sustainability

MDPI

Article

Detection and Prevention of False Data Injection Attacks in the Measurement Infrastructure of Smart Grids

Muhammad Awais Shahid [1,*], Fiaz Ahmad [1,*], Fahad R. Albogamy [2], Ghulam Hafeez [3,*] and Zahid Ullah [4]

[1] Department of Electrical & Computer Engineering, Air University, Islamabad 44230, Pakistan
[2] Computer Sciences Program, Turabah University College, Taif University, P.O. Box 11099, Taif 21944, Saudi Arabia; f.alhammdani@tu.edu.sa
[3] Department of Electrical Engineering, University of Engineering and Technology, Mardan 23200, Pakistan
[4] Department of Electrical Engineering, University of Management and Technology Lahore, Sialkot Campus, Sialkot 51310, Pakistan; zahid.ullah@skt.umt.edu.pk
[*] Correspondence: awaisshahid.au.2020@gmail.com (M.A.S.); fiaz.ahmad@mail.au.edu.pk (F.A.); ghulamhafeez393@gmail.com (G.H.)

Abstract: The smart grid has become a cyber-physical system and the more cyber it becomes, the more prone it is to cyber-attacks. One of the most important cyber-attacks in smart grids is false data injection (FDI) into its measurement infrastructure. This attack could manipulate the control center in a way to execute wrong control actions on various generating units, causing system instabilities that could ultimately lead to power system blackouts. In this study, a novel false data detection and prevention paradigm was proposed for the measurement infrastructure in smart grids. Two techniques were devised to manage cyber-attacks, namely, the fixed dummy value model and the variable dummy value model. Limitations of the fixed dummy value model were identified and addressed in the variable dummy value model. Both methods were tested on an IEEE 14 bus system and it was shown through the results that an FDI attack that easily bypassed the bad data filter of the state estimator was successfully identified by the fixed dummy model. Second, attacks that were overlooked by the fixed dummy model were identified by the variable dummy method. In this way, the power system was protected from FDI attacks.

Keywords: smart grid; cyber-physical system; false data injection attacks; false data detection; cyber security

check for updates

Citation: Shahid, M.A.; Ahmad, F.; Albogamy, F.R.; Hafeez, G.; Ullah, Z. Detection and Prevention of False Data Injection Attacks in the Measurement Infrastructure of Smart Grids. *Sustainability* **2022**, *14*, 6407. https://doi.org/10.3390/su14116407

Academic Editors: Luis Hernández-Callejo, Sergio Nesmachnow and Sara Gallardo Saavedra

Received: 30 March 2022
Accepted: 20 May 2022
Published: 24 May 2022

1. Introduction

"Smart grid" is taken as an umbrella term for different technologies. Those technologies are considered alternatives to the traditional methods used to operate the power system. Some of these technologies are advanced metering infrastructure (AMI), demand response, outage management, wide-area measurement system (WAMS), active fault level monitoring, etc. In a smart grid, the power resources can be used efficiently [1,2]. A smart grid has a high dependence on the advanced communication infrastructure, as there is an exchange of a huge amount of data for the proper operation of such a complex network [3–5]. In fact, the smart grid is taken as a network consisting of computers, as well as power infrastructure. All of these are used for monitoring and managing energy usage [6,7]. An automated and distributed energy network is created by the smart grid [8]. Self-monitoring is carried out in the case of a smart grid, which makes the smart grid distinct from a traditional grid [9]. Distributed power resources (DPR) can be accommodated in a smart grid [10,11].

In a power system, if there exists a mismatch between the generation and utilization of power, there will be a deviation of electrical quantities from their actual values. The two-way communication is carried out in a smart grid to have a safe and reliable power flow. That communication should be secure. Sometimes attackers hack these communication links to change the values of power flow in the power network. The hackers attack the power system to obtain different goals. Multiple purposes can be achieved by these attacks. Attacks can be used to obtain financial benefits; create technical problems, such as blackouts of power; and a combination of the two [12–18].

Considering the target of attacks, they can be further divided into three types. The first category involves attacks that target availability. In these attacks, the aim of the attackers is to corrupt, block, or delay the communication in the power system. The second type is attacks that target integrity. In these types of attacks, the attackers try to illegally disrupt data exchange in the smart grid. The final category is attacks that target confidentiality. In these attacks, the attackers try to obtain unauthorized information from the smart network [19].

1.1. Power System State Estimation

The power system state estimation (PSSE) technique is used for the detection of bad data received in the control room. All the received measurements are placed in a vector, which is denoted by **z**. The measurement vector contains the real forward powers, reactive forward powers, real backward powers, reactive backward powers, real powers injected into all the buses, reactive powers injected into all buses, voltage magnitudes, and voltage angles [20–23]. The measurement vector **z** and the state variable **x** have the following relationship:

$$\mathbf{z} = \mathbf{h}(\mathbf{x}) + \mathbf{e} \tag{1}$$

h(x) represents the non-linear function that gives the dependencies between measured values and the state variables, and it can be found using the power system topology. **e** represents random noise of Gaussian form with a zero mean and some known covariance.

In the case of AC state estimation (SE), the weighted least-squares method is adopted for solving the state variables with an objective function [24,25]:

$$\min F(\mathbf{x}) = (\mathbf{z} - \mathbf{h}(\mathbf{x}))^{\mathrm{T}} \mathbf{W} (\mathbf{z} - \mathbf{h}(\mathbf{x})) \tag{2}$$

where **W** is the weighting matrix, as given in [26]. This is an unconstrained optimization problem whose first-order optimality condition is given by:

$$\left. \frac{\partial F(\mathbf{x})}{\partial \mathbf{x}} \right|_{\mathbf{x}=\hat{\mathbf{x}}} = -2\mathbf{H}^{\mathrm{T}}(\hat{\mathbf{x}}) \mathbf{W} (\mathbf{z} - \mathbf{h}(\hat{\mathbf{x}})) = 0 \tag{3}$$

Here, **H** represents the Jacobian matrix and $\hat{\mathbf{x}}$ is taken as the vector of the estimated states. An iterative process can be used for solving this non-linear equation [27].

The non-linear function can be approximated by a linear function by using some DC assumptions. Those assumptions are given as follows:

1. The voltage magnitudes of all the buses are very close to each other and they are assumed to be "1 pu".
2. The active power transmission through the transmission lines is taken as lossless, i.e., there are no losses in the transmission lines.
3. The value of reactive power injected into all the buses, as well as flowing through the transmission lines, is taken as zero.
4. There is a small difference in the voltage angles of two buses such that "*Sin*$(\delta\phi) \approx \delta\phi$"

After applying the DC assumptions, we can rewrite the above equations in this form:

$$\mathbf{z} = \mathbf{H}\mathbf{x} + \mathbf{e} \tag{4}$$

H is known as the Jacobian matrix of the power system topology. If the measurement vector has m values and the number of states is n, then the Jacobian matrix **H** will have an order of "$m \times n$". In (4), **x** contains the bus voltage angles. **z** contains the values of active powers flowing through the transmission lines and injected into all the buses.

The Jacobian matrix $\mathbf{H}$ is constant during each iteration of the linearization process. In the DC power flow model (4), the Jacobian matrix $\mathbf{H}$ is constant throughout. Equation (4) will be valid for each iteration of the linearization model (3). Therefore, the same notation is adopted for both the linearized model (3) and the DC power flow model (4).

The weighted least square (WLS) approach is used for estimating the states. In the WLS algorithm, the estimated state $\hat{\mathbf{x}}$ can be written as follows [19,22]:

$$\hat{\mathbf{x}} = \left(\mathbf{H}^{\mathrm{T}}\mathbf{R}^{-1}\mathbf{H}\right)^{-1}\mathbf{H}^{\mathrm{T}}\mathbf{R}^{-1}\mathbf{z} \tag{5}$$

$\mathbf{R}$ represents the covariance matrix of $\mathbf{e}$. The estimated states, as well as the measurement vector $\mathbf{z}$, are used for the calculation of the measurement residue.

$$\mathbf{r} = \mathbf{z} - \mathbf{H}\hat{\mathbf{x}} \tag{6}$$

Then, the normalized L_2-norm is calculated for $\mathbf{r}$.

$$L(\mathbf{r}) = \mathbf{r}^{\mathrm{T}}\mathbf{R}^{-1}\mathbf{r} \tag{7}$$

A comparison of $L(\mathbf{r})$ is done with the threshold $\boldsymbol{\tau}$ for finding the presence of bad data. The X_2—test is used for the determination of the threshold $\boldsymbol{\tau}$.

$$\mathbf{r}^{\mathrm{T}}\mathbf{R}^{-1}\mathbf{r} \leq \boldsymbol{\tau} \tag{8}$$

Bad data do not exist if the condition in (8) is satisfied. Similarly, when the condition is not satisfied, bad data exist in the system.

1.2. Stealth False Data Injection (FDI) Attack

A stealth attack is a special type of attack that bypasses the PSSE technique test. The residual test is not able to detect a stealth attack. This attack is also known as an unobservable attack or undetectable attack. In a stealth attack, the Jacobian matrix $\mathbf{H}$ is fully known to the attacker. $\mathbf{H}$ is used for the construction of an undetectable attack. Stealth false data injection (FDI) is given as follows [17,19,22,28–30]:

$$\mathbf{z_a} = \mathbf{z} + \mathbf{a} \tag{9}$$

where $\mathbf{a}$ represents the vector of false data that is added to the measurement vector $\mathbf{z}$. The attacker hacks the data from the communication line and injects the attack vector $\mathbf{a}$ into it, where $\mathbf{a} = \mathbf{Hc}$.

The attack is done on the communication line by the attacker and all measurements of power are hacked. The Jacobian matrix $\mathbf{H}$ is determined with the help of those measurements of power. The whole power system topology can be understood with the help of $\mathbf{H}$. The dependence of one power value on the other powers can be found using $\mathbf{H}$. This leads the attacker to make an undetectable attack. In fact, it tells the attacker which specific values of power the attacker will have to change with one particular change in power. To understand the whole power network, the formation of the Jacobian matrix $\mathbf{H}$ is the most important component. The vector $\mathbf{c}$ is multiplied by matrix $\mathbf{H}$ and the resultant is added to the actual measurements when undertaking a stealth attack.

The stealth attack is executed against the PSSE in the power network and that is the attack of injecting false data into the system measurements. The state estimation technique is bypassed by the stealth attack [31]. In case of an attack, the estimated state becomes:

$$\hat{\mathbf{x}}_{\mathbf{a}} = \left(\mathbf{H}^{\mathrm{T}}\mathbf{R}^{-1}\mathbf{H}\right)^{-1}\mathbf{H}^{\mathrm{T}}\mathbf{R}^{-1}\mathbf{z_a} \tag{10}$$

$$\hat{\mathbf{x}}_{\mathbf{a}} = \hat{\mathbf{x}} + \mathbf{c} \tag{11}$$

The estimated state is changed in the case of a stealth attack. Now, the estimated state is equal to the original estimated state plus the addition of a constant vector **c**. It is assumed that **c**~$N(0,\sigma_c^2)$, where the false state variance is represented by σ_c^2.

$$\mathbf{z_a} = \mathbf{Hx} + \mathbf{e} + \mathbf{a} = \mathbf{Hx} + \mathbf{e} + \mathbf{Hc} \tag{12}$$

$$\mathbf{z_a} = \mathbf{Hx_a} + \mathbf{e} \tag{13}$$

Therefore, the attack changes the state of the power system. The technique used in the system for bad data detection is bypassed by the stealth false data injection attack in this way:

$$\mathbf{r_a} = \mathbf{z_a} - \mathbf{H\hat{x}_a} = \mathbf{r} \tag{14}$$

The attacked residual is represented by $\mathbf{r_a}$. In the attack, the attacked residue is the same as that of the normal residue. Therefore, the technique of bad data detection using residue is bypassed by this attack and the defender is not able to detect the stealth attack.

1.3. Contributions

The key contributions of this study are the following:

1. It was shown that the bad data filter of the state estimation was only useful for detecting bad measurement data and could not efficiently detect a stealth FDI, making the system vulnerable to all such attacks.
2. A fixed dummy value model was proposed and it was shown that the false data attacks that went undetected by the bad data filter could be successfully detected.
3. Since the dummy value in the fixed dummy value model is kept fixed, the intruder may obtain a clue about it and may change the measurement, keeping the same dummy value, therefore causing this model to be vulnerable to FDI attacks. To address the vulnerability of the fixed dummy value model, another technique for the variable dummy value model was also proposed, which was shown to successfully counter such attacks.

In this work, a quasi-steady state system was assumed to carry out the AC state estimation model. Therefore, the dynamic model of the system is not discussed. For the AC state estimator, the Jacobian matrix H is obtained after the linearization of the measurement model at every iteration. Thus, Equation (5) is solved at each iteration until a stopping threshold is reached.

The organization of the rest of the paper is as follows. Section 2 contains a brief literature review of the different methods and frameworks used for the detection of attacks. Section 3 consists of the proposed model of the fixed dummy value model. Section 4 discusses the simulations and results of DC state estimation, AC state estimation, and fixed dummy value model. The limitations of the fixed dummy value model are also given in that section. Section 5 covers the variable dummy value model. The simulations and results of the variable dummy value model are present in Section 6. Moreover, Section 7 is devoted to the discussion of results and future work. Section 8 contains the conclusion.

2. Literature Review

A large variety of methods and algorithms have been used for detecting stealth attacks. Machine learning methods achieved significant success in this area. In [32], supervised learning based on recurrent neural networks (RNNs) was used for detecting FDI attacks. In [16], three supervised machine learning classifiers, namely, SVM, k-nearest neighbor (kNN), and the extended nearest neighbor (ENN), were used. Different machine learning algorithms are proposed in [28] for measurement classification. Measurements are classified as attacked or secure. Sparse logistic regression, SVM, and k-nearest neighbor methods were used in that study. Another technique was proposed in [33] for the detection of FDI attacks, which used the Gaussian mixture model. The contribution in [34] was based on unsupervised learning. Four machine learning methods, namely, a one-class SVM, local outlier factor, isolation forest, and robust covariance estimation, were employed for FDI attack detection. In [35], a machine-learning-based scheme was used that employed ensemble learning. In ensemble learning, there is a use of multiple classifiers, and the decisions obtained by the individual classifiers are further classified. The proposed scheme used two ensembles. Supervised classifiers were used in the first ensemble and the unsupervised classifiers were employed in the second ensemble. Supervised learning was proposed in [36], which used a two-layer hierarchical framework. The first layer distinguished the mode of operation, such as a normal state or cyberattack. The second layer classified the type of cyberattack. An approach based on machine learning was adopted in [37] for cyber-attacks, which used an extremely randomized trees algorithm. In [38], three machine learning techniques, namely, a support vector machine (SVM), k-nearest neighbor, and artificial neural network, were implemented for detecting FDI attacks. Each technique was used with three different feature selection techniques.

An extreme learning machine framework was used in [39] for detecting FDI attacks. In [40], auto-encoders were used for detecting FDI attacks. The hidden correlation structures were learned in the data by using auto-encoders. The correlation was learned in two dimensions, namely, the time and the spatial dimensions. Denoising auto-encoders were also used to clean the corrupted data. The approaches based on the auto-encoder neural network [41] and attention-based auto-encoders [42] were also used for the detection of attacks.

The contribution of [15] distinguished the normal function of the power system from the function in which there was a stealth attack. The stealth attacks were detected by using two machine-learning-based techniques. In the first technique, supervised learning was used for a set of labeled data. That data was used for the training of a support vector machine (SVM). The second technique did not use any training data and the deviation of the measurements was detected. An anomaly detection algorithm was applied to detect stealth attacks.

Deep learning models were also used for the purpose of detecting FDI attacks. The deep neural network (DNN) model was used [43] for the classification of cyber-attacks in a smart grid. Another deep learning-based method was proposed in [44] to detect FDI attacks. The proposed approach consisted of a convolutional neural network (CNN) and a long short-term memory (LSTM) network for the detection of attacks. The data integrity attacks in AC power systems can be detected by using a deep Q-network detection (DQND) scheme proposed in [45]. It is a deep reinforcement learning approach. A neural network model was used in [46] for detecting false data. In this case, the residual elements obtained from state estimation were the inputs given to the perceptron model. An algorithm based on deep learning was proposed in [47] to detect FDI attacks. The dimensionality reduction, as well as feature extraction from measurement datasets, was done by using auto-encoders. Then auto-encoders were integrated into an advanced generative adversarial network (GAN) framework, which was used for detecting the FDI attacks.

The methods based on machine learning had great success in the detection of FDI attacks. However, at the same time, they have certain limitations and drawbacks. The methods based on supervised learning need a labeled dataset. They are built on some conventional attack assumptions. Similarly, deep learning techniques also have some limitations. In these methods, there is a need for extensive training. More memory space is also required for deep learning methods.

The main aim of the detection frameworks is to protect the whole communication system against attacks. One of the key features of microgrids is a secure communication network. For the development of a communication network, its design has vital importance. For the deployment of a heterogeneous automation and monitoring system, a multi-layered architecture was proposed in [48]. For the organization of hardware, as well as software equipment in an integrated manner, six functional layers were structured in the proposed architecture. In [49], a clear description of a smart grid and the type of communication methods were given. The communication methods were explained based on their advantages and the lacking feature. The contribution of [50] was based on the hybrid communication simulation model. In hybrid network architectures, both wireless and dedicated wired media are used. A suite of hybrid communication simulation models was developed for the validation of critical system design criteria.

A mathematical model of the power system was presented in [51] and a robust security framework was proposed. A Kalman filter was used to estimate variables in the model. In [52], an online data-driven algorithm was presented for detecting FDI attacks toward synchrophasor measurements. The proposed algorithm applied density-based LOF (local outlier factor) analysis for detecting anomalies in the data. Another method was proposed in [53] in which the modeling of the system was done as a discrete-time linear dynamic system. There was the use of the Kalman filter for performing the state estimation (SE). A generalized cumulative sum algorithm achieved the quickest detection of the attacks. In [18,19], the economic impact due to stealth FDI attacks on the market operations in real-time was considered. The construction of a profitable attacking plan for the attacker was also shown. In [20], it was explained that the attacker can construct the stealth FDI attack without knowing the structure of the system. The attacker can find the system structure and make an attack.

In [54], a distributed state estimation method based on the alternating direction method of multipliers (ADMM) was presented for detecting cyber-attacks. In this case, the partitioning of regional subsystems was done using the K-means method. An online detection algorithm was proposed in [55] for detecting cyber-attacks. The online estimation of the unknown and time-varying attack parameters was provided by the algorithm. The FDI attacks were detected by proposing an active data modification scheme in [56]. In that scheme, there was an amendment of measurements and control data before they are transmitted through communication networks. In [57], an FDI attack detection method was proposed that was based on the equivalent model of a load frequency control (LFC) system and a Kalman filter algorithm.

The work of [21] formulated the problem of false data detection as a low-rank matrix recovery. Convex optimization was used for solving the problem. The adopted methodology normalized the combination of the l_1 norm and nuclear norm. This mixed norm optimization problem was solved using the augmented Lagrange method of multipliers in order to obtain a good convergence rate. In [22], the false data detection problem was considered a matrix separation problem. FDI attacks are sparse in nature. To separate the states of the power system from the anomalies, a mechanism was developed. The problem was solved using two methods, namely, low-rank matrix factorization and nuclear norm minimization.

3. Proposed Model

The methods used in the literature for the detection of attacks are successful up to a certain limit. If the attacker knows the whole network of the smart grid and makes an attack, it becomes difficult to detect those attacks. Therefore, we proposed a new power system model for an AC power flow network that is safe against stealth FDI attacks and the control room is able to detect these attacks in an efficient manner. The introduced model was based on the concept of dummy value. The smart grid meters will transmit both values, i.e., the actual value and the dummy value. No additional transmission lines and no extra buses will be used. There is no need for any extra meters in the proposed model. The vulnerabilities of the communication networks in supervisory control and data acquisition (SCADA) systems in the smart grid, such as unsophisticated bugs or communication failures, were not considered in this work. The application of the measured value and the dummy value in this article did not consider the error caused by the measurement equipment itself or any other reason. In this work, the error due to parametric variation of the meter or any other unknown reason was not taken into consideration. However, it may be incorporated into our future work. Moreover, this work focused on false data injection attacks in which the intruder hacks the measurement vector and injects the attack vector into the measurement vector before it is received by the control room. Therefore, this study only considered targeted attacks.

The measurement vector for the AC power flow network contains the active and reactive powers injected into all the buses, active and reactive powers flowing through transmission lines in the forward direction, and active and reactive powers flowing in the backward direction. If a system has *b* number of buses and *t* number of transmission lines, then the measurement vector for the AC power flow network is given by

$$\mathbf{z_y} = \begin{bmatrix}\mathbf{p_{v(y)}} & \mathbf{q_{v(y)}} & \mathbf{p_{vw(y)}} & \mathbf{q_{vw(y)}} & \mathbf{p_{wv(y)}} & \mathbf{q_{wv(y)}}\end{bmatrix}^{\mathrm{T}} \tag{15}$$

where $\mathbf{z}_y$ is the measurement vector at the yth instant and $\mathbf{y}$ = 1, 2, 3, … , *mt*. Here, *mt* represents the total number of instances. $\mathbf{p_{v(y)}}$ and $\mathbf{q_{v(y)}}$ are the vectors containing the active and reactive powers injected to all the buses at the yth instant. Both vectors will have a dimension of $1 \times b$. Similarly, $\mathbf{p_{vw(y)}}$ and $\mathbf{q_{vw(y)}}$ denote vectors having the active and reactive powers flowing through all the transmission in the forward direction at the yth instant. Both vectors have dimensions of $1 \times t$. Moreover, $\mathbf{p_{wv(y)}}$ and $\mathbf{q_{wv(y)}}$ represent the vectors of the active and reactive powers flowing through all the transmission lines in the backward direction at the yth instant. The complete measurement vector will have a dimension of $m \times 1$. The state vector $\mathbf{x}$ contains the voltage magnitudes and voltage angles of all the buses. However, the Jacobian matrix will have a dimension of $m \times n$, where m is the total number of values in the measurement vector and n is the total number of values in the state vector. The measurement vectors at all the instances can be placed together to obtain the measurement matrix as follows:

$$\mathbf{Z} = [\mathbf{z}_1 \quad \mathbf{z}_2 \quad \mathbf{z}_3 \ldots\ldots\ldots\ldots\ldots\ldots \mathbf{z_{mt}}]^{\mathrm{T}} \tag{16}$$

The dimensions of the measurement matrix are $mt \times m$. The measurement vector after implementing the proposed system will become like this:

$$\mathbf{z_{dy}} = \begin{bmatrix} p_{v(y)}(1); p'_{v(y)}(1); \ldots\ldots; q_{v(y)}(b); q'_{v(y)}(b); \\ p_{vw(y)}(1); p'_{vw(y)}(1); \ldots\ldots; q_{vw(y)}(t); q'_{vw(y)}(t); \\ p_{wv(y)}(1); p'_{wv(y)}(1); \ldots\ldots; q_{wv(y)}(t); q'_{wv(y)}(t) \end{bmatrix}$$

The measurement vector containing the actual and dummy values is represented by $\mathbf{z_{dy}}$. Here, $\mathbf{p_{v(y)}}(1)$ represents the first entry of the vector $\mathbf{p_{v(y)}}$ and $\mathbf{q_{v(y)}}(\mathbf{b})$ is the bth entry of the vector $\mathbf{q'_{v(y)}}$. The dummy values of the power are present on the even indexes of the new measurement vector. The vectors of the dummy values containing the active and reactive powers injected to all the buses at the yth instant are $\mathbf{p'_{v(y)}}$ and $\mathbf{q'_{v(y)}}$. Similarly, other vectors containing dummy values of the active and reactive powers for transmission lines at the yth instant are denoted by $\mathbf{p'_{vw(y)}}$, $\mathbf{q'_{vw(y)}}$, $\mathbf{p'_{wv(y)}}$, and $\mathbf{q'_{wv(y)}}$. $\mathbf{z_{dy}}$ will have dimensions of $2m \times 1$. The measurement matrix after including the dummy values will be

$$\mathbf{Z_d} = [\mathbf{z_{d1}} \quad \mathbf{z_{d2}} \quad \mathbf{z_{d3}} \ldots\ldots\ldots\ldots\ldots\ldots \mathbf{z_{dmt}}]^{\mathrm{T}} \tag{17}$$

This measurement vector will have dimensions of $mt \times 2m$. The Jacobian matrix of the proposed system at the yth instant is represented by $\mathbf{H_{dy}}$ and its dimensions are $2m \times n$. There are different methods to find the Jacobian matrix. To make a stealth attack, it is necessary for the attacker to determine the Jacobian matrix. The attacker hacks both the dummy and actual values and creates a Jacobian matrix to attack the system.

Realistic data of the AC power flow network was used for implementing and evaluating the proposed model. For this purpose, the load curves of a transmission organization known as PJM, which serves 13 states of the United States and the District of Columbia, were taken as a reference to generate the data of the power flow network. These load curves were based on realistic data. Therefore, our generated data were very close to the realistic data of an AC power flow network. The data were generated for four different seasons, namely, summer, fall, winter, and spring, based on the standard realistic load curves given for each season.

The overall proposed model was divided into two scenarios. In the first scenario, a fixed dummy value was sent to the control room. However, in the second case, a variable dummy value was sent and it changed with the change of the actual value of power.

Fixed Dummy Value Model

In this case, a fixed dummy value, along with each of the actual values, was sent to the control room. The dummy value of the power was not dependent on the load. It did not vary with the variation in load or variation in the actual value of power. In the fixed dummy value model, to select the dummy value of a particular power, the average value was calculated from all the actual measured values that occurred for that value at all the instances. That average value was selected as the dummy value of power. In this case, the dummy values were determined by taking the mean of the last year's worth of historical measurement data, i.e., real-time measured values are stored from the past year and utilized for the calculation of fixed dummy values based on Equations (18)–(21). Later, these values were inserted into the memory of the meters and were simply appended or added to all the newly acquired measurements accordingly. It should be noted that the dummy value will no longer change with the newly acquired measurements. The calculation of the fixed dummy value was done by using these formulas:

$$\begin{gathered} p'_{v(y)}(l) = \frac{\sum_{s=1}^{mt} z_s(lp)}{mt} \\ l = 1,2,3,\ldots\ldots,b \quad and \quad lp = 1,2,3,\ldots\ldots,b \end{gathered} \tag{18}$$

$$\begin{gathered} q'_{v(y)}(l) = \frac{\sum_{s=1}^{mt} z_s(lq)}{mt} \\ l = 1,2,3,\ldots\ldots,b \quad and \quad lq = b+1, b+2,\ldots\ldots,2b \end{gathered} \tag{19}$$

$$\begin{gathered} p'_{vw(y)}(l) = \frac{\sum_{s=1}^{mt} z_s(lpv)}{mt} \\ l = 1,2,3,\ldots\ldots,t \quad and \quad lpv = 2b+1, 2b+2,\ldots\ldots,2b+t \end{gathered} \tag{20}$$

$$\begin{gathered} q'_{vw(y)}(l) = \frac{\sum_{s=1}^{mt} z_s(lqv)}{mt} \\ l = 1,2,3,\ldots,t \quad and \quad lqv = 2b+t+1, 2b+t+2,\ldots\ldots,2b+2t \end{gathered} \tag{21}$$

In (18), $p'_{v(y)}(l)$ represents the lth entry of the dummy values vector $\mathbf{p}'_{\mathbf{v(y)}}$. $z_s(lp)$ denotes the lpth entry of the sth historical measurement vector. mt is the total number of instances for which the historical measurement vectors are obtained. To calculate the first entry of the dummy measurement vector $\mathbf{p}'_{\mathbf{v(y)}}$, the sum of the first entries of all the historical measurement vectors is calculated and then divided by the total number of instances for which those historical measurement vectors are obtained. Similarly, the second entry of the dummy values vector $\mathbf{p}'_{\mathbf{v(y)}}$ can be calculated by finding the mean of the second entries of mt historical measurement vectors. The same procedure is adopted for finding all the entries of $\mathbf{p}'_{\mathbf{v(y)}}$ and the dummy values of all the active powers injected into the buses are calculated in this way. In (19), $q'_{v(y)}(l)$ denotes the lth entry of the dummy values vector $\mathbf{q}'_{\mathbf{v(y)}}$, and $z_s(lq)$ represents the lqth entry of the sth historical measurement vector. mt gives the total number of historical measurement vectors. The lth entry of the dummy values vector $\mathbf{q}'_{\mathbf{v(y)}}$ is found by calculating the mean of the lqth entry of mt historical measurement vectors. By using this procedure, the dummy values of all the reactive powers injected into the buses can be calculated. In (20) and (21), $p'_{vw(y)}(l)$ and $q'_{vw(y)}(l)$ represent the lth entry of each of the dummy measurement vectors $\mathbf{p}'_{\mathbf{vw(y)}}$ and $\mathbf{q}'_{\mathbf{vw(y)}}$, respectively. $z_s(lpv)$ and $z_s(lqv)$ denote the lpvth and lqvth entries of the sth historical measurement vector, respectively. The lth entry of each of the dummy measurement vectors $\mathbf{p}'_{\mathbf{vw(y)}}$ and $\mathbf{q}'_{\mathbf{vw(y)}}$ is calculated by finding the mean of the lpvth and lqvth entries of mt historical measurement vectors, respectively.

Therefore, the dummy values of the active and reactive powers flowing through all the transmission lines can be calculated by using Equations (20) and (21), respectively.

By applying Equations (18)–(21), the dummy values are calculated at a single instant by using *mt* historical measurement vectors and then those calculated dummy values are kept the same for all the instances, i.e., the dummy values do not change for the other instances. In fact, in the fixed dummy value model, the dummy values depend only on the historical measurement values and they do not depend on the real-time measurement values.

$\mathbf{p}'_{\mathbf{wv(y)}}$ and $\mathbf{q}'_{\mathbf{wv(y)}}$ can also be calculated using this method and all the dummy values are selected in this way. These dummy values are placed in $\mathbf{z_{dy}}$, which is embedded in the meters. These values are also placed in another vector **d** present in the control room. When the system is hacked by the attacker, 2*m* power values will be obtained by the attacker in $\mathbf{z_{dy}}$ instead of *m* values. In the next step, the Jacobian matrix will be constructed by the attacker and a stealthy attack will be done in this way:

$$\mathbf{z_{dyr}} = \mathbf{z_{dy}} + \mathbf{H_{dy}} * \mathbf{c} \tag{22}$$

Here, $\mathbf{z_{dyr}}$ denotes the measurement vector received in the control room at the *y*th instant. For the detection of an attack, a comparison is made between the dummy values obtained from $\mathbf{z_{dyr}}$ and those dummy values set by the control room. The following equation is used in the control room to detect the attack:

$$r(u) = d(u) - z_{dyr}(v) \tag{23}$$

where *u* = 1, 2, 3 . . . , *m* and

v = 2,4, 6 . . . , 2*m*

Here *d(u)* denotes the *u*th entry of the dummy values vector *d*, which is selected and set by the defender. Meanwhile, $z_{dyr}(v)$ denotes the *v*th entry of the received measurement vector. In the case of a secure system:

$$|r(u)| = 0 \tag{24}$$

where *u* = 1,2, 3, . . . , *m*.

During the case of no attack, $\mathbf{z_{dyr}} = \mathbf{z_{dy}}$.

To launch an attack, the attacker changes the actual and dummy values according to the construction of the stealth attack. As the dummy values are fixed, they should not change for a secure system. Therefore, for an attack, the value of $|r(u)|$ will come out to be greater than zero and the attack will be detected in this way.

The conventional technique for bad data detection (BDD), such as DC state estimation (SE), fails to detect a stealth FDI attack. Moreover, AC SE is also bypassed by this attack. However, our model with a fixed dummy value was capable enough to detect the FDI attacks in the AC power flow network and all the attacks could be detected by the control room.

4. Simulations and Results of the Fixed Dummy Value Model

We implemented the proposed model for the AC power flow network on an IEEE 14-bus system, which had 14 buses and 20 transmission lines. Therefore, at every instant, the measurement vector had 54 values of active power and 54 values of reactive power i.e., 108 measurement values in total. The system had 28 state variables. In this case, the voltage magnitudes and voltage angles were taken as the states of the system.

4.1. Data Generation

The seasonal data was generated for the IEEE 14-bus test system. The standard realistic load curve of every season was followed by the generated data. For this purpose, the measurements of the power flow network were varied with the variation of the load that was connected to buses. The measurements were taken after a time interval of one hour. Therefore, there was a time of one hour between the two measurement vectors. For a complete day, the values were recorded in the control room 24 times. We generated the data for one year, i.e., 365 days. Therefore, for the whole system, we obtained values for 8760 different instances. MATPOWER 7.0 was used for the simulation of the system model. The load was varied from 61% to 118.5% of its average value in the reference load curves. Therefore, we also varied the load between these two values. For one day, a specific pattern was followed for every different season by the load that was connected to the buses. We generated the data for one day of every season by using the pattern of that specific season. We selected all the load values in a particular range for a whole day to follow that specific pattern. After varying the total load of the power system, four load curves for one day of every season are shown in Figure 1. The values of the loads are shown at 24 different instances in one complete day. These load curves follow the standard realistic load curves and realistic data was generated according to these curves.

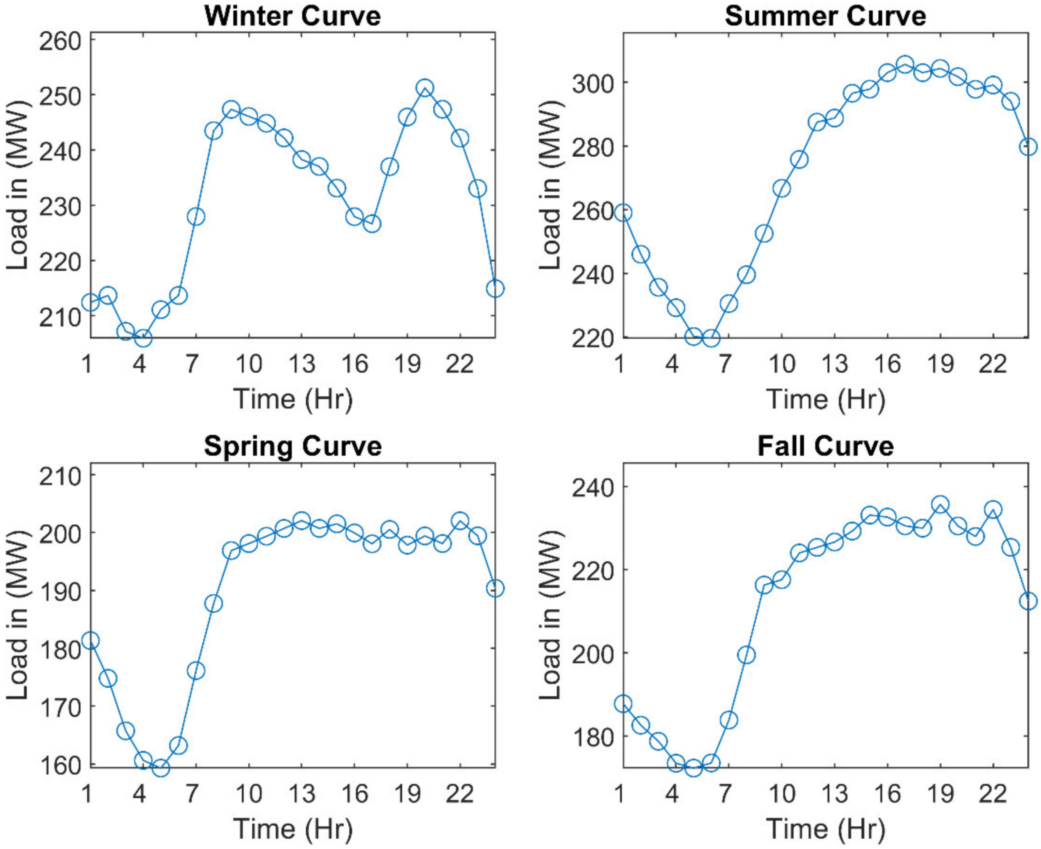

Figure 1. Seasonal load curves of four different seasons based on which data was generated.

4.2. DC State Estimation

By using the generated data, the DC state estimation, which was made by applying the DC assumptions, was implemented for the detection of simple and stealth attacks. For the simulations, the attacks were done according to a certain method, and that method was adopted in the whole manuscript wherever the attacks were made. For a complete day, 25% of the measurement vectors were considered as attacks, i.e., the attacks were made in the measurement vectors at six different instances. The choice of instances was made randomly to make it generalized. In 50% of the measurement vectors chosen for attacks, simple attacks were done. However, stealth attacks were made in the remaining 50% of the measurement vectors that were randomly chosen to be attacked. To create the simple attacks, the attack vector was constructed in such a way that at a particular instant, any value of power was randomly chosen between 0.5% of the maximum value and 0.5% of the minimum value of power at that instant. In the case of stealth attacks, the

Jacobian matrix was first constructed and then the Jacobian matrix was multiplied with a vector **c** to make the attack vector. The values of vector c were selected randomly between −1 and 1 such that it had zero mean and a variance of 2. The attack vector was added to the measurement vector to make the attack. The results of the DC state estimation are shown in Figures 2 and 3. Three types of measurements are shown in Figure 2, namely, safe measurements, simple attack measurements, and the measurements for a stealth attack. A safe zone based on the threshold is also shown in the figure. The measurements outside the safe zone are considered as attacked. The results show that the safe measurement points were present in the safe zone and points of simple attacks were outside the zone. However, measurements affected by stealth attacks are also found in the safe zone, i.e., they are declared as safe by the DC state estimation. They should have to appear outside the safe zone. Therefore, DC SE is not capable of detecting stealth FDI attacks. Similarly, Figure 3 also shows the results of DC state estimation in the form of a bar graph. The residue was calculated for every measurement and the difference of that residue from the threshold is plotted along the vertical axis. For a safe measurement, the value of the difference should be positive, as the residue of that measurement should be less than the threshold. In the graph, the safe measurements are labeled with 1, measurements of simple attacks are labeled with 0, and stealth-attacked measurements are labeled with −1. The results show that the safe measurements and stealth-attacked measurements had positive values of difference. However, the value of the difference was negative for simple attacks. This means that the simple-attacked measurements were termed as attacked by the DC state estimation but measurements having stealth attacks were considered safe. Therefore, simple attacks were detected by the DC state estimation, but stealth attacks bypassed detection.

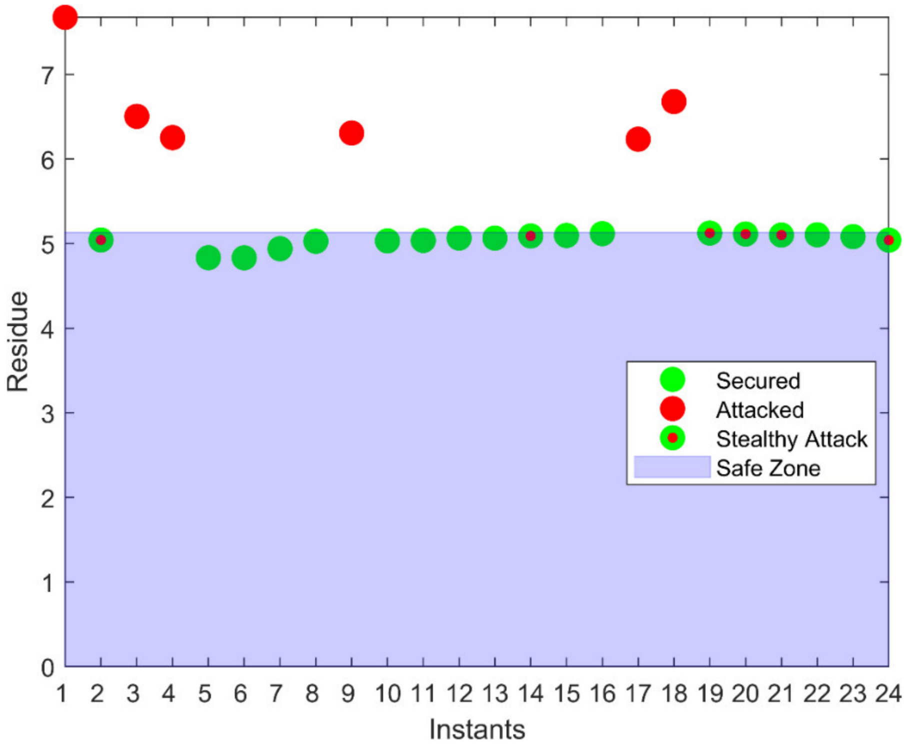

Figure 2. Categorization of safe measurements, simple attacks, and stealth attacks based on the threshold in a DC SE.

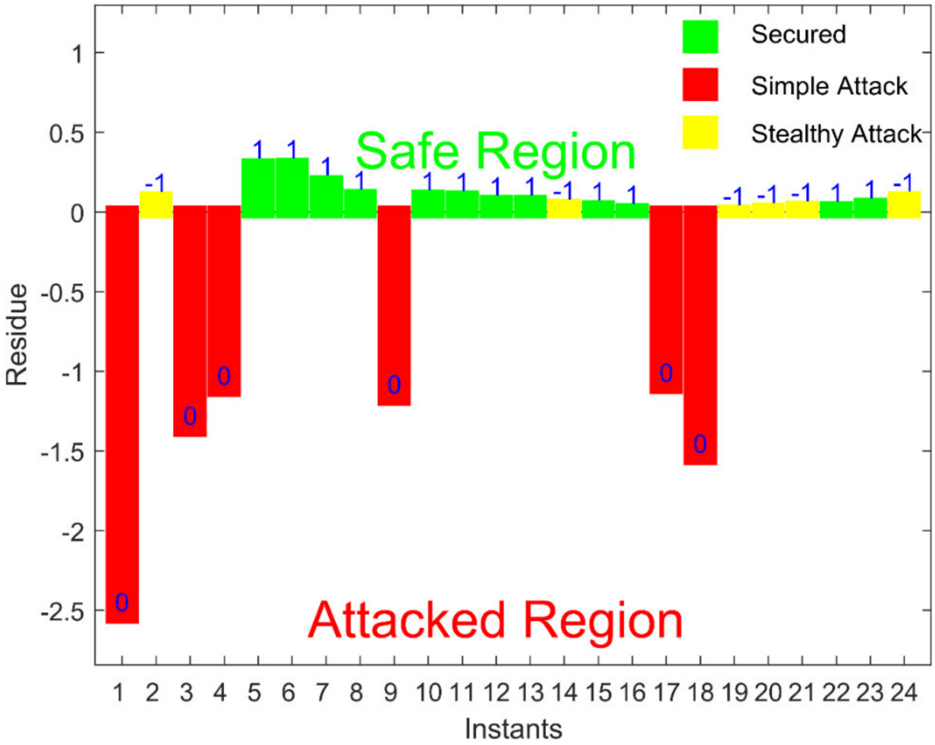

Figure 3. The results of a DC SE for simple and stealth attacks in the form of a bar graph.

4.3. AC State Estimation

For the AC power flow network, an AC SE is used for the detection of attacks. We also used AC SE for the detection of simple and stealth attacks, and the results are given in Figures 4 and 5. The conventions used in a DC state estimation for displaying the results are also used in these figures. In Figure 4, a safe zone, simple-attacked measurements, and stealth-attacked measurements are plotted. Safe measurements and stealth attacks are present in the safe zone, and simple-attacked measurements are outside the zone. It shows that stealth attacks were not detected by the AC state estimation. Similarly, in Figure 5, these results are shown in the form of a bar graph. The value of the difference in the residue from the threshold was positive for safe measurements and stealth-attacked measurements. However, the difference was negative for simple-attacked measurements. This indicated that the AC SE could detect a simple attack but it could not detect the stealth attack. Therefore, it is displayed in the results that simple attacks were detected by the DC state estimation, as well as the AC state estimation techniques, but stealth attacks bypassed these techniques.

4.4. Fixed Dummy Value Model (Results)

The proposed model of a fixed dummy value was implemented for the AC power flow network of the IEEE 14-bus system. The meters sent the actual value and the fixed dummy value to the control room in the form of a measurement vector. Table 1 shows the actual values and the fixed dummy values at the first instant for the first five buses and first five transmission lines. In the control room, the difference, i.e., the residue of two dummy values, was calculated. One dummy value was obtained from the measurement vector and the other was already present in the control room. As the dummy value was fixed in this case, it should not change at any instance. Therefore, for a secure system, the value of the residue should be zero.

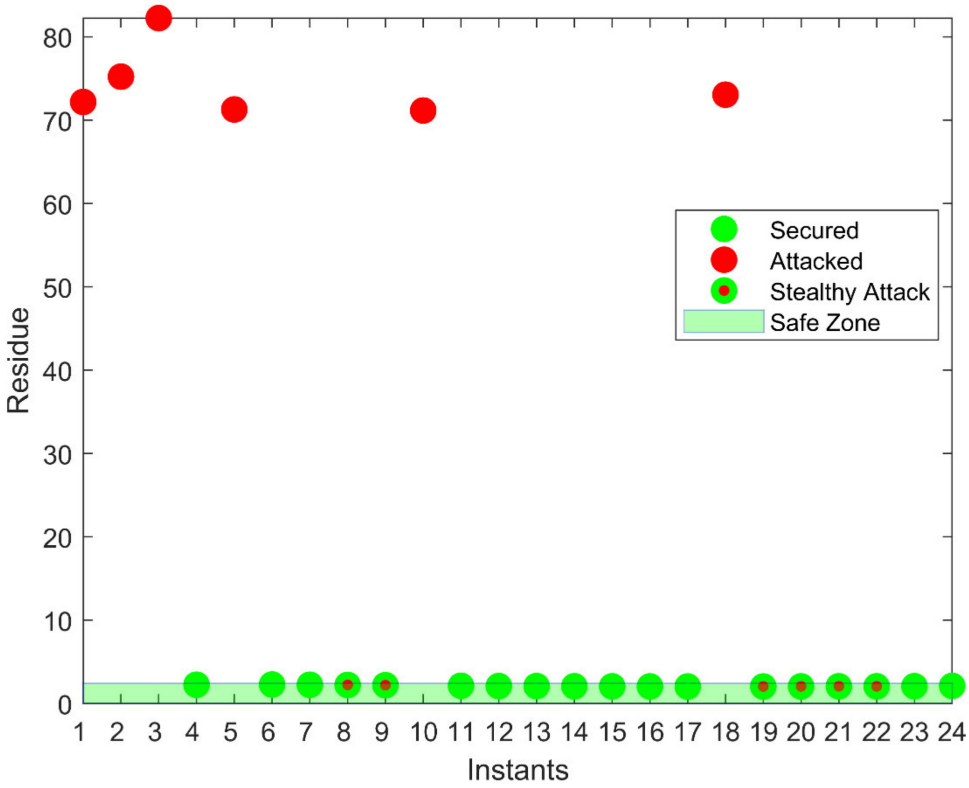

Figure 4. Categorization of safe measurements, simple attacks, and stealth attacks based on the threshold in an AC SE.

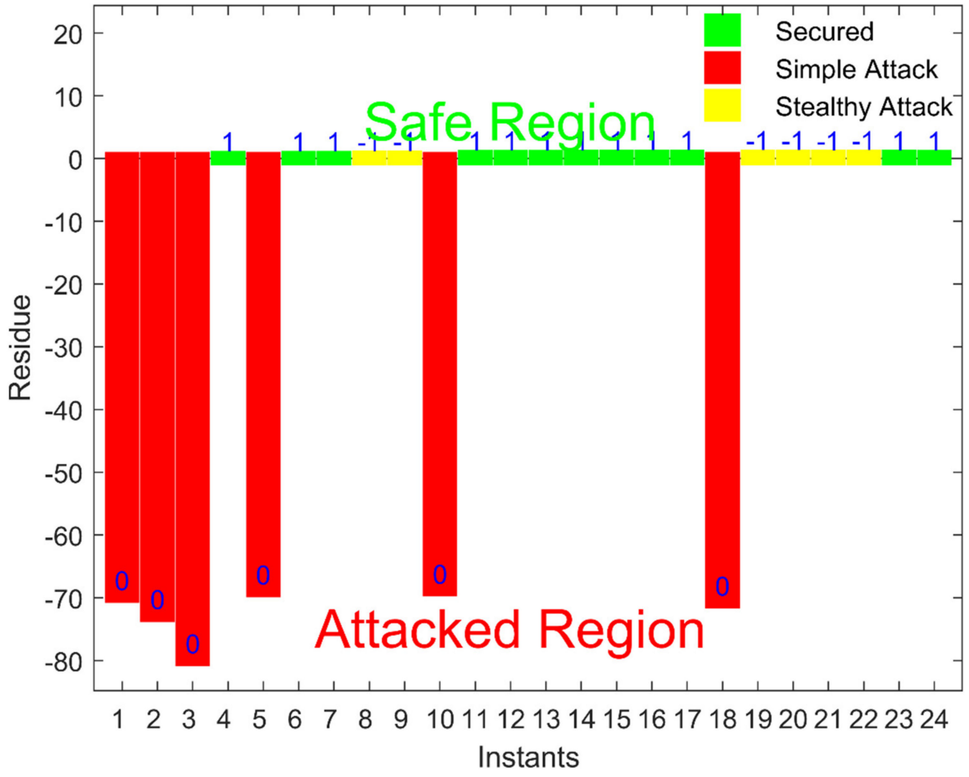

Figure 5. The results of an AC SE for simple and stealth attacks in the form of a bar graph.

Table 1. Active and reactive powers injected into the first 5 buses and the active and reactive powers flowing through the first 5 transmission lines in the forward and backward directions.

Active Powers Injected into the Buses			
Bus No.		**Actual Value (MW)**	**Dummy Value (MW)**
1		232.11	196.3
2		18.41	21.06
3		−93.94	−82.22
4		−47.88	−41.72
5		−7.58	−6.63
Reactive Powers Injected into the Buses			
Bus No.		Actual Value (MVAR)	Dummy Value (MVAR)
1		−16.49	−10.3
2		30.79	21.73
3		5.98	−0.27
4		3.9	3.9
5		−1.6	−1.6
Active Powers Flowing through the Transmission Lines in Forward Direction			
From	To	Actual Value (MW)	Dummy Value (MW)
1	2	156.65	131.57
1	5	75.46	64.73
2	3	73.11	63.66
2	4	56.14	49.21
2	5	41.53	36.6
Reactive Powers Flowing through the Transmission Lines in Forward Direction			
From	To	Actual Value (MVAR)	Dummy Value (MVAR)
1	2	−20.35	−14.04
1	5	3.86	3.74
2	3	3.57	4.71
2	4	−1.54	−1.62
2	5	1.17	0.81
Active Powers Flowing through the Transmission Lines in Backward Direction			
From	To	Actual Value (MW)	Dummy Value (MW)
1	2	−152.37	−128.41
1	5	−72.7	−62.63
2	3	−70.79	−61.85
2	4	−54.46	−47.89
2	5	−40.62	−35.88
Reactive Powers Flowing through the Transmission Lines in Backward Direction			
From	To	Actual Value (MVAR)	Dummy Value (MVAR)
1	2	27.58	17.83
1	5	2.21	−0.38
2	3	1.55	−1.68
2	4	3.01	2
2	5	−2.1	−2.31

The results are shown in Figure 6. The bar graph shows the results for safe measurements, simple-attacked measurements, and stealth-attacked measurements. Safe measurements are labeled as 1, simple-attacked measurements as 0, and stealth-attacked measurements as -1. The residue was calculated for each measurement and plotted along the vertical axis. For safe measurements, the value of the residue was zero, as shown in the bar graph. In the case of simple-attacked measurements and stealth-attacked measurements, the residue was not zero, as the dummy value was changed. Therefore, our proposed model could detect all kinds of attacks, such as simple attacks and stealth attacks. Stealth FDI attacks remained undetected by the DC and AC state estimation, but they could be detected by using our proposed approach.

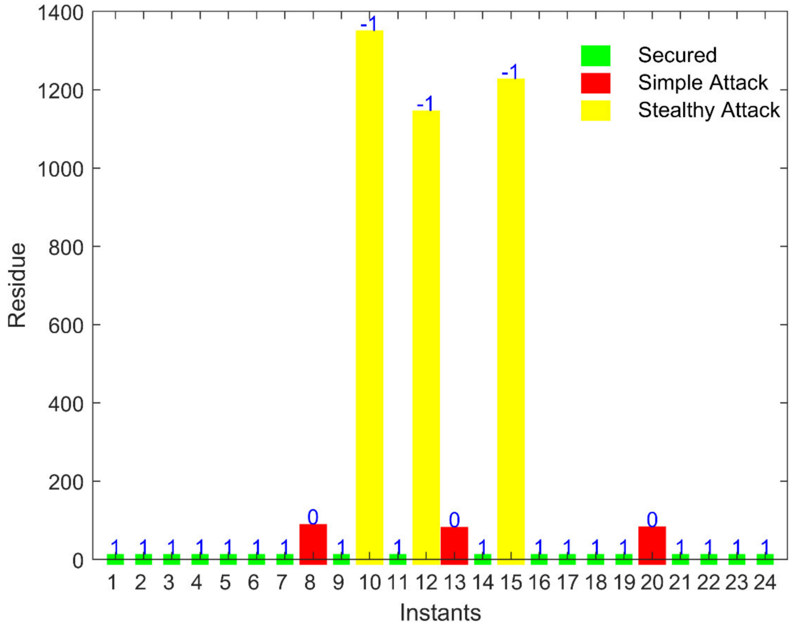

Figure 6. Detection results of the fixed dummy value model for simple and stealth attacks based on dummies.

4.5. Limitations of Fixed Dummy Value Model

The proposed fixed dummy value model could detect the stealth FDI attacks but, at the same time, there was a limitation of the model. As the dummy value does not change, by looking at the measurements continuously for some time, the attacker will come to know which one is the dummy value and the attacker will not change that value while doing an attack. In this way, the attack may be done such that it is unable to be detected. Figure 7 shows the results where the fixed dummy value model was bypassed by the stealth attack. It can be seen from the graph that the value of the residue in the case of attacks came out to be zero, as the attacker did not change the dummy values while launching the attack. Therefore, this limitation of the fixed dummy value was evaluated using the results.

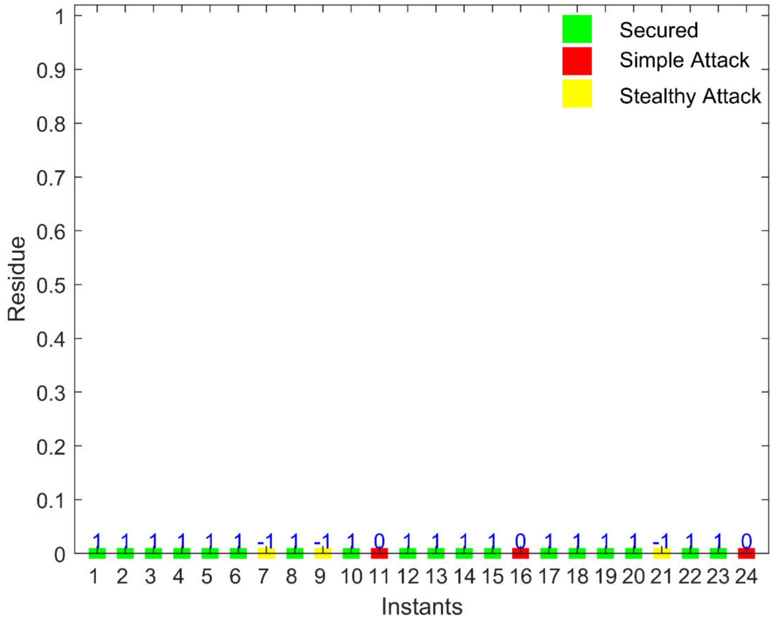

Figure 7. Limitations of the fixed dummy value model for simple and stealth attacks.

5. Variable Dummy Value Model

In the proposed model with a fixed dummy value, the attacker may attack the system by remaining undetected because the dummy value is fixed for all instances. Therefore, the dummy value should vary to protect the system against attacks. For this purpose, the model with a variable dummy value was introduced. In this scenario, the dummy value will change at every instant, and it will depend on the actual value, as well as some other values of the power in the system. Therefore, the dummy value of the power changes with the change in either of those values on which it depends. In the variable dummy value model, a linear function is implemented for the calculation of the dummy value and that function uses the actual measured value of that meter and the measured value of some other meter that has a relationship with that actual value. The function is only known to the control room. In the fixed dummy value model, the calculated dummy values are embedded into the meters. Similarly, in the variable dummy value model, the function used for the calculation of dummy values is embedded into the meters. This work assumed that the intruder does not have access to the meters, i.e., the intruder only has access to the measurements sent to the control room. The following functions are used in the case of the variable dummy value model for the calculation of dummy values for buses:

$$\begin{gathered} p'_{v(y)}(i) = \beta_{1vpi} p_{v(y)}(i) + \beta_{2vpi} p_{viz(y)} + \beta_{3vpi} \\ i = 1, 2, 3, \ldots\ldots, b \end{gathered} \tag{25}$$

$$\begin{gathered} q'_{v(y)}(i) = \beta_{1vqi} q_{v(y)}(i) + \beta_{2vqi} q_{viz(y)} + \beta_{3vqi} \\ i = 1, 2, 3, \ldots\ldots, b \end{gathered} \tag{26}$$

where $p'_{v(y)}(i)$ and $q'_{v(y)}(i)$ represent the ith entries of the dummy values vectors $\mathbf{p'_{v(y)}}$ and $\mathbf{q'_{v(y)}}$, respectively. $p_{v(y)}(i)$ and $q_{v(y)}(i)$ denote the ith entries of $\mathbf{p_{v(y)}}$ and $\mathbf{q_{v(y)}}$, respectively. Similarly, $p_{viz(y)}$ and $q_{viz(y)}$ represent the active power and reactive power flowing through the first transmission line connected to the ith bus at the yth instant, respectively. β_{1vpi}, β_{2vpi}, β_{3vpi}, β_{1vqi}, β_{2vqi}, and β_{3vqi} are the constants that have to be learned to calculate the dummy values. Similarly, the calculation of the dummy values of the active and reactive powers flowing through the transmission lines can be done by using the following functions:

$$\begin{gathered} p'_{vw(y)}(i) = \beta_{1vwpi} p_{v(y)}(i) + \beta_{2vwpi} p_{w(y)}(i) + \beta_{3vwpi} \\ i = 1, 2, 3, \ldots\ldots, t \end{gathered} \tag{27}$$

$$\begin{gathered} q'_{vw(y)}(i) = \beta_{1vwqi} q_{v(y)}(i) + \beta_{2vwqi} q_{w(y)}(i) + \beta_{3vwqi} \\ i = 1, 2, 3, \ldots\ldots, t \end{gathered} \tag{28}$$

$$\begin{gathered} p'_{wv(y)}(i) = \beta_{1wvpi} p_{w(y)}(i) + \beta_{2wvpi} p_{v(y)}(i) + \beta_{3wvpi} \\ i = 1, 2, 3, \ldots\ldots, t \end{gathered} \tag{29}$$

$$\begin{gathered} q'_{wv(y)}(i) = \beta_{1wvqi} q_{w(y)}(i) + \beta_{2wvqi} q_{v(y)}(i) + \beta_{3wvqi} \\ i = 1, 2, 3, \ldots\ldots, t \end{gathered} \tag{30}$$

$p'_{vw(y)}(i)$ and $q'_{vw(y)}(i)$ denote the ith entries of vectors $\mathbf{p'_{vw(y)}}$ and $\mathbf{q'_{vw(y)}}$, respectively, which contain the dummy values of powers flowing through the transmission lines in the forward direction at yth instant. $p_{w(y)}(i)$ and $q_{w(y)}(i)$ represent the active power and reactive power injected into ith bus at yth instant, respectively. $p_{w(y)}(i)$ and $q_{w(y)}(i)$ belong to $\mathbf{p_{v(y)}}$ and $\mathbf{q_{v(y)}}$, respectively. Similarly, $p'_{wv(y)}(i)$ and $q'_{wv(y)}(i)$ show the ith entries of vectors $\mathbf{p'_{wv(y)}}$ and $\mathbf{q'_{wv(y)}}$, respectively, which have the dummy values of the active power and reactive power flowing through transmission lines in the backward direction. Constants are also used in the equations proposed for the calculation of dummy values.

The Equations (25)–(30) are used for finding the dummy values at the yth instant. In the variable dummy value model, the dummy values depend on the real-time measurement values. As the real-time measurement values are used for the calculation of the dummy values, the dummy values change at every instant in this case.

There is a key point to consider while selecting the dummy value, which is that the dummy value of a meter should be close to its actual value. There should not be too much difference between the actual and dummy value such that the attacker can find the dummy value and construct an undetectable attack. Therefore, when these linear functions are implemented for the calculation of the dummy value, we may obtain a dummy value that is far away from its actual value. The reason for this is that these dummy values depend on two different values of the power and there might be a high variance in the values of a certain meter depending upon the load connected to a bus. If the variance of either of the two actual values is high for a whole day, the dummy value will not be close to the actual value.

This problem may be minimized due to the selection of appropriate values of the constants. The selection of constants is done in such a way that all dummy values of a specific power for the whole day must remain close to the actual value of that power. For this purpose, a machine-learning technique, namely, multivariate linear regression (MLR), was used for finding the best values of the constants. The procedure of MLR to find the constants of the equation used to calculate the dummy values of the active power injected to all the buses is explained here. In this case, the hypothesis is written as

$$\mathrm{g}_{\boldsymbol{\beta}_\mathbf{k}}(\mathbf{p_k}) = \beta_{1vpk} p_v(k) + \beta_{2vpk} p_{vkz} + \beta_{3vpk} \tag{31}$$

Here, $\mathrm{g}_{\boldsymbol{\beta}_\mathbf{k}}(\mathbf{p_k})$ is a function of $\mathbf{p_k}$ that is parameterized using $\boldsymbol{\beta}_\mathbf{k}$. $\mathbf{p_k}$ represents the kth input vector, where k = 1, 2, 3, . . . , b and $\mathbf{p_k}$ = $[1\ p_{vkz}\ p_v(k)]^{\mathrm{T}}$. $\boldsymbol{\beta}_\mathbf{k}$ denotes the kth parameter vector and $\boldsymbol{\beta}_\mathbf{k}$ = $[\beta_{3vpk}\ \beta_{2vpk}\ \beta_{1vpk}]^{\mathrm{T}}$. β_{1vpk}, β_{2vpk}, and β_{3vpk} are the constants to be learned for each dummy value of the active power injected into the buses. Therefore, for each dummy value, a different vector of constants is used. Depending upon the hypothesis, the cost function for the multivariate linear regression can be written as

$$\mathrm{J}(\boldsymbol{\beta}_\mathbf{k}) = \frac{1}{2mt} \sum_{y=1}^{mt} \left(\left(\sum_{f=1}^{3} \beta_{kf} p_{kf(y)} \right) - p_{v(y)}(k) \right)^2 \tag{32}$$

Here, mt represents the total number of instances, i.e., the total number of training examples in this case. $p_{v(y)}(k)$ represents the output of the yth training example of the active power injected to the kth bus. We must minimize the cost function so that we obtain the best values of the parameters. For this purpose, the gradient descent algorithm was applied, which is based on the update rule. The gradient descent can be written as

$$\beta_{kf} := \beta_{kf} - \alpha \frac{1}{mt} \sum_{y=1}^{mt} \left(\mathrm{g}_{\boldsymbol{\beta}_\mathbf{k}}\left(\mathbf{p}_{\mathbf{k}(\mathbf{y})}\right) - p_{v(y)}(k) \right) p_{kf(y)} \tag{33}$$

β_{kf} represents the fth entry of the kth parameter vector. $p_{kf(y)}$ denotes the fth entry of the kth input vector at the yth instant. The β's are calculated again and again, and those parameters are used to calculate the cost. The above process is repeated until convergence occurs. When the cost converges, this produces the best values of the parameters.

By adopting the same procedure, the constants for the remaining equations are also found and those constants are put in their respective functions to calculate the dummy values of the active and reactive power. Then, these functions are embedded into the meters for the calculation of the dummy values. The meters measure the actual values of power and then use those functions to calculate the dummy values of power to send them to the control room. These functions are only known to the control room.

In the control room, to detect the FDI attacks, these functions are used to recalculate the dummy value by using the actual values obtained from the measurement vector. Then, the recalculated dummy value is compared with the dummy value obtained from the measurement vector for attack detection. The following equations are used in the control room to compare the calculated dummy values and received dummy values of active and reactive powers injected into all the buses:

$$r_{vp(y)}(j) = p'_{vr(y)}(j) - (\beta_{1vpj} p_{vr(y)}(j) + \beta_{2vpj} p_{vrjz(y)} + \beta_{3vpj}) \\ j = 1, 2, 3, \ldots\ldots, b \tag{34}$$

$$r_{vq(y)}(j) = q'_{vr(y)}(j) - \left(\beta_{1vqj} q_{vr(y)}(j) + \beta_{2vqj} q_{vrjz(y)} + \beta_{3vqj}\right) \\ j = 1, 2, 3, \ldots\ldots, b \tag{35}$$

The measurement vector received in the control room at the yth instant is $\mathbf{z_{dyr}}$. Here, $p'_{vr(y)}(j)$ and $q'_{vr(y)}(j)$ represent the jth entries of the received vectors $\mathbf{p'_{vr(y)}}$ and $\mathbf{p'_{vr(y)}}$, respectively, which contain the dummy values of the active power and reactive power received in the control room at the yth instant. $p_{vr(y)}(j)$ and $q_{vr(y)}(j)$ denote the jth entries of the received vectors $\mathbf{p_{vr(y)}}$ and $\mathbf{q_{vr(y)}}$, respectively, which contain the actual values of the active power and reactive power received in the control room at the yth instant. $p_{vrjz(y)}$ and $q_{vrjz(y)}$ are taken from the received measurement vector. $r_{vp(y)}(j)$ and $r_{vq(y)}(j)$ represent the jth entries of the residue vectors $\mathbf{r_{vp(y)}}$ and $\mathbf{r_{vq(y)}}$, respectively, which contain the residues for the active and reactive powers injected into the buses at the yth instant. Similarly, the equations for calculating the residues for the forward and backward powers flowing through the transmission lines are given by:

$$r_{vwp(y)}(j) = p'_{vwr(y)}(j) - \left(\beta_{1vwpj} p_{vr(y)}(j) + \beta_{2vwpj} p_{wr(y)}(j) + \beta_{3vwpj}\right) \\ j = 1, 2, 3, \ldots\ldots, t \tag{36}$$

$$r_{vwq(y)}(j) = q'_{vwr(y)}(j) - \left(\beta_{1vwqj} q_{vr(y)}(j) + \beta_{2vwqj} q_{wr(y)}(j) + \beta_{3vwqj}\right) \\ j = 1, 2, 3, \ldots\ldots, t \tag{37}$$

$$r_{wvp(y)}(j) = p'_{wvr(y)}(j) - \left(\beta_{1wvpj} p_{wr(y)}(j) + \beta_{2wvpj} p_{vr(y)}(j) + \beta_{3wvpj}\right) \\ j = 1, 2, 3, \ldots\ldots, t \tag{38}$$

$$r_{wvq(y)}(j) = q'_{wvr(y)}(j) - \left(\beta_{1wvqj} q_{wr(y)}(j) + \beta_{2wvqj} q_{vr(y)}(j) + \beta_{3wvqj}\right) \\ j = 1, 2, 3, \ldots\ldots, t \tag{39}$$

In these equations, the dummy and actual values are obtained from the received measurement vector in the control room. $r_{vwp(y)}(j)$, $r_{vwq(y)}(j)$, $r_{wvp(y)}(j)$, and $r_{wvq(y)}(j)$ represent the jth entries of the residue vectors $\mathbf{r_{vwp(y)}}$, $\mathbf{r_{vwq(y)}}$, $\mathbf{r_{wvp(y)}}$, and $\mathbf{r_{wvq(y)}}$, respectively, which contain the residues for the active and reactive powers flowing through the transmission lines in the forward and backward directions at the yth instant. The overall residue at the yth instant is calculated using

$$r = \left|\mathbf{r_{vp(y)}}\right| + \left|\mathbf{r_{vq(y)}}\right| + \left|\mathbf{r_{vwp(y)}}\right| + \left|\mathbf{r_{vwq(y)}}\right| + \left|\mathbf{r_{wvp(y)}}\right| + \left|\mathbf{r_{wvq(y)}}\right| \tag{40}$$

For a secure system:

$$r = 0$$

If the total residue has some value other than zero, the system is considered attacked. The attacker hacks the measurement vector $\mathbf{z_{dy}}$ and sends the vector $\mathbf{z_{dyr}}$ to the control room after making the attack. As the attacker does not know which are the dummy values, the attacker will attack dummy values too. The attacker also does not know about the relationship used to calculate the dummy value. As a result, the attack is easily detected in the control room, as the value of r will not be equal to zero.

This proposed model of the variable dummy value can tackle the limitations of the fixed dummy value model and the stealth FDI attacks can be detected in an efficient way.

6. Results of the Variable Dummy Value Model

The proposed model with the fixed dummy value can be bypassed, as the dummy value is constant for all the instances. The dummy value should change with the change in the actual value. In the variable dummy value model, the limitation of the fixed value dummy model is overcome by changing the dummy value at every instant. The variable dummy value model was implemented for the AC power flow model of the IEEE 14-bus system. A dummy value was selected in such a way that it should remain close to the actual value of that power and this feature depends upon the values of constants used in the linear function. For the selection of the constants, the MLR model is built for the calculation of all dummy values. Before using the MLR model, we must select the dummy values as outputs to find the relationship between the input and output. To select the dummy value of power at any instant for MLR, any value is picked from its actual values that occurred for the whole one year prior to that instant. The multivariate linear regression model was run for all the linear equations, and we obtained the best values of the constants for a particular equation that gave the minimum cost for that equation. Table 2 shows the values of constants at the first instant for the first five buses and the first five transmission lines.

Figure 8 shows the learning of the MLR model when finding the parameters of the linear equation used to find the dummy values of P_1. The constants of the equation of the line that best fit the training data were found. Constants for all the linear equations were found in this way and those equations were embedded in the meters to calculate the dummy values. Table 3 shows the actual values and the dummy values for the variable dummy value model at a single instant for the first five buses and first five transmission lines.

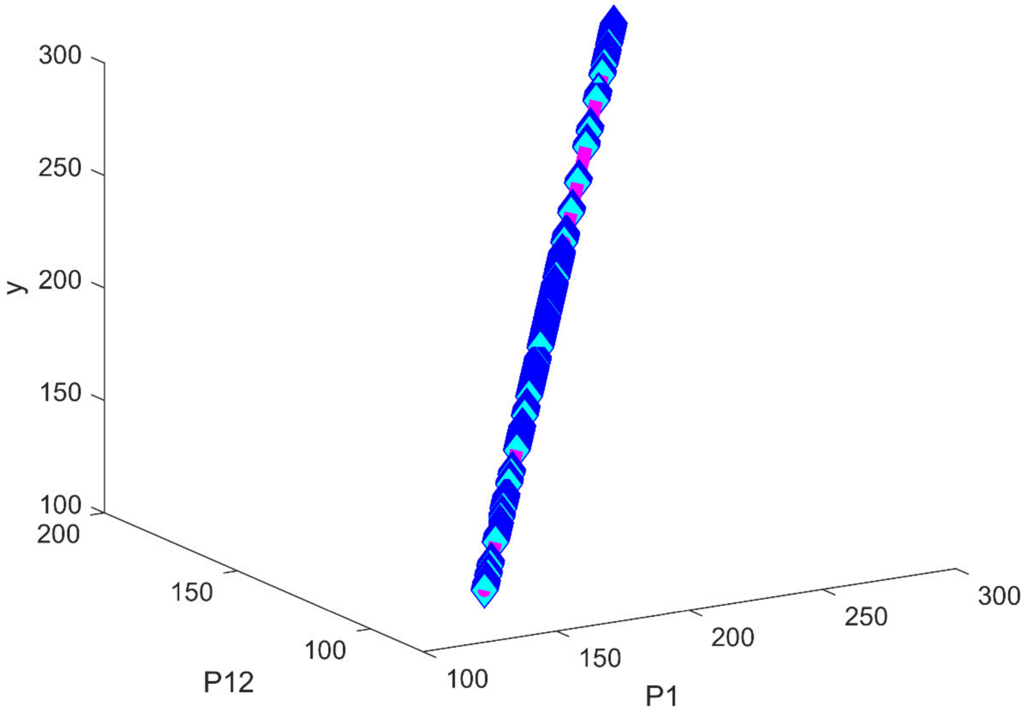

Figure 8. Training of the multivariate linear regression model to find the constants of the equation used to calculate the dummy values of P_1.

Table 2. Constants used for the calculation of dummy values of active and reactive powers injected into the first 5 buses and the active and reactive powers flowing through the first five transmission lines in the forward and backward directions.

Calculation of Dummy Values of Active Powers Injected into the Buses

Bus No.	β_1	β_2	β_3
1	0	40.81	196.30
2	0	3.1	21.06
3	0	13.45	−82.22
4	0	6.83	−41.72
5	0	1.09	−6.63

Calculation of Dummy Values of Reactive Powers Injected into the Buses

Bus No.	β_1	β_2	β_3
1	0	6.73	−10.30
2	0	10.78	21.73
3	0	7.29	−0.27
4	0	1.13	5.13
5	0	8.25	−9.88

Calculation of Dummy Values of Active Powers Flowing through the Transmission Lines in Forward Direction

From	To	β_1	β_2	β_3
1	2	0.91	29.57	131.57
1	5	−1.22	10.93	64.73
2	3	−9.36	−1.44	63.66
2	4	−5.18	−2.62	49.21
2	5	−3.07	−2.48	36.6

Calculation of Dummy Values of Reactive Powers Flowing through the Transmission Lines in Forward Direction

From	To	β_1	β_2	β_3
1	2	5.97	−1.03	−14.04
1	5	4.91	5.21	3.74
2	3	1.08	0.13	4.71
2	4	−0.13	−0.03	−1.62
2	5	−0.22	−0.27	0.81

Calculation of Dummy Values of Active Powers Flowing through the Transmission Lines in Backward Direction

From	To	β_1	β_2	β_3
1	2	2.8	−24.45	−128.41
1	5	2.8	−8.55	−62.63
2	3	8.85	1.35	−61.85
2	4	4.9	2.48	−47.89
2	5	2.95	2.38	−35.88

Calculation of Dummy Values of Reactive Powers Flowing Through the Transmission Lines in Backward Direction

From	To	β_1	β_2	β_3
1	2	5.35	16.66	17.83
1	5	1.65	4.65	−0.38
2	3	−3.25	−0.53	−1.68
2	4	−0.74	−0.39	2
2	5	−0.16	−0.04	−2.31

Table 3. Active and reactive powers injected into the first 5 buses and the active and reactive powers flowing through the first 5 transmission lines in the forward and backward directions for the variable dummy value model.

Active Powers Injected to the Buses			
Bus No.		**Actual Value (MW)**	**Dummy Value (MW)**
1		232.11	232.02
2		18.41	14.74
3		−93.94	−154.82
4		−47.88	−87.64
5		−7.58	−9.95
Reactive Powers Injected into the Buses			
Bus No.		Actual Value (MVAR)	Dummy Value (MVAR)
1		−16.49	−45.96
2		30.79	−26.41
3		5.98	−32.63
4		3.9	0.58
5		−1.6	−44.16
Active Powers Flowing through the Transmission Lines in Forward Direction			
From	To	Actual Value (MW)	Dummy Value (MW)
1	2	156.65	131.57
1	5	75.46	64.73
2	3	73.11	63.66
2	4	56.14	49.21
2	5	41.53	36.6
Reactive Powers Flowing through the Transmission Lines in Forward Direction			
From	To	Actual Value (MVAR)	Dummy Value (MVAR)
1	2	−20.35	−14.04
1	5	3.86	3.74
2	3	3.57	4.71
2	4	−1.54	−1.62
2	5	1.17	0.81
Active Powers Flowing through the Transmission Lines in Backward Direction			
From	To	Actual Value (MW)	Dummy Value (MW)
1	2	−152.37	−128.41
1	5	−72.7	−62.63
2	3	−70.79	−61.85
2	4	−54.46	−47.89
2	5	−40.62	−35.88
Reactive Powers Flowing through the Transmission Lines in Backward Direction			
From	To	Actual Value (MVAR)	Dummy Value (MVAR)
1	2	27.58	17.83
1	5	2.21	−0.38
2	3	1.55	−1.68
2	4	3.01	2
2	5	−2.1	−2.31

In the control room, the dummy values were again calculated by using the obtained actual values from the measurement vector and those recalculated dummy values were subtracted from the obtained dummy values to find the residue. The residue should be zero for a secured system. The results of the proposed model of the variable dummy value are shown in Figure 9, where the model was evaluated using simple and stealth attacks. Safe measurements are also shown in the figure. The residue is plotted along the vertical axis. For safe measurements, the value of the residue was zero, as shown in the bar graph. However, for simple attacks and stealth attacks, the residue had some value greater than zero. Therefore, simple and stealth attacks were detected by our proposed variable dummy value model. As a result, the limitations of the fixed dummy value approach were handled by this variable dummy value model, and stealth FDI attacks were easily detected in the control room.

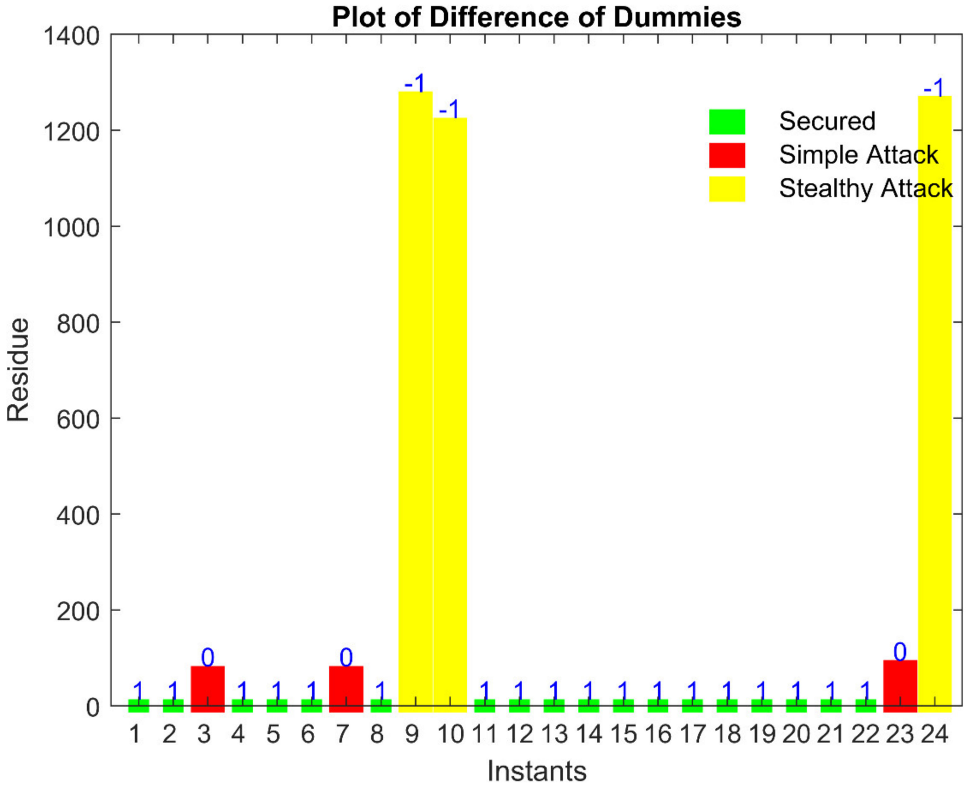

Figure 9. Results of the variable dummy value model for simple and stealth attacks.

7. Discussion

Stealth false data injection attacks create huge damage to a power system. Such kinds of attacks should be detected for a smooth and reliable power flow in a smart grid. The proposed model was applied for the detection of such attacks. The model was based on a dummy measurement. The meters in the smart grid send the actual measurement and the dummy measurement. There are two techniques in the proposed model, namely, the fixed dummy value model and the variable dummy value model.

Both techniques were validated through the experimental results. The first technique of the fixed dummy value model could detect FDI attacks. However, at the same time, this technique has some limitations. When the attacker does not attack the dummy value of measurement, i.e., only the actual measurement is attacked, the control room is not able to detect that attack. The second technique of the proposed model, such as the variable dummy value model overcomes the limitation and the FDI attacks that were left unnoticed by the fixed dummy value model were detected by the variable dummy value model, as validated by the results.

The proposed model does not require the installation of any extra buses or transmission lines. There is no need to install any extra meters. Therefore, the model can be effectively applied to a smart grid and is economically efficient. From the viewpoint of long-term operation, the proposed model can be applied to make a smart grid more protected and secured. In the future, an extension of this work can be done to practically implement the model for a smart grid, which will protect the smart grid from FDI attacks. Some other methods can be adopted to set the dummy values of the power in the future. The probability of launching the attack can be minimized in this way.

8. Conclusions

Two-way communication is one of the most important features of a smart grid. These communication links may be hacked by attackers to launch attacks. A lot of damage, as well as loss, can be caused by cyber-attacks on a power system. Financial benefits can be obtained by the attacker through these attacks. An attacker can also create technical problems. Power information can be corrupted or blocked. The values of power can be increased or decreased, which will cause power blackouts or power outages. The accurate and continuous power flow can be ensured by detecting and minimizing cyber-attacks. The methods of DC state estimation, as well as AC state estimation, are unable to detect stealth FDI attacks.

For this purpose, in this study, a model based on dummy measurement values was proposed and implemented for the detection of stealth FDI attacks. The overall proposed model consisted of a fixed dummy value model and a variable dummy value model. The fixed dummy value model showed promising results against FDI attacks but with some limitations. The variable dummy value model handled those limitations and the stealth FDI attacks were efficiently detected in the control room using our proposed model. Simulations were performed for the model and the results indicated that all the stealth FDI attacks were detected in the control room. We made the power system a secure one.

Author Contributions: Conceptualization, M.A.S., F.A. and F.R.A.; methodology, M.A.S., F.A. and G.H.; software, M.A.S. and Z.U.; validation, M.A.S., F.A. and Z.U.; investigation, F.A. and G.H.; data curation, M.A.S. and F.R.A.; writing—original draft preparation, M.A.S., F.A. and Z.U.; writing—review and editing, M.A.S., F.R.A. and G.H.; supervision, F.A. and G.H. All authors have read and agreed to the published version of the manuscript.

Funding: This work was funded by the Taif University Researchers Supporting Project Number (TURSP-2020/331), Taif University, Taif, Saudi Arabia.

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Acknowledgments: The authors would like to acknowledge the support from Taif University Researchers Supporting Project Number (TURSP-2020/331), Taif University, Taif, Saudi Arabia.

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

References

1. Cui, L.; Qu, Y.; Gao, L.; Xie, G.; Yu, S. Detecting false data attacks using machine learning techniques in smart grid: A survey. *J. Netw. Comput. Appl.* **2020**, *170*, 102808. [CrossRef]
2. Hamidi, V.; Smith, K.S.; Wilson, R.C. Smart grid technology review within the transmission and distribution sector. In Proceedings of the IEEE PES Innovative Smart Grid Technologies Conference Europe (ISGT Europe), Gothenburg, Sweden, 11–13 October 2010; pp. 1–8.
3. Mohammadi, F. Emerging Challenges in Smart Grid Cybersecurity Enhancement: A Review. *Energies* **2021**, *14*, 1380. [CrossRef]
4. Aoufi, S.; Derhab, A.; Guerroumi, M. Survey of false data injection in smart power grid: Attacks, countermeasures and challenges. *J. Inf. Secur. Appl.* **2020**, *54*, 102518. [CrossRef]
5. Mohammadi, F.; Nazri, G.A.; Saif, M. A fast fault detection and identification approach in power distribution systems. In Proceedings of the International Conference on Power Generation Systems and Renewable Energy Technologies (PGSRET), Istanbul, Turkey, 26–27 August 2019; pp. 1–4.
6. Sen, Ö.; van der Velde, D.; Peters, S.N.; Henze, M. An Approach of Replicating Multi-Staged Cyber-Attacks and Countermeasures in a Smart Grid Co-Simulation Environment. *arXiv* **2021**, arXiv:2110.02040.
7. McDaniel, P.; McLaughlin, S. Security and privacy challenges in the smart grid. *IEEE Secur. Priv.* **2009**, *7*, 75–77. [CrossRef]
8. Fang, X.; Misra, S.; Xue, G.; Yang, D. Smart grid—The new and improved power grid: A survey. *IEEE Commun. Surv. Tutor.* **2011**, *14*, 944–980. [CrossRef]
9. Dileep, G. A survey on smart grid technologies and applications. *Renew. Energy* **2020**, *146*, 2589–2625. [CrossRef]

10. Kolhe, M. Smart grid: Charting a new energy future: Research, development and demonstration. *Electr. J.* **2012**, *25*, 88–93. [CrossRef]
11. Gunduz, M.Z.; Das, R. Cyber-security on smart grid: Threats and potential solutions. *Comput. Netw.* **2020**, *169*, 107094. [CrossRef]
12. Jayachandran, M.; Reddy, C.; Padmanaban, S.; Milyani, A.H. Operational planning steps in smart electric power delivery system. *Sci. Rep.* **2021**, *11*, 1–21.
13. Chen, J.; Mohamed, M.A.; Dampage, U.; Rezaei, M.; Salmen, S.H.; Obaid, S.A.; Annuk, A. A Multi-Layer Security Scheme for Mitigating Smart Grid Vulnerability against Faults and Cyber-Attacks. *Appl. Sci.* **2021**, *11*, 9972. [CrossRef]
14. Shaukat, N.; Ali, S.M.; Mehmood, C.A.; Khan, B.; Jawad, M.; Farid, U.; Ullah, Z.; Anwar, S.M.; Majid, M. A survey on consumers empowerment, communication technologies, and renewable generation penetration within Smart Grid. *Renew. Sustain. Energy Rev.* **2018**, *81*, 1453–1475. [CrossRef]
15. Esmalifalak, M.; Liu, L.; Nguyen, N.; Zheng, R.; Han, Z. Detecting stealthy false data injection using machine learning in smart grid. *IEEE Syst. J.* **2014**, *11*, 1644–1652. [CrossRef]
16. Yan, J.; Tang, B.; He, H. Detection of false data attacks in smart grid with supervised learning. In Proceedings of the International Joint Conference on Neural Networks (IJCNN), Vancouver, BC, Canada, 24–29 July 2016; pp. 1395–1402.
17. 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. [CrossRef]
18. Xie, L.; Mo, Y.; Sinopoli, B. Integrity data attacks in power market operations. *IEEE Trans. Smart Grid.* **2011**, *2*, 659–666. [CrossRef]
19. Esmalifalak, M.; Han, Z.; Song, L. Effect of stealthy bad data injection on network congestion in market based power system. In Proceedings of the IEEE Wireless Communications and Networking Conference (WCNC), Paris, France, 1–4 April 2012; pp. 2468–2472.
20. Esmalifalak, M.; Nguyen, H.; Zheng, R.; Han, Z. Stealth false data injection using independent component analysis in smart grid. In Proceedings of the IEEE International Conference on Smart Grid Communications (SmartGridComm), Brussels, Belgium, 17–20 October 2011; pp. 244–248.
21. Liu, L.; Esmalifalak, M.; Han, Z. Detection of false data injection in power grid exploiting low rank and sparsity. In Proceedings of the IEEE International Conference on Communications (ICC), Budapest, Hungary, 9–13 June 2013; pp. 4461–4465.
22. Liu, L.; Esmalifalak, M.; Ding, Q.; Emesih, V.A.; Han, Z. Detecting false data injection attacks on power grid by sparse optimization. *IEEE Trans. Smart Grid.* **2014**, *5*, 612–621. [CrossRef]
23. Sayghe, A.; Hu, Y.; Zografopoulos, I.; Liu, X.; 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. [CrossRef]
24. Hug, G.; Giampapa, J.A. Vulnerability assessment of AC state estimation with respect to false data injection cyber-attacks. *IEEE Trans Smart Grid.* **2012**, *3*, 1362–1370. [CrossRef]
25. Liang, J.; Kosut, O.; Sankar, L. Cyber attacks on AC state estimation: Unobservability and physical consequences. In Proceedings of the IEEE PES General Meeting | Conference & Exposition, National Harbor, MD, USA, 27–31 July 2014; pp. 1–5.
26. Motiyani, M.R.; Chudasama, A.R.; Desai, M.A. Electrical Power System State Estimation: Theory and Implementation; 2015. Available online: https://www.semanticscholar.org/paper/ELECTRICAL-POWER-SYSTEM-STATE-ESTIMATION-%3A-THEORY-Motiyani-Chudasama/f5e8da4e8a6253575780b2ddc89725998eb35591 (accessed on 29 March 2022).
27. Monticelli, A. Electric power system state estimation. *Proc. IEEE* **2000**, *88*, 262–282. [CrossRef]
28. Ozay, M.; Esnaola, I.; Vural, F.T.; Kulkarni, S.R.; Poor, H.V. Machine learning methods for attack detection in the smart grid. *IEEE Trans. Neural Netw. Learn. Syst.* **2015**, *27*, 1773–1786. [CrossRef]
29. Huang, Y.; Esmalifalak, M.; Nguyen, H.; Zheng, R.; Han, Z.; Li, H.; Song, L. Bad data injection in smart grid: Attack and defense mechanisms. *IEEE Commun. Mag.* **2013**, *51*, 27–33. [CrossRef]
30. Kosut, O.; Jia, L.; Thomas, R.J.; Tong, L. Malicious data attacks on smart grid state estimation: Attack strategies and countermeasures. In Proceedings of the IEEE International Conference on Smart Grid Communications, Gaithersburg, MD, USA, 4–6 October 2010; pp. 220–225.
31. Chaojun, G.; Jirutitijaroen, P.; Motani, M. Detecting false data injection attacks in ac state estimation. *IEEE Trans. Smart Grid.* **2015**, *6*, 2476–2483. [CrossRef]
32. Ayad, A.; Farag, H.E.; Youssef, A.; El-Saadany, E.F. Detection of false data injection attacks in smart grids using recurrent neural networks. In Proceedings of the IEEE Power & Energy Society Innovative Smart Grid Technologies Conference (ISGT), Washington, DC, USA, 19–22 February 2018; pp. 1–5.
33. Foroutan, S.A.; Salmasi, F.R. Detection of false data injection attacks against state estimation in smart grids based on a mixture Gaussian distribution learning method. *IET Cyber-Phys. Syst. Theory Appl.* **2017**, *2*, 161–171. [CrossRef]
34. Yang, C.; Wang, Y.; Zhou, Y.; Ruan, J.; Liu, W. False data injection attacks detection in power system using machine learning method. *J. Comput. Commun.* **2018**, *6*, 276. [CrossRef]
35. Ashrafuzzaman, M.; Das, S.; Chakhchoukh, Y.; Shiva, S.; Sheldon, F.T. Detecting stealthy false data injection attacks in the smart grid using ensemble-based machine learning. *Comput. Secur.* **2020**, *97*, 101994. [CrossRef]
36. Farrukh, Y.A.; Khan, I.; Ahmad, Z.; Elavarasan, R.M. A sequential supervised machine learning approach for cyber attack detection in a smart grid system. *arXiv* **2021**, arXiv:2108.00476.
37. Acosta, M.R.; Ahmed, S.; Garcia, C.E.; Koo, I. Extremely randomized trees-based scheme for stealthy cyber-attack detection in smart grid networks. *IEEE Access* **2020**, *8*, 19921–19933. [CrossRef]

38. Sakhnini, J.; Karimipour, H.; Dehghantanha, A. Smart grid cyber attacks detection using supervised learning and heuristic feature selection. In Proceedings of the IEEE 7th International Conference on Smart Energy Grid Engineering (SEGE), Oshawa, ON, Canada, 12–14 August 2019; pp. 108–112.
39. Xue, D.; Jing, X.; Liu, H. Detection of false data injection attacks in smart grid utilizing ELM-based OCON framework. *IEEE Access* **2019**, *7*, 31762–31773. [CrossRef]
40. Aboelwafa, M.M.; Seddik, K.G.; Eldefrawy, M.H.; Gadallah, Y.; Gidlund, M. A machine-learning-based technique for false data injection attacks detection in industrial IoT. *IEEE Internet Things J.* **2020**, *7*, 8462–8471. [CrossRef]
41. Wang, C.; Tindemans, S.; Pan, K.; Palensky, P. Detection of false data injection attacks using the autoencoder approach. In Proceedings of the International Conference on Probabilistic Methods Applied to Power Systems (PMAPS), Liège, Belgium, 18–21 August 2020; pp. 1–6.
42. Kundu, A.; Sahu, A.; Serpedin, E.; Davis, K. A3d: Attention-based auto-encoder anomaly detector for false data injection attacks. *Electr. Power Syst. Res.* **2020**, *189*, 106795. [CrossRef]
43. Zhou, L.; Ouyang, X.; Ying, H.; Han, L.; Cheng, Y.; Zhang, T. Cyber-attack classification in smart grid via deep neural network. In Proceedings of the 2nd International Conference on Computer Science and Application Engineering, Hohhot, China, 22–24 October 2018; pp. 1–5.
44. Niu, X.; Li, J.; Sun, J.; Tomsovic, K. Dynamic detection of false data injection attack in smart grid using deep learning. In Proceedings of the IEEE Power & Energy Society Innovative Smart Grid Technologies Conference (ISGT), Washington, DC, USA, 17–20 February 2019; pp. 1–6.
45. An, D.; Yang, Q.; Liu, W.; Zhang, Y. Defending against data integrity attacks in smart grid: A deep reinforcement learning-based approach. *IEEE Access* **2019**, *7*, 110835–110845. [CrossRef]
46. Tabakhpour, A.; Abdelaziz, M.M. Neural network model for false data detection in power system state estimation. In Proceedings of the IEEE Canadian Conference of Electrical and Computer Engineering (CCECE), Edmonton, AB, Canada, 5–8 May 2019; pp. 1–5.
47. Zhang, Y.; Wang, J.; Chen, B. Detecting false data injection attacks in smart grids: A semi-supervised deep learning approach. *IEEE Trans. Smart Grid.* **2020**, *12*, 623–634. [CrossRef]
48. González, I.; Calderón, A.J.; Portalo, J.M. Innovative multi-layered architecture for heterogeneous automation and monitoring systems: Application case of a photovoltaic smart microgrid. *Sustainability* **2021**, *13*, 2234. [CrossRef]
49. Kabalci, Y. A survey on smart metering and smart grid communication. *Renew. Sustain. Energy Rev.* **2016**, *57*, 302–318. [CrossRef]
50. Zhang, J.; Hasandka, A.; Wei, J.; Alam, S.M.; Elgindy, T.; Florita, A.R.; Hodge, B.M. Hybrid communication architectures for distributed smart grid applications. *Energies* **2018**, *11*, 871. [CrossRef]
51. Manandhar, K.; Cao, X.; Hu, F.; Liu, Y. Detection of faults and attacks including false data injection attack in smart grid using Kalman filter. *IEEE Trans. Control Netw.* **2014**, *1*, 370–379. [CrossRef]
52. Wu, M.; Xie, L. Online detection of false data injection attacks to synchrophasor measurements: A data-driven approach. In Proceedings of the 50th Hawaii International Conference on System Sciences, Village, HI, USA, 4–7 January 2017.
53. Kurt, M.N.; Yılmaz, Y.; Wang, X. Distributed quickest detection of cyber-attacks in smart grid. *IEEE Trans. Inf. Forensics Secur.* **2018**, *13*, 2015–2030. [CrossRef]
54. Du, D.; Li, X.; Li, W.; Chen, R.; Fei, M.; Wu, L. ADMM-based distributed state estimation of smart grid under data deception and denial of service attacks. *IEEE Trans. Syst. Man Cybern. Syst.* **2019**, *49*, 1698–1711. [CrossRef]
55. Kurt, M.N.; Yılmaz, Y.; Wang, X. Real-time detection of hybrid and stealthy cyber-attacks in smart grid. *IEEE Trans. Inf. Forensics Secur.* **2018**, *14*, 498–513. [CrossRef]
56. Pang, Z.H.; Fan, L.Z.; Sun, J.; Liu, K.; Liu, G.P. Detection of stealthy false data injection attacks against networked control systems via active data modification. *Inf. Sci.* **2021**, *546*, 192–205. [CrossRef]
57. Zhu, R.; Huang, C.; Deng, S.; Li, Y. Detection of False Data Injection Attacks Based on Kalman Filter and Controller Design in Power System LFC. *J. Phys. Conf. Ser.* **2021**, *1861*, 012120. [CrossRef]