the anomaly data are, and therefore our certainty that the data capture a real anomaly. Such certainty measures are valuable when combining multiple approaches, generating warning flags, and conveying results to human users in a trustworthy manner. We propose two statistical approaches for anomaly detection. The first, termed *Bayesian anomaly detection*, tracks and updates moment estimates, then uses a Bayesian score to identify anomalies. The second, termed Changepoint detection uses a CUSUM (Cumulative Sum Control Chart) [23] algorithm to track variations in time-series data.

1) Bayesian anomaly Detection: Consider a measurement point at time t, denoted $X_t \in \mathbb{R}^m$. The data point could be multidimensional, $m > 1$ including measurements from multiple PMUs. Let D_{μ,σ^2} denote the generative distribution underlying the data under normal conditions, parameterized by a mean μ and variance σ^2. Then, an anomaly can be flagged based on the posterior probability of X_t given some estimates of μ and σ^2. This is expressed as:

$$P(X_t \mid \mu, \sigma^2) < p \quad \longrightarrow \quad X_t \text{ is an anomaly.} \tag{1}$$

where p is the anomaly threshold probability. The challenge is that μ and σ^2 are not known *a priori* and may change as the system moves between operating regimes. A standard approach to Bayesian anomaly detection (commonly called change point detection in the wider literature) is to estimate μ and σ^2 from a length w window of data preceding X_t: $X_{t-1}, ..., X_{t-w}$. However, this approach is not suited to a real-time application with streaming data, in which multiple anomalies may occur over a length w window. Instead, here we update our knowledge of μ and σ^2 with each new measurement in a Bayesian framework, where a prior over μ and σ^2 captures information from previous data points. Let $p_t(\mu, \sigma^2)$ denote the prior distribution over μ and σ^2 at time t. Given data point X_t, we can compute a posterior distribution over μ and σ^2. This leads to the prior for the next time step:

$$p_{t+1}(\mu, \sigma^2) \propto p(X_t \mid \mu, \sigma^2) p_t(\mu, \sigma^2) \tag{2}$$

Using a Normal-inverse-chi-squared (NIX) distribution as the prior leads to tractable updates [24]. At time t, the four parameters of the NIX distribution are the mean of and certainty over μ–denoted μ_t and κ_t–and the mean of and certainty over σ^2–denoted σ_t^2 and υ_t. These parameters are

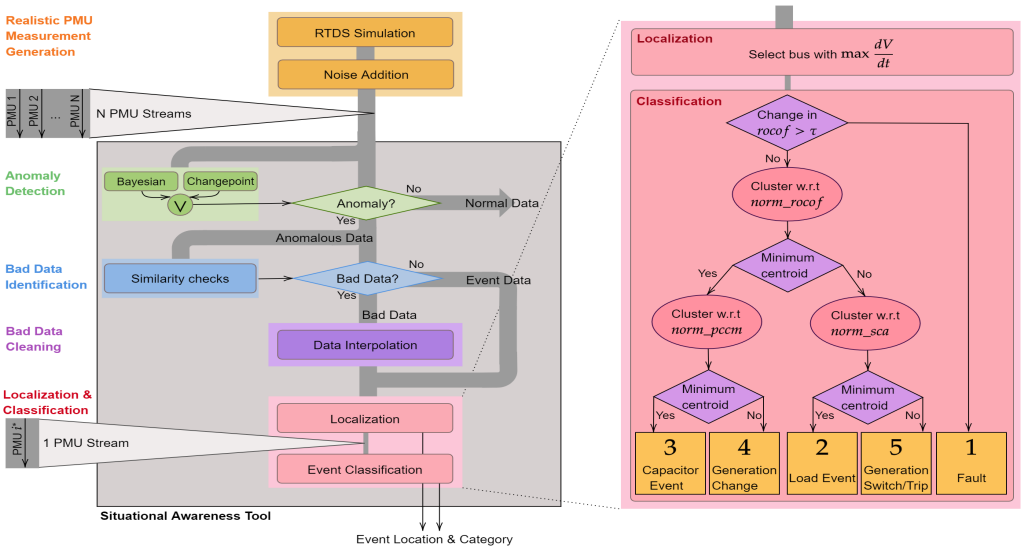


Fig. 1: Measurement Data Generation and Data Flow Architecture for Anomaly Detection and Event classification

updated with new measurement X_t according to the following equations:

$$\begin{aligned} \kappa_{t+1} &= \kappa_t + 1 \\ \upsilon_{t+1} &= \upsilon_t + 1 \\ \mu_{t+1} &= \frac{\kappa_t \mu_t + X_t}{\kappa_t + 1} \\ \sigma^2_{t+1} &= \frac{1}{\upsilon_t}\left(\upsilon_t \sigma_t^2 + \frac{\kappa_t}{\kappa_t + 1}(X_t - \mu_t)^2\right) \end{aligned} \tag{3}$$

We initialize the prior with arbitrary estimates of mean and variance, denoted μ_0 and σ_0^2, and low certainty values, denoted κ_0 and υ_0. Before carrying out the above update, we check the likelihood of X_t given $p_t(\mu_t, \sigma_t^2)$. When $p(X_t \mid \mu_t, \sigma_t^2) < p$, we flag an anomaly at t and reset $\mu_{t+1} = \mu_0$, $\sigma_t^2 = \sigma_0^2$, $\kappa_t = \kappa_0$ and $\upsilon_t = \upsilon_0$. Anomalies are detected in each data stream independently in this Bayesian framework. We apply the detector to voltage *magnitudes* measured at a subset of the system buses. That is, X_t will be the voltage magnitude measurement on one phase of one PMU at time t.

2) Changepoint Detection: We use the CUSUM algorithm to identify the start and end timestamps of an anomaly as well as the amplitude of the deviation. The number of false positives and negatives associated with this identification can be tuned by selecting a proper threshold.

B. Bad data identification

A detected anomaly can either be a physical event or bad data. Bad data in PMU measurement streams is of several types. *Incorrect data* are measurements which are randomly corrupted. This manifests as noisy spikes distributed randomly over the measurement stream. *Missing data* manifests as a zero or "Not a Number" (NaN) value. Sometimes, an entire packet of data is missing. These bad data instances must be removed before events can be localized and classified. However, it is critical that only bad data are removed and true measurements—which carry informative event signatures—are not erroneously replaced. Once all anomalies (encompassing both physical events and bad data) are flagged as described in Section III-A, bad data is identified by considering the similarity of an anomaly across PMUs. A physical anomaly will manifest across PMUs due to the physical links of the network. If an anomaly does not appear across measurement streams, it is classified as bad data. The assumption here is that, the bad data is basically the sensor noise and not an inherent noise in the electrical lines. A physical anomaly carrying the signature of any event change or fault, will propagate at the speed of light and hence its effect will be manifested across the PMUs immediately based on the data sampling interval. As we are working with data sampling rate close to 0.0165 seconds, so any effect of event changes at a particular bus is supposed to propagate to the other PMUs within the same time interval if it is a physical anomaly. On the other hand, the bad data is a random sensor noise which does not appear across all PMUs in the same time interval.

Before the next steps of event localization and classification, the identified bad data are removed. The missing data point is then interpolated with a constant. A single missing point is replaced with the preceding measurement value. Similarly, all points in a missing packet are replaced with the preceding measurement.

C. Event Localization

For event localization, we use nodal voltage measurements only, normalized to be in per-unit (p.u.). With very high time resolution, nodal voltage magnitudes are revealing of the event location. Let $V^{(i)}$ denote the voltage magnitude time series at node i. The i can denote a specific phase and bus, though the events we consider here are visible across phases. Once an event is detected at time t, we compute the absolute value derivatives of the voltage magnitudes at all buses in a 60 sample (1 second) window including the event—i.e. 30 samples preceding and 30 following. Let $\delta V^{(i)}$ denote the absolute value of the 120 sample derivative time series

of voltage magnitude at bus i. Then, the event at time t is localized to index i^* according to:

$$i^* = arg \min_i \delta V^{(i)} \quad (4)$$

Note that the minimum is over every time point at every bus. The physical justification for this approach is based on two simplifying assumptions:

1) An event consists of a change in the power injection at a *single* bus.
2) The following power flow linearization holds: $V \approx RP$ where $V \in \mathbb{R}^N$ is the set of bus voltage magnitudes, $P \in \mathbb{R}^N$ is the set of real power injections at each bus, and $R \in \mathbb{R}^{N \times N}$ is the system resistance matrix.

Under these assumptions, and using the fact that the diagonal elements of R have the largest magnitude [25], Eq. (4) will correctly localize the event to the source bus.

D. Event Classification

Once an event is localized to a particular bus, we aim to classify it into one of five broad categories:

1) **Category 1** (Fault Event: include the faulting of a line in the network).
2) **Category 2** (Load Event: include changes in load real power demand, the switching of real power loads, and load trips).
3) **Category 3** (Capacitor Event: includes capacitor in or out, capacitor switching)
4) **Category 4** (Generation change events: changes in the output of generators).
5) **Category 5** Generator switching and tripping events)

To classify events, we depend on the distinctive time series signatures in certain raw measurements and derived features within a short window preceding and following the event instance. The derived features we use are the percent change in current magnitude, deviation of the rate of change of frequency, and the change in the slope of current angle.

Let $f_1^i, ..., f_m^i$ denote the m feature values corresponding to event i. Suppose we have a total of n events. Then, we have m feature sets: $\mathcal{F}_1 = \{f_1^1, ..., f_1^n\}$ to $\mathcal{F}_m = \{f_m^1, ..., f_1^m\}$. We normalize each feature set as follows. For feature j, we calculate the z-score of each point in the feature set $\mathcal{F}_j = \{f_j^1, ..., f_j^n\}$. We remove outliers from $\mathcal{F}_j$ based on the z-score, and normalize the remaining points so they lie between 0 and 1. We then set all the outliers to 1 and return them to $\mathcal{F}_j$.

Classification begins by identifying fault (Category 1) events, based on the change in the rate of change of frequency ($rocof$). If the change is greater than a threshold τ, the event is classified as type 1. Classification proceeds with sequential k-means clustering, as visualized in the right of Fig. 1. First we cluster the events into two classes with respect to the normalized rate of change of frequency ($norm\_rocof$). The cluster with the minimum centroid, denoted $\mathcal{C}_A$, consists of events in Category (3) or (4) (Capacitor event and generation change events respectively) while the other cluster, denoted $\mathcal{C}_B$, consists of events in Category (2) or (5) (Load event and generator switching or tripping events respectively). We again cluster the events of $\mathcal{C}_A$ into two sets, with respect to the normalized percentage change in current magnitude ($norm\_pccm$). The cluster with the smaller centroid consists of events in Category 3, while the remaining events are in Category 4. Similarly, we cluster the events of $\mathcal{C}_B$ into two sets with respect to the change in current angle slope ($norm\_sca$). The cluster with the smaller centroid consists of events in Category 2, while the other is events in Category 5. In this way, we identify the five event classes.

TABLE I: PMU Location and Observed Measurements.

PMU	Location	Measurements
1	Bus 1	V1, I1-2, f and ROCOF
2	Bus 2	V2, I2-3, f and ROCOF
3	Bus 3	V3, I3-4, f and ROCOF
4	Bus 4	V4, I4-2, f and ROCOF
5	Bus 5	V5, I5-1, f and ROCOF
6	Bus 6	V6, I6-11, f and ROCOF
7	Bus 4	V4, I4-5, f and ROCOF
8	Bus 9	V9, I9-10, f and ROCOF

TABLE II: Performance of Anomaly Detection

PMU	Event Detection						Event & Bad Data Detection	
	Gaussian 30dB		Gaussian 45dB		Laplace		Gaussian 45dB	
	Precision	Recall	Precision	Recall	Precision	Recall	Precision	Recall
1	0.9	0.60	1.0	0.60	0.45	0.6	1.0	0.99
2	0.9	0.60	1.0	0.60	0.47	0.6	1.0	0.99
3	0.85	0.73	1.0	0.73	0.55	0.73	1.0	1.0
4	0.88	1.0	1.0	1.0	0.60	1.0	1.0	0.99
5	0.83	1.0	1.0	1.0	0.63	1.0	1.0	1.0
6	0.79	1.0	1.0	1.0	0.63	1.0	1.0	1.0
7	0.83	1.0	1.0	1.0	0.54	1.0	1.0	0.99
8	0.88	1.0	1.0	1.0	0.63	1.0	1.0	1.0

IV. Results and Discussion

A. Data Simulation Description

We demonstrate our algorithms on simulated measurements from the IEEE 14 bus test system [26]. The system was modeled in Real Time Digital Simulator (RTDS) and simulated under several different events. Eight PMUs were placed on different buses in the IEEE 14 bus system. The location of and quantities measured by each PMU (three-phase voltages and currents, frequency and rate of change of frequency (ROCOF)) are recorded in table I. The PMUs had a 60 Hz sampling rate.

We add noise and bad data effects to the ideal measurements returned by RTDS. We create three noisy data sets each with a different type of noise: Gaussian noise with SNR 30 dB, Gaussian noise with SNR 45 dB, and Laplacian noise. We also artificially add bad data of the three types described in Section III-B: incorrect data, missing data, and missing packets.

B. Evaluation Metrics

We report two performance metrics when evaluating our anomaly detection and bad data detection algorithms. The precision is the ratio of the number of true detected anomalies to the total number of detected anomalies (or bad data).

TABLE III: Performance of Bad Data Identification

	Bad data identification	
PMU number	Precision	Recall
1	0.9632	0.9771
2	0.9499	0.9779
3	0.9485	0.9727
4	0.9468	0.9788
5	0.9450	0.9738
6	0.9712	0.9864
7	0.9443	0.9746
8	0.9472	0.9814

TABLE IV: Event Identification on Noiseless Simulated PMU Data

S No.	Time of operation	Actual Event	Actual Location	Simulated data				
				Classified Category	Detected Bus		Score	
					PMU A	PMU B	PMU A	PMU B
1	56	Cap bank Closed	9	Category 3	9	6	4.5	2.5
2	76	3-Phase fault	Between 2 & 3	Category 1	2	3	4.6×10^3	3.5×10^3
3	96	Load increased	3	Category 2	3	4	29	15
4	116	Generation increased	2	Category 4	2	4	3.0	2.7
5	136	Load Removed	6	Category 2	5	6	44	34
6	156	Generation Removed	3	Category 5	3	4	360	200
7	176	Load decreased	3	Category 2	3	4	83	43
8	196	1-phase to ground fault	Between 3 & 4	Category 1	3	4	5.8×10^3	3.1×10^3
9	216	Generation decreased	2	Category 4	3	2	3.5	3.3
10	236	Load decreased	4	Category 2	4	9	28	26
11	256	Load Switched ON	6	Category 2	5	4	37	33
12	276	Cap bank Removed	9	No Detection	-	-	-	-
13	276	Load Removed	6	Category 2	5	4	41	32
14	296	3-Phase fault	Between 2 & 3	Category 1	2	3	5.4×10^3	4.1×10^3
15	316	Load Decreased	9	Category 2	9	4	56	35

The recall is the ratio of the number of true detected anomalies to the total number of true anomalies. A low precision implies many false positives, while a low recall implies many false negatives. Let $\mathcal{T}_d = \{t_1, ..., t_d\}$ denotes the set of detected anomalies or bad data and $\mathcal{T}_g = \{t_1, ..., t_g\}$ denote the set of ground truth anomalies or bad data. Mathematically:

$$Precision = \frac{\mathcal{T}_d \cap \mathcal{T}_g}{\mathcal{T}_d} \tag{5}$$

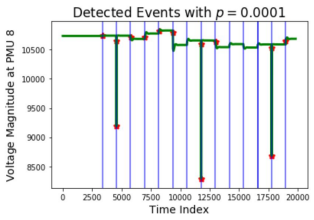
$$Recall = \frac{\mathcal{T}_d \cap \mathcal{T}_g}{\mathcal{T}_g} \tag{6}$$

C. Simulation Results and Validation

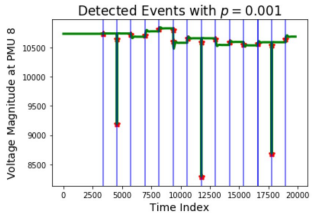
We separately report the performance of each piece of our algorithm workflow.

First, we run the anomaly detection described in Section III-A on PMU measurements with Gaussian noise and those with bad data. The anomaly detection algorithm may flag multiple points corresponding to the same anomaly (especially in the case of events). Therefore, we consolidate all flagged points within 2 seconds as a single event. Fig. 2 visualizes the performance of the algorithm on one stream of noisy PMU measurements for different choices of the anomaly probability threshold p. We see that too small a p misses several events, while too large a p leads to too much noise being flagged as an event. Based on these results, we set $p = 0.001$ and apply the anomaly detection to noisy measurements containing both bad data and physical events. The algorithm flags both bad data and physical events. These are then classified and can be handled differently (for example, bad data is cleaned, while physical events generate a warning). The results across the PMU measurements are summarized in table II. Notice the performance variation across PMUs. This is because, depending on the event location, event visibility varies across the PMUs. However, as long as every event is detected at *some* PMU, the algorithm performance is unaffected.

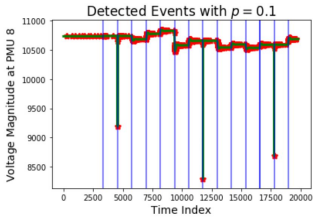
Of the resulting anomalies, we must detect and replace those that are bad data. It is necessary to identify three different types of bad data, according to the algorithm of Section III-B. Table III reports the performance of this algorithm. In table III, the ability to detect the inserted bad data scores above 94% and



(a) $p = 0.0001$



(b) $p = 0.001$



(c) $p = 0.01$

Fig. 2: (a)-(c) Visualization of event detection performance on one stream of PMU measurements for different choices of anomaly threshold probability (p). Vertical blue lines indicate ground truth of event occurrence. Red stars indicate events flagged by algorithm.

100% in the precision metric for missing data and missing packet, whereas the recall metric is above 97% for bad data and 100% for missing data and missing packet for all PMU streams.

Those anomalies which are not bad data are physical events. These events are localized to a source bus by the algorithm of Section III-C. The current limitation of our approach is that it can not separately identify the locations of simultaneous events. Similarly, events associated with lines between buses are localized to a single bus. Once the event is localized, measurements at the source bus are used to classify the event type according to the process described in Section III-D. The simulation result for noiseless simulated PMU data for the test system can be seen from table IV. It is clear from table IV that all the events were localized and classified successfully except three events, the load event on bus 6 at

TABLE V: Event identification on Simulated PMU Data with Measurement noise

S No.	Time of operation	Actual Event	Actual Location	PMU data with gaussian noise					PMU data with Laplacian noise				
				Classified Category	Detected Bus		Score		Classified Category	Detected Bus		Score	
					PMUA	PMUB	PMUA	PMUB		PMUA	PMUB	PMUA	PMUB
1	56	Cap bank Closed	9	Category 3	9	6	4.6	2.5	Category 3	9	6	4.5	2.4
2	76	3-Phase fault	Between 2 & 3	Category 1	2	3	4.6×10^{3}	3.5×10^{3}	Category 1	2	3	4.6×10^{3}	3.5×10^{3}
3	96	Load increased	3	Category 2	3	4	29	15	Category 2	3	4	29	15
4	116	Generation increased	2	Category 4	2	4	2.9	2.8	Category 4	2	4	2.9	2.7
5	136	Load Removed	6	Category 2	5	6	44	34	Category 2	5	6	44	34
6	156	Generation Removed	3	Category 5	3	4	360	200	Category 5	3	4	360	200
7	176	Load decreased	3	Category 2	3	4	83	43	Category 2	3	4	83	43
8	196	1-phase to ground fault	Between 3 & 4	Category 1	3	4	5.8×10^{3}	3.1×10^{3}	Category 1	3	4	5.8×10^{3}	3.1×10^{3}
9	216	Generation decreased	2	Category 4	3	2	3.5	3.3	Category 4	3	2	3.5	3.3
10	236	Load decreased	4	Category 2	4	9	28	26	Category 2	4	9	28	26
11	256	Load Switched ON	6	Category 2	5	4	37	33	Category 2	5	4	37	33
12	276	Cap bank Removed	9	No Detection	-	-	-	-	No Detection	-	-	-	-
13	276	Load Removed	6	Category 2	5	4	41	32	Category 2	5	4	41	32
14	296	3-Phase fault	Between 2 & 3	Category 1	2	3	5.4×10^{3}	4.1×10^{3}	Category 1	2	3	5.4×10^{3}	4.1×10^{3}
15	316	Load Decreased	9	Category 2	9	4	56	35	Category 2	9	4	56	35

136 sec and 276 sec was wrongly localized but classified correctly and Capacitor switching on bus 9 at 276 sec. At 276 sec, two events happened simultaneously and the load event dominated the capacitor switching.Tables V contain the results of event localization and classification on the noisy measurement streams. In this work, we have considered two noise models, namely (1) Gaussian noise with two levels, 30 dB (a conservatively high noise level) and 45 dB (a realistic noise level); and (2) Laplacian measurement noise with zero mean and scale parameter 0.001. By comparing the result in table-IV and table-V shows that the proposed method is robust enough to deal with the measurement noise.

V. Conclusions

In this work, realistic synchrophasor data has been generated considering noise and cyber-physical events. Algorithms have been developed using a suite of mathematical and statistical techniques for anomaly and event detection and localization, including a multi-step clustering approach for event classification. The simulation results demonstrate the efficacy of the algorithm to detect, locate and classify the events, even in the presence of measurement noise. In the future, root cause analysis and proactive control actions to minimize impact of physical and cyber-intrusions using PMU, SCADA telemetry measurement and cyber logs will be integrated into the developed algorithm. Furthermore, more cyber-attack scenarios will be modeled and expanded for classification models to distinguish known attacks, as part of the future work.

References

[1] V. Terzija, G. Valverde, D. Cai, P. Regulski, V. Madani, J. Fitch, S. Skok, M. M. Begovic, and A. Phadke, "Wide-area monitoring, protection, and control of future electric power networks," *Proceedings of the IEEE*, vol. 99, no. 1, pp. 80–93, Jan 2011.

[2] J. De La Ree, V. Centeno, J. S. Thorp, and A. G. Phadke, "Synchronized phasor measurement applications in power systems," *IEEE Transactions on smart grid*, vol. 1, no. 1, pp. 20–27, 2010.

[3] A. Kummerow, D. Rösch, C. Monsalve, S. Nicolai, P. Bretschneider, C. Brosinsky, and D. Westermann, "Challenges and opportunities for phasor data based event detection in transmission control centers under cyber security constraints," in *2019 IEEE Milan PowerTech*, June 2019, pp. 1–6.

[4] NASPI, "Power system oscillatory behaviors: Sources, characteristics, & analyses," 2017.

[5] ——, "Using synchrophasor data during system islanding events and blackstart restoration," 2015.

[6] ——, "Diagnosing equipment health and mis-operations with pmu data." 2015.

[7] B. Cui, A. K. Srivastava, and P. Banerjee, "Automated failure diagnosis in transmission network protection system using synchrophasors," *IEEE Transactions on Power Delivery*, vol. 33, no. 5, pp. 2207–2216, Oct 2018.

[8] M. Cui, J. Wang, A. R. Florita, and Y. Zhang, "Generalized graph laplacian based anomaly detection for spatiotemporal micropmu data," *IEEE Transactions on Power Systems*, vol. 34, no. 5, pp. 3960–3963, Sep. 2019.

[9] S. Sridhar and M. Govindarasu, "Model-based attack detection and mitigation for automatic generation control," *IEEE Transactions on Smart Grid*, vol. 5, no. 2, pp. 580–591, March 2014.

[10] D. Pokrajac, A. Lazarevic, and L. J. Latecki, "Incremental local outlier detection for data streams," in *Computational intelligence and data mining, 2007. CIDM 2007. IEEE symposium on*. IEEE, 2007, pp. 504–515.

[11] M. Zhou, Y. Wang, A. K. Srivastava, Y. Wu, and P. Banerjee, "Ensemble-based algorithm for synchrophasor data anomaly detection," *IEEE Transactions on Smart Grid*, vol. 10, no. 3, pp. 2979–2988, May 2019.

[12] A. Ahmed, V. V. G. Krishnan, S. A. Foroutan, M. Touhiduzzaman, C. Rublein, A. Srivastava, Y. Wu, A. Hahn, and S. Suresh, "Cyber physical security analytics for anomalies in transmission protection systems," *IEEE Transactions on Industry Applications*, vol. 55, no. 6, pp. 6313–6323, Nov 2019.

[13] S. Pan, T. Morris, and U. Adhikari, "Developing a hybrid intrusion detection system using data mining for power systems," *IEEE Transactions on Smart Grid*, vol. 6, no. 6, pp. 3104–3113, 2015.

[14] Y. Chen, L. Xie, and P. Kumar, "Dimensionality reduction and early event detection using online synchrophasor data," in *Power and Energy Society General Meeting (PES), 2013 IEEE*. IEEE, 2013, pp. 1–5.

[15] L. Xie, Y. Chen, and P. R. Kumar, "Dimensionality reduction of synchrophasor data for early event detection: Linearized analysis," *IEEE Transactions on Power Systems*, vol. 29, no. 6, pp. 2784–2794, 2014.

[16] P. Trachian, "Machine learning and windowed subsecond event detection on pmu data via hadoop and the openpdc," in *Power and Energy Society General Meeting, 2010 IEEE*. IEEE, 2010, pp. 1–5.

[17] Y. Zhou, R. Arghandeh, I. Konstantakopoulos, S. Abdullah, A. von Meier, and C. J. Spanos, "Abnormal event detection with high resolution micro-pmu data," in *Power Systems Computation Conference (PSCC), 2016*. IEEE, 2016, pp. 1–7.

[18] Y. Dong and N. Japkowicz, "Threaded ensembles of autoencoders for stream learning," *Computational Intelligence*, vol. 34, no. 1, pp. 261–281, 2018.

[19] P. J. Rousseeuw and M. Hubert, "Robust statistics for outlier detection," *Wiley Interdisciplinary Reviews: Data Mining and Knowledge Discovery*, vol. 1, no. 1, pp. 73–79, 2011.

[20] Y. Dong and N. Japkowicz, "Threaded ensembles of autoencoders for stream learning," *Computational Intelligence*, vol. 34, no. 1, pp. 261–281, 2018.

[21] M. Brown, M. Biswal, S. Brahma, S. Ranade, and H. Cao, "Characterizing and quantifying noise in pmu data," in *2016 IEEE Power and Energy Society General Meeting (PESGM)*. IEEE.

[22] M. Bariya, K. Moffat, and A. von Meier, "Empirical noise estimation in distribution synchrophasor measurements," in *International Conference on Smart Grid Synchronized Measurements and Analytics (SGSMA)*. IEEE, 2019.

[23] E. S. Page, "Continuous inspection schemes," *Biometrika*, vol. 41, no. 1-2, pp. 100–115, 06 1954.

[24] K. P. Murphy, "Conjugate bayesian analysis of the gaussian distribution."

[25] P. V. Mieghem, K. Devriendt, and H. Cetinay, "Pseudoinverse of the laplacian and best spreader node in a network." *Physical Review E*, vol. 96, 2017.

[26] IEEE, "IEEE std 14-bus system. available online:," https://icseg.iti.illinois.edu/ieee-14-bus-system/, accessed: 10-25-2019.