AI based approach to identify compromised meters in data integrity attacks on smart grid

Kush Khanna[*], Bijaya Ketan Panigrahi[*]and Anupam Joshi[†]

Abstract

False data injection attacks can pose serious threats to the operation and control of power grid. The smarter the power grid gets, the more vulnerable it becomes to cyber attacks. Various detection methods of cyber attacks have been proposed in the literature in recent past. However, to completely alleviate the possibility of cyber threats, the compromised meters must be identified and secured. In this paper, we are presenting an Artificial Intelligence (AI) based identification method to correctly single out the malicious meters. The proposed AI based method successfully identifies the compromised meters by anticipating the correct measurements in the event of the cyber attack. NYISO load data is mapped with the IEEE 14 bus system to validate the proposed method. The efficiency of the proposed method is compared for Artificial Neural Network (ANN) and Extreme Learning Machine (ELM) based AI techniques. It is observed that both the techniques identify the corrupted meters with high accuracy.

Index Terms: Cyber security, false data injection, power system optimization, smart grid.

Nomenclature

$\boldsymbol{a}$	Attack vector.
$\boldsymbol{c}$	Error caused in the state vector due to attack vector $\boldsymbol{a}$.
$\boldsymbol{e}$	Gaussian meter error vector.
$\boldsymbol{H}$	Measurement Jacobian.

[*] K. Khanna and B. K. Panigrahi are with the Department of Electrical Engineering, Indian Institute of Technology Delhi, New Delhi, India e-mail: (kushkhanna06@gmail.com, bkpanigrahi@ee.iitd.ac.in).

[†] Anupam Joshi is with the Computer Science and Electrical Engineering Department, University of Maryland Baltimore County, Baltimore MD 21250, USA (email: joshi@umbc.edu).

$\boldsymbol{V}$	Complex voltage $V\angle\theta$.
$\boldsymbol{x_{bad}}$	State vector after attack.
$\boldsymbol{x}$	System state vector.
$\boldsymbol{Y}$	Bus admittance matrix.
$\boldsymbol{z_{bad}}$	Perturbed measurements after attack.
$\boldsymbol{z}$	Measurement vector.
σ_i	Standard deviation of measurement z_i.
f, t	From bus and To bus matrix for transmission lines.
g_{ij}, b_{ij}	Conductance and susceptance of line $i-j$.
g_{si}, b_{si}	Shunt conductance and shunt susceptance at bus i.
$h(\boldsymbol{x})$	Measurement function.
m	Number of measurements available.
N_A^i	Set of buses affected by change in state θ_i or V_i.
N_b^i	Set of buses directly connected to the bus i.
N_{bus}	Set of all the buses in the network.
n_{flow}^i	Total number of real power flow meters required to be attack to cause change in state θ_i or V_i.
n_{inj}^i	Total number of real and reactive power injection meters required to be attack to cause change in state θ_i or V_i.
N_{line}	Set of transmission lines affected by change in state θ_i or V_i.
N_{line}^i	Set of transmission lines directly connected to the bus i.
P_i	Real power injection at bus i.
P_{ij}	Real power flow in the line $i-j$.
Q_i	Reactive power injection at bus i.
Q_{ij}	Reactive power flow in the line $i-j$.
V, θ	System states (Voltage magnitude and Angle).

1 Introduction

Utilization of electrical energy is recognized as the most efficient way of energy consumption. The electrical power system, a complex web of generating stations, transmission lines, and distribution systems, ensures that this electrical energy is supplied to the end users efficiently and reliably. The real time monitoring of the events in the power system is very crucial for its secure operation. Energy management system (EMS) uses state estimation (SE) to estimate the complex voltage ($V\angle\theta$) at each bus in the power system [1]. SE uses field sensors data which are collected from Supervisory Control and Data Acquisition (SCADA) to accurately estimate the real time voltages of the network. Once the system states are estimated, the system operator performs the security analysis to ensure the reliable and secure operation of power system. The futuristic '*smart grid*' offers improved reliability of electrical power and robust operation and control of the power grid. Information and communication infrastructure enables power systems to be available from outside networks which allow remote control; faster location and isolation of faults; and quick restoration of electrical power [2].

Accessibility of information to the end users facilitates Demand Response (DR) and Advanced Metering Infrastructure (AMI). Smart metering at the consumer end provides two-way communication between the utility and the customer [3], which enables the end users to access real-time pricing and usage. In the advent of information and communication technology (ICT), apart from physical security of power system, cyber security has also gained great importance. Securing the cyber aspect means securing all the communication between physical power system components like remote terminal units (RTUs) and intelligent electronic devices (IEDs) as well as communication between SCADA and field sensors. Any weak link in the cyber security of power system can threaten the physical security of the power system due to interconnected cyber-physical infrastructure. Despite multifold advantages, ICT integration in the power system has also unlocked the possibilities of cyber intrusions.

The data obtained from the field sensors and meters also contains meter noise as well as errors due to fault in the meters. The accuracy of estimated states depends on the quality of measurement sensors. Bad data detection is incorporated in SE to identify the faulty meters which are the source of the errors. To achieve the accurate state estimates, the redundancy in the measurements is important to identify and detect the source of bad data [4]. The researchers have shown that false data injection (FDI) attack can be launched by injecting the small errors in the meters within the toleration of bad data detection algorithm [5]. However, if the attacker succeeds in gaining network information (network topology, line parameters and access to meters), can launch a far more serious form of FDI attacks [6]. In [7], it is presented that the adversary can still launch a successful (formulation of attack vector which bypasses the bad data detection is considered here as *'successful'* or *'well-crafted'* attack. Here-onwards, 'successful' and 'well-crafted' will be used interchangeably throughout the paper.) FDI attack against SE with limited network knowledge and restricted access to the meters in the network. Load redistribution attacks can be formulated by intelligently modifying the load meters data for accessible meters in such a way that the total load on the system remains unchanged [8]. Load redistribution attack can also cause incorrect security constrained economic dispatch (SCED), resulting in an uneconomic power system operation, load shedding and in the worst case system wide disruptions [9, 10]. In addition to the false data injected in the meters, attack on the topology can also be launched by deceiving the system operator with falsified network topology. To carry out such attack, meter reading and *on/off* states of the network switches are manipulated simultaneously and intelligently to project false system operating point [11].

FDI attacks have many adverse effects on the operation of power system. The cyber threats are not only limited to the security of the power system. A well-constructed attack on the electricity markets can also be launched for gaining financial benefits. In [12], an optimised attack to gain economic benefits in the real time market is presented. Xie et al. presented an attack to affect the deregulated energy market [13]. It is shown that the attacker can make profits by buying virtual power at the lower price in the day ahead market and selling it at the higher price in real time market.

To secure the power grid from the aforementioned attack strategies, various methods to alleviate the possibilities of the attack are presented by the researchers in recent years. Defensive approaches against false data injection attacks can be broadly classified into two categories; *protecting meters (PMUs, IEDs, and RTUs)*; and *real time attack detection*. In the former approach, protecting the set of critical measurements in the network is presented in [14]. It is rather idealistic to ensure the security of the critical meter all the time. Moreover, in the case of attack considering limited network knowledge, attacker confines the attack in relatively smaller and remote region. Tampering the meter security and launching a successful attack is still possible [12]. However, it is worth noting that placing sufficient PMUs in the network can aid in detecting FDI attacks. The cost of deploying PMUs is high, therefore, an optimized number of PMUs and their strategic locations are presented in [15] for detecting cyber attacks. Real time detection based approach for FDI attacks are presented in [16, 17, 18]. In [16], CUSUM detector based approach is presented. Collaborative intrusion detection system against the false data injection attacks is given in [17]. Attack vectors can be separated out from the measurements using sparse optimization as shown in [18].

Chaojun et al. [19], presented real time detection of false data injection attacks based on the comparison of measurement variations obtained from historical measurements and real time measurement variation in real time. Kullback-Leibler divergence (KLD) is used to compare the historical and real time measurement variations. In [20], a joint transformation based approach to detect FDI attacks is presented. The technique has higher detection probability but the method fails to identify the attacked meters. In this paper, we went beyond the detection and propose an AI based identification of the attacked meters by accurate estimation the loads and measurements in the event of FDI attack. To detect the attack, the same approach as proposed in [19, 20] is used. After successful detection, AI based load estimator accurately identifies the attacked meters so that a corrective action can be taken by the system operator to maintain the integrity of the SE. The proposed approach efficiently identifies the FDI attacks in smart grid with minimum perturbed meters, therefore, it is assured that the scheme can correctly identify the attacks with larger perturbation irrespective of the kind/motive of the attack. Hence, the scheme ensures secure and economic operation and control of the power system.

The remaining sections of the paper are organized as follows. In section 2 a brief overview of state estimation (SE) and false data injection attacks is presented. Section 3 describes the ANN/ELM based identification methodology, section 4 presents results and discussion for IEEE 14 bus test system and section 5 conclude the paper with possible future outlooks.

2 Brief summary of State Estimation (SE) and False Data Injection (FDI) attacks

2.1 Power system state estimation

To estimate the power system states, the SE uses the field measurements data collected by SCADA from the field sensors. The redundant measurements are often used to ensure that the bad measurements (containing meter errors or due to telemetry errors) can be easily filtered out. The field measurements includes, voltage measurement for PV (generator) bus, real and reactive nodal power injections and real and reactive power flows in the transmission lines. For a N_{bus} power system, considering polar co-ordinates, the number of states defining the power system completely are $2N_{bus}-1$. The state vector x contains N_{bus} voltage magnitude and $N_{bus}-1$ phase angles. θ_1 is given an arbitrary value 0 for a reference. Therefore, x can be denoted as;

$$\boldsymbol{x} = [\underbrace{\theta_2, \theta_3, \ldots, \theta_{N_{bus}}}_{\text{Angles}}, \underbrace{V_1, V_2, \ldots, V_{N_{bus}}}_{\text{Voltage magnitudes}}] \tag{1}$$

For z measurement set available with m measurements, Weighted Least Square (WLS) estimates the state by minimizing $J(\boldsymbol{x})$, which is given as;

$$J(\boldsymbol{x}) = \sum_{i=1}^{m} (z_i - h(\boldsymbol{x}))/\sigma_i^2 \tag{2}$$

The measurement function $h(x)$ is formulated by defining the real and reactive power flow and power injection measurements as given in (3)-(6).

$$P_i = \Re\{\boldsymbol{V_i^*} \sum_{k=1,k\neq i}^{N_{bus}} \boldsymbol{V_k} Y_{ik}\} \quad \forall i \in N_{bus} \tag{3}$$

$$Q_i = -\Im\{\boldsymbol{V_i^*} \sum_{k=1,k\neq i}^{N_{bus}} \boldsymbol{V_k} Y_{ik}\} \quad \forall i \in N_{bus} \tag{4}$$

$$\begin{aligned} P_{ij} =& V_i^2(g_{si} + g_{ij}) - \\ & V_i V_j (g_{ij} \cos\theta_{ij} + b_{ij} \sin\theta_{ij}) \quad \forall i, j \in N_{bus} \end{aligned} \tag{5}$$

$$\begin{aligned} Q_{ij} =& - V_i^2(b_{si} + b_{ij}) - \\ & V_i V_j (g_{ij} \sin\theta_{ij} - b_{ij} \cos\theta_{ij}) \quad \forall i, j \in N_{bus} \end{aligned} \tag{6}$$

2.2 False data injection attacks

Since Liu et al. [6] identified the vulnerability in power grid against false data injection attacks, the power engineering community has witnessed extensive research in the area of cyber-physical power systems. As explained in [6], the adversary with the knowledge of certain power system and network related information can launch FDI attacks in order to deceive the system operator with incorrect estimated states. The motives behind such attacks can be multiple, ranging from making financial misconducts to jeopardizing entire operation and control of power system.

Cyber-threats can be broken down into the core components of the information security triad; Confidentiality, Integrity, and Availability (CIA). False data injection attacks can be considered as the combination of loss of integrity and confidentiality. An attacker with access to the critical network and system information (loss of confidentiality) can inject a false data into the smart meters (loss of integrity) to mislead the system operator with false system states.

The general FDI attack can be launched by finding a suitable attack vector as long as the normalized residue is less than the threshold for bad data detection as shown below,

$$J(\hat{\boldsymbol{x}}_{bad}) = \sum_{i=1}^{m}(z_i - h(\hat{\boldsymbol{x}}) + a_i)/\sigma_i^2 \leq \tau \tag{7}$$

here a_i is the injected error in the measurement z_i. This problem can be solved for the set of meters accessible by the adversary ($a_i \neq 0$). The feasibility of launching the attack with the specified set of accessible meters are not guaranteed, however, a possible combination of meters can be found out to form a suitable attack vector with small errors which are tolerated by state estimation algorithm.

FDI attacks bypasses the bad data detection of the state estimation as shown in [6], if $\|\boldsymbol{z} - \boldsymbol{H}\hat{\boldsymbol{x}}\| \leq \tau$, an attack vector $\boldsymbol{a}$, which is the linear combination of column vector of $\boldsymbol{H}$ (i.e. $\boldsymbol{a} = \boldsymbol{Hc}$), can bypass the bad data detection test as shown below,

$$\begin{aligned}\|(\boldsymbol{z} + \boldsymbol{a}) - H(\hat{\boldsymbol{x}} + \boldsymbol{c})\| &= \|\boldsymbol{z} - \boldsymbol{H}\hat{\boldsymbol{x}} + \boldsymbol{a} - \boldsymbol{Hc}\| \\ &= \|\boldsymbol{z} - \boldsymbol{H}\hat{\boldsymbol{x}}\| \leq \tau \end{aligned} \tag{8}$$

Based on the above lemma (8), many different attack strategies are proposed in the recent years. By keeping (8) satisfied, attacks can also be launched with limited information [7, 21]. This brings in the idea of separating out the attacking and non-attacking region from the network based on the information of the network and accessible meters possessed by the attacker. The attack is launched by forming the attack vector in such a way that the states of the boundary buses remain unchanged and the attack is confined only in the attacking region, thereby, satisfying (8) for launching a successful attack.

3 AI based Identification of malicious meters

It can be concluded from the previous section, that all FDI attacks, irrespective of their modeling, eventually misleads the system operator with falsified system states. Furthermore, as the targeted state variable increases, a higher number of meters are required by the adversary to launch the 'successful' attack. Therefore, it is logical to design a protection scheme which is capable of detecting the attack with a minimum set of compromised meters. As given in [19, 20], historical measurement variations can be used to detect the FDI attacks in the real-time. The Kullback Leibler Divergence gives the difference

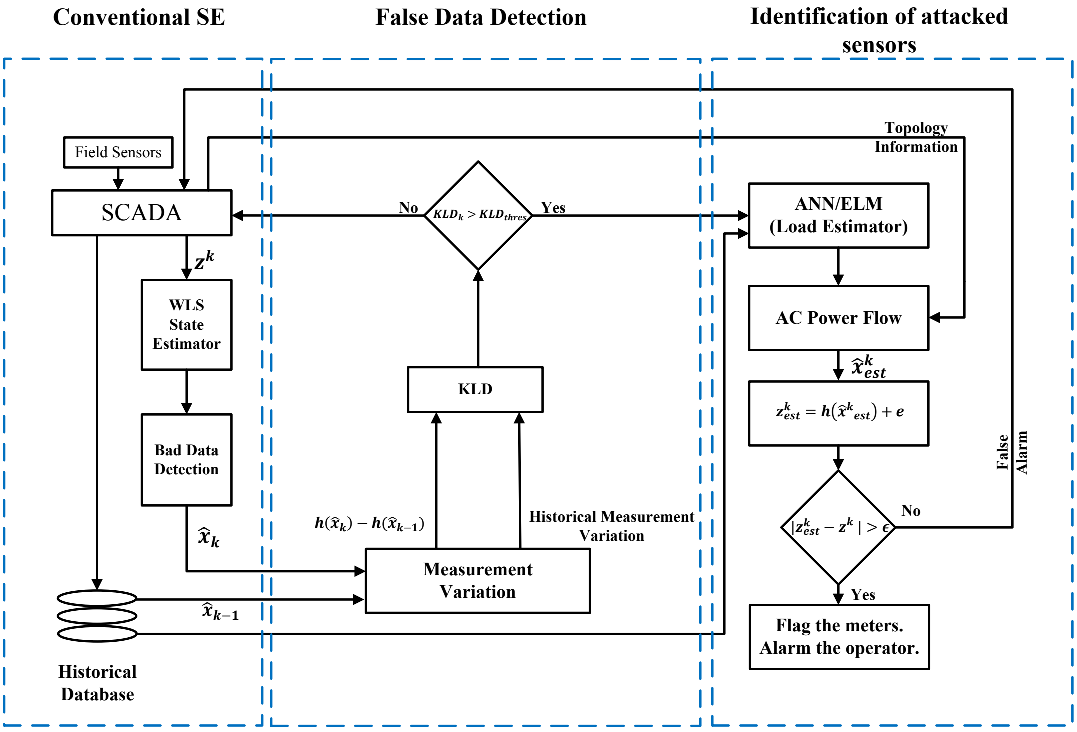


Figure 1: Proposed detection and identification scheme for FDI attacks

between historical measurement variation and real time measurement variation. If KLD value for the real time measurement sample is greater than the threshold (obtained from true historical measurements), it can be deduced that the FDI attack is present in the measurement sample. Once the attack is successfully detected, AI based load estimator is used to predict the load for the present sample using older correct samples, which identifies the attacked measurement sensors and alarm the system operator. The complete detection and identification scheme against FDI attacks is shown in Fig. 1.

3.1 Conventional SE

Measurement data from the field sensors (RTUs, PMUs, and IEDs) is collected by the SCADA system. System operator runs the WLS (Weighted Least Square) state estimator to estimate the current operating states of the power system. Bad data detection, a part of SE process detects and identifies the source of bad data in the measurements by obtaining the normalized residues as explained in section 2.2. The output of the SE process (WLS state estimator and bad data detection) is the estimated $\hat{x}$. System operator visualizes the entire power grid using the estimated $\hat{x}$ to run critical programs like contingency analysis, optimal power flow, and security analysis to ensure secure operation of the grid. To ensure the integrity of estimated state $\hat{x}$, the false data detection is implemented after state estimation as shown in Fig. 1.

3.2 False data detection

For the k^{th} measurement sample, the measurement variation can be obtained from the estimated state $\hat{x}_k$ and previous state $\hat{x}_{k-1}$ as given in (9).

$$\begin{aligned} \Delta \boldsymbol{z} &= \boldsymbol{z_k} - \boldsymbol{z_{k-1}} \\ &= h(\hat{\boldsymbol{x}}_k) - h(\hat{\boldsymbol{x}}_{k-1}) \end{aligned} \tag{9}$$

here $z_k = h(\hat{\boldsymbol{x}}_k) + \boldsymbol{e}_k$ and $z_{k-1} = h(\hat{\boldsymbol{x}}_{k-1}) + \boldsymbol{e}_{k-1}$. Assuming meter errors at both time samples k and $k-1$ are approximately equal, i.e. $\boldsymbol{e}_k \approx \boldsymbol{e}_{k-1}$), $\Delta \boldsymbol{z} = h(\hat{\boldsymbol{x}}_k) - h(\hat{\boldsymbol{x}}_{k-1})$.

Similarly the measurement variation of the historical data is obtained from the historical database. It is assumed that the measurements in the historical database are true measurements and does not have any FDIs.

In [19], KLD is calculated directly by comparing the historical measurement variations with k^{th} measurement variation. The Kullback-Leibler distance is a measure of the information lost when $p(s)$ is used to approximate $q(s)$. The Kullback- Leibler distance (KLD) between two probability mass functions $p(s)$ and $q(s)$ is represented as,

$$D(p\|q) = \sum p(s) \ln \frac{p(s)}{q(s)} \tag{10}$$

The Kullback-Leibler Divergence can be calculated from (10), here $p(s)$ and $q(s)$ are probability distribution of measurement variation data set 's' for the current measurement sample k and for the historical measurements respectively. The KLD calculated for the sample k is known as 'run time KLD'. The measurement variation $q(s)$ is constructed from the six months old historical measurement variation data set. In order to confirm the presence of false data injection, the run time KLD (KLD_k) is compared with the predefined threshold value (KLD_{thres}). It is worth noting here that setting a threshold value is very critical for detecting false data injection attacks. Setting lower threshold results in higher false positive rate, whereas, a higher value of threshold results in poor detection efficiency.

To calculate the threshold value, historical measurement variations are compared with the measurement variations of one month samples prior to the k^{th} sample in consideration. In this paper, we have taken measurement samples from 1^{st} Jan to 30^{th} June as historical measurements and samples for the complete month of July to calculate the threshold value. As stated earlier, all the measurement samples from 1^{st} Jan to 31^{st} July are considered true with no false data injection attack. Once the KLDs for all the measurement sample for the complete month of July is obtained, a histogram KLD values are plotted. KLD_{thres} is the KLD value in the histogram which is more than that of 99% of measurement samples. KLD_{thres} denotes that for the measurement variation of a complete month, 99% of the run time KLDs are less than the threshold value. In other words, it can be concluded that if the run time KLD is greater than this threshold, operator confirms the presence of FDI attack with 99% confidence level.

3.3 Identification of attacked meters

For mapping complex nonlinear input-output relations, feed forward neural networks are extensively used in various domains and applications. Single hidden Layer Feed forward Neural networks (SLFN) also known as Extreme Learning Machine (ELM) has faster learning time as compared to the conventional feed forward neural networks [22]. As applied in this work, ANN and ELM are used to predict the load from older load sample. The load estimator has 17 inputs (11 loads for 11 zones for $(k-1)^{th}$ sample, which will be explained in Section 4.1; 3 inputs for the weather details (weather input includes temperature, dew point and humidity) of the $(k-1)^{th}$ sample; and 3 inputs for weather details of k^{th} sample) and 11 outputs (11 predicted loads for k^{th} sample). For ANN, hidden layer has 35 neurons and for ELM, hidden layer is assumed to have 2000 nodes. To train the network, load measurement samples of past fifteen days at 5 minutes interval are used.

Once the load is predicted, AC power flow considering the predicted load and the topology information, gives the predicted measurements (real and reactive power injections; and real power flows in the transmission line) for the k^{th} sample. To validate the predicted measurements, the measurements are compared with the true measurements values for the complete month prior to the k^{th} sample in consideration (i.e. the predicted values for the complete month of July is compared with the true measurements from the historical database). The percentage errors for each measurement sample is plotted in the histogram for the month of July which gives the variance of the error over the period of a month for each meter. Error threshold for identifying the attacked meter is set similarly as explained for detecting false data. Here each meter is given a threshold error based error variance. The error value which is greater than 99% of the values obtained for the complete one month measurements of July is set as the threshold for that particular meter and similarly for the remaining meters. If for the k^{th} sample, the difference between the actual measurement and predicted measurement (z_{est}^{k} must not be confused with the measurement vector obtained after state estimation process which is denoted by z^{k}. z_{est}^{k} here is obtained after running the AC power flow on the predicted/estimated load at the sample k by the artificial neural network (ANN) as shown in Fig 1) $(z_{est}^{k} - z^{k})$ is greater than threshold ϵ, then the meter corresponds to that measurement is flagged as attacked and system operator is alarmed.

The proposed methodology for detecting and identifying the false data injection attack with compromised meters is tested for IEEE 14 bus system. The system details and the discussion on the results are presented in the subsequent section.

4 Results and Discussion

4.1 System Details

IEEE 14 bus system is used to test and validate the effectiveness of the proposed methodology. The test system is shown in Fig. 2. IEEE 14 bus system has eleven loads connected to the buses as shown by the arrow in the Fig. 2. The test system has 2 generators denoted by 'G' and three synchronous condensers denoted by 'C'. To simulate the attack detection and meter identification in real time, the actual load data from New York Independent System Operator (NYISO) is taken from 1^{st} Jan 2014 to 31^{st} Aug 2014 at 5-minute interval [23].

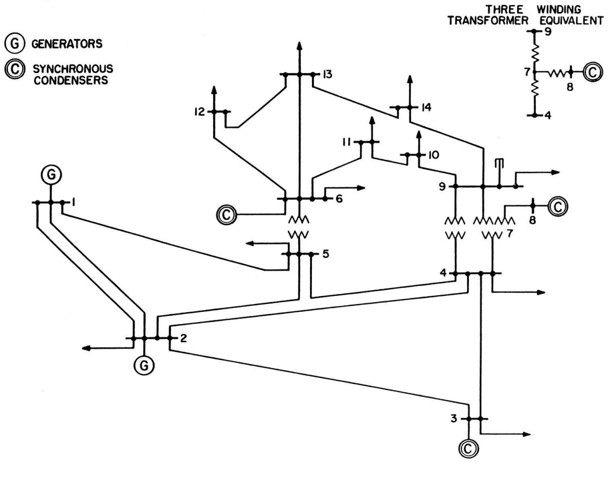


Figure 2: IEEE 14 bus system.

As shown in Fig. 3, NYISO has eleven load zones which are mapped with eleven loads in IEEE 14 bus system as given in [19]. The steps, for forming the test data are enumerated as follows,

1. Due to the unavailability of the reactive load data, information about the power factor at each bus is used from standard IEEE 14 bus data. Reactive power demand for each bus at 5 minutes interval is calculated by keeping same power factor for the load buses as given in standard data.

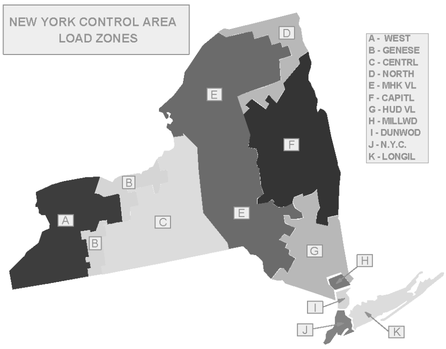


Figure 3: NYISO map showing 11 load zones.

2. For calculating, real and reactive generation for each 5 min interval, real and reactive power generation data from the standard IEEE 14 bus system is proportionally varied depending on the net load during the considered time sample.

3. Complex system voltage ($V\angle\theta$) at each bus for each 5-minute interval is obtained by running the AC power flow program. Gaussian noise of 1% standard deviation is added to the measurements obtained using (3)-(6).

A fully measured power system is considered, therefore we have, real and reactive power injection measurements for all the load buses, real power injection for all the generator buses and to and fro real power flow measurements for all the transmission lines. Therefore, a total of 57 measurements is considered at each 5 minutes time interval.

4.2 Attack Formulation

The attack can be crafted by using any formulation methodology presented in section 2.2. However, as explained earlier, irrespective of the motive of launching the FDI attack, the ultimate effect to the power system is falsified system states. Depending on the formulation of the attack, the affected state variable may be single or multiple. Due to the complex web of transmission lines, the number of meters required to launch the perfect attack increases significantly with the increase in the targeted state variables. Furthermore, as the number of targeted state variables increases, the cost of launching a perfect attack (number of meters required to be accessed) also increases, therefore, an adversary tries to limit the meters by limiting the target states and tries to maximize the impact with a minimum set of meters. The defense strategy, therefore, must be robust enough to detect FDI launched with minimum affected meters. In a fully measured power system, attack on single state variable requires the minimum set of meters (depending on the connectivity of the network, attack on one state variable requires power injection meters associated with the buses which are directly connected to the target state variable bus and flow meters on connecting transmission lines). Hence a generalized attack is formulated affecting only one state variable at a time.

For IEEE 14 bus, 27 state variables corresponds to 27 attacks scenarios taking one state at a time. An attack on state variable θ_i or V_i will require N^i_{inj} and N^i_{flow} injection and power flow meters which are define as follows,

$$N^i_A = \{\{i\} \cup N^i_b\} \tag{11}$$

$$n^i_{inj} = 2 \times |N^i_A| \tag{12}$$

here, N^i_A is the set of buses which are affected by the change in the state variable θ_i or V_i, N^i_b is the set of buses directly connected to bus i and n^i_{inj} is total number of real and reactive power injection meters affected by the change in the state variable θ_i or V_i.

$$N^i_{line} \subset N_{line} : f(j), t(j) \in N^i_A \quad \forall j \in N_{line} \tag{13}$$

$$n^i_{flow} = 2 \times |N^i_{line}| \tag{14}$$

To launch a generalised attack, adversary modifies all the measurements for real and reactive power injections; and real power flows by injecting the false data in meters affecting the targeted state variable given by set N^i_A and N^i_{line} for power injection and power flow meters respectively as obtained from (11) and (13). If the targeted state variable is θ_2 adversary can launch the attack by injecting an error of -10% in θ_2, the error injected in the state vector (c) can be formulated by considering,

$$\boldsymbol{c} = [\underbrace{-0.1\theta_2, 0, \ldots, 0}_{\theta_{[1\times(N_{bus}-1)]}}, \underbrace{0, \ldots, 0}_{V_{[1\times N_{bus}]}}]; \tag{15}$$

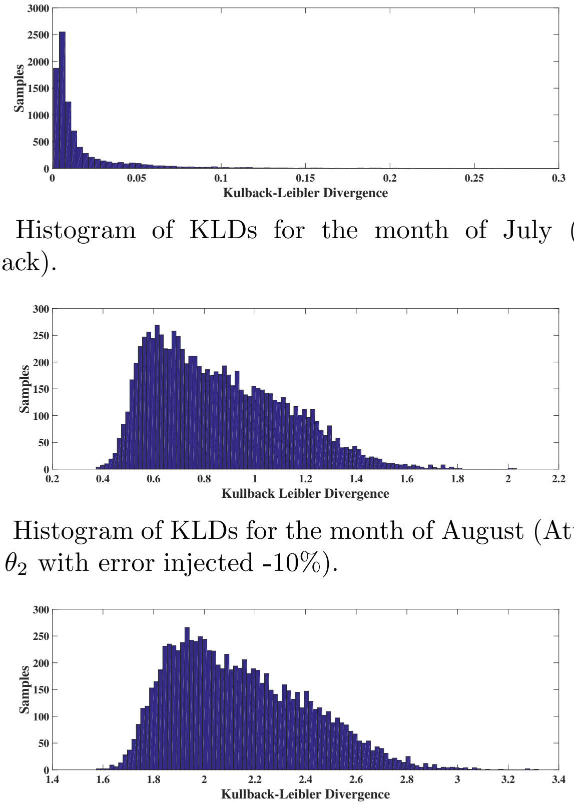
Post-attack measurements can be calculated by using state vector, $x_{bad} = \hat{x} + c$ and solving (3)-(6). For successfully launching the attack, it is assumed that the attacker has knowledge of the network adjoining the bus corresponding to the target state vector. The post-attack measurements are given by,

$$\boldsymbol{z_{bad}} = h(\boldsymbol{x_{bad}}) + \boldsymbol{e} \tag{16}$$

4.3 False Data Detection

To detect the FDI attack in real time, run time KLD (KLD_k) is compared with the threshold (KLD_{thres}). To calculate the threshold, measurement variations for the complete month of July are compared with past six months historical measurement variations (1st Jan to 30 June). The KLD for each measurement sample in July is calculated and plotted as a histogram shown in Fig. 4(a).

The threshold KLD_{thres} is the value of KLD which is higher than 99% of the values in the histogram shown in Fig. 4(a), which is equal to 0.1382. The attack is simulated for each 5 min time interval for the complete month of Aug 2014. The measurement variation for the month of August considering attack is calculated as $z_{bad}^{k} - z_{true}^{k-1}$, where z_{bad}^{k} is attacked measurement sample at time sample k, obtained from (16), and z_{true}^{k-1} is the true measurement sample at the previous time sample $k-1$.



(a) Histogram of KLDs for the month of July (No-attack).

(b) Histogram of KLDs for the month of August (Attack on θ_2 with error injected -10%).

(c) Histogram of KLDs for the month of August (Attack on V_2 with error injected -10%).

Figure 4: Histogram of KLDs for the month of July and August

The histogram of runtime KLD for each sample k in August for attack in θ_2 and V_2 with percentage change in targeted state variable -10% ($c = -10\%$) is shown in Fig. 4(b) and Fig. 4(c) respectively. It is clear from the fig that the runtime KLD (KLD_k) for all the samples in the month of August, considering an attack on θ_2 and V_2 is greater than the threshold 0.1382. Similarly the attack is simulated for other state variables with $c(\%)$ equal to -10, -5, +5 and +10. It is observed that the method detects the FDI attack for each time sample in the month of August.

4.4 Identification of attacked meters

To identify the meters in which the false data is injected, we use ANN/ENN based load estimator to predict the load for the k^{th} sample based on the loading condition of the immediately preceding sample $(k-1)$ and the weather condition of k^{th} and $(k-1)^{th}$ sample. To ensure efficient identification of attacked meters, a threshold of error between the measurements obtained from predicted/estimated loads (load estimator) and actual measurements is calculated considering the true samples from the month of July. The mean absolute percentage error (MAPE) for different measurements obtained from predicted load is shown in the Table 1 and Table 2 for ANN and Table 3 and Table 4 for ELM.

Table 1: MAPE and Threshold for Real and Reactive Power Injection Meters (ANN)

P_{inj}	MAPE	Threshold (ϵ)	Q_{inj}	MAPE	Threshold (ϵ)
P_2	2.33	20.71	Q_4	1.02	5.90
P_3	2.11	20.29	Q_5	0.69	4.10
P_4	1.02	5.90	Q_9	1.22	10.51
P_5	0.69	4.10	Q_{10}	1.09	8.55
P_6	1.24	11.05	Q_{11}	1.82	10.68
P_9	1.21	10.51	Q_{12}	0.99	6.68
P_{10}	1.09	8.55	Q_{13}	0.73	3.64
P_{11}	1.82	10.68	Q_{14}	0.87	4.18
P_{12}	0.99	6.68			
P_{13}	0.73	3.64			
P_{14}	0.87	4.18			

The threshold ϵ, which is the absolute percentage error greater than 99% of the samples in the month of July is tabulated for power injection meters and flow meters given in the Table 1 and Table 2 respectively for ANN and in Table 3 and Table 4 respectively for ELM. Load estimation using ANN is more accurate as compared to ELM, however, the time taken to train an untrained network is 2.88 minutes for ANN and 36.61 seconds for ELM. Every transmission line is assumed to have two real power meters at each end. The threshold and MAPE for both the meters were approximately same, hence threshold and MAPE for only one meter in the line is shown.

Once the attack is detected by the false data detection, the load is predicted for the measurement sample for which the attack is detected. The estimated measurements

Table 2: MAPE and Threshold for Real Power Flow Meters (ANN)

Line Index	Line	MAPE	Threshold (ϵ)	Line Index	Line	MAPE	Threshold (ϵ)
1	$P_{1,2}$	1.20	10.27	11	$P_{6,11}$	1.56	12.65
2	$P_{1,5}$	1.07	8.98	12	$P_{6,12}$	0.80	5.21
3	$P_{2,3}$	1.74	16.18	13	$P_{6,13}$	0.72	4.63
4	$P_{2,4}$	1.02	8.41	15	$P_{7,9}$	0.83	7.02
5	$P_{2,5}$	0.92	7.54	16	$P_{9,10}$	1.47	7.55
6	$P_{3,4}$	3.51	34.96	17	$P_{9,14}$	0.82	4.11
7	$P_{4,5}$	1.31	11.02	18	$P_{10,11}$	2.42	18.75
8	$P_{4,7}$	0.83	7.02	19	$P_{12,13}$	1.63	12.82
9	$P_{4,9}$	0.82	6.94	20	$P_{13,14}$	1.65	10.97
10	$P_{5,6}$	0.83	6.35				

Table 3: MAPE and Threshold for Real and Reactive Power Injection Meters (ELM)

P_{inj}	MAPE	Threshold (ϵ)	Q_{inj}	MAPE	Threshold (ϵ)
P_2	4.15	14.18	Q_4	2.70	9.33
P_3	2.44	7.99	Q_5	2.71	10.19
P_4	2.70	9.33	Q_9	3.34	10.66
P_5	2.71	10.19	Q_{10}	4.42	14.60
P_6	4.11	14.88	Q_{11}	8.14	27.04
P_9	3.34	10.66	Q_{12}	5.07	15.84
P_{10}	4.42	14.60	Q_{13}	3.96	12.12
P_{11}	8.14	27.04	Q_{14}	4.04	14.27
P_{12}	5.07	15.84			
P_{13}	3.96	12.12			
P_{14}	4.04	14.27			

Table 4: MAPE and Threshold for Real Power Flow Meters (ELM)

Line Index	Line	MAPE	Threshold (ϵ)	Line Index	Line	MAPE	Threshold (ϵ)
1	$P_{1,2}$	2.43	8.02	11	$P_{6,11}$	4.77	15.94
2	$P_{1,5}$	2.47	8.20	12	$P_{6,12}$	3.88	12.08
3	$P_{2,3}$	2.52	8.31	13	$P_{6,13}$	3.33	10.75
4	$P_{2,4}$	2.46	8.27	15	$P_{7,9}$	2.75	9.35
5	$P_{2,5}$	2.51	8.43	16	$P_{9,10}$	7.59	23.99
6	$P_{3,4}$	2.72	9.20	17	$P_{9,14}$	4.28	15.20
7	$P_{4,5}$	2.36	7.87	18	$P_{10,11}$	6.69	19.45
8	$P_{4,7}$	2.75	9.35	19	$P_{12,13}$	6.72	20.61
9	$P_{4,9}$	2.73	9.31	20	$P_{13,14}$	5.80	18.91
10	$P_{5,6}$	3.03	10.05				

z^k_{est} are compared with the attacked measurement sample z^k suspected by the false data detection. The absolute percentage error obtained for each measurement is compared with the corresponding threshold ϵ. Table 5 and Table 6 shows the identified meters for the attack on all θ_i with different injected errors $c(\%)$ for ANN and ELM respectively. As shown in the table, the proposed method identifies all the meters quite efficiently and accurately. Furthermore, the proposed method accurately discriminate true samples from the attacked one in the case of falsely detected by the false data detection process. Last row of the Table 5 and Table 6 shows that how the true measurement sample is accurately differentiated.

Table 5: Identification of Meters considering attack on θ with different c (%) (ANN)

θ_i	$c(\%)$	P_{inj}											Q_{inj}								P_{flow}																		
		2	3	4	5	6	9	10	11	12	13	14	4	5	9	10	11	12	13	14	1	2	3	4	5	6	7	8	9	10	11	12	13	15	16	17	18	19	20
θ_2	-10	100	0	99	100	0	0	0	3	0	1	1	100	100	0	0	3	0	1	1	8	0	0	51	100	0	0	0	0	0	0	1	1	0	0	1	0	1	0
	-5	100	0	13	100	0	0	0	3	0	1	1	100	100	0	0	3	0	1	1	0	0	0	1	9	0	0	0	0	0	0	1	1	0	0	1	0	1	0
	5	100	0	5	100	0	0	0	3	0	1	1	100	100	0	0	3	0	1	1	0	0	0	0	3	0	0	0	0	0	0	1	1	0	0	1	0	1	0
	10	100	0	98	100	0	0	0	3	0	1	1	100	100	0	0	3	0	1	1	19	0	0	37	100	0	0	0	0	0	0	1	1	0	0	1	0	1	0
θ_3	-10	100	91	100	2	0	0	0	3	0	1	1	100	2	0	0	3	0	1	1	0	0	10	0	0	100	0	0	0	0	0	1	1	0	0	1	0	1	0
	-5	100	0	100	2	0	0	0	3	0	1	1	100	2	0	0	3	0	1	1	0	0	0	0	0	0	0	0	0	0	0	1	1	0	0	1	0	1	0
	5	100	0	100	2	0	0	0	3	0	1	1	100	2	0	0	3	0	1	1	0	0	0	0	0	0	0	0	0	0	0	1	1	0	0	1	0	1	0
	10	100	96	100	2	0	0	0	3	0	1	1	100	2	0	0	3	0	1	1	0	0	24	0	0	100	0	0	0	0	0	1	1	0	0	1	0	1	0
θ_4	-10	100	0	100	100	0	94	0	3	0	1	1	100	100	0	0	3	0	1	1	0	0	0	100	0	94	100	100	100	0	0	1	1	0	0	1	0	1	0
	-5	100	0	100	100	0	1	0	3	0	1	1	100	100	0	0	3	0	1	1	0	0	0	61	0	0	100	100	99	0	0	1	1	0	0	1	0	1	0
	5	100	0	100	100	0	1	0	3	0	1	1	100	100	0	0	3	0	1	1	0	0	0	72	0	0	100	100	100	0	0	1	1	0	0	1	0	1	0
	10	100	0	100	100	0	92	0	3	0	1	1	100	100	0	0	3	0	1	1	0	0	0	100	0	86	100	100	100	0	0	1	1	0	0	1	0	1	0
θ_5	-10	100	0	100	100	100	0	0	3	0	1	1	100	100	0	0	3	0	1	1	0	61	0	0	100	0	100	0	0	100	0	1	1	0	0	1	0	1	0
	-5	100	0	100	100	100	0	0	3	0	1	1	100	100	0	0	3	0	1	1	0	0	0	0	99	0	100	0	0	97	0	1	1	0	0	1	0	1	0
	5	99	0	100	100	100	0	0	3	0	1	1	100	100	0	0	3	0	1	1	0	1	0	0	99	0	100	0	0	97	0	1	1	0	0	1	0	1	0
	10	100	0	100	100	100	0	0	3	0	1	1	100	100	0	0	3	0	1	1	0	73	0	0	100	0	100	0	0	100	0	1	1	0	0	1	0	1	0
θ_6	-10	0	0	0	100	100	0	0	100	100	100	1	0	100	0	0	100	100	100	1	0	0	0	0	0	0	0	0	0	100	100	100	100	0	0	1	0	1	0
	-5	0	0	0	100	100	0	0	100	100	100	1	0	100	0	0	100	100	100	1	0	0	0	0	0	0	0	0	0	100	100	100	100	0	0	1	0	1	0
	5	0	0	0	100	100	0	0	100	100	100	1	0	100	0	0	100	100	100	1	0	0	0	0	0	0	0	0	0	100	100	100	100	0	0	1	0	1	0
	10	0	0	0	100	100	0	0	100	100	100	1	0	100	0	0	100	100	100	1	0	0	0	0	0	0	0	0	0	100	100	100	100	0	0	1	0	1	0
θ_7	-10	0	0	100	2	0	100	0	3	0	1	1	70	2	0	0	3	0	1	1	0	0	0	0	0	0	0	100	0	0	0	1	1	100	0	1	0	1	0
	-5	0	0	100	2	0	100	0	3	0	1	1	10	2	0	0	3	0	1	1	0	0	0	0	0	0	0	100	0	0	0	1	1	100	0	1	0	1	0
	5	0	0	100	2	0	100	0	3	0	1	1	41	2	0	0	3	0	1	1	0	0	0	0	0	0	0	100	0	0	0	1	1	100	0	1	0	1	0
	10	0	0	100	2	0	100	0	3	0	1	1	99	2	0	0	3	0	1	1	0	0	0	0	0	0	0	100	0	0	0	1	1	100	0	1	0	1	0
θ_8	-10	0	0	0	2	0	0	0	3	0	1	1	0	2	0	0	3	0	1	1	0	0	0	0	0	0	0	0	0	0	0	1	1	0	0	1	0	1	0
	-5	0	0	0	2	0	0	0	3	0	1	1	0	2	0	0	3	0	1	1	0	0	0	0	0	0	0	0	0	0	0	1	1	0	0	1	0	1	0
	5	0	0	0	2	0	0	0	3	0	1	1	0	2	0	0	3	0	1	1	0	0	0	0	0	0	0	0	0	0	0	1	1	0	0	1	0	1	0
	10	0	0	0	2	0	0	0	3	0	1	1	0	2	0	0	3	0	1	1	0	0	0	0	0	0	0	0	0	0	0	1	1	0	0	1	0	1	0
θ_9	-10	0	0	100	2	0	100	100	3	0	1	100	28	2	100	100	3	0	1	100	0	0	0	0	0	0	0	0	100	0	0	1	1	100	100	100	0	1	0
	-5	0	0	26	2	0	100	100	3	0	1	100	2	2	100	100	3	0	1	100	0	0	0	0	0	0	0	0	100	0	0	1	1	100	100	100	0	1	0
	5	0	0	14	2	0	100	100	3	0	1	100	4	2	100	100	3	0	1	100	0	0	0	0	0	0	0	0	100	0	0	1	1	100	100	100	0	1	0
	10	0	0	100	2	0	100	100	3	0	1	100	84	2	100	100	3	0	1	100	0	0	0	0	0	0	0	0	100	0	0	1	1	100	100	100	0	1	0
θ_{10}	-10	0	0	0	2	0	100	100	100	0	1	1	0	2	100	100	100	0	1	1	0	0	0	0	0	0	0	0	0	0	0	1	1	0	100	1	100	1	0
	-5	0	0	0	2	0	100	100	100	0	1	1	0	2	100	100	100	0	1	1	0	0	0	0	0	0	0	0	0	0	0	1	1	0	100	1	100	1	0
	5	0	0	0	2	0	100	100	100	0	1	1	0	2	100	100	100	0	1	1	0	0	0	0	0	0	0	0	0	0	0	1	1	0	100	1	100	1	0
	10	0	0	0	2	0	100	100	100	0	1	1	0	2	100	100	100	0	1	1	0	0	0	0	0	0	0	0	0	0	0	1	1	0	100	1	100	1	0
θ_{11}	-10	0	0	0	2	100	0	100	100	0	1	1	0	2	0	100	100	0	1	1	0	0	0	0	0	0	0	0	0	0	100	1	1	0	0	1	100	1	0
	-5	0	0	0	2	100	0	100	100	0	1	1	0	2	0	100	100	0	1	1	0	0	0	0	0	0	0	0	0	0	100	1	1	0	0	1	100	1	0
	5	0	0	0	2	100	0	100	100	0	1	1	0	2	0	100	100	0	1	1	0	0	0	0	0	0	0	0	0	0	100	1	1	0	0	1	100	1	0
	10	0	0	0	2	100	0	100	100	0	1	1	0	2	0	100	100	0	1	1	0	0	0	0	0	0	0	0	0	0	100	1	1	0	0	1	100	1	0
θ_{12}	-10	0	0	0	2	100	0	0	3	100	100	1	0	2	0	0	3	100	100	1	0	0	0	0	0	0	0	0	0	0	0	100	1	0	0	1	0	100	0
	-5	0	0	0	2	100	0	0	3	100	100	1	0	2	0	0	3	100	100	1	0	0	0	0	0	0	0	0	0	0	0	100	1	0	0	1	0	100	0
	5	0	0	0	2	100	0	0	3	100	100	1	0	2	0	0	3	100	100	1	0	0	0	0	0	0	0	0	0	0	0	100	1	0	0	1	0	100	0
	10	0	0	0	2	100	0	0	3	100	100	1	0	2	0	0	3	100	100	1	0	0	0	0	0	0	0	0	0	0	0	100	1	0	0	1	0	100	0
θ_{13}	-10	0	0	0	2	100	0	0	3	100	100	100	0	2	0	0	3	100	100	100	0	0	0	0	0	0	0	0	0	0	0	1	100	0	0	1	0	100	100
	-5	0	0	0	2	100	0	0	3	100	100	100	0	2	0	0	3	100	100	100	0	0	0	0	0	0	0	0	0	0	0	1	100	0	0	1	0	100	100
	5	0	0	0	2	100	0	0	3	100	100	100	0	2	0	0	3	100	100	100	0	0	0	0	0	0	0	0	0	0	0	1	100	0	0	1	0	100	100
	10	0	0	0	2	100	0	0	3	100	100	100	0	2	0	0	3	100	100	100	0	0	0	0	0	0	0	0	0	0	0	1	100	0	0	1	0	100	100
θ_{14}	-10	0	0	0	2	0	100	0	3	0	100	100	0	2	100	0	3	0	100	100	0	0	0	0	0	0	0	0	0	0	0	1	1	0	0	100	0	1	100
	-5	0	0	0	2	0	99	0	3	0	100	100	0	2	97	0	3	0	100	100	0	0	0	0	0	0	0	0	0	0	0	1	1	0	0	100	0	1	100
	5	0	0	0	2	0	100	0	3	0	100	100	0	2	96	0	3	0	100	100	0	0	0	0	0	0	0	0	0	0	0	1	1	0	0	100	0	1	100
	10	0	0	0	2	0	100	0	3	0	100	100	0	2	100	0	3	0	100	100	0	0	0	0	0	0	0	0	0	0	0	1	1	0	0	100	0	1	100
	NA	0	0	0	2	0	0	0	3	0	1	1	0	2	0	0	3	0	1	1	0	0	0	0	0	0	0	0	0	0	0	1	1	0	0	1	0	1	0

Similarly for the attacks involving V_i state variables, meters identified for all the samples for the month of August is shown in Table 7 and Table 8 for ANN and ELM respectively. Complementing the results obtained for θ_i, the results for V_i also shows the same accuracy in identifying the attacked sensors for all the samples in consideration. Identification efficiency for both ANN and ELM are nearly same for all the 27 attack

Table 6: Identification of Meters considering attack on θ with different c (%) (ELM)

θ_i	c(%)	P_{inj}											Q_{inj}								P_{flow}																		
		2	3	4	5	6	9	10	11	12	13	14	4	5	9	10	11	12	13	14	1	2	3	4	5	6	7	8	9	10	11	12	13	15	16	17	18	19	20
θ_2	-10	100	9	41	100	1	1	2	1	1	3	2	100	100	1	2	1	1	3	2	72	2	19	46	82	2	2	2	2	2	1	2	3	2	0	1	2	1	2
	-5	100	3	5	100	1	1	2	1	1	3	2	99	100	1	2	1	1	3	2	11	2	4	7	15	2	2	2	2	2	1	2	3	2	0	1	2	1	2
	5	100	4	6	100	1	1	2	1	1	3	2	100	100	1	2	1	1	3	2	10	2	5	8	18	2	2	2	2	2	1	2	3	2	0	1	2	1	2
	10	100	11	47	100	1	1	2	1	1	3	2	100	100	1	2	1	1	3	2	63	2	20	55	91	2	2	2	2	2	1	2	3	2	0	1	2	1	2
θ_3	-10	100	100	99	2	1	1	2	1	1	3	2	100	2	1	2	1	1	3	2	2	2	99	2	2	100	2	2	2	2	1	2	3	2	0	1	2	1	2
	-5	100	93	67	2	1	1	2	1	1	3	2	100	2	1	2	1	1	3	2	2	2	41	2	2	100	2	2	2	2	1	2	3	2	0	1	2	1	2
	5	99	85	77	2	1	1	2	1	1	3	2	100	2	1	2	1	1	3	2	2	2	36	2	2	99	2	2	2	2	1	2	3	2	0	1	2	1	2
	10	100	99	100	2	1	1	2	1	1	3	2	100	2	1	2	1	1	3	2	2	2	96	2	2	100	2	2	2	2	1	2	3	2	0	1	2	1	2
θ_4	-10	100	71	100	100	1	64	2	1	1	3	2	100	100	1	2	1	1	3	2	2	2	3	100	2	100	100	100	99	2	1	2	3	2	0	1	2	1	2
	-5	100	12	100	100	1	8	2	1	1	3	2	100	100	1	2	1	1	3	2	2	2	3	62	2	98	100	96	66	2	1	2	3	2	0	1	2	1	2
	5	98	14	100	100	1	8	2	1	1	3	2	100	100	1	2	1	1	3	2	2	2	3	53	2	100	100	99	77	2	1	2	3	2	0	1	2	1	2
	10	100	81	100	100	1	72	2	1	1	3	2	100	100	1	2	1	1	3	2	2	2	3	98	2	100	100	100	100	2	1	2	3	2	0	1	2	1	2
θ_5	-10	100	3	100	100	100	1	2	1	1	3	2	100	100	1	2	1	1	3	2	2	71	3	2	100	2	100	2	2	92	1	2	3	2	0	1	2	1	2
	-5	100	3	100	100	99	1	2	1	1	3	2	100	100	1	2	1	1	3	2	2	11	3	2	80	2	100	2	2	27	1	2	3	2	0	1	2	1	2
	5	97	3	100	100	100	1	2	1	1	3	2	100	100	1	2	1	1	3	2	2	9	3	2	69	2	100	2	2	32	1	2	3	2	0	1	2	1	2
	10	100	3	100	100	100	1	2	1	1	3	2	100	100	1	2	1	1	3	2	2	62	3	2	99	2	100	2	2	98	1	2	3	2	0	1	2	1	2
θ_6	-10	2	3	1	100	100	1	2	100	100	100	2	1	100	1	2	100	100	100	2	2	2	3	2	2	2	2	2	2	100	100	100	100	2	0	1	2	1	2
	-5	2	3	1	100	100	1	2	100	100	100	2	1	95	1	2	100	100	100	2	2	2	3	2	2	2	2	2	2	86	100	100	100	2	0	1	2	1	2
	5	2	3	1	100	100	1	2	100	100	100	2	1	99	1	2	100	100	100	2	2	2	3	2	2	2	2	2	2	76	100	100	100	2	0	1	2	1	2
	10	2	3	1	100	100	1	2	100	100	100	2	1	100	1	2	100	100	100	2	2	2	3	2	2	2	2	2	2	99	100	100	100	2	0	1	2	1	2
θ_7	-10	2	3	100	2	1	100	2	1	1	3	2	32	2	2	2	1	1	3	2	2	2	3	2	2	2	2	100	2	2	1	2	3	100	0	1	2	1	2
	-5	2	3	79	2	1	100	2	1	1	3	2	6	2	1	2	1	1	3	2	2	2	3	2	2	2	2	100	2	2	1	2	3	100	0	1	2	1	2
	5	2	3	89	2	1	100	2	1	1	3	2	9	2	1	2	1	1	3	2	2	2	3	2	2	2	2	99	2	2	1	2	3	100	0	1	2	1	2
	10	2	3	100	2	1	100	2	1	1	3	2	71	2	1	2	1	1	3	2	2	2	3	2	2	2	2	100	2	2	1	2	3	100	0	1	2	1	2
θ_8	-10	2	3	1	2	1	1	2	1	1	3	2	1	2	1	2	1	1	3	2	2	2	3	2	2	2	2	2	2	2	1	2	3	2	0	1	2	1	2
	-5	2	3	1	2	1	1	2	1	1	3	2	1	2	1	2	1	1	3	2	2	2	3	2	2	2	2	2	2	2	1	2	3	2	0	1	2	1	2
	5	2	3	1	2	1	1	2	1	1	3	2	1	2	1	2	1	1	3	2	2	2	3	2	2	2	2	2	2	2	1	2	3	2	0	1	2	1	2
	10	2	3	1	2	1	1	2	1	1	3	2	1	2	1	2	1	1	3	2	2	2	3	2	2	2	2	2	2	2	1	2	3	2	0	1	2	1	2
θ_9	-10	2	3	59	2	1	100	100	1	1	3	100	10	2	100	100	1	1	3	100	2	2	3	2	2	2	2	2	100	2	1	2	3	100	100	100	2	1	2
	-5	2	3	7	2	1	100	100	1	1	3	100	3	2	100	100	1	1	3	100	2	2	3	2	2	2	2	2	99	2	1	2	3	100	100	100	2	1	2
	5	2	3	9	2	1	100	100	1	1	3	100	3	2	100	100	1	1	3	100	2	2	3	2	2	2	2	2	95	2	1	2	3	100	100	100	2	1	2
	10	2	3	69	2	1	100	100	1	1	3	100	24	2	100	100	1	1	3	100	2	2	3	2	2	2	2	2	100	2	1	2	3	100	100	100	2	1	2
θ_{10}	-10	2	3	1	2	1	100	100	100	1	3	2	1	2	100	100	100	1	3	2	2	2	3	2	2	2	2	2	2	2	1	2	3	2	100	1	100	1	2
	-5	2	3	1	2	1	100	100	100	1	3	2	1	2	100	100	100	1	3	2	2	2	3	2	2	2	2	2	2	2	1	2	3	2	100	1	100	1	2
	5	2	3	1	2	1	100	100	100	1	3	2	1	2	100	100	100	1	3	2	2	2	3	2	2	2	2	2	2	2	1	2	3	2	100	1	100	1	2
	10	2	3	1	2	1	100	100	100	1	3	2	1	2	100	100	100	1	3	2	2	2	3	2	2	2	2	2	2	2	1	2	3	2	100	1	100	1	2
θ_{11}	-10	2	3	1	2	100	1	100	100	1	3	2	1	2	1	100	100	1	3	2	2	2	3	2	2	2	2	2	2	2	100	2	3	2	0	1	100	1	2
	-5	2	3	1	2	100	1	100	100	1	3	2	1	2	1	100	100	1	3	2	2	2	3	2	2	2	2	2	2	2	100	2	3	2	0	1	100	1	2
	5	2	3	1	2	100	1	100	100	1	3	2	1	2	1	100	100	1	3	2	2	2	3	2	2	2	2	2	2	2	100	2	3	2	0	1	100	1	2
	10	2	3	1	2	100	1	100	100	1	3	2	1	2	1	100	100	1	3	2	2	2	3	2	2	2	2	2	2	2	100	2	3	2	0	1	100	1	2
θ_{12}	-10	2	3	1	2	100	1	2	1	100	100	2	1	2	1	2	1	100	100	2	2	2	3	2	2	2	2	2	2	2	1	100	3	2	0	1	2	100	2
	-5	2	3	1	2	100	1	2	1	100	94	2	1	2	1	2	1	100	100	2	2	2	3	2	2	2	2	2	2	2	1	100	3	2	0	1	2	100	2
	5	2	3	1	2	100	1	2	1	100	100	2	1	2	1	2	1	100	100	2	2	2	3	2	2	2	2	2	2	2	1	100	3	2	0	1	2	100	2
	10	2	3	1	2	100	1	2	1	100	100	2	1	2	1	2	1	100	100	2	2	2	3	2	2	2	2	2	2	2	1	100	3	2	0	1	2	100	2
θ_{13}	-10	2	3	1	2	100	1	2	1	100	100	100	1	2	1	2	1	100	100	100	2	2	3	2	2	2	2	2	2	2	1	2	100	2	0	1	2	100	100
	-5	2	3	1	2	100	1	2	1	100	100	95	1	2	1	2	1	100	100	100	2	2	3	2	2	2	2	2	2	2	1	2	100	2	0	1	2	100	100
	5	2	3	1	2	100	1	2	1	100	100	97	1	2	1	2	1	100	100	100	2	2	3	2	2	2	2	2	2	2	1	2	100	2	0	1	2	100	100
	10	2	3	1	2	100	1	2	1	100	100	100	1	2	1	2	1	100	100	100	2	2	3	2	2	2	2	2	2	2	1	2	100	2	0	1	2	100	100
θ_{14}	-10	2	3	1	2	1	100	2	1	1	100	100	1	2	100	2	1	1	100	100	2	2	3	2	2	2	2	2	2	2	1	2	3	2	0	100	2	1	100
	-5	2	3	1	2	1	90	2	1	1	97	100	1	2	80	2	1	1	100	100	2	2	3	2	2	2	2	2	2	2	1	2	3	2	0	100	2	1	100
	5	2	3	1	2	1	96	2	1	1	100	100	1	2	70	2	1	1	99	100	2	2	3	2	2	2	2	2	2	2	1	2	3	2	0	100	2	1	100
	10	2	3	1	2	1	100	2	1	1	100	100	1	2	100	2	1	1	100	100	2	2	3	2	2	2	2	2	2	2	1	2	3	2	0	100	2	1	100
	NA	2	3	1	2	1	1	2	1	1	3	2	1	2	1	2	1	1	3	2	2	2	3	2	2	2	2	2	2	2	1	2	3	2	0	1	2	1	2

scenarios. However, considering the training time, using ELM is advantageous. Moreover, the ANN/ELM learning is an off-line task and is not critical for real time application. In real time application, predicting load measurements and identification of attacked meters from a trained network takes 0.192 seconds for one sample measurement set. Once the attacked meters are identified, the system operator can remove attacked meters from the state estimation provided that the system still remains observable. As we have considered the fully measured power system, removing all the identified meters will make the system unobservable. However, in the practical scenario, system operator have pseudo measurements to maintain observability of system. Otherwise, taking measures to ensure the security of the identified meters or replacing the identified meters can be a possible solution to mitigate similar future FDI attacks.

Table 7: Identification of Meters considering attack on V_i with different c (%) (ANN)

V_i	$c(\%)$	P_{inj}											Q_{inj}								P_{flow}																		
		2	3	4	5	6	9	10	11	12	13	14	4	5	9	10	11	12	13	14	1	2	3	4	5	6	7	8	9	10	11	12	13	15	16	17	18	19	20
V_1	-10	100	0	0	100	0	0	0	3	0	1	1	0	100	0	0	3	0	1	1	100	100	0	0	0	0	0	0	0	0	0	1	1	0	0	1	0	1	0
	-5	100	0	0	100	0	0	0	3	0	1	1	0	100	0	0	3	0	1	1	100	100	0	0	0	0	0	0	0	0	0	1	1	0	0	1	0	1	0
	5	100	0	0	100	0	0	0	3	0	1	1	0	100	0	0	3	0	1	1	100	100	0	0	0	0	0	0	0	0	0	1	1	0	0	1	0	1	0
	10	100	0	0	100	0	0	0	3	0	1	1	0	100	0	0	3	0	1	1	100	100	0	0	0	0	0	0	0	0	0	1	1	0	0	1	0	1	0
V_2	-10	100	99	100	100	0	0	0	3	0	1	1	100	100	0	0	3	0	1	1	100	0	100	100	100	0	0	0	0	0	0	1	1	0	0	1	0	1	0
	-5	100	1	100	100	0	0	0	3	0	1	1	100	100	0	0	3	0	1	1	100	0	83	100	100	0	0	0	0	0	0	1	1	0	0	1	0	1	0
	5	100	1	100	100	0	0	0	3	0	1	1	100	100	0	0	3	0	1	1	100	0	91	100	100	0	0	0	0	0	0	1	1	0	0	1	0	1	0
	10	100	99	100	100	0	0	0	3	0	1	1	100	100	0	0	3	0	1	1	100	0	100	100	100	0	0	0	0	0	0	1	1	0	0	1	0	1	0
V_3	-10	100	100	100	2	0	0	0	3	0	1	1	100	2	0	0	3	0	1	1	0	0	67	0	0	100	0	0	0	0	0	1	1	0	0	1	0	1	0
	-5	99	59	100	2	0	0	0	3	0	1	1	100	2	0	0	3	0	1	1	0	0	1	0	0	100	0	0	0	0	0	1	1	0	0	1	0	1	0
	5	100	77	100	2	0	0	0	3	0	1	1	100	2	0	0	3	0	1	1	0	0	2	0	0	100	0	0	0	0	0	1	1	0	0	1	0	1	0
	10	100	100	100	2	0	0	0	3	0	1	1	100	2	0	0	3	0	1	1	0	0	62	0	0	100	0	0	0	0	0	1	1	0	0	1	0	1	0
V_4	-10	100	100	100	100	0	0	0	3	0	1	1	100	100	100	0	3	0	1	1	0	0	0	100	0	100	100	100	100	0	0	1	1	0	0	1	0	1	0
	-5	100	34	100	100	0	0	0	3	0	1	1	100	100	100	0	3	0	1	1	0	0	0	100	0	100	100	2	2	0	0	1	1	0	0	1	0	1	0
	5	100	45	100	100	0	0	0	3	0	1	1	100	100	100	0	3	0	1	1	0	0	0	100	0	100	100	4	4	0	0	1	1	0	0	1	0	1	0
	10	100	100	100	100	0	0	0	3	0	1	1	100	100	100	0	3	0	1	1	0	0	0	100	0	100	100	99	99	0	0	1	1	0	0	1	0	1	0
V_5	-10	100	0	100	100	100	0	0	3	0	1	1	100	100	0	0	3	0	1	1	0	95	0	0	100	0	100	0	0	100	0	1	1	0	0	1	0	1	0
	-5	100	0	100	100	100	0	0	3	0	1	1	100	100	0	0	3	0	1	1	0	41	0	0	100	0	100	0	0	5	0	1	1	0	0	1	0	1	0
	5	100	0	100	100	100	0	0	3	0	1	1	100	100	0	0	3	0	1	1	0	30	0	0	100	0	100	0	0	12	0	1	1	0	0	1	0	1	0
	10	100	0	100	100	100	0	0	3	0	1	1	100	100	0	0	3	0	1	1	0	99	0	0	100	0	100	0	0	99	0	1	1	0	0	1	0	1	0
V_6	-10	0	0	0	100	100	0	0	100	100	100	1	0	100	0	0	100	100	100	1	0	0	0	0	0	0	0	0	0	100	100	100	100	0	0	1	0	1	0
	-5	0	0	0	100	100	0	0	100	100	100	1	0	100	0	0	100	100	100	1	0	0	0	0	0	0	0	0	0	5	100	100	100	0	0	1	0	1	0
	5	0	0	0	100	100	0	0	100	100	100	1	0	100	0	0	100	100	100	1	0	0	0	0	0	0	0	0	0	12	100	100	100	0	0	1	0	1	0
	10	0	0	0	100	100	0	0	100	100	100	1	0	100	0	0	100	100	100	1	0	0	0	0	0	0	0	0	0	99	100	100	100	0	0	1	0	1	0
V_7	-10	0	0	45	2	0	12	0	3	0	1	1	100	2	100	0	3	0	1	1	0	0	0	0	0	0	0	100	0	0	0	1	1	100	0	1	0	1	0
	-5	0	0	3	2	0	0	0	3	0	1	1	100	2	100	0	3	0	1	1	0	0	0	0	0	0	0	2	0	0	0	1	1	2	0	1	0	1	0
	5	0	0	1	2	0	0	0	3	0	1	1	100	2	100	0	3	0	1	1	0	0	0	0	0	0	0	4	0	0	0	1	1	4	0	1	0	1	0
	10	0	0	28	2	0	21	0	3	0	1	1	100	2	100	0	3	0	1	1	0	0	0	0	0	0	0	99	0	0	0	1	1	99	0	1	0	1	0
V_8	-10	0	0	0	2	0	0	0	3	0	1	1	0	2	0	0	3	0	1	1	0	0	0	0	0	0	0	0	0	0	0	1	1	0	0	1	0	1	0
	-5	0	0	0	2	0	0	0	3	0	1	1	0	2	0	0	3	0	1	1	0	0	0	0	0	0	0	0	0	0	0	1	1	0	0	1	0	1	0
	5	0	0	0	2	0	0	0	3	0	1	1	0	2	0	0	3	0	1	1	0	0	0	0	0	0	0	0	0	0	0	1	1	0	0	1	0	1	0
	10	0	0	0	2	0	0	0	3	0	1	1	0	2	0	0	3	0	1	1	0	0	0	0	0	0	0	0	0	0	0	1	1	0	0	1	0	1	0
V_9	-10	0	0	4	2	0	100	100	3	0	1	100	100	2	100	100	3	0	1	100	0	0	0	0	0	0	0	0	100	0	0	1	1	100	100	100	0	1	0
	-5	0	0	0	2	0	100	100	3	0	1	100	100	2	100	100	3	0	1	100	0	0	0	0	0	0	0	0	2	0	0	1	1	2	100	100	0	1	0
	5	0	0	0	2	0	100	100	3	0	1	100	100	2	100	100	3	0	1	100	0	0	0	0	0	0	0	0	4	0	0	1	1	4	100	100	0	1	0
	10	0	0	1	2	0	100	100	3	0	1	100	100	2	100	100	3	0	1	100	0	0	0	0	0	0	0	0	99	0	0	1	1	99	100	100	0	1	0
V_{10}	-10	0	0	0	2	0	100	100	100	0	1	1	0	2	100	100	100	0	1	1	0	0	0	0	0	0	0	0	0	0	0	1	1	0	100	1	100	1	0
	-5	0	0	0	2	0	100	100	100	0	1	1	0	2	100	100	100	0	1	1	0	0	0	0	0	0	0	0	0	0	0	1	1	0	100	1	100	1	0
	5	0	0	0	2	0	100	100	100	0	1	1	0	2	100	100	100	0	1	1	0	0	0	0	0	0	0	0	0	0	0	1	1	0	100	1	100	1	0
	10	0	0	0	2	0	100	100	100	0	1	1	0	2	100	100	100	0	1	1	0	0	0	0	0	0	0	0	0	0	0	1	1	0	100	1	100	1	0
V_{11}	-10	0	0	0	2	100	0	100	100	0	1	1	0	2	0	100	100	0	1	1	0	0	0	0	0	0	0	0	0	0	100	1	1	0	0	1	100	1	0
	-5	0	0	0	2	100	0	100	100	0	1	1	0	2	0	100	100	0	1	1	0	0	0	0	0	0	0	0	0	0	100	1	1	0	0	1	100	1	0
	5	0	0	0	2	100	0	100	100	0	1	1	0	2	0	100	100	0	1	1	0	0	0	0	0	0	0	0	0	0	100	1	1	0	0	1	100	1	0
	10	0	0	0	2	100	0	100	100	0	1	1	0	2	0	100	100	0	1	1	0	0	0	0	0	0	0	0	0	0	100	1	1	0	0	1	100	1	0
V_{12}	-10	0	0	0	2	100	0	0	3	100	100	1	0	2	0	0	3	100	100	1	0	0	0	0	0	0	0	0	0	0	0	100	1	0	0	1	0	100	0
	-5	0	0	0	2	100	0	0	3	100	100	1	0	2	0	0	3	100	100	1	0	0	0	0	0	0	0	0	0	0	0	100	1	0	0	1	0	100	0
	5	0	0	0	2	100	0	0	3	100	100	1	0	2	0	0	3	100	100	1	0	0	0	0	0	0	0	0	0	0	0	100	1	0	0	1	0	100	0
	10	0	0	0	2	100	0	0	3	100	100	1	0	2	0	0	3	100	100	1	0	0	0	0	0	0	0	0	0	0	0	100	1	0	0	1	0	100	0
V_{13}	-10	0	0	0	2	100	0	0	3	100	100	100	0	2	0	0	3	100	100	100	0	0	0	0	0	0	0	0	0	0	0	1	100	0	0	1	0	100	100
	-5	0	0	0	2	100	0	0	3	100	100	100	0	2	0	0	3	100	100	100	0	0	0	0	0	0	0	0	0	0	0	1	100	0	0	1	0	100	100
	5	0	0	0	2	100	0	0	3	100	100	100	0	2	0	0	3	100	100	100	0	0	0	0	0	0	0	0	0	0	0	1	100	0	0	1	0	100	100
	10	0	0	0	2	100	0	0	3	100	100	100	0	2	0	0	3	100	100	100	0	0	0	0	0	0	0	0	0	0	0	1	100	0	0	1	0	100	100
V_{14}	-10	0	0	0	2	0	100	0	3	0	100	100	0	2	100	0	3	0	100	100	0	0	0	0	0	0	0	0	0	0	0	1	1	0	0	100	0	1	100
	-5	0	0	0	2	0	100	0	3	0	100	100	0	2	100	0	3	0	100	100	0	0	0	0	0	0	0	0	0	0	0	1	1	0	0	100	0	1	100
	5	0	0	0	2	0	100	0	3	0	100	100	0	2	100	0	3	0	100	100	0	0	0	0	0	0	0	0	0	0	0	1	1	0	0	100	0	1	100
	10	0	0	0	2	0	100	0	3	0	100	100	0	2	100	0	3	0	100	100	0	0	0	0	0	0	0	0	0	0	0	1	1	0	0	100	0	1	100
	NA	0	0	0	2	0	0	0	3	0	1	1	0	2	0	0	3	0	1	1	0	0	0	0	0	0	0	0	0	0	0	1	1	0	0	1	0	1	0

Table 8: Identification of Meters considering attack on V_i with different c (%)(ELM)

V_i	c(%)	P_{inj}											Q_{inj}								P_{flow}																		
		2	3	4	5	6	9	10	11	12	13	14	4	5	9	10	11	12	13	14	1	2	3	4	5	6	7	8	9	10	11	12	13	15	16	17	18	19	20
V_1	-10	100	3	1	100	1	1	2	1	1	3	2	1	100	1	2	1	1	3	2	100	100	3	2	2	2	2	2	2	2	1	2	3	2	0	1	2	1	2
	-5	100	3	1	100	1	1	2	1	1	3	2	1	100	1	2	1	1	3	2	100	100	3	2	2	2	2	2	2	2	1	2	3	2	0	1	2	1	2
	5	100	3	1	100	1	1	2	1	1	3	2	1	100	1	2	1	1	3	2	100	99	3	2	2	2	2	2	2	2	1	2	3	2	0	1	2	1	2
	10	100	3	1	100	1	1	2	1	1	3	2	1	100	1	2	1	1	3	2	100	100	3	2	2	2	2	2	2	2	1	2	3	2	0	1	2	1	2
V_2	-10	100	100	100	100	1	1	2	1	1	3	2	100	100	1	2	1	1	3	2	100	2	100	100	100	2	2	2	2	2	1	2	3	2	0	1	2	1	2
	-5	100	99	100	100	1	1	2	1	1	3	2	100	100	1	2	1	1	3	2	100	2	100	100	100	2	2	2	2	2	1	2	3	2	0	1	2	1	2
	5	100	94	100	100	1	1	2	1	1	3	2	100	100	1	2	1	1	3	2	100	2	99	100	100	2	2	2	2	2	1	2	3	2	0	1	2	1	2
	10	100	100	100	100	1	1	2	1	1	3	2	100	100	1	2	1	1	3	2	100	2	100	100	100	2	2	2	2	2	1	2	3	2	0	1	2	1	2
V_3	-10	100	100	100	2	1	1	2	1	1	3	2	100	2	1	2	1	1	3	2	2	2	98	2	2	100	2	2	2	2	1	2	3	2	0	1	2	1	2
	-5	100	100	100	2	1	1	2	1	1	3	2	100	2	1	2	1	1	3	2	2	2	56	2	2	100	2	2	2	2	1	2	3	2	0	1	2	1	2
	5	100	100	100	2	1	1	2	1	1	3	2	100	2	1	2	1	1	3	2	2	2	62	2	2	100	2	2	2	2	1	2	3	2	0	1	2	1	2
	10	100	100	100	2	1	1	2	1	1	3	2	100	2	1	2	1	1	3	2	2	2	99	2	2	100	2	2	2	2	1	2	3	2	0	1	2	1	2
V_4	-10	100	100	100	100	1	6	2	1	1	3	2	100	100	100	2	1	1	3	2	2	2	3	100	2	100	100	64	64	2	1	2	3	2	0	1	2	1	2
	-5	100	100	100	100	1	2	2	1	1	3	2	100	100	100	2	1	1	3	2	2	2	3	100	2	100	100	9	9	2	1	2	3	2	0	1	2	1	2
	5	100	99	100	100	1	2	2	1	1	3	2	100	100	100	2	1	1	3	2	2	2	3	100	2	100	100	8	8	2	1	2	3	2	0	1	2	1	2
	10	100	100	100	100	1	6	2	1	1	3	2	100	100	100	2	1	1	3	2	2	2	3	100	2	100	100	53	53	2	1	2	3	2	0	1	2	1	2
V_5	-10	100	3	100	100	100	1	2	1	1	3	2	100	100	1	2	1	1	3	2	2	93	3	2	100	2	100	2	2	54	1	2	3	2	0	1	2	1	2
	-5	100	3	100	100	70	1	2	1	1	3	2	100	100	1	2	1	1	3	2	2	42	3	2	100	2	100	2	2	9	1	2	3	2	0	1	2	1	2
	5	100	3	100	100	79	1	2	1	1	3	2	100	100	1	2	1	1	3	2	2	46	3	2	100	2	100	2	2	8	1	2	3	2	0	1	2	1	2
	10	100	3	100	100	100	1	2	1	1	3	2	100	100	1	2	1	1	3	2	2	96	3	2	100	2	100	2	2	45	1	2	3	2	0	1	2	1	2
V_6	-10	2	3	1	100	100	1	2	100	100	100	2	1	100	1	2	100	100	100	2	2	2	3	2	2	2	2	2	2	54	100	100	100	2	0	1	2	1	2
	-5	2	3	1	100	100	1	2	100	100	100	2	1	100	1	2	100	100	100	2	2	2	3	2	2	2	2	2	2	9	100	100	100	2	0	1	2	1	2
	5	2	3	1	100	100	1	2	100	100	100	2	1	100	1	2	100	100	100	2	2	2	3	2	2	2	2	2	2	8	100	100	100	2	0	1	2	1	2
	10	2	3	1	100	100	1	2	100	100	100	2	1	100	1	2	100	100	100	2	2	2	3	2	2	2	2	2	2	45	100	100	100	2	0	1	2	1	2
V_7	-10	2	3	9	2	1	36	2	1	1	3	2	100	2	100	2	1	1	3	2	2	2	3	2	2	2	2	64	2	2	1	2	3	64	0	1	2	1	2
	-5	2	3	2	2	1	4	2	1	1	3	2	100	2	100	2	1	1	3	2	2	2	3	2	2	2	2	9	2	2	1	2	3	9	0	1	2	1	2
	5	2	3	3	2	1	4	2	1	1	3	2	100	2	100	2	1	1	3	2	2	2	3	2	2	2	2	8	2	2	1	2	3	8	0	1	2	1	2
	10	2	3	11	2	1	33	2	1	1	3	2	100	2	100	2	1	1	3	2	2	2	3	2	2	2	2	53	2	2	1	2	3	53	0	1	2	1	2
V_8	-10	2	3	1	2	1	1	2	1	1	3	2	1	2	1	2	1	1	3	2	2	2	3	2	2	2	2	2	2	2	1	2	3	2	0	1	2	1	2
	-5	2	3	1	2	1	1	2	1	1	3	2	1	2	1	2	1	1	3	2	2	2	3	2	2	2	2	2	2	2	1	2	3	2	0	1	2	1	2
	5	2	3	1	2	1	1	2	1	1	3	2	1	2	1	2	1	1	3	2	2	2	3	2	2	2	2	2	2	2	1	2	3	2	0	1	2	1	2
	10	2	3	1	2	1	1	2	1	1	3	2	1	2	1	2	1	1	3	2	2	2	3	2	2	2	2	2	2	2	1	2	3	2	0	1	2	1	2
V_9	-10	2	3	2	2	1	100	100	1	1	3	100	100	2	100	100	1	1	3	100	2	2	3	2	2	2	2	2	64	2	1	2	3	64	100	100	2	1	2
	-5	2	3	1	2	1	100	100	1	1	3	100	100	2	100	100	1	1	3	100	2	2	3	2	2	2	2	2	9	2	1	2	3	9	100	100	2	1	2
	5	2	3	2	2	1	100	100	1	1	3	100	100	2	100	100	1	1	3	100	2	2	3	2	2	2	2	2	8	2	1	2	3	8	100	100	2	1	2
	10	2	3	3	2	1	100	100	1	1	3	100	100	2	100	100	1	1	3	100	2	2	3	2	2	2	2	2	53	2	1	2	3	53	100	100	2	1	2
V_{10}	-10	2	3	1	2	1	100	100	100	1	3	2	1	2	100	100	100	1	3	2	2	2	3	2	2	2	2	2	2	2	1	2	3	2	100	1	100	1	2
	-5	2	3	1	2	1	100	100	100	1	3	2	1	2	100	100	100	1	3	2	2	2	3	2	2	2	2	2	2	2	1	2	3	2	100	1	100	1	2
	5	2	3	1	2	1	100	100	100	1	3	2	1	2	100	100	100	1	3	2	2	2	3	2	2	2	2	2	2	2	1	2	3	2	100	1	100	1	2
	10	2	3	1	2	1	100	100	100	1	3	2	1	2	100	100	100	1	3	2	2	2	3	2	2	2	2	2	2	2	1	2	3	2	100	1	100	1	2
V_{11}	-10	2	3	1	2	100	1	100	100	1	3	2	1	2	1	100	100	1	3	2	2	2	3	2	2	2	2	2	2	2	100	2	3	2	0	1	100	1	2
	-5	2	3	1	2	100	1	100	100	1	3	2	1	2	1	100	100	1	3	2	2	2	3	2	2	2	2	2	2	2	100	2	3	2	0	1	100	1	2
	5	2	3	1	2	100	1	100	100	1	3	2	1	2	1	100	100	1	3	2	2	2	3	2	2	2	2	2	2	2	100	2	3	2	0	1	100	1	2
	10	2	3	1	2	100	1	100	100	1	3	2	1	2	1	100	100	1	3	2	2	2	3	2	2	2	2	2	2	2	100	2	3	2	0	1	100	1	2
V_{12}	-10	2	3	1	2	100	1	2	1	100	100	2	1	2	1	2	1	100	100	2	2	2	3	2	2	2	2	2	2	2	1	100	3	2	0	1	2	100	2
	-5	2	3	1	2	100	1	2	1	100	100	2	1	2	1	2	1	100	100	2	2	2	3	2	2	2	2	2	2	2	1	100	3	2	0	1	2	100	2
	5	2	3	1	2	100	1	2	1	100	100	2	1	2	1	2	1	100	100	2	2	2	3	2	2	2	2	2	2	2	1	100	3	2	0	1	2	100	2
	10	2	3	1	2	100	1	2	1	100	100	2	1	2	1	2	1	100	100	2	2	2	3	2	2	2	2	2	2	2	1	100	3	2	0	1	2	100	2
V_{13}	-10	2	3	1	2	100	1	2	1	100	100	100	1	2	1	2	1	100	100	100	2	2	3	2	2	2	2	2	2	2	1	2	100	2	0	1	2	100	100
	-5	2	3	1	2	100	1	2	1	100	100	100	1	2	1	2	1	100	100	100	2	2	3	2	2	2	2	2	2	2	1	2	100	2	0	1	2	100	100
	5	2	3	1	2	100	1	2	1	100	100	100	1	2	1	2	1	100	100	100	2	2	3	2	2	2	2	2	2	2	1	2	100	2	0	1	2	100	100
	10	2	3	1	2	100	1	2	1	100	100	100	1	2	1	2	1	100	100	100	2	2	3	2	2	2	2	2	2	2	1	2	100	2	0	1	2	100	100
V_{14}	-10	2	3	1	2	1	100	2	1	1	100	100	1	2	100	2	1	1	100	100	2	2	3	2	2	2	2	2	2	2	1	2	3	2	0	100	2	1	100
	-5	2	3	1	2	1	100	2	1	1	100	100	1	2	100	2	1	1	100	100	2	2	3	2	2	2	2	2	2	2	1	2	3	2	0	100	2	1	100
	5	2	3	1	2	1	100	2	1	1	100	100	1	2	100	2	1	1	100	100	2	2	3	2	2	2	2	2	2	2	1	2	3	2	0	100	2	1	100
	10	2	3	1	2	1	100	2	1	1	100	100	1	2	100	2	1	1	100	100	2	2	3	2	2	2	2	2	2	2	1	2	3	2	0	100	2	1	100
	NA	2	3	1	2	1	1	2	1	1	3	2	1	2	1	2	1	1	3	2	2	2	3	2	2	2	2	2	2	2	1	2	3	2	0	1	2	1	2

5 Conclusion and Future Outlook

Protection against the malicious attacks arising due to the onset of cyber and physical interconnection of power system components is considered to be of critical importance. By only increasing the security of the meters we can increase the attack cost but cannot assure that system will always remain hack-proof. To ensure the authenticity of the measurements received by SCADA from the field sensors, it is important for the system operator to cross-check the information using the algorithms which are precisely optimised to detect a malicious data injection by the adversary. In this paper we proposed an artificial intelligence based algorithm to identify the compromised sensors in the event of cyber-intrusion. The method can detect and identify the attacks if the cumulative injected error in the state variable is greater than ±1%. However, if the attacker injects the errors within the limits of the expected load patterns, such attack may not be detected. Moreover, it is worth mentioning that injecting errors within the limits of the expected load patterns may will not cause significant change in the system states. However, one may argue, attack vector injected cumulatively over the period of time (if the meters are continuously attacked) can have a significant impact, but feasibility of such attack depends on the condition that loads, transformer taps, network topology, scheduled outages and generator schedules remains as per the prediction of the adversary for the entire duration of the attack, but such assumption is rather idealistic. Furthermore, in the event of a coordinated attack which causes instant power system stability issues, the proposed method is not applicable. Our research on detecting and alleviating attacks causing power system instability is ongoing.

References

[1] Abur A, Exposito AG. Power system state estimation: theory and implementation. CRC press; 2004.

[2] Kezunovic M. Smart fault location for smart grids. IEEE Trans on Smart Grid. 2011;2(1):11–22.

[3] Ashok A, Hahn A, Govindarasu M. Cyber-physical security of Wide-Area Monitoring, Protection and Control in a smart grid environment. J Adv Res. 2014;5(4):481 – 489.

[4] Schweppe FC. Power System Static-State Estimation, Part III: Implementation. IEEE Trans on Power Apparatus and Systs. 1970 Jan;PAS-89(1):130–135.

[5] Liang G, Zhao J, Luo F, Weller S, Dong ZY. A Review of False Data Injection Attacks Against Modern Power Systems. IEEE Trans on Smart Grid. 2016;PP(99):1–1.

[6] Liu Y, Ning P, Reiter MK. False data injection attacks against state estimation in electric power grids. ACM Trans on Information and System Security. 2011;14(1):13.

[7] Liu X, Li Z. Local load redistribution attacks in power systems with incomplete network information. IEEE Trans on Smart Grid. 2014;5(4):1665–1676.

[8] Yuan Y, Li Z, Ren K. Modeling load redistribution attacks in power systems. IEEE Trans on Smart Grid. 2011;2(2):382–390.

[9] Yuan Y, Li Z, Ren K. Quantitative Analysis of Load Redistribution Attacks in Power Systems. IEEE Trans Parallel Distrib Syst. 2012 Sept;23(9):1731–1738.

[10] Khanna K, Panigrahi BK, Joshi A. Bi-level Modelling of False Data Injection Attacks on Security Constrained Optimal Power Flow. IET Gener Transm Distrib. 2017;PP:1–8.

[11] Kim J, Tong L. On Topology Attack of a Smart Grid: Undetectable Attacks and Countermeasures. IEEE J Sel Areas Commun. 2013 July;31(7):1294–1305.

[12] Khanna K, Panigrahi BK, Joshi A. Data integrity attack in smart grid: optimised attack to gain momentary economic profit. IET Gener Transm Distrib. 2016;10(16):4032–4039.

[13] Xie L, Mo Y, Sinopoli B. Integrity Data Attacks in Power Market Operations. IEEE Trans on Smart Grid. 2011 Dec;2(4):659–666.

[14] Bobba RB, Rogers KM, Wang Q, Khurana H, Nahrstedt K, Overbye TJ. Detecting false data injection attacks on dc state estimation. In: Preprints of the First Workshop on Secure Control Systems, CPSWEEK. vol. 2010; 2010. .

[15] Kim TT, Poor HV. Strategic Protection Against Data Injection Attacks on Power Grids. IEEE Trans on Smart Grid. 2011 June;2(2):326–333.

[16] Li S, Ylmaz Y, Wang X. Quickest Detection of False Data Injection Attack in Wide-Area Smart Grids. IEEE Trans on Smart Grid. 2015 Nov;6(6):2725–2735.

[17] Liu X, Zhu P, Zhang Y, Chen K. A Collaborative Intrusion Detection Mechanism Against False Data Injection Attack in Advanced Metering Infrastructure. IEEE Trans on Smart Grid. 2015 Sept;6(5):2435–2443.

[18] Liu L, Esmalifalak M, Ding Q, Emesih VA, Han Z. Detecting False Data Injection Attacks on Power Grid by Sparse Optimization. IEEE Trans on Smart Grid. 2014 March;5(2):612–621.

[19] Chaojun G, Jirutitijaroen P, Motani M. Detecting False Data Injection Attacks in AC State Estimation. IEEE Trans on Smart Grid. 2015 Sept;6(5):2476–2483.

[20] Singh SK, Khanna K, Bose R, Panigrahi BK, Joshi A. Joint Transformation based Detection of False Data Injection Attacks in Smart Grid. IEEE Transactions on Industrial Informatics. 2017;PP(99):1–1.

[21] Khanna K, Panigrahi BK, Joshi A. Feasibility and mitigation of false data injection attacks in smart grid. In: 2016 IEEE 6th International Conference on Power Systems (ICPS); 2016. p. 1–6.

[22] Huang GB, Zhu QY, Siew CK. Extreme learning machine: theory and applications. Neurocomputing. 2006;70(1):489–501.

[23] Load Data: Market and Operational Data (NYISO);. Available from: `http://www.nyiso.com/public/markets_operations/index.jsp`.