IET Smart Grid

*Special Section: Privacy and Security in Smart Grids*

IET Journals
The Institution of Engineering and Technology

# Ensemble CorrDet with adaptive statistics for bad data detection

eISSN 2515-2947
Received on 31st January 2020
Revised 27th May 2020
Accepted on 22nd June 2020
E-First on 14th July 2020
doi: 10.1049/iet-stg.2020.0029
www.ietdl.org

*Keerthiraj Nagaraj[1], Sheng Zou[1], Cody Ruben[1] ✉, Surya Dhulipala[1], Allen Starke[1], Arturo Bretas[1], Alina Zare[1], Janise McNair[1]*

[1]*Electrical and Computer Engineering, University of Florida, 1064 Center Dr, Gainesville, FL, USA*

✉ *E-mail: cruben31@ufl.edu*

**Abstract:** Smart grid (SG) systems are designed to leverage digital automation technologies for monitoring, control and analysis. As SG technology is implemented in increasing number of power systems, SG data becomes increasingly vulnerable to cyber-attacks. Classic analytic physics-model based bad data detection methods may not detect these attacks. Recently, physics-model and data-driven methods have been proposed to use the temporal aspect of the data to learn multivariate statistics of the SG such as mean and covariance matrices of voltages, power flows etc., and then make decisions based on fixed values of these statistics. However, as loads and generation change within a system, these statistics may change rapidly. In this study, an adaptive data-driven anomaly detection framework, Ensemble CorrDet with Adaptive Statistics (ECD-AS), is proposed to detect false data injection cyber-attacks under a constantly changing system state. ECD-AS is tested on the IEEE 118-bus system for 15 different sets of training and test datasets for a variety of current state-of-the-art bad data detection strategies. Experimental results show that the proposed ECD-AS solution outperforms the related strategies due to its unique ability to capture and account for rapidly changing statistics in SG.

## Nomenclature

| | |
|---|---|
| $d$ | number of measurements – $\mathbb{R}^{1\times 1}$ |
| $\boldsymbol{z}$ | vector of measurements – $\mathbb{R}^{1\times d}$ |
| $\boldsymbol{Z}$ | training set – $\mathbb{R}^{d\times K_1}$ |
| $\hat{\boldsymbol{Z}}$ | testing set – $\mathbb{R}^{d\times K_2}$ |
| $K_1$ | number of samples in training set – $\mathbb{R}^{1\times 1}$ |
| $K_2$ | number of samples in testing set – $\mathbb{R}^{1\times 1}$ |
| $N$ | number of states – $\mathbb{R}^{1\times 1}$ |
| $\boldsymbol{\Sigma}$ | covariance of measurement vector – $\mathbb{R}^{d\times d}$ |
| $\delta^{\mathrm{ECD-AS}}$ | squared Mahalanobis distance value – $\mathbb{R}^{1\times 1}$ |
| $\boldsymbol{\mu}$ | mean of measurement vector – $\mathbb{R}^{1\times d}$ |
| $\tau$ | threshold value to classify abnormal samples on $\Phi_R$ – $\mathbb{R}^{1\times 1}$ |
| $\tau_m$ | threshold value to classify abnormal samples on $\phi_m$ – $\mathbb{R}^{1\times 1}$ |
| $\boldsymbol{T}$ | set of $\tau$ ($\mathbb{R}^{1\times M}$) |
| $\alpha$ | weight value for incoming data sample – $\mathbb{R}^{1\times 1}$ |
| $\eta$ | magnitude parameter for threshold estimation – $\mathbb{R}^{1\times 1}$ |
| $\beta$ | window size for threshold update – $\mathbb{R}^{1\times 1}$ |
| $M$ | number of buses/local CorrDet detectors with adaptive statistics – $\mathbb{R}^{1\times 1}$ |
| $\boldsymbol{Y}$ | label for training samples – $\mathbb{R}^{1\times K_1}$ |
| $\hat{\boldsymbol{Y}}$ | label for testing samples – $\mathbb{R}^{1\times K_2}$ |
| $\phi_m$ | symbol for $m$th Local CorrDet with adaptive statistics detector |
| $\Phi_{\mathrm{E}}$ | symbol for Ensemble CorrDet with adaptive statistics detector |
| $\Phi_{\mathrm{R}}$ | symbol for CorrDet detector |
| $\mu_{\mathrm{thr},m}$ | mean of the Mahalanobis distance values of $\boldsymbol{z}_m$ of all normal samples in training data |
| $\sigma_{\mathrm{thr},m}$ | variance of the Mahalanobis distance values of $\boldsymbol{z}_m$ of all normal samples in training data |

## 1 Introduction

As a sensor, communication, control, and other technologies continue to advance into the digital age, the power systems industry begins to transition to the smart grid (SG). These next-generation power systems aim to achieve greater stability, efficiency and robustness of the physical processes on the grid through the integration of control, communication and computation. With the transition toward the SG paradigm and advanced technology implementations, there is an increasing vulnerability to cyber-threats, especially among critical infrastructures [1]. Although the technologies themselves have advanced rapidly, research into the cyber-physical security of SGs is still immature. In recent years, two major cyber-attacks on power grids have occurred. The first confirmed blackout from a cyber-attack on a power grid happened in Ukraine and caused a power outage that affected 225,000 customers [2, 3]. The Stuxnet malware was used to implement a malicious cyber-attack on Iran's Nuclear Technology Center, destroying a large number of centrifuges [4].

To guarantee the reliable operation of power grids, it is crucial to have accurate monitoring of the power system. Currently, real-time monitoring is performed using Power System State Estimation (PSSE) [5]. PSSE uses static and dynamic data to provide information about the condition of the system. These readings are commonly transmitted to a Supervisory Control and Data Acquisition (SCADA) system, which implements centralised monitoring and control for the electrical grid, Before state estimation, the data is pre-filtered to discard measurements that are clearly inconsistent or incorrect. After state estimation using pre-filtered data, a post-processing step called 'bad data analysis' is performed to detect bad data or gross errors (GEs), which correspond to statistically large errors.

To guarantee cyber-security, SG research must address relevant types of cyber attacks. One key concern is false data injection (FDI).

In an FDI attack, a subset of measurement values is modified by an adversarial attacker aiming to disrupt the operation of the power grid. Physics-model based Bad Data Analysis is capable of detecting many instances of GE via tests such as $J(\hat{x})$ [5], largest normalised residual [6], or innovation-based [7–10] approaches.

However, cyber-attacks can be engineered to be very difficult to detect in measurement data [11–18]. Methods devised to treat FDI attacks include Generalised Likelihood Ratio Detector with L-1 Norm Regularisation [19], a scheme for protecting a selected set of measurements and verifying the values of a set of state variables independently [20] and the estimation of the normalised composed measurement error for detection of malicious data attacks [8, 9].

Another advancement in bad data analysis in power systems is the surge in machine learning and artificial intelligence research. These studies are mainly based on neural network, deep learning and fuzzy clustering approaches [21–24]. More recently, physics-model based solutions have been integrated with data-driven solutions [25, 26] to take advantage of the temporal characteristics of real-time data. However, these solutions struggle with the fast-changing state of power systems. As both loads and generation change on a power system, the statistics used by data-driven solutions can change rapidly. In [26], the authors introduce the Ensemble CorrDet (ECD) algorithm, a hybrid physics-model based and data-driven method of FDI detection. However, the ECD algorithm described and leveraged in [26] uses fixed estimated mean and covariance of normal samples after training rather than adapting to the changing state of power systems. This means that when applied to a realistic load profile for power systems, ECD statistics will quickly become outdated and the performance of the algorithm will decrease. There is a need for new algorithms that can adapt to the real-time environment. This can be accomplished by applying prediction techniques, such as using the maximum likelihood estimate of the prediction weights in a linear prediction model [27].

In this paper, we present an enhanced, adaptive and responsive data-driven method for FDI cyber-attack detection, called Ensemble CorrDet with Adaptive Statistics (ECD-AS), that accounts for the rapidly changing power system state of the SG. This new algorithm makes the following novel contributions:

- Explores the time-varying nature of real-time power systems and their impact on bad data detection, using a common daily load profile-based data set.
- Employs 'adaptive statistics', including adaptive mean, adaptive covariance, and adaptive anomaly thresholds.
- Implements a sliding window approach to update the statistics based on recent samples.
- It is demonstrated that CD and ECD cannot capture the temporal changing dynamics of the various buses and fail to separate normal samples from anomalous samples, while these cases can be successfully addressed in the proposed ECD-AS framework.

The remainder of the paper is organised as follows. A literature review and relevant background information for the proposed framework are shown in Section 2. Section 3 presents the details of the proposed ECD-AS algorithm. The numerical results, as well as an analysis of the tests used in the performance evaluation, are shown in Section 4. Finally, Section 5 presents the conclusions of this work.

## 2 Background information

This section provides a review of background literature and information about the foundational work related to the presented framework.

### *2.1 Literature review*

Since the invention of PSSE, the problem of bad data detection has been a topic of great interest [5]. At first, GEs were considered to come only from faulty meters or communication errors, but the advent of SG has introduced the threat of cyber-attacks and increased potential for system-harming GEs [1–4]. The FDI attack in which a subset of measurement values is modified can have significant impacts on a power system if it goes undetected. These impacts include overloading transmission lines, damaging equipment, or potentially causing blackouts [28–32].

*2.1.1 Physics-based techniques:* To combat the problem of GEs in PSSE, much research has been done using the physics-model based framework, i.e. using the known topology of a power system, along with real-time measurements, to estimate the voltages at each bus throughout the system (the state). The results of PSSE are the state estimation itself and residual value for each real-time measurement used to complete the PSSE process. The basic approach to detecting GE is to analyse those residual values using the common chi-square test to determine if the residuals are statistically large for that set of measurement values [5]. From there, research in [6] explored the use of the largest normalised residual test as a detection method. Later on, the authors of [33] expand upon the chi-square test, using the normalised residual within the test itself and showed significant improvement. Another significant improvement upon the chi-square test came along when the geometrical interpretation of the measurement residuals was explored [34]. With this geometrical view of the PSSE process, it was discovered that errors and residuals were in different mathematical spaces. Because of this, there existed an undetectable component of the measurement error that was not captured by the residual values. The Innovation Index was developed to mathematically calculate this undetectable component, which was used to compute the Composed Measurement Error. The Innovation concept was explored and expanded upon in a variety of papers [7–10, 35].

Other potential methods of FDI treatment such as [19, 20] deviate from the standard processes of utility companies without enough improvement upon chi-square test strategies to warrant their implementation. All of the chi-square based methods above are easily implemented using the already existing results of the PSSE process. Therefore, this paper uses the method from [9] as the baseline test for physics-model based FDI detection. However, one major limitation that all of these physics-model based methods share is that they are quasi-static strategies, meaning they essentially look at a single snapshot in time and analyse only that single snapshot. Especially with the increasing amount of data that comes with the SG, it makes sense to develop a strategy that uses not only spatial information (topology and measurements), but temporal information as well (previous measurements). This makes machine learning techniques an obvious candidate, which has led to much research applying machine learning to the PSSE bad data analysis problem.

*2.1.2 Machine learning-based techniques:* A variety of machine learning methods have been developed to detect FDI attacks in the literature. Some methods rely on neural network-based approaches to identify FDI samples, such as using a simple neural network architecture [24] or deep belief networks [21, 23]. Neural network-based methods are capable of learning a non-linear classifier to detect abnormal samples but with the high cost of computation complexity especially when the network is deep. Another work by Ozay *et al*. [22] investigated some of the commonly used machine learning methods, such as *K*-nearest neighbour (KNN), support vector machine and sparse logistic regression to detector FDI samples. However, only temporal information of data is considered in these models, while spatial, localised relationship are ignored. The authors in [36] proposed ELM-based One-Class-One-Network framework to detect FDI attacks and test it on IEEE-14 bus system. This framework considers a distributed approach by having a separate deep learning model for each bus and a global layer for final decision making which enables the framework to detect multiple simultaneous FDI attacks. A deep learning model for each bus makes this framework data and computation intense. Although this framework uses spatial relationships in the grid, it fails to capture temporal variations in the normal and abnormal data as the model does not update over time. Modified k-NN has been proposed in [37] to detect FDI attacks in sensors for a smart infrastructure setting. The authors focus their tests on data collected from sensors placed inside a single building to avoid computation issues and compare the performance of modified k-NN with other machine learning approaches using accuracy metric. Accuracy fails to effectively capture model performance for unbalanced data which is usually

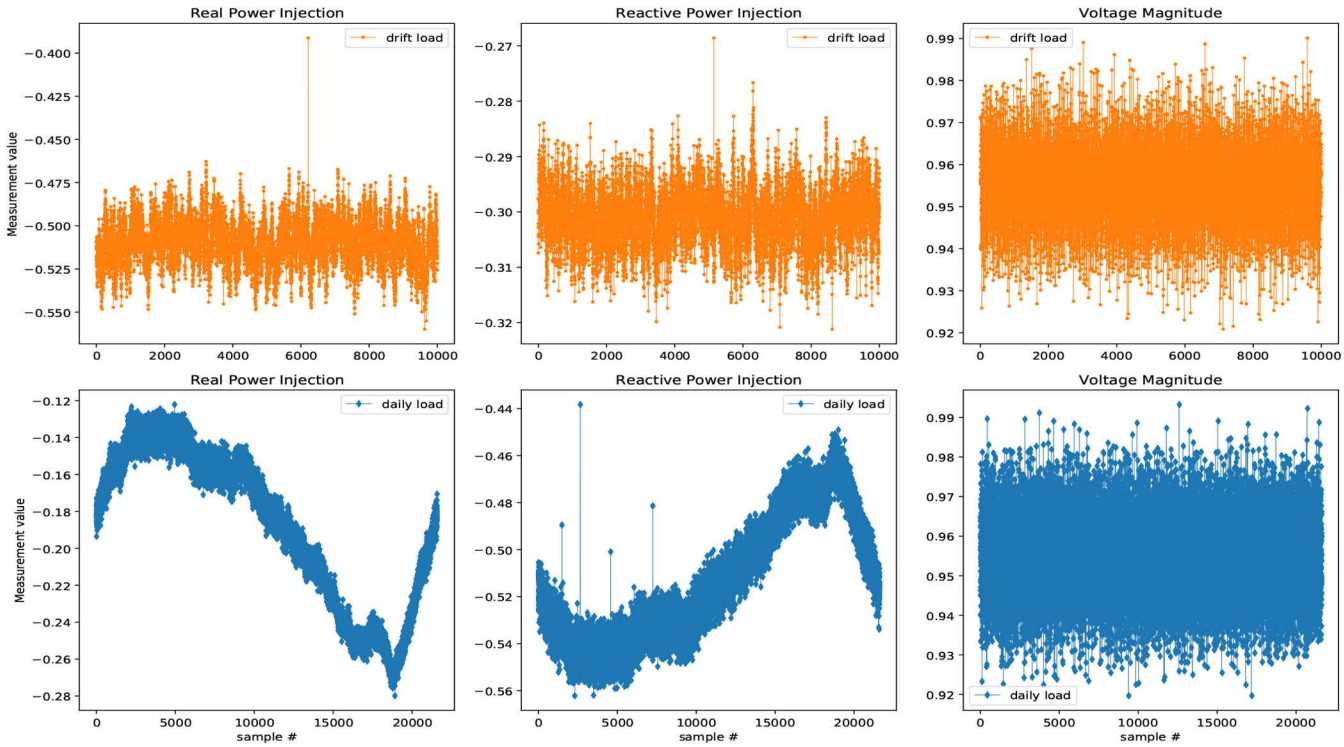


**Fig. 1** *Comparison of measurement values for drift load profile (first row plots) and daily load profile datasets (second row plots)*

the case for FDI attacks. The proposed scheme incurs high computational cost when the number of sensors increases due to the usage of k-NN based algorithm. Ashrafuzzaman *et al*. [38] proposed a simple deep learning-based model for FDI attack detection using Multi-Layer Perceptron Neural Network (MLPNN) and compare the attack detection capabilities of their scheme with other machine learning approaches on IEEE-14 bus system. The proposed scheme fails to capture both spatial correlations of the measurements and temporal variations in the data even when the load profile used is not realistic. Choosing values for a variety of hyper-parameters in the MLPNN model also becomes an issue as large amount of training data is needed select optimal values and model tuning.

### *2.2 Foundation for the proposed data-driven scheme*

The CorrDet anomaly detection algorithm [27, 39] is initialised with a sample mean and covariance matrix for the first $k$ number of incoming samples that are not labelled as anomalies to generate statistics for underlying distribution of normal samples and to make a linear prediction of the next sample. However, in our current implementation we simply use first $k$ number of incoming samples to estimate the sample mean and covariance matrix of the normal samples, and future work could investigate linear prediction.

Using these initialised mean and covariance values for normal samples, the squared Mahalanobis distance [40] of a new incoming sample is calculated. The computed distance measure is compared to a decision threshold. If the distance measure is below the threshold, then a new sample is detected as a normal sample. Otherwise, the new sample is flagged as an anomaly. For the dynamic dataset, the CorrDet detector provides a way to adapt statistics with changing trends. Each time a new sample is detected as normal, mean and covariance matrices can be updated using the Woodbury Matrix Identity [41–43]. CD algorithm with fixed statistics was proposed for FDI detection in a dataset where the load profile was kept constant, but with random white noise added to the system in [25]. The authors used fixed statistics in this work as the load profile of the power system does not change for different buses over time. CD algorithm with fixed statistics performs poorly for a dataset that has drifting load profile and when different buses in power systems have different local statistics, as a full mean and covariance matrix estimated during the training phase of CD algorithm with fixed statistics fails to capture these dynamics.

The ECD algorithm extended the strategies from the CD algorithm and applied it to a dataset that has a drifting load profile in [26]. The drift was modelled by the Ornstein–Uhlenbeck process [44], which is a stochastic process similar to a random walk, but has a tendency to move back towards the original load. This presents a greater challenge to the data-driven solution since the statistics of the different measurements in the power system will no longer be similar. ECD algorithm provides a distributed anomaly detection scheme while combining measurements using the spatial information of the power system, to form local anomaly detector that learns normal statistics for each bus based on the concept of CD algorithm. An optimal threshold is selected for each local anomaly detector and the results are combined with physics-based solution to make final decisions on FDI detection. This work uses fixed statistics for each local anomaly detector and does not update them after initial training as the state of different buses in power systems does not change over time in a drifting load dataset. ECD algorithm performs poorly for a dataset that has varying system states over time like a common daily load profile, which is more realistic compared to constant load profile or drifting load profile. Fig. 1 shows how different measurements such as Real Power Injection, Reactive Power Injection, Voltage Magnitude change over time for drifting load profile and daily load profile. We can observe that especially different power measurements have large varying normal statistics over time compared to drifting load profile even though variation voltage magnitude is fairly similar for different load profiles. The daily load profile considered in this work has a measurement set that includes real and reactive power flows, real and reactive power injections, and all voltage magnitudes in the grid.

In previous work [25, 26], the anomaly detection threshold is a fixed value estimated from the initialisation stage and not updated with new incoming data. Specifically, the standard deviation and mean of squared Mahalanobis distance values of initial $k$ normal samples are calculated first. The threshold that results in the highest $F1$-score for $k$ training normal samples is selected as optimal for testing phase for the entire system in [25] and each local anomaly detector in [26]. The authors now propose a novel approach that integrates machine learning techniques to enable an anomaly detection algorithm with an adaptive response to the real-time environment.

## 3 Ensemble CorrDet with adaptive statistics

We envision a machine learning layer of the smart power grid that uses the knowledge of already verified data to learn the normal state of a properly functioning grid. Once the normal state is known (estimated), the system will then be able to detect anomalies introduced into the system as well as alert a network and communications layer (network layer). The network layer can then identify the source of the anomaly, isolate it from the remainder of the system and take appropriate action to prevent contamination within the connected power distribution systems and within the data assimilation itself.

As mentioned previously, the proposed ECD-AS algorithm extends the work of the CorrDet [25] algorithm and the ECD algorithm [26]. ECD-AS can be interpreted as a set of CorrDet detectors where adaptive statistics are collected for each local CorrDet environment. The CorrDet anomaly detector (CD) learns a set of statistics, ($\boldsymbol{\mu}$, $\Sigma$ and $\tau$) for all buses $\Phi_{\mathrm{R}}$ in power grid topology, and ECD detector learns a series of statistics ($\boldsymbol{\mu}_m$, $\Sigma_m$ and $\tau_m$), one for each bus $\phi_m$. The ECD-AS detectors learn a series of statistics ($\boldsymbol{\mu}_m$, $\boldsymbol{\Sigma}_m$ and $\tau_m$), one for each bus $\phi_m$ and then processes them with new incoming data samples to adapt them. In this work, an adaptive mean and covariance estimation of normal samples is developed, as well as an adaptive threshold strategy.

Furthermore, learning the full covariance over all measurements of all buses in the SG is costly and unnecessary (nearly sparse covariance), especially when training data is limited. In the SG topology, spatially neighbouring buses are more highly correlated and can be more easily affected by an attack, while buses that are further apart have lower correlation. We focus on data from local buses with fewer dimensional measurement sets to offer a more accurate statistic estimation and a computationally cheaper, more sensitive anomaly detection. Unlike the previous algorithms, ECD-AS prevents the numerical issue of estimating a high-dimensional mean and covariance for the distribution of the normal samples (in CorrDet detector) in the space of all measurements when the number of measurements is high and the number of training samples is low, by learning a lower-dimensional statistics in the space of only the measurements associated with each bus.

Let the total number of measurements be $d$. There are $m_j, m_j < d$, measurements on each bus $m$, where each bus is considered as a local, spatial region, corresponding to one Local CorrDet detector with adaptive statistics, $\phi_m$. For $\Phi_{\mathrm{R}}$, the learning process consists of estimating $\boldsymbol{\mu}$ and $\boldsymbol{\Sigma}^{-1}$ from normal training samples $z$ ($z \in \mathbb{R}^{1\times d}$). A similar strategy is proposed to learn the series of statistics for the ECD-AS detector. The learning of $\Phi_{\mathrm{E}}$ involves the estimation of a set of Local CorrDet detectors with adaptive statistics, $\phi_m$. For each $\phi_m$, similarly, the learning process consists of estimating its $\boldsymbol{\mu}_m$ and $\boldsymbol{\Sigma}_m^{-1}$ from the normal training samples with selected measurements $z_m$ ($z_m$ is a $1 \times m_j$ vector).

First, the $\boldsymbol{\mu}_m$ and $\boldsymbol{\Sigma}_m^{-1}$ are initialised with the sample mean and with the covariance of selected measurements of the first $k$ samples that are labelled as normal. Then, the detector starts to accept new samples and classify each new sample as follows. For each new incoming sample $z$, a set of squared Mahalanobis distances, $\delta_m^{\mathrm{ECD-AS}}$, are computed using (1)

$$\delta_m^{\mathrm{ECD-AS}}(z_m) = (z_m - \boldsymbol{\mu}_m)^T \boldsymbol{\Sigma}_m^{-1}(z_m - \boldsymbol{\mu}_m), \tag{1}$$

where $\boldsymbol{\mu}_m$ is the mean and $\boldsymbol{\Sigma}_m^{-1}$ is the inverse covariance matrix of normal samples on the mth local CorrDet detector. Then, the Mahalanobis distances are compared with the corresponding set of thresholds, $T$, where $T = \{\tau_m\}_{m=1:M}$. If at least one squared Mahalanobis distance in $\Phi_{\mathrm{E}}$ is greater than its corresponding threshold, this incoming sample is classified as an anomaly. Otherwise, it is classified as a normal sample.

Furthermore, for each new sample that is classified as normal, the anomaly detector must be able to adapt with changing trends to be able to capture data that is dynamic and changes gradually over time. Therefore, the mean, $\mu_{\boldsymbol{m}}$ and inverse covariance matrix, $\boldsymbol{\Sigma}_m$ are updated using the Woodbury Matrix Identity [41–43] using (2) and (3), respectively. Note that this update is done only if the incoming data is considered normal data. The mean will be updated such that

$$\boldsymbol{\mu}_{\mathrm{new},m} = (1-\alpha)\boldsymbol{\mu}_m + \alpha(z_m - \boldsymbol{\mu}_m)', \tag{2}$$

while the inverse covariance matrix is updated by

$$\sum_{\mathrm{new},m}^{-1} = \frac{1}{1-\alpha}\left[\sum_m^{-1} = \frac{(z_m - \boldsymbol{\mu}_m)(z_m - \boldsymbol{\mu}_m)^T}{(1-\alpha/\alpha) + (z_m - \boldsymbol{\mu}_m)^T(z_m - \boldsymbol{\mu}_m)}\right], \tag{3}$$

where $\boldsymbol{\mu}_m$ is the old mean of mth local CorrDet detector with adaptive statistics, $\boldsymbol{\Sigma}_m^{-1}$ is the old inverse covariance matrix of mth local CorrDet detector with adaptive statistics and $\alpha$ is a hyper-parameter value between zero and one that determines how much importance is given to the new data sample versus the old mean. We determine the value of $k$ and $\alpha$ through experimentation.

The threshold can be assumed to be fixed for a dataset that has constant mean and small variation in the time domain. A fixed threshold $T = \{\tau_m\}_{m=1:M}$ can be estimated using (4)

$$\boldsymbol{\tau}_m = \boldsymbol{\mu}_{\mathrm{thr},m} + \eta \times \boldsymbol{\sigma}_{\mathrm{thr},m}, \tag{4}$$

where $\boldsymbol{\mu}_{\mathrm{thr},m}$ and $\boldsymbol{\sigma}_{\mathrm{thr},m}$ are the mean and standard deviation of the squared Mahalanobis distance values of all normal training samples, respectively, with selected measurements associated with mth local CorrDet detector with adaptive statistics.

The fixed threshold assumption holds on a dataset that has constant mean and small variation in the time domain such as constant load profile and drifting load profile. However, for the daily load profile dataset in this work, the statistics of normal samples have a larger dynamically changing mean and covariance with time as shown in Fig. 1. This ensures that the previously fixed threshold assumption does not hold. So, in addition to adaptive mean and covariance estimation of normal samples, an adaptive threshold strategy is presented.

Unlike the fixed threshold estimation in CD algorithm and the authors' previous ECD algorithm, adaptive threshold estimation in the proposed ECD-AS algorithm initialises the threshold values $\tau_m$ for each local CorrDet detector with adaptive statistics (bus-level) following (4), and updates $\tau_m$ in an online sliding window fashion. For every new incoming sample $z$, the threshold values $\tau_m$ are inferred from the most recent $\beta$ normal samples before it. In other words, the standard deviation ($\sigma_{\mathrm{thr},m,-\beta}$) and mean ($\boldsymbol{\mu}_{\mathrm{thr},m,-\beta}$) of squared Mahalanobis distance values of $\beta$ normal samples past of the new sample $z$ are calculated for each local CorrDet detector with adaptive statistics $\phi_m$. Here $\beta$ is the sliding window size. The threshold value $\tau_m$ for each local CorrDet detector with adaptive statistics is updated using (5) with updated $\boldsymbol{\mu}_{\mathrm{thr},m,-\beta}$ and $\sigma_{\mathrm{thr},m,-\beta}$, where $-\beta$ signifies the use of past $\beta$ number of samples for updating the threshold:

$$\tau_m = \mu_{\mathrm{thr},m,-\beta} + \eta \times \sigma_{\mathrm{thr},m,-\beta}. \tag{5}$$

Let $K_1$ and $K_2$ be the number of training and testing samples, respectively, and let $\boldsymbol{Z}$ ($\boldsymbol{Z} \in \mathbb{R}^{d\times K_1}$) and $\tilde{\boldsymbol{Z}}$ ($\tilde{\boldsymbol{Z}} \in \mathbb{R}^{d\times K_2}$) be the training and testing samples, respectively. Let $\boldsymbol{Y}$ ($\boldsymbol{Y} \in \mathbb{R}^{1\times K_1}$) and $\tilde{\boldsymbol{Y}}$ ($\tilde{\boldsymbol{Y}} \in \mathbb{R}^{1\times K_2}$) be the corresponding labels. $\boldsymbol{\delta}_{Z,m}$ ($\boldsymbol{\delta}_{Z,m}$ in $\mathbb{R}^{1\times K_1}$) denotes the squared Mahalanobis distances of all training samples with respect to the mth CorrDet detector with adaptive statistics, $\phi_m$. $\boldsymbol{\delta}_{\tilde{z}_k}$ ($\boldsymbol{\delta}_{\tilde{z}_k} \in \mathbb{R}^{1\times M}$) denotes the squared Mahalanobis distances of the kth testing sample with respect to all local classifiers, $\Phi_{\mathrm{E}}$. Let $\boldsymbol{B}$ be the squared Mahalanobis distances of all normal samples in the sliding window with a length of $\beta$ ($\boldsymbol{B} \in \mathbb{R}^{1\times\beta}$).

The pseudo-code for the proposed ECD-AS algorithm is shown in Procedure 1 (Fig. 2).

*Train an ensemble CorrDet with adaptive statistics classifier:*
**Input:** $\mathbf{Z}, \mathbf{Y}, \widetilde{\mathbf{Z}}$
**for** Every local classifier $m = 1 : M$ **do**
  Initialize the mean $\mu_m$ and covariance $\Sigma_m^{-1}$ of normal statistics using the sample mean and covariance of normal samples in the training set with selected measurements associated with $\phi_m$
  Initialize the squared Mahalanobis distance $\delta_{Z,m}$ using (1)
  Initialize the threshold $\tau_m$ using (4)
**end for**
*Test using the ensemble CorrDet with adaptive statistics classifier:*
**for** Every test sample $k = 1 : K_2$ **do**
  Compute the squared Mahalanobis distance $\delta_{\widetilde{z}_k}$ using (1)
  **if** $\forall m, \delta_{\widetilde{z}_k} < \tau_m$ **then**
    Classify $\widetilde{z}_k$ as normal sample: $\widetilde{y}_k = 0$
    Update the mean $\mu_m$ and covariance $\Sigma_m^{-1}$ using (2) and (3)
    Update the sliding window by adding $\delta_{\widetilde{z}_k}$ to $\mathbf{B}$ and removing the oldest value from $\mathbf{B}$.
    Update the mean $\mu_{thr,m,-\beta}$ and variance $\sigma_{thr,m,-\beta}$ of squared Mahalanobis distances in the updated sliding window of each local CorrDet detector with adaptive statistics
    Update the threshold value $\tau_m$ for each local CorrDet detector with adaptive statistics using (5)
  **else**
    Classify $\widetilde{z}_k$ as abnormal sample: $\widetilde{y}_k = 1$
  **end if**
**end for**
**Output:** $\widetilde{\mathbf{Y}}$

**Fig. 2** *Procedure 1 ECD-AS algorithm*

## 4 Case study

### 4.1 Dataset

The proposed strategy for bad data detection was validated using the IEEE 118-bus system. The measurement set includes real and reactive power flows, real and reactive power injections, and all voltage magnitudes, resulting in 691 measurements. Using the MATLAB package MATPOWER, one day's worth of samples, or measurement sets, were generated with Gaussian noise. Since SCADA obtains measurements every 4 s, this means the dataset has 21,600 samples, which were generated based on a common daily load profile that was applied to all of the loads on the system and contains the temporal information of a power system's changing state. A total of 1080 (5%) of these samples were chosen at random to insert an FDI into a single measurement within the sample, which is the only type of attack considered in this work. These FDIs were of random size between 7 and 23 standard deviations away from the true measurement value and the standard deviation of each measurement was 1% of the measurement value. FDI attacks like these have been shown to have a significant impact on the optimal power flow (OPF) application that uses the results of State Estimation if they go undetected [28, 29]. Out of these 21,600 samples, 1800 ($K_1$) were used for training while the remaining 19,800 ($K_2$) samples were used for testing. The implementation of the data driven machine learning model ECD-AS and evaluation of results was conducted using Python libraries such as NumPy [45], Pandas [46], SciPy [47], Matplotlib [48] and Scikit-learn [49] in Anaconda environment.

### 4.2 Performance analysis

To properly evaluate the performance of the strategies included in this paper, we make use of the following classification metrics [50].

Anomalous samples are the ones in which an FDI attack is introduced. True Negatives (TN) refer to normal samples that are predicted as normal samples. True Positives (TP) refer to anomalous samples correctly predicted as anomalous. False Negatives (FN) refers to anomalous samples predicted to be normal, and False Positives (FP) refers to normal samples predicted to be anomalous.

Accuracy is the ratio of the number of correctly predicted samples to the total number of samples in the test dataset. Accuracy is calculated as shown in (6):

$$\text{Accuracy} = 100 \times \frac{\text{TP} + \text{TN}}{\text{TP} + \text{FP} + \text{TN} + \text{FN}}. \tag{6}$$

Precision is the ratio of the number of correctly predicted anomalies to the overall predicted anomalies. A model with high precision can limit the mitigation cost by reducing unnecessary actions due to false positives. Precision is calculated as in (7)

$$\text{Precision} = 100 \times \frac{\text{TP}}{\text{TP} + \text{FP}}. \tag{7}$$

The recall is the ratio of the number of correctly predicted anomalous samples to the number of true anomalous samples. A model with a high recall can reduce the number of false negatives, thereby reducing the number of missed FDI attacks. Equation (8) shows the recall metric calculation

$$\text{Recall} = 100 \times \frac{\text{TP}}{\text{TP} + \text{FN}}. \tag{8}$$

F1-score is the harmonic mean of Precision and Recall. The resulting value is closer to the lower value among Precision and Recall than arithmetic mean, hence resulting in a more appropriate performance metric. This metric is more useful than accuracy since we usually have an uneven class distribution for anomaly detection problems like FDI detection considered in this work. Equation (9) shows the F1-score calculation

$$\text{F1}-\text{score} = \frac{2 \times \text{Recall} \times \text{Precision}}{\text{Recall} + \text{Precision}}. \tag{9}$$

### 4.3 Experiments for hyper-parameters in adaptive statistics

There are three hyper-parameters namely $\eta$, $\beta$ and $\alpha$ in the adaptive statistics of the presented ECD-AS framework. Extensive experimentation was conducted to choose the optimal hyper-parameters.

The candidate parameter set for $\eta$ is from 4 to 18, $\beta$ is from 0 to 450 and $\alpha$ is from 0 to $10^{-4}$. Different combinations of hyper-parameters from their candidate sets are used for training the model, and then for evaluating the model using F1-score on the testing dataset. Fig. 3 shows a 3D scatter plot for $\eta$, $\beta$ and $\alpha$ where the colour and height is an indicator for F1-score. For each subplot (certain $\beta$ value), the highest F1-score is highlighted. The optimal combination of hyper-parameters is estimated as $\eta = 9$, $\beta = 90$ and $\alpha$=8×10$^{-5}$. These values of $\eta$, $\beta$ and $\alpha$ are used in (5), (2), and (3) during model training and update of adaptive statistics phase of the ECD-AS framework.

The hyper-parameter $\eta$ is a parameter choosing how far the classification threshold $\tau_m$ should be away from the mean of normal samples. In this experiment, $\eta$ varies while the two other hyper-parameters remain the same for each run. Fig. 4 shows adaptive thresholds for various values of $\eta$ for a fixed $\alpha = 8 \times 10^{-5}$ and $\beta = 90$, compared to the decision score for bus-1 (local region number 1). The corresponding F1-scores for different values of $\eta$ are also provided in the figure. Adaptive threshold with $\eta = 9$ yields the highest F1-score in this experiment, leading to a moderate threshold curve with the time that is not too far from normal samples (missing more anomalies) and not too close to the normal samples (having more false alarms).

### 4.4 Numerical results

Table 1 shows the mean ($\mu_{cv}$) and standard deviation ($\sigma_{cv}$) values of accuracy, precision, recall and F1-score values for 15 different sets of training and test datasets for a variety of bad data detection strategies included in our analysis namely, K-nearest neighbours (KNN) [22], multilayer perceptron neural networks (MLPNNs)

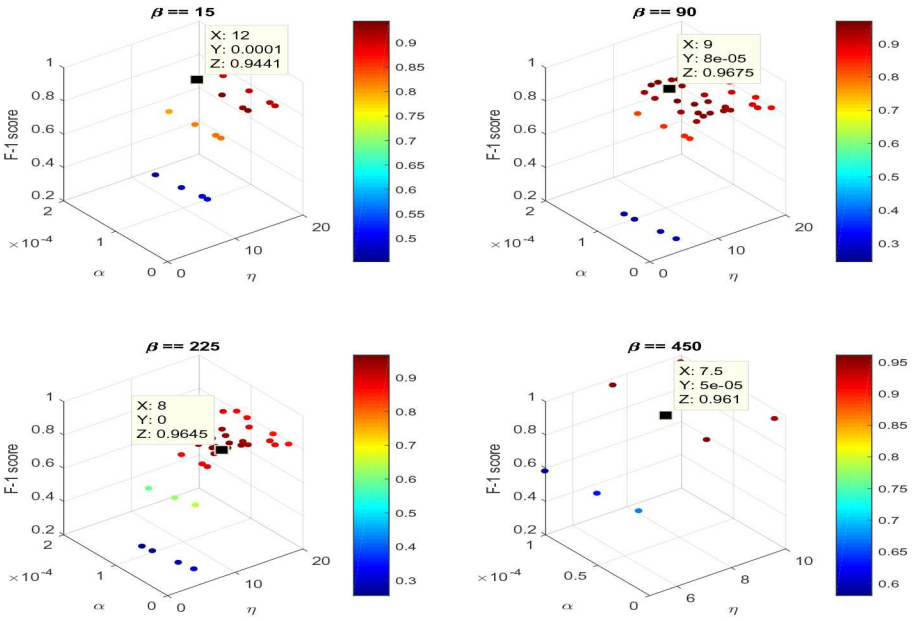


**Fig. 3** *F1-score for FDI detection using ECD-AS for various values of hyper-parameters* $\boldsymbol{\alpha}$, $\boldsymbol{\beta}$ *and* $\boldsymbol{\eta}$

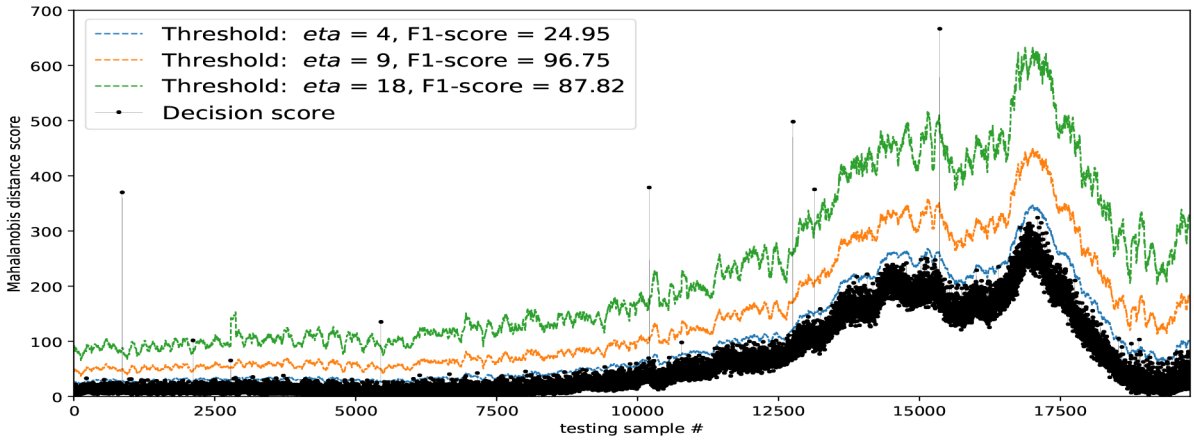


**Fig. 4** *Multiple Adaptive threshold curves corresponding to different* ***eta*** $(\boldsymbol{\eta})$ *values versus Mahalanobis decision score for bus-1*

**Table 1** Performance comparison of various bad data detection methodologies

| Method | Accuracy | Precision | Recall | F1-score |
|---|---|---|---|---|
| | $\mu_{cv} \pm \sigma_{cv}$ | $\mu_{cv} \pm \sigma_{cv}$ | $\mu_{cv} \pm \sigma_{cv}$ | $\mu_{cv} \pm \sigma_{cv}$ |
| KNN | 93.05 ± 02.71 | 13.36 ± 09.24 | 03.94 ± 03.35 | 04.64 ± 02.97 |
| MLPNN [38] | 78.04 ± 20.64 | 08.75 ± 11.98 | 20.89 ± 24.21 | 05.29 ± 04.09 |
| GNB | 49.81 ± 38.06 | 28.26 ± 38.50 | 51.35 ± 39.73 | 07.94 ± 04.47 |
| ADT | 45.56 ± 22.03 | 05.66 ± 02.33 | 57.84 ± 23.87 | 09.54 ± 01.54 |
| SVC | 55.68 ± 25.75 | 11.46 ± 12.14 | 60.57 ± 22.11 | 14.89 ± 06.75 |
| SE [9] | 94.07 ± 00.25 | 36.56 ± 02.15 | 80.64 ± 02.21 | 57.03 ± 01.92 |
| CD [25] | 04.88 ± 00.24 | 04.88 ± 00.24 | 99.07±00.00 | 09.31 ± 00.43 |
| ECD [26] | 97.28 ± 01.40 | 46.52 ± 28.03 | 44.08 ± 29.63 | 55.42 ± 27.71 |
| ECD-AS | **99.35** ± 00.45 | **87.24** ± 09.30 | **86.94** ± 09.87 | **92.54** ± 05.74 |

The bold values emphasise the metrics for the ECD-AS method presented in this paper.

[38], Gaussian Naive Bayes (GNB), adaptive boosting with decision trees (ADT), support vector classifier (SVC) [22], the physics-based state estimator (SE) [9], our previous work, CorrDet anomaly detector (CD) [27] and ensemble CorrDet anomaly detector (ECD) [26], and our proposed ECD-AS anomaly detector.

The SE analysis is the classical WLS SE with bad data detection via the Chi-squared test with a confidence of 0.95 and degrees of freedom of $d$ - $N$, where $N$ is the number of states [5]. Each experiment in the cross-validation had 1800 ($K_1$) samples for training and 5800 ($K_2$) samples for testing.

We have compared the performance of ECD-AS with five popular machine learning classification models such as KNN, MLPNN, GNB, ADT and SVC, a physics-based SE, and two data-driven threshold-based anomaly detection strategies. To have a fair comparison between the results of different methodologies, the same samples are used for training and testing of all the models.

The hyper-parameters for the various machine learning models were chosen through experimentation and the optimal values were used to obtain the results shown in Table 1. The results are as follows. For KNN, the value of the number of nearest neighbours is chosen as 1 (higher value of $k$ resulted in lower performance). For MLPNN, 3 hidden layers with 250, 100 and 50 processing elements were used, along with ReLu activation function, and an ADAM solver for weight optimisation. For GNB, a variance

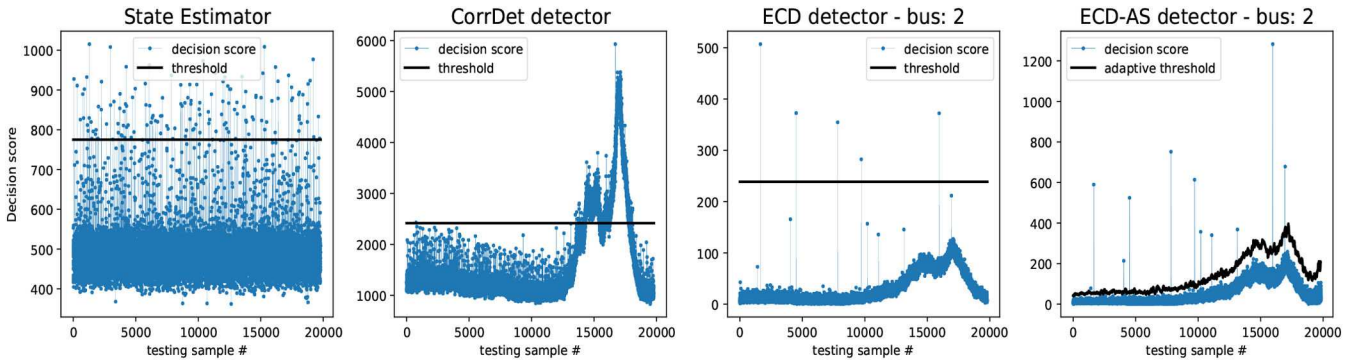


**Fig. 5** *Comparison of Mahalanobis decision score and decision threshold for multiple FDI detection schemes*

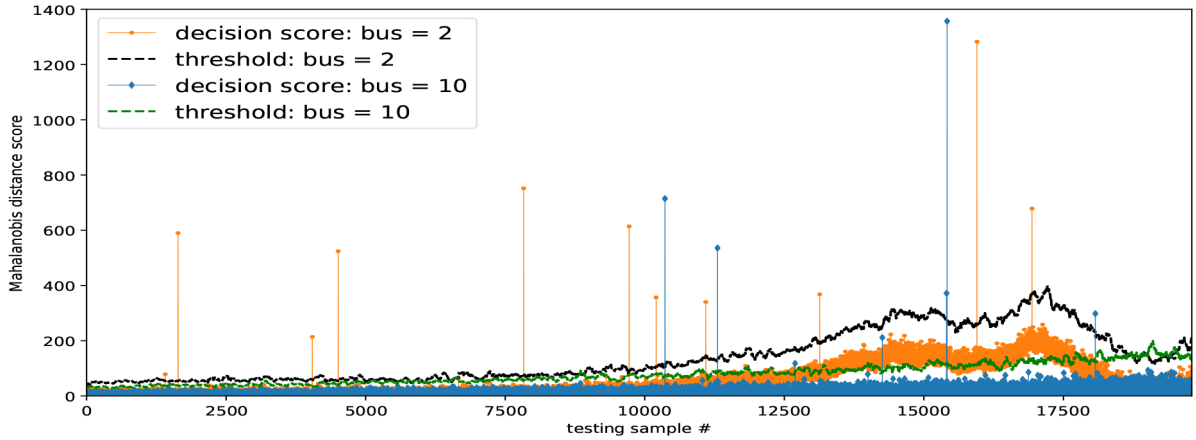


**Fig. 6** *Adaptive threshold versus Mahalanobis decision score for multiple buses*

smoothing factor of $10^{-6}$ was used. For ADT, 500 decision tree estimators each with a maximum depth of 500 were used, and finally, for SVC, a radial basis function kernel with balanced class weights was used. Other hyper-parameters of these models were set with default choices from the scikit-learn library as they were implemented using it.

In Table 1, we can observe that the proposed ECD-AS outperforms all eight methodologies in terms of Accuracy, Precision and F1-score. Although CorrDet anomaly detector has a better recall score than the ECD-AS method, it results in extremely low values of precision and F1-score (As described for (9), the F1-score is the harmonic mean of precision and recall. An F1 score reaches its best value at 1 for perfect precision and recall). Compared to the results in [26] based on a drifting load profile, the ECD performance drops when applied to the changing daily load profile in this work. The adaptive statistics using a sliding window approach in the ECD-AS proved to be effective in dealing with the changing state of a daily load profile and produced a much higher F1-score than the ECD framework.

*4.4.1 Physical significance and impact of undetected FDI attacks:* While the F1-scores in Table 1 are significant results, few individual samples can be analysed to show the physical significance of undetected attacks. As discussed in [28], an attack that leads to a 1% error in a power injection estimation can have a large impact on the results of the OPF application, which depends directly on the SE results. There are samples where the physics-model based SE [9] solution failed to detect FDI and the ECD-AS successfully detected FDI. An FDI attack directly imposed on the real power injection measurement of bus 27 leads to an estimate that is off by over 1%. This error would be distributed among the lines connected to bus 27. An FDI attack on the real power flow measurement between buses 46 and 48 would cause a power flow error of over 1% as well. Examples like these are seen throughout the SE failures and have a real impact on the OPF application. Just a 1% error in OPF can cause lines on the system to be overloaded, which can lead to line outages [28]. While these errors may not lead to large scale blackouts they can certainly lead to outages on the system, damaged equipment, and loss of resources, all of which are bad for utilities and their customers.

### *4.5 Analysis of adaptive threshold and decision scores*

To illustrate the effectiveness of the presented ECD-AS framework compared to other threshold-based anomaly detection schemes considered in this analysis, we show the values of decision scores (squared Mahalanobis distance measure) and corresponding optimal thresholds obtained using physics-based SE [9], CorrDet anomaly detection [25], ECD anomaly detection [26] and ECD-AS anomaly detector in Fig. 5. It is important to notice that SE and CD detection algorithms only provide system-level decision scores, whereas ECD and ECD-AD provide decision scores for each bus. We have selected region-2 as an example to show the behaviour of decision scores and threshold obtained by fixed statistics in the previous work ECD versus the decision score and adaptive threshold obtained by the use adaptive statistics in the proposed ECD-AS. Similar observations can be made for other regions in ECD and ECD-AS results. In Fig. 5, we can notice that SE results in a large number of false positives, hence resulting in low precision value. The fixed statistics nature of CD and ECD bad data detection algorithms cannot capture the temporal changing dynamics of the measurements and fails to separate normal samples from anomalous samples. These cases can be successfully addressed in the proposed ECD-AS framework.

In ECD-AS, the threshold value $\tau_m$ is estimated for every local CorrDet detector with adaptive statistics, which is necessary due to the fact that different buses (local regions) have their own dynamics over time as they consist different measurements. Fig. 6 shows adaptive thresholds and decision score for the optimal values of $\eta$, $\beta$ and $\alpha$ for bus-2 and bus-10. It is noticeable that the threshold values for bus-10 cannot be used for bad data detection of bus-2. The adaptive threshold of bus-10 would label a large number of the normal samples of bus-2 to be anomalous. Similarly, the adaptive threshold of bus-2 cannot be used for bus-10 as it would miss many of the anomalous samples in bus-10. Similar behaviour can be observed for all the buses, which shows that each

local CorrDet detector with adaptive statistics is needed to effectively detect FDI attacks.

## 5 Conclusion

This paper presents a method to use adaptive statistics in the detection of bad data in power systems such that the constantly changing state of a power system is taken into account. The data-driven bad data detection technique proposed in this paper uses adaptive mean, adaptive covariance, and adaptive anomaly threshold calculated with a sliding window approach for the incoming data such that it adapts to changes in the system state. In the case study on the IEEE 118-bus system, extensive experimentation with the hyper-parameters of the ECD-AS process shows an optimal solution with much better bad data detection results than the state-of-the-art. The ECD-AS has a mean F1-score of 92.5, whereas the ECD has a mean F1-score of 55.4 and the SE method has mean F1-score of 57.0. This shows that the adaptive statistics presented are critical in bad data analysis for realistic power system data. The distributed nature of the ECD-AS framework using local detectors enables it to identify multiple simultaneous FDI attacks and also helps in the identification of the attacked buses. The improved performance of the presented technique can be attributed for its ability to understand normal and bad data behaviour at both spatial (local detectors at each bus) and temporal (time-varying adaptive threshold) levels using adaptive statistics.

## 6 Acknowledgment

This material was based upon work supported by the National Science Foundation under grant no. 1809739.

## 7 References

[1] Farag, M., Azab, M., Mokhtar, B.: 'Cross-layer security framework for smart grid: physical security layer'. IEEE PES Innovative Smart Grid Technologies Europe (ISGT Europe), Istanbul, Turkey, 2014, pp. 1–7

[2] Volz, D.: 'U.S. Government concludes cyber attack caused Ukraine power outage'. Reuters, 2016. Available from: https://www.reuters.com/article/us-ukraine-cybersecurity/u-s-governmentower-outage-idUSKCN0VY30K

[3] Fairley, P.: '*Upgrade coming to grid cybersecurity in U.S.*' (IEEE Spectrum, 2016). Available from: https://spectrum.ieee.org/energy/thesmarter-grid/upgrade-coming-to-grid-cybersecurityin-us?bt_alias=eyj1c2vyswqioiaimmnjzjayndytmdlkos00mzliltlizmqtnzm0yze0zwjjzjlkin0\%3D

[4] Zetter, K.: '*An unprecedented look at Stuxnet, the world's first digital weapon*' (Wired.com, USA, 2014) Available from: https://www.wired.com/2014/11/countdown-to-zero-day-stuxnet/

[5] Monticelli, A.: '*State estimation in electric power systems: a generalized approach*' vol. 507 (Springer Science & Business Media, USA, 1999)

[6] Handschin, E., Schweppe, F.C., Kohlas, J., *et al.*: 'Bad data analysis for power system state estimation', *IEEE Trans. Power Appar. Syst.*, 1975, **94**, (2), pp. 329–337

[7] Bretas, N.G., Bretas, A.S., Piereti, S.A.: 'Innovation concept for measurement gross error detection and identification in power system state estimation', *IET Gener., Transm. Distrib.*, 2011, **5**, (6), pp. 603–608

[8] Bretas, A.S., Bretas, N.G., Carvalho, B., *et al.*: 'Smart grids cyber-physical security as a malicious data attack: an innovation approach', *Electr. Power Syst. Res.*, 2017, **149**, pp. 210–219. Available from: http://www.sciencedirect.com/science/article/pii/S0378779617301657

[9] Bretas, N.G., Bretas, A.S.: 'The extension of the Gauss approach for the solution of an overdetermined set of algebraic non linear equations', *IEEE Trans. Circuits Syst. II, Express Briefs*, 2018, **65**, (9), pp. 1269–1273

[10] Bretas, A.S., Bretas, N.G., Carvalho, B.E.B.: 'Further contributions to smart grids cyber-physical security as a malicious data attack: proof and properties of the parameter error spreading out to the measurements and a relaxed correction model', *Int. J. Electr. Power Energy Syst.*, 2019, **104**, pp. 43–51. Available from: http://www.sciencedirect.com/science/article/pii/S0142061518303946

[11] Liu, Y., Ning, P., Reiter, M.K.: 'False data injection attacks against state estimation in electric power grids'. Proc. of the 16th ACM Conf. on Computer and Communications Security. CCS '09, ACM, Chicago, IL, USA, 2009, pp. 21–32. Available from: http://doi.acm.org/10.1145/1653662.1653666

[12] Hug, G., Giampapa, J.A.: 'Vulnerability assessment of AC state estimatmion with respect to false data injection cyber-attacks', *IEEE Trans. Smart Grid*, 2012, **3**, pp. 1362–1370

[13] Sridhar, S., Manimaran, G.: 'Data integrity attacks and their impacts on SCADA control system'. Proc. Power Energy Society General Meeting, CDC, Minneapolis, MN, USA, 2010

[14] Xie, L., Mo, Y., Sinopoli, B.: 'False data injection attacks in electricity markets'. Proc. 1st IEEE Int. Conf. Smart Grid Communications, SmartGridComm, Gaithersburg, MD, USA, 2010

[15] Sandberg, H., Teixeira, A., Johansson, K.H.: 'On security indices for state estimators in power networks'. Proc. 1st Workshop Secure Control Systems, Stockholm, Sweden, 2010

[16] Esfahani, P.M., Vrakopoulou, M., Margellos, K., *et al.*: 'Cyber-attack in a two-area power system: impact identification using reachability'. Proc. American Control Conf. (ACC), Baltimore, MD, USA, 2010

[17] Esfahani, P.M., Vrakopoulou, M., Margellos, K., *et al.*: 'A robust policy for automatic generation control cyber-attack in two area power network'. Proc. 2010 49th IEEE Conf. Decision Control (CDC), Atlanta, GA, USA, 2018, pp. 5973–5978

[18] Bhattarai, B.P., Paudyal, S., Luo, Y., *et al.*: 'Big data analytics in smart grids: state-of-the-art, challenges, opportunities, and future directions', *IET Smart Grid*, 2019, **2**, (2), pp. 141–154

[19] Kosut, O., Jia, L., Thomas, R.J., *et al.*: 'Malicious data attacks on smart grid state estimation: attack strategies and counter measures'. 2010 First IEEE Int. Conf. on Smart Grid Communications, Gaithersburg, MD, USA, 2010, pp. 220–225

[20] Bobba, R.B., Rogers, K.M., Wang, Q., *et al.*: 'Detecting false data injection attacks on dc state estimation'. Preprints of the First Workshop on Secure Control Systems, CPSWEEK, Stockholm, Sweden, 2010, vol. 2010

[21] He, Y., Mendis, G.J., Wei, J.: 'Real-time detection of false data injection attacks in smart grid: a deep learning-based intelligent mechanism', *IEEE Trans. Smart Grid*, 2017, **8**, (5), pp. 2505–2516

[22] Ozay, M., Esnaola, I., Vural, Y.F.T., *et al.*: 'Machine learning methods for attack detection in the smart grid', *IEEE Trans. Neural Netw. Learning Syst.*, 2016, **27**, (8), pp. 1773–1786

[23] Wei, L., Gao, D., Luo, C.: 'False data injection attacks detection with deep belief networks in smart grid'. 2018 Chinese Automation Congress (CAC), Xi'an, China, 2018, pp. 2621–2625

[24] Potluri, S., Diedrich, C., Sangala, G.K.R.: 'Identifying false data injection attacks in industrial control systems using artificial neural networks'. 2017 22nd IEEE Int. Conf. on Emerging Technologies and Factory Automation (ETFA), Limassol, Cyprus, 2017, pp. 1–8

[25] Trevizan, R.D., Ruben, C., Nagaraj, K., *et al.*: 'Data-driven physics-based solution for false data injection diagnosis in smart grids'. 2019 IEEE PES GM, Atlanta, GA, USA, 2019

[26] Ruben, C., Dhulipala, S.C., Nagaraj, K., *et al.*: 'Hybrid data-driven physics model-based framework for enhanced cyber-physical smart grid security', *IET Smart Grid*, Available from: https://digital-library.theiet.org/content/journals/10.1049/iet-stg.201

[27] Ho, K.C., Gader, P.D.: 'Correlation-based land mine detection using GPR'. Detection and Remediation Technologies for Mines and Minelike Targets V., Int. Society for Optics and Photonics, Orlando, FL, USA, 2000, vol. 4038, pp. 1088–1096

[28] Liang, J., Sankar, L., Kosut, O.: 'Vulnerability analysis and consequences of false data injection attack on power system state estimation', *IEEE Trans. Power Syst.*, 2016, **31**, (5), pp. 3864–3872

[29] Teixeira, A., Sandberg, H., Dan, G., *et al.*: 'Optimal power flow: closing the loop over corrupted data'. 2012 American Control Conf. (ACC), Montreal, Canada, 2012, pp. 3534–3540

[30] Ashok, A., Govindarasu, M.: 'Cyber attacks on power system state estimation through topology errors'. Power and Energy Society General Meeting, 2012 IEEE, San Diego, CA, USA, 2012, pp. 1–8

[31] Margossian, H., Sayed, M.A., Fawaz, W., *et al.*: 'Partial grid false data injection attacks against state estimation', *Int. J. Electr. Power Energy Syst.*, 2019, **110**, pp. 623–629

[32] Stefanov, A., Liu, C.: 'Cyber-power system security in a smart grid environment'. 2012 IEEE PES Innovative Smart Grid Technologies (ISGT), Washington, DC, USA, 2012, pp. 1–3

[33] Abur, A., Expósito, A.G.: '*Power system state estimation: theory and implementation*'. Power Engineering (Willis). (CRC Press, USA, 2004). Available from: https://books.google.com/books?id=NQhbtFC6_40C

[34] Bretas, N.G., Piereti, S.A., Bretas, A.S., *et al.*: 'A geometrical view for multiple gross errors detection, identification, and correction in power system state estimation', *IEEE Trans. Power Syst.*, 2013, **28**, (3), pp. 2128–2135

[35] Bretas, N.G., Bretas, A.S., Martins, A.C.P.: 'Convergence property of the measurement gross error correction in power system state estimation, using geometrical background', *IEEE Trans. Power Syst.*, 2013, **28**, (4), pp. 3729–3736

[36] Xue, D., Jing, X., Liu, H.: 'Detection of false data injection attacks in smart grid utilizing ELM-based OCON framework', *IEEE Access*, 2019, **7**, pp. 31762–31773

[37] Krundyshev, V., Kalinin, M.: 'Prevention of false data injections in smart infrastructures'. 2019 IEEE Int. Black Sea Conf. on Communications and Networking (BlackSeaCom), Sochi, Russia, 2019, pp. 1–5

[38] Ashrafuzzaman, M., Chakhchoukh, Y., Jillepalli, A.A., *et al.*: 'Detecting stealthy false data injection attacks in power grids using deep learning'. 2018 14th Int.Wireless Communications Mobile Computing Conf. (IWCMC), Limassol, Cyprus, 2018, pp. 219–225

[39] Ho, K., Gader, P.D.: 'A linear prediction land mine detection algorithm for hand held ground penetrating radar', *IEEE Trans. Geosci. Remote Sens.*, 2002, **40**, (6), pp. 1374–1384

[40] Chang, C.I., Chiang, S.S.: 'Anomaly detection and classification for hyperspectral imagery', *IEEE Trans. Geosci. Remote Sens.*, 2002, **40**, (6), pp. 1314–1325

[41] Alvey, B., Zare, A., Cook, M., *et al.*: 'Adaptive coherence estimator (ACE) for explosive hazard detection using wideband electromagnetic induction (WEMI)', *ProcSPIE*, 2016, **9823**, pp. 9823–9823 Available from: https://doi.org/10.1117/12.2223347

[42] Zhao, C., Wang, Y., Qi, B., *et al.*: 'Global and local real-time anomaly detectors for hyperspectral remote sensing imagery', *Remote Sens.*, 2015, **7**, (4), pp. 3966–3985
[43] Wang, Y., Zhao, C., Chang, C.I.: 'Anomaly detection using sliding causal windows'. 2014 IEEE Geoscience and Remote Sensing Symp. IEEE, Quebec, Canada, 2014, pp. 4600–4603
[44] Bibbona, E., Panfilo, G., Tavella, P.: 'The ornstein–Uhlenbeck process as a model of a low pass filtered white noise', *Metrologia*, 2008, **45**, p. S117
[45] Oliphant, T.E.: '*A guide to NumPy*' vol. 1 (Trelgol Publishing, USA, 2006)
[46] Pandas Development Team, T.: '*Pandas-Dev/Pandas: Pandas*' (Zenodo, Switzerland, 2020). Available from: https://doi.org/10.5281/zenodo.3509134
[47] Virtanen, P., Gommers, R., Oliphant, T.E., *et al.*: 'SciPy 1.0: fundamental algorithms for scientific computing in python', *Nat. Methods*, 2020, **17**, pp. 261–272
[48] Hunter, J.D.: 'Matplotlib: A 2D graphics environment', *Comput. Sci. Eng.*, 2007, **9**, (3), pp. 90–95
[49] Pedregosa, F., Varoquaux, G., Gramfort, A., *et al.*: 'Scikit-learn: machine learning in Python', *J. Mach. Learn. Res.*, 2011, **12**, pp. 2825–2830
[50] Godbole, S., Sarawagi, S.: 'Discriminative methods for multi-labeled classification', in Dai, H., Srikant, R., Zhang, C. (eds.): '*Advances in knowledge discovery and data mining*' (Springer Berlin Heidelberg, Berlin, Heidelberg, 2004), pp. 22–30