




Article

Cyber Attacks and Faults Discrimination in Intelligent Electronic Device-Based Energy Management Systems

B. M. Ruhul Amin ^{1,*} , M. J. Hossain ^{2,*}, Adnan Anwar ³  and Shafquat Zaman ¹ 

¹ School of Engineering, Macquarie University, Sydney, NSW 2109, Australia; zamanshafquat@gmail.com

² School of Electrical and Data Engineering, University Technology Sydney, Ultimo, NSW 2007, Australia

³ Centre for Cyber Security Research and Innovation (CSRI), Deakin University, Waurn Ponds, VIC 3216, Australia; adnan.anwar@deakin.edu.au

* Correspondence: ruhul.amin@students.mq.edu.au (B.M.R.A.); jahangir.hossain@uts.edu.au (M.J.H.)

Abstract: Intelligent electronic devices (IEDs) along with advanced information and communication technology (ICT)-based networks are emerging in the legacy power grid to obtain real-time system states and provide the energy management system (EMS) with wide-area monitoring and advanced control capabilities. Cyber attackers can inject malicious data into the EMS to mislead the state estimation process and disrupt operations or initiate blackouts. A machine learning algorithm (MLA)-based approach is presented in this paper to detect false data injection attacks (FDIAs) in an IED-based EMS. In addition, stealthy construction of FDIAs and their impact on the detection rate of MLAs are analyzed. Furthermore, the impacts of natural disturbances such as faults on the system are considered, and the research work is extended to distinguish between cyber attacks and faults by using state-of-the-art MLAs. In this paper, state-of-the-art MLAs such as Random Forest, OneR, Naive Bayes, SVM, and AdaBoost are used as detection classifiers, and performance parameters such as detection rate, false positive rate, precision, recall, and f-measure are analyzed for different case scenarios on the IEEE benchmark 14-bus system. The experimental results are validated using real-time load flow data from the New York Independent System Operator (NYISO).

Keywords: intelligent electronic device (IED); cyber attacks; energy management system (EMS); false data injection attack (FDIA)



Citation: Amin, B.M.R.; Hossain, M.J.; Anwar, A.; Zaman, S. Cyber Attacks and Faults Discrimination in Intelligent Electronic Device-Based Energy Management Systems. *Electronics* **2021**, *10*, 650. <https://doi.org/10.3390/electronics10060650>

Academic Editor: Taha Selim Ustun

Received: 13 February 2021

Accepted: 8 March 2021

Published: 11 March 2021

Publisher's Note: MDPI stays neutral with regard to jurisdictional claims in published maps and institutional affiliations.



Copyright: © 2021 by the authors. Licensee MDPI, Basel, Switzerland. This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license (<https://creativecommons.org/licenses/by/4.0/>).

1. Introduction

The demand for power supply is growing with time, and various types of efficient and renewable energy sources are being integrated into the legacy power grid. In addition, new types of loads and storage devices are emerging from the consumers' side. Diverse intelligent electronic devices (IEDs) such as inverters, digital relays, and phasor measurement units (PMUs) are deployed to monitor and control this complex and dynamic network of power systems [1]. Furthermore, the physical grid components of a smart grid starting from generation to end users are tightly coupled with a cyber network of physical process-oriented control, computational resources, and information technology-based communication systems [2]. As a consequence, new types of contingencies such as cyber-attacks are occurring at a high-frequency on power system monitoring, control, and operations [3].

Attackers can break into a computer or industrial control system (ICS) by deploying malware through phishing or spoofing attacks and take control of the entire system or part of the system to mislead the operation or disable it for a certain period of time. False data could also be injected into the power system energy management system (EMS) by compromising the physical IEDs' functionalities or exploiting the flaws and vulnerabilities in software and communication protocols [4]. Spurious injection in supervisory control and data acquisition (SCADA)-based ICSs results in the false or incorrect calculation of system states, which eventually misleads EMS operations such as optimal power flow, economic dispatch, contingency analysis, and many more. In general, the chi-square test

and the largest normalized residual (LNR) methods are used to detect and identify corrupt or distorted measurements present in a SCADA database [5]. However, in a recent study, Liu et al. demonstrated that an attacker equipped with power system topology information can inject false or misleading data into the measurement vector that remains undetected by the conventional chi-square-based bad data detection method [6]. Unless prevented, cyber attacks in power system EMSs can cause disruptions in power system operations and eventually initiate cascading failures, leading to complete blackouts [7].

A large number of research studies have been carried out to investigate the construction and stealthiness of FDIAs against power system EMSs [8]. In addition, IT-based security measures such as cryptography-based protection systems, firewalls, antivirus, and many more are currently used to defend against cyber attacks. Due to the tight coupling between physical processes of smart grids and the communication and cyber networks among them, the existing only-IT-based security solutions are inadequate for ensuring cyber security in smart power grids [9]. Significant efforts have been made to protect meter measurements by implementing PMUs in critical locations in a cost-effective manner [10]. However, GPS-based PMUs are also not hack-proof [11]. On the other hand, detection-based defense techniques are proposed that include the generalized likelihood ratio, Kullback–Leibler distance method, Markov chains, unscented Kalman filter (UKF), fast-go decomposition, Bayesian framework, diagnostic generalized potential, cosine similarity matching scheme, and many more [12]. However, many of the proposed methods are not scalable, and thus they are physically unfeasible for large-scale, highly complex cyber-physical smart power systems [13]. In addition, the large number of data collected from different smart meter locations requires proper data analysis and anomaly detection techniques.

Due to the scalability towards large systems, the development and implementation of MLAs for detecting anomalies in various research and industrial sectors are gradually increasing [14]. Many supervised machine learning algorithms (MLAs) have been developed that can successfully detect false data injections in the state estimation process [15]. Furthermore, an unsupervised ensemble learning method in [16] and a deep autoencoder model in [17] have been developed to detect false data injection attacks in PMUs, whereas PMUs' data are difficult to label due to their fast data streaming. Although deep learning methods exhibit impressive results in detecting FDIAs [18,19], they require large training data sets, high computational costs, and specialized equipment.

In addition, the detection of cyber attacks becomes complicated when measurement data disruptions due to natural disturbances such as faults are considered [20]. The incorrect identification of attacks as faults, or vice versa, can cause inappropriate control actions by control center operators. Although the detection techniques used in a large number of anomalous cyber and physical events have been well studied, the development of methods to distinguish between cyber attacks and physical anomalies is still in the preliminary stage. Therefore, a simple and realistic machine learning-based approach is presented in this paper to detect cyber attacks in an IED-based power system EMS and assess the feasibility of state-of-the-art MLAs in distinguishing between FDIAs and faults. The key contributions of this paper are as follows:

- An assessment of the feasibility of state-of-the-art MLAs in detecting cyber attacks is performed.
- The construction of stealthy FDIAs is analyzed, and the performance of MLAs in detecting stealthy attacks is evaluated.
- The research study is further extended to discriminate between cyber attacks and faults in an IED-based EMS by using state-of-the-art MLAs such as Random Forest, OneR, Naive Bayes, SVM, and AdaBoost.

The rest of the paper's architecture is as follows. In Section 2, the IED-based smart grid model, the EMS operation and its state estimation, and bad data detection functionalities are discussed. Section 3 presents cyber-vulnerable nodes in the power system EMS and the construction strategy of stealthy cyber attacks using system information and measurement

signals. The experiential setup, test system, and data generation processes are presented in Section 4. Results and findings from different case scenarios are presented and thoroughly discussed in Section 5. The conclusion and future directions of this research are presented in Section 6.

2. The IED-Based Smart Power System

The smart power system is a complex infrastructure of tightly coupled physical and cyber networks. In this large and complex cyber-physical network, an advanced metering infrastructure comprised of several IEDs such as PMUs is used to monitor and measure important physical quantities such as voltages, currents, power, and angles at different bus and node locations of a power system. All IED-measured data are sent to the control center via a high-speed communication network for making control decisions as shown in Figure 1. The control center processes the received measurement data and sends control commands to the actuators.

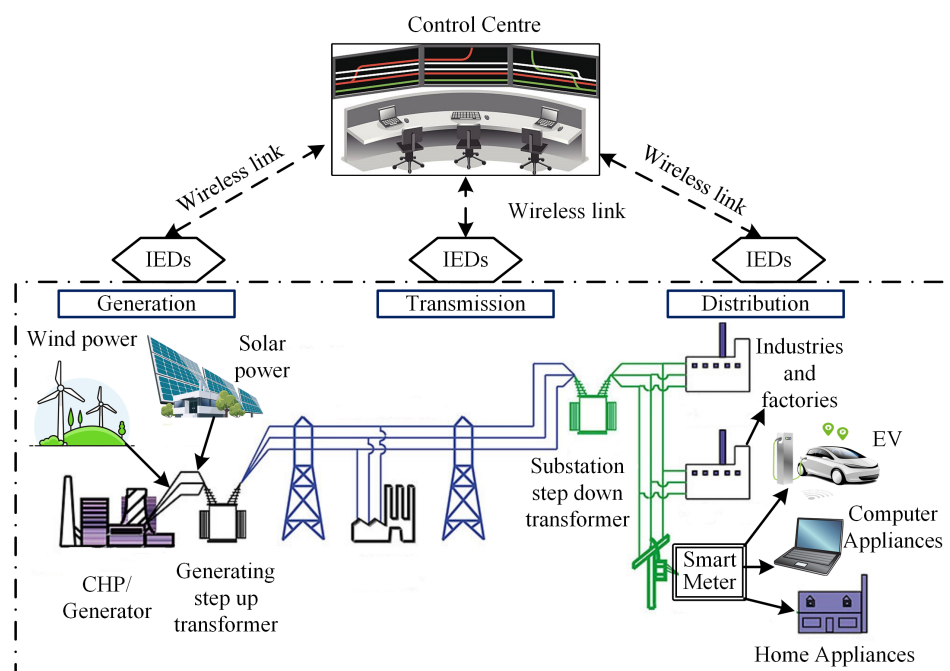


Figure 1. The intelligent electronic device (IED)-based smart cyber-physical power system.

Advanced IEDs have enabled the real-time monitoring and control of power systems and improved the reliability, maintenance, and power quality of the network. A brief discussion of different categories of IEDs in the distribution system is given as follows:

- **Customer Monitoring IEDs:** Customer revenue meters are the best way to obtain data on the electric supply performance. Modems, Zig-Bee, IIRIG-B, and many others are the multi-functional meters used by commercial, industrial, and residential customers.
- **Feeder Monitoring IEDs:** Mainly, electronic controllers such as voltage regulators, switches, recloser, and capacitor banks are used as feeder monitoring infrastructure. The SCADA-based control center collects information from these devices on steady-state conditions.
- **Substation Monitoring IEDs:** Several RTUs such as PMUs are used in the substation monitoring system to collect status data, voltages, currents, and powers. Other IEDs, such as digital intelligent relays, are also deployed to generate autonomous control decisions.

2.1. The Energy Management System

The control center in EMS continuously monitors the power system through different types of IEDs deployed in various critical geographical locations and generates necessary control decisions based on the current status and/or states of the system. The ICT-based cyber layer is a fundamental element for providing accurate information between IEDs and the control center by using diverse transmission media within specific protocols. Two types of data: (1) Topological and system configuration data such as transformer settings, circuit breakers' (CBs) status, and line impedance data, and (2) measurement data from remote IEDs that are collected by the control center for estimating the system's states and generating necessary control operations. Status data and measurement data sent by IEDs can be corrupted or disrupted while transmitting through the communication channel. Bad data detection techniques are utilized to detect and eliminate those corrupt and disrupted data. The state estimation process and bad data detection mechanism are discussed below.

2.1.1. State Estimation

The state estimator processes redundant measurements to determine the optimal current operating system's states such as bus voltages, currents, angles, and many others. Based on reliable real-time data, the state estimator analyses the contingencies and determines the required control actions [5]. As nonlinear power flow equations are computationally intensive for an attacker, a weighted least square (WLS) static state estimation model is considered in this paper to estimate voltage phasors at a given point in time.

For the WLS state estimation, it is considered that the network topology and parameters are completely known, and system states include bus-voltage phasors only. Therefore, the state vector of the network can be expressed as

$$\theta = [\theta_1, \theta_2, \dots, \theta_{N-1}]^T \quad (1)$$

where θ represents the state vector. In addition, θ_i is a system state where $i = 1, 2, 3, \dots, N$ and N is the total number of states. T represents the transpose of the vector matrix for rest of the article. The received measurement vector z can be represented as

$$z = h(\theta) + e \quad (2)$$

where $h(\theta) = [h_1(\theta), h_2(\theta), \dots, h_m(\theta)]^T$ is a function of state variables and the measurement error due to communication noise, $e = [e_1, e_2, \dots, e_m]$ is a Gaussian vector with known covariance R .

All branch resistances and shunt elements can be neglected in the DC state estimation process, while real power flow measurements are obtainable by performing DC load flow analysis only. The power flow equation can be expressed as

$$P_{km} = \frac{\theta_k - \theta_m}{x_{km}} + v \quad (3)$$

where P_{km} is the power flow from bus k to bus m , θ_k and θ_m are phase angles related to bus k and m , x_{km} represents the branch reactance, and v is the measurement error. Similarly, the power injection at bus k can be expressed as

$$P_k = \sum_{m \in N_m} P_{km} + w \quad (4)$$

where N_m represents the number of connecting buses at the bus m . P_k is the power injection to bus k and w is the measurement error. Therefore, the real power flow measurement vector for the DC state estimation model is represented as

$$z = H\theta + e \quad (5)$$

where real power flows and real power injections are considered, and the Jacobian matrix \mathbf{H} is a function of branch reactance only.

Assuming $m \geq n$ and $\mathbf{H} \in \mathbb{R}^{m \times n}$, the rank of the Jacobian matrix, $\mathbf{H} = n$. As a result, system's state vector, θ can be obtained by using the weighted least square (WLS) estimator which can be formulated as

$$\underset{\theta}{\operatorname{argmin}} J(\theta) = \frac{1}{\sigma^2} \|\mathbf{z} - \mathbf{H}\theta\|^2 \quad (6)$$

where σ^2 is the meter measurement variance. The formulated problem can be solved iteratively (e.g., using gradient-based Newton's method [5]). The estimated state vector $\hat{\theta}$ is obtained as

$$\hat{\theta} = (\mathbf{H}^T \mathbf{W} \mathbf{H})^{-1} \mathbf{H}^T \mathbf{W} \mathbf{z} \quad (7)$$

where $\mathbf{W} = \mathbf{R}^{-1}$ and \mathbf{R} is the measurement error variances.

Now, the measurement residue \mathbf{r} can be calculated as

$$\mathbf{r} = \mathbf{z} - \mathbf{H}\hat{\theta} \quad (8)$$

The BDD module uses this calculated residue as a key parameter to detect incorrect received measurements.

2.1.2. Bad Data Detection

The measurement data can be corrupted or misleading because of a meter malfunction or the low service efficiency of communication networks. The poor quality of data can affect the state estimation process and mislead control decisions. As a common practice, a chi-square (χ^2) test is performed on the measurement residue between original and estimated measurements. It is assumed that the noise in the communication channel are independent and follow a normal distribution with zero mean. Therefore, the objective function $J(\theta)$ will follow the chi-square distribution with $\psi = (m - n)$ degree of freedom. A detection threshold $\tau = \chi^2_{(m-n), p}$ for a particular detection confidence can be obtained using the chi-square distribution table. The measurement vector is suspected as containing the bad measurement if the objective function, $J(\theta) \geq \tau$; otherwise, the measurement vector is free from bad measurements. After that, the largest normalized residual (LNR) test is conducted to identify and eliminate bad data from the measurement vector.

3. Cyber Attacks on the EMS

As described in Section 2.1, several IEDs are emerging along with advanced ICT-based cyber networks for the real-time monitoring and control of power systems. Smart remote terminal units (RTUs) such as PMUs or other sensor-based meters are sparsely deployed throughout the power network to measure power system quantities and the current status of the system. The measurements can be corrupted or distorted due to the meter malfunctions or communication noise. In addition to that, RTUs, communication channels, and SCADA databases are subject to cyber attacks. However, an attacker can inject malicious or false measurements into the SCADA system with the aim of misleading the state estimation process by evading the bad data detector. An EMS model indicating all vulnerable cyber nodes are portrayed in the Figure 2.

In most cases, bad or corrupt measurements and randomly generated malicious injections are detected by the traditional chi-square-based BDD. However, attack signals constructed by using the complete or partial system topological information bypass the BDD and the state estimation converges [21]. Another study also proved that attack signals can be constructed without the prior knowledge of the topological information by using measurement signals only [22]. Both types of stealthy FDIAs construction are discussed in the following subsections.

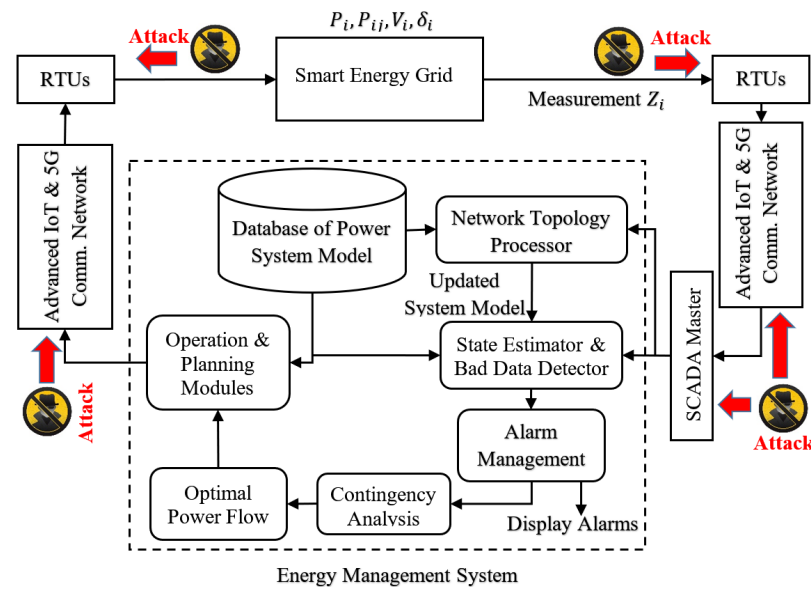


Figure 2. A supervisory control and data acquisition (SCADA)-based energy management system (EMS) representing different cyber-vulnerable nodes.

3.1. Knowledge Based FDI Attack Model

An attacker can compromise physical meters to inject cyber attacks into the SCADA system. As meters are sparsely distributed and attackers have limited resource to compromise a sufficient number of meters to launch stealthy attacks, a man-in-the-middle (MITM)-type attack scenario is considered in this research. In MITM, the attacker invades the communication channel and injects a false attack vector \mathbf{a} into the SCADA measurement vector \mathbf{z} . Therefore, the measurement vector received by the control center is $\mathbf{z}_a = \mathbf{z} + \mathbf{a}$. For instance, it is assumed that the attacker has complete information of the system's Jacobian matrix \mathbf{H} . Therefore, the system state vector $\hat{\theta}_a$ is estimated by using compromised measurements as follows:

$$\begin{aligned}\hat{\theta}_a &= (\mathbf{H}^T \mathbf{W} \mathbf{H})^{-1} \mathbf{H}^T \mathbf{W} \mathbf{z}_a \\ &= (\mathbf{H}^T \mathbf{W} \mathbf{H})^{-1} \mathbf{H}^T \mathbf{W} (\mathbf{z} + \mathbf{a}) \\ &= \hat{\theta} + (\mathbf{H}^T \mathbf{W} \mathbf{H})^{-1} \mathbf{H}^T \mathbf{W} \mathbf{a}\end{aligned}\quad (9)$$

If the attack injection vector $\mathbf{a} = \mathbf{H} \mathbf{c}$, where \mathbf{c} is a randomly generated vector; the 2-Norm of the measurement residual can be written as

$$\begin{aligned}\|\mathbf{z}_a - \mathbf{H} \hat{\theta}_a\| &= \|\mathbf{z} + \mathbf{a} - \mathbf{H} (\hat{\theta} + (\mathbf{H}^T \mathbf{W} \mathbf{H})^{-1} \mathbf{H}^T \mathbf{W} \mathbf{a})\| \\ &= \|\mathbf{z} - \mathbf{H} \hat{\theta} + (\mathbf{a} - \mathbf{H} (\mathbf{H}^T \mathbf{W} \mathbf{H})^{-1} \mathbf{H}^T \mathbf{W} \mathbf{a})\| \\ &= \|\mathbf{z} - \mathbf{H} \hat{\theta} + (\mathbf{H} \mathbf{c} - \mathbf{H} \mathbf{c})\| \\ &= \|\mathbf{z} - \mathbf{H} \hat{\theta}\| \leq \tau\end{aligned}\quad (10)$$

where τ is the bad or corrupted data detection threshold. As both normal and attack cases have 2-Norm measurement residue values lower than the chi-square threshold, the BDD will fail to detect false data injections into the measurement vector.

3.2. Blind FDI Attack Model

In reality, the topology of the network and impedance of transmission lines are confidential information and updated periodically over time. Therefore, generating stealthy attack vector using measurement signals is a more practical approach from the attacker's point of view. A blind false data injection method is proposed in [23] by using the principal component analysis (PCA) approximation method. By using this technique, an approximate system Jacobian matrix \mathbf{H} can be calculated from measurement data aiming to construct a

successful stealthy attack vector. After the successful implementation of the PCA technique on the collected time series measurement matrix $\mathbf{Z}_{d \times m}$, the attacker achieves a transformation matrix $\tilde{\mathbf{M}}$ and a vector of principal components \mathbf{x} . The PCA transformation can be expressed as

$$\tilde{\mathbf{M}}^T \mathbf{Z} = \mathbf{x} \quad (11)$$

As \mathbf{H} is an n rank matrix, the system's Jacobian matrix construction will involve only n number of eigenvectors. Therefore, the representation of the measurement matrix is

$$\mathbf{Z} \approx \begin{bmatrix} \tilde{M}_{1,1} & \tilde{M}_{1,2} & \cdot & \cdot & \cdot & \tilde{M}_{1,n} \\ \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\ \tilde{M}_{m,1} & \tilde{M}_{m,2} & \cdot & \cdot & \cdot & \tilde{M}_{m,n} \end{bmatrix} \begin{bmatrix} \tilde{x}_1 \\ \cdot \\ \cdot \\ \cdot \\ x_n \end{bmatrix} \quad (12)$$

where the approximated Jacobian matrix is a $m \times n$ matrix.

Now, an attack vector $\mathbf{a}_{\text{pca}} = \mathbf{H}_{\text{pca}} \mathbf{c}$ can easily be constructed that will remain hidden during the chi-square test and bypass the BDD module. The readers are referred to the work in [23] for further details of blind PCA-based stealthy attack construction and its impacts.

4. Data Preparation and Attack Detection Methods

In this paper, the IEEE benchmark 14-bus power system is considered as a test system, and cyber attacks and fault scenarios are simulated in this system by utilizing one year of real-time load flow data from NYISO [24]. The 14-bus test system is comprised of five generators, fourteen node buses, and twenty interconnecting branches. As shown in the Figure 3, a total of 54 power sensor-based IEDs are deployed in different locations to measure power injections and power flows in different nodes and buses. Meter measurements are transmitted to the control center through wireless communication channels for contingency analysis and other different EMS operations. Meter readings received by the control center during different case scenarios such as with-communication noise, cyber attacks, and faults are utilized to generate training and test data set for MLAs. After that, performances of different state-of-the-art MLAs are evaluated for several case scenarios to discriminate between faults and cyber-attack data in the SCADA-EMS.

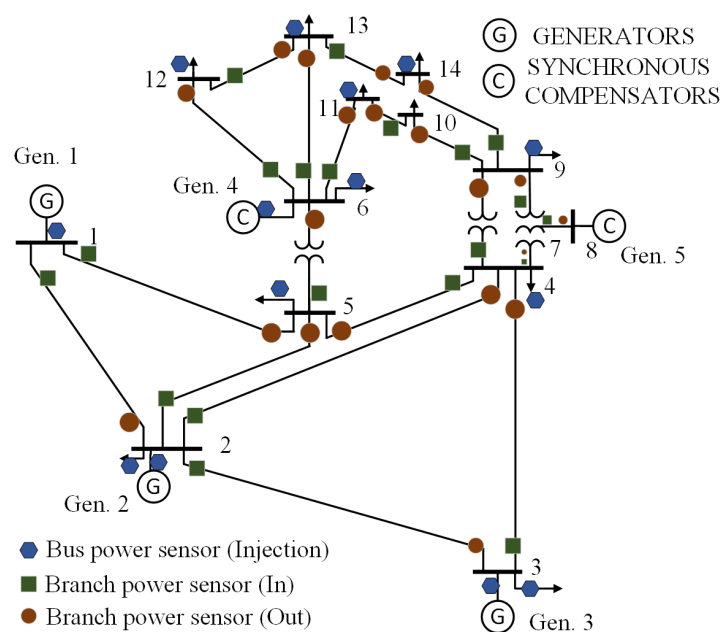


Figure 3. The IEEE 14-Bus system with sensors in different locations [22].

4.1. Dataset Preparation

Three case scenarios—normal operation, cyber attacks, and faults—are considered in this paper to generate training and test data. The data generation processes of different case scenarios and their impacts on the state estimation process are briefly discussed below.

4.1.1. Original and With-Noise Measurements

The original measurement refers to the actual value of power flow in a node or bus. On the other hand, Gaussian noise with an SNR between 20~35 DB is considered in this paper as a communication and sensor noise. The measurement residue between the estimated measurement and received original measurement is very small, whereas the measurement residue due to noise shows a value greater than the value with the original measurement. However, the measurement residue calculated for the noise signal remains below the BDD threshold value, and thus it bypasses the module. A chi-square detection threshold can be obtained for a particular confidence interval value. For example, the detection threshold is 56.94 considering 95% confidence interval of a chi-square test [5]. Measurement residues of original measurements and with-noise measurements are below 56.94, and thus bypass the BDD module. In contrast, measurement data are considered corrupted while the residue value is more than the threshold value. The original and with-noise measurements data are considered as no-attack data. In this research, no-attack data are generated by using yearly load flow data collected from the NYISO.

4.1.2. Random and Stealthy Attack Measurements

During gross error or random attacks on measurement signals, the residue is greater than the chi-square threshold and detected by the BDD module. However, in cases of stealthy attacks, the measurement residue between the attack measurement and estimated measurement is below the detection threshold and remains hidden in the system. Figure 4a shows the original measurements, estimated measurements, and attack measurements, and Figure 4b shows the actual system states and the system states during stealthy attacks. In Figure 4a, although attack measurements are different from original measurements, the estimated measurements are very close to the original measurements. As a result, measurement residues between the original and estimated measurement will remain below the chi-square threshold value and will bypass the BDD. Furthermore, the system's states are deviated from the original states as shown in the Figure 4b. Two sets of random attack and stealthy attack data are generated for the training and testing of machine learning-based algorithms.

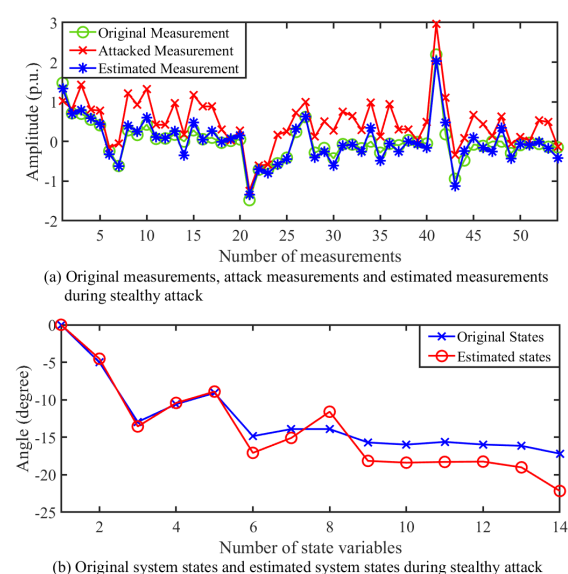


Figure 4. Estimated measurements and system states during cyber attacks.

4.1.3. During-Fault Measurements

Faults in a power system are considered natural disturbances. When fault data are detected, the control center generates certain control actions to mitigate the effects on the system. To avoid any undesired situation, the operator must differentiate between attack signals and faults. The three-phase-to-ground fault is the most severe type of fault and is considered in this research to generate during-fault data. To demonstrate practical case scenarios, faults are considered in different nodes for various load variations. In addition, fault impedance is also randomly varied throughout the simulation process.

4.1.4. Overview of the Complete Dataset

In the NYISO, the measurement samples are taken as five-minute intervals. Therefore, a total of 290 instances of measurement data are recorded for a day, and a total 212,338 sets of measurement data are generated for each no-noise, with-noise, random attack, stealthy attack, and fault cases throughout a year. The total number of data generated for no-attack, with-attack, and fault data are presented in Table 1. Both original data and with noise data are incorporated in the no-attack data set. Random attacks are randomly generated attack signals and stealthy attacks are those attack signals, which have ability to successfully bypass the BDD.

Table 1. Data for no-attack, cyber attack, and fault scenarios.

Situation	No. of Records
No-Attack/Normal operation	424,676
Randomly generated attacks	212,338
Stealthy Attacks (PCA, SVD, and Known H) [6,23,25,26]	212,338
Fault	212,338

4.2. Performance Metrics for Machine Learning Algorithms

MLAs learn from the provided training data and build mathematical models to make decisions on test data. In this paper, five popular state-of-the-art MLAs—Random Forests, OneR, Naive Bayes, SVM, and AdaBoost—are selected from five distinct categories to evaluate their performance in detecting normal data, cyber attacks, and faults. The MLAs and their respective categories are presented in the Table 2.

Table 2. Machine learning algorithms and their respective categories.

Name	Category
Random Forests	Decision tree learning
OneR	Rule induction
AdaBoost	Boosting, a meta-algorithm for learning
Naive Bayes	Probabilistic classification
SVM	Non-probabilistic binary classification

The performance of an MLA for given data can be evaluated using different performance metrics. The detection rate and the false positive rate of an MLA can be obtained using following equations:

$$\text{Detection Rate} = \frac{x_{ta} - x_{fn}}{x_{ta}} \times 100 \quad (13)$$

$$\text{False Positive Rate} = \frac{x_{fp}}{x_t} \times 100 \quad (14)$$

where x_{ta} = the total number of anomalies, number of false positives, x_{fp} = the number of normal data classified as anomalous data, the number of false negatives, x_{fn} = the number of anomalies classified as normal data, and x_t = the total number of data.

The detection rate always does not show the actual performance of the algorithm. For that, there are many other performance parameters such as precision, recall, and f-measure. The precision parameter is used to identify the ability of a classifier to predict overall positive values and can be expressed as

$$\text{Precision} = \frac{x_{tp}}{x_{tp} + x_{fp}} \quad (15)$$

where number of true positives, x_{tp} = the number of normal data classified as normal data.

The Recall is a metric that measures the true positive rate and is expressed as

$$\text{Recall} = \frac{x_{tp}}{x_{tp} + x_{fn}} \quad (16)$$

where x_{tp} and x_{fn} have the same meaning as Equations (13)–(15).

The f-Measure parameter represents the mean of both precision and recall and is expressed as

$$\text{F-Measure} = \frac{2 \times \text{Precision} \times \text{Recall}}{\text{Precision} + \text{Recall}} \quad (17)$$

The machine learning performance parameters such as precision, recall, and f-measures are the ratios of two different numbers and the performance score varies from 0 to 1 to the robustness of an MLA.

5. Results and Discussions

Different case scenarios of normal operational, random, and stealthy cyber attacks and faults are simulated in the IEEE 14-bus test system. Cyber attack detection and the discrimination between faults and cyber attacks are performed by using a machine learning analytical platform called WEKA [27].

5.1. Cyber Attack Detection

Two types of cyber attacks—random and stealthy attacks—are considered in this paper. Random attacks are detected by the BDD module because of their high measurement residue value, but stealthy attacks can successfully circumvent the BDD. Therefore, two case scenarios are considered to evaluate the cyber attack detection performance of MLAs: successful stealthy cyber attacks in the historical data and synthesized stealthy attacks in the historical data. Successful stealthy cyber attacks circumvent the BDD and labeled as normal data. On the other hand, synthesized data are prepared by using a proper mathematical model and are labelled as attack data to train MLA classifiers.

5.1.1. CASE A: Considering Successful Stealthy Cyber Attacks in the Historical Data

In this case study, cleverly generated attacks are considered hidden and bypassed through the BDD module. The original and with-Gaussian-noise data are considered as normal operational data. Randomly generated attack data and stealthy attack data generated by using a known system Jacobian matrix and using PCA and SVD methods are considered as cyber attack data. In addition, the measurement residue of some of the random attack data can be below the detection threshold and hence are labeled as normal data.

5.1.2. CASE B: Considering Synthesized Stealthy Attacks in the Historical Data

In this case study, synthesized stealthy attacks are generated to train the classifiers and considered as historical attack data. Unlike CASE A, stealthy data are not labeled as normal data; rather, they are labeled as attack data.

The detection rate and the false positive rate of different state-of-the-art classifiers are presented in Tables 3 and 4. As MLA classifiers are trained with a similar kind of normal data, the detection rate of normal data is higher in both CASE A and B. However, attack

data are considered stealthy in CASE A. Therefore, all classifiers show a detection rate that is below 75%, and the false positive rate is higher than 0.25%. In contrast, MLA classifiers are trained with synthesized stealthy data for CASE B, and very high detection rates and low false positive rates are achieved by all classifiers. The lower detection rate of CASE A and higher detection rate of CASE B show that the performance of MLAs are highly dependent on their training data types and their availability. However, providing relevant historical or synthesized data highly improves the detection rates and reduce the chances of being false positives which are clearly manifested in Tables 3 and 4.

Table 3. Detection rate (%) for CASES A and B.

	Random Forests	OneR	Naive Bayes	SVM	AdaBoost
CASE A	74.92	74.15	25.10	74.92	72.97
CASE B	99.79	98.58	99.79	99.76	93.78

Table 4. False positive rate (%) for CASE A and B.

	Random Forests	OneR	Naive Bayes	SVM	AdaBoost
CASE A	0.251	0.259	0.251	0.251	0.271
CASE B	0.002	0.014	0.002	0.002	0.062

The precision, recall, and f-measure values of different classifiers for CASE A and B are depicted in Figure 5. The weighted values of performance parameters show that CASE B is more robust in detecting cyber attacks. In CASE A, all performance parameters are low because of the stealthy attacks in the system data. However, the average performance parameters reach up to 0.83 because of the successful detection of normal data.

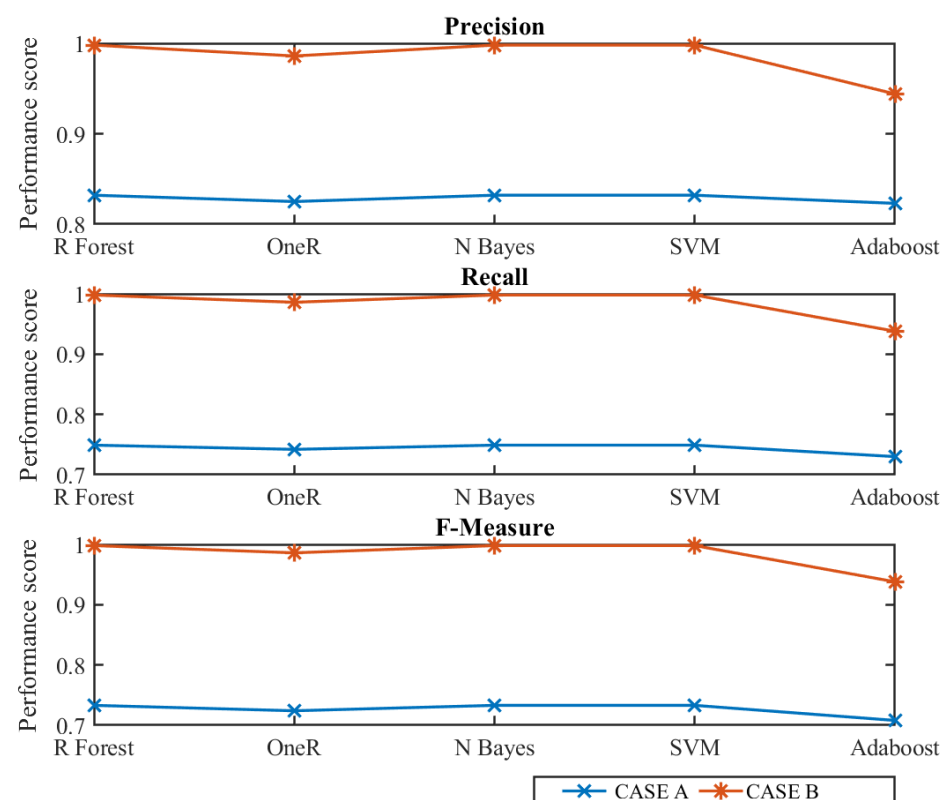


Figure 5. Precision, Recall, and F-measure of different MLAs for CASES A and B.

5.2. Discriminating between Cyber Attacks and Faults

For distinguishing between cyber attacks and faults, five case scenarios of no-attacks, cyber attacks, and faults are considered as training and testing classes of selected state-of-the-art MLAs and are presented in Table 5.

Table 5. Different case scenarios for discriminating between cyber attacks and faults.

CASES	Training Class 1	Training Class 2	Test Class 1	Test Class 2
1	Attack	Normal	Attack	Normal
2	Fault	Normal	Fault	Normal
3	Attack	Fault	Attack	Fault
4	Fault & Attack	Normal	Fault & Attack	Normal
5	Fault	Normal	Fault & Attack	Normal

For distinguishing between cyber attacks and faults, both random and stealthy attacks are considered as attacks, and a three-phase-to-ground fault in the transmission line is considered as a fault. The successful detection rate of instances for different case scenarios is presented in Table 6, and the false positive rate is presented in Table 7.

Table 6. Detection rate (%) for different case scenarios.

CASES	Random Forests	OneR	Naive Bayes	SVM	AdaBoost
1	99.90	98.70	99.90	99.90	99.87
2	99.81	99.84	99.84	95.58	99.44
3	99.84	99.87	90.01	93.97	99.87
4	99.92	98.67	99.44	98.16	99.54
5	91.66	60.26	93.85	62.76	76.44

Table 7. False positive rate (%) for different case scenarios.

CASES	Random Forests	OneR	Naive Bayes	SVM	AdaBoost
1	0.001	0.013	0.001	0.001	0.001
2	0.002	0.002	0.002	0.087	0.087
3	0.002	0.002	0.197	0.098	0.002
4	0.001	0.011	0.004	0.013	0.003
5	0.059	0.269	0.044	0.252	0.161

In CASE 1, attacks (both random and stealthy attacks) and normal data are provided as training data and test data. All classifiers learn from training data and successfully detect most of the instances, and their false positive rates are also negligible. As training and test data of similar categories are provided for CASES 2–4, analogous results were obtained. This proves that similar data type in the historical and present data provide a higher detection rate and lower false positive rate.

In CASE 5, only faults and normal data are considered as historical data and used as training classes for MLAs. However, the test class contains both stealthy and random types cyber attack data. As a result, the detection rates of all classifiers are decreased and false positive rates are increased.

In Figure 6, the MLA performance parameters such as precision, recall, and f-measures for CASES 1–5 are depicted. For CASES 1–4, MLA classifiers show a very high performance, but this degrades for CASE 5 because of the absence of cyber attack data in the historical dataset. However, reduced performance parameters are not less than 0.6, which indicate that either enough historical data or appropriate modifications are needed to increase the successful detect rate of stealthy type cyber intrusions.

In addition to the discrimination between during fault measurements and FDIAs, significant efforts are required to separate inaccurate measurements and faulted measurement devices' (current and voltage transformers and sensors) data from false data injections.

To achieve satisfactory results, additional historical data from transformers and circuit breakers are required to train MLAs. In addition, deployment of more IEDs with higher data transfer capability can assist the control centre to distinguish between the inaccurate measurements and faulted measurement devices' measurements.

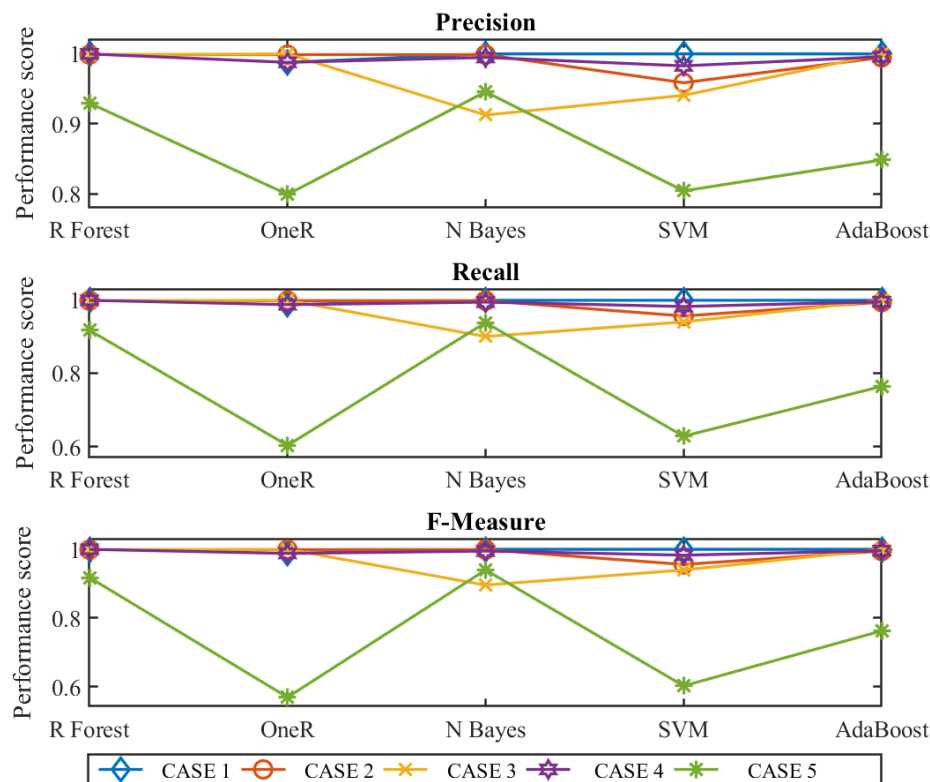


Figure 6. Precision, Recall, and F-measure of different machine learning algorithms for different case scenarios.

6. Conclusions

A MLA-based cyber attack and fault discrimination approach is presented in this paper. First, normal operational data, random and stealthy attack data, and three-phase-to-ground fault data are generated. Second, different case scenarios are considered to evaluate MLA performance parameters such as the detection rate, false positive rate, precision, recall, and f-measure in detecting stealthy cyber attacks. Finally, state-of-the-art MLA classifiers—Random Forest, OneR, Naive Bayes, SVM, and AdaBoost—are used to distinguish between cyber attacks and faults in an IED-based EMS. The results show that synthesized stealthy attacks in historical data highly improve the detection rate of MLA classifiers. In addition, the robustness of all classifiers in detecting cyber attacks decreases when they are trained only with faults and normal operational data. All MLAs, except Naive Bayes, showed similar results during successful stealthy attacks (CASE A). However, detection rates improved for all MLAs while stealthy attacks (CASE B) are considered. In contrast, all MLAs show similar performance for CASES 1–4 while discriminating faults and attacks. However, detection rates of OneR and SVM drop below 65%, while historical attack data are absent from the training data set.

The future scopes of this paper include the analysis of other types of cyber attacks, such as DoS, DDos, replay, and many others, and generate synthesized data for the early training of MLAs in distinguishing between cyber attacks and faults.

Author Contributions: Conceptualization, B.M.R.A. and A.A.; methodology, B.M.R.A.; validation, B.M.R.A., M.J.H., A.A., and S.Z.; formal analysis, B.M.R.A.; writing—original draft preparation, B.M.R.A.; writing—review and editing, S.Z., M.J.H., and A.A.; visualization, B.M.R.A. and S.Z.; supervision, M.J.H. All authors have read and agreed to the published version of the manuscript.

Funding: This research received no external funding.

Conflicts of Interest: The authors declare no conflicts of interest.

References

1. Mlakic, D.; Reza Baghaee, H.; Nikolovski, S.; Vukobratovic, M.; Balkic, Z. Conceptual Design of IoT-Based AMR Systems Based. *Energies* **2019**, *12*, 4281. [CrossRef]
2. Gong, S.; Lee, C. Cyber Threat Intelligence Framework for Incident Response in an Energy Cloud Platform. *Electronics* **2021**, *10*, 239. doi:10.3390/electronics10030239. [CrossRef]
3. ICS Vulnerabilities Key Findings. Available online: <https://www.dragos.com/review/2019-ics-year-in-review-ics-vulnerabilities/> (accessed on 22 January 2021).
4. Wang, Q.; Tai, W.; Tang, Y.; Ni, M. Review of the false data injection attack against the cyber-physical power system. *IET Cyber-Phys. Syst. Theory Appl.* **2019**, *4*, 101–107. doi:10.1049/iet-cps.2018.5022. [CrossRef]
5. Abur, A.; Expósito, A.G. *Power System State Estimation: Theory and Implementation*; CRC: Boca Raton, FL, USA, 2004; p. 327.
6. Liu, Y.; Ning, P.; Reiter, M.K. False Data Injection Attacks against State Estimation in Electric Power Grids. *ACM Trans. Inf. Syst. Secur.* **2011**, *14*, 1–33. doi:10.1145/1952982.1952995. [CrossRef]
7. Liang, G.; Weller, S.R.; Zhao, J.; Luo, F.; Dong, Z.Y. The 2015 Ukraine Blackout: Implications for False Data Injection Attacks. *IEEE Trans. Power Syst.* **2017**, *32*, 3317–3318. doi:10.1109/TPWRS.2016.2631891. [CrossRef]
8. Liang, G.; Zhao, J.; Luo, F.; Weller, S.R.; Dong, Z.Y. A Review of False Data Injection Attacks Against Modern Power Systems. *IEEE Trans. Smart Grid* **2017**, *8*, 1630–1638. [CrossRef]
9. Anwar, A.; Mahmood, A.N.; Tari, Z. Ensuring Data Integrity of OPF Module and Energy Database by Detecting Changes in Power Flow Patterns in Smart Grids. *IEEE Trans. Ind. Inform.* **2017**, *13*, 3299–3311. doi:10.1109/TII.2017.2740324. [CrossRef]
10. Pei, C.; Xiao, Y.; Liang, W.; Han, X. PMU Placement Protection Against Coordinated False Data Injection Attacks in Smart Grid. *IEEE Trans. Ind. Appl.* **2020**, *56*, 4381–4393. doi:10.1109/TIA.2020.2979793. [CrossRef]
11. Gong, S.; Zhang, Z.; Li, H.; Dimitrovski, A.D. Time Stamp Attack in Smart Grid: Physical Mechanism and Damage Analysis. *arXiv* **2012**, arXiv:1201.2578
12. Musleh, A.S.; Chen, G.; Dong, Z.Y. A Survey on the Detection Algorithms for False Data Injection Attacks in Smart Grids. *IEEE Trans. Smart Grid* **2020**, *11*, 2218–2234. [CrossRef]
13. Wei, J.; Mendis, G.J. A deep learning-based cyber-physical strategy to mitigate false data injection attack in smart grids. In Proceedings of the 2016 Joint Workshop on Cyber-Physical Security and Resilience in Smart Grids (CPSR-SG), Vienna, Austria, 12 April 2016; pp. 5–10.
14. Sayghe, A.; Hu, Y.; Zografopoulos, I.; Liu, X.R.; Dutta, R.G.; Jin, Y.; Konstantinou, C. Survey of Machine Learning Methods for Detecting False Data Injection Attacks in Power Systems. *IET Smart Grid* **2020**, *3*, 581–595. doi:10.1049/iet-stg.2020.0015. [CrossRef]
15. Sakhnini, J.; Karimipour, H.; Dehghantanha, A. Smart Grid Cyber Attacks Detection Using Supervised Learning and Heuristic Feature Selection. In Proceedings of the 2019 IEEE 7th International Conference on Smart Energy Grid Engineering (SEGE), Oshawa, ON, Canada, 12–14 August 2019; pp. 108–112.
16. Ahmed, S.; Lee, Y.; Hyun, S.H.; Koo, I. Unsupervised Machine Learning-Based Detection of Covert Data Integrity Assault in Smart Grid Networks Utilizing Isolation Forest. *IEEE Trans. Inf. Forensics Secur.* **2019**, *14*, 2765–2777. [CrossRef]
17. Zhou, M.; Wang, Y.; Srivastava, A.K.; Wu, Y.; Banerjee, P. Ensemble-Based Algorithm for Synchrophasor Data Anomaly Detection. *IEEE Trans. Smart Grid* **2019**, *10*, 2979–2988. [CrossRef]
18. Yu, J.J.Q.; Hou, Y.; Li, V.O.K. Online False Data Injection Attack Detection With Wavelet Transform and Deep Neural Networks. *IEEE Trans. Ind. Inform.* **2018**, *14*, 3271–3280. doi:10.1109/TII.2018.2825243. [CrossRef]
19. Abu Al-Haija, Q.; Zein-Sabatto, S. An Efficient Deep-Learning-Based Detection and Classification System for Cyber-Attacks in IoT Communication Networks. *Electronics* **2020**, *9*, 2152. doi:10.3390/electronics9122152. [CrossRef]
20. Guo, X.; Tan, Y.; Wang, F. Modeling and fault propagation analysis of cyber-physical power system. *Energies* **2020**, *13*, 539. doi:10.3390/en13030539. [CrossRef]
21. Li, Y.; Wang, Y. False Data Injection Attacks with Incomplete Network Topology Information in Smart Grid. *IEEE Access* **2019**, *7*, 3656–3664. doi:10.1109/ACCESS.2018.2888582. [CrossRef]
22. Anwar, A.; Mahmood, A.N.; Pickering, M. Modeling and performance evaluation of stealthy false data injection attacks on smart grid in the presence of corrupted measurements. *J. Comput. Syst. Sci.* **2017**, *83*, 58–72. doi:10.1016/j.jcss.2016.04.005. [CrossRef]
23. Yu, Z.H.; Chin, W.L. Blind False Data Injection Attack Using PCA Approximation Method in Smart Grid. *IEEE Trans. Smart Grid* **2015**, *6*, 1219–1226. doi:10.1109/TSG.2014.2382714. [CrossRef]
24. New York Independent System Operator (NYISO) Real Time Actual Load Data—2018. Available online: <http://mis.nyiso.com/public/P-58Blist.htm> (accessed on 22 January 2021).

-
25. Anwar, A.; Mahmood, A.N. Stealthy and Blind False Injection Attacks on SCADA EMS in the Presence of Gross Errors. In Proceedings of the 2016 IEEE Power and Energy Society General Meeting (PESGM), Boston, MA, USA, 17–21 July 2016; pp. 8–12. doi:10.1109/PESGM.2016.7741557. [[CrossRef](#)]
 26. Kim, J.; Tong, L.; Thomas, R.J. Subspace Methods for Data Attack on State Estimation: A Data Driven Approach. *IEEE Trans. Signal Process.* **2015**, *63*, 1102–1114. doi:10.1109/TSP.2014.2385670. [[CrossRef](#)]
 27. Frank, E.; Hall, M.A.; Witten, I.H. *The WEKA Workbench. Online Appendix for “Data Mining: Practical Machine Learning Tools and Techniques”*, 4th ed.; Morgan Kaufmann: San Francisco, CA, USA, 2016; p. 327.