Intrusion Detection in Cyber-physical Layer of Smart Grid using Intelligent Loop Based Artificial Neural Network Technique

P. K. Gupta, N. K. Singh, V. Mahajan*

Electrical Engineering Department, Sardar Vallabhbhai National Institute of Technology, Surat, Gujarat-India

**Paper Info**

**Abstract**

This paper, proposes an Intelligent Loop Based Artificial Neural Network (ILANN) based detection technique for the detection of cyber intrusion in a smart grid against False Data Injection Attack (FDIA). This method compares the deviation of a system with the equipment load profile present on the system node(s) and any deviation from predefined values generates an alarm. Every 2 milliseconds (ms) the data obtained by the measurement is passed through the attack detection system, in case if the deviation is continuously for 5 measurement cycles i.e. for 10 ms and it does not match with the load combination the operator will get the first alert alarm. In case the deviation is not fixed after 8 measurement cycles then the system alerts the control centre. FDI attack is used by attackers to affect the healthy operation of the smart grid. Using FDI the hackers can permanently damage many power system’s equipment’s which may lead to higher fixing costs. The result and analysis of the proposed cyber detection approach helps operator and control centre to identify cyber intrusion in the smart grid scenario. The method is used to detect a cyberattack on IEEE-9 Bus test system using MATLAB software.

**Keywords:** Intelligent Loop Based Artificial Neural Network Technique; False Data Injection Attack; Modern Power System; Cybersecurity

**Introduction**

The smart grid is an intelligent and complex system designed to work more efficiently, reliable, and economical with the help of computational technologies, advanced communication infrastructure, and state-of-the-art monitoring stations [1, 2]. This goal is achieved by continuous monitoring of power consumption, which leads to large data exchange of information giving opportunity for various cyber intrusion [3]. The main target of ICT is to gather equipment’s data, process and transfer to control/monitoring station for proper operation. Integrating with ICT, power grid performance gets enhanced in the following terms (but not limited to):

- Fault detection and analysis
  - With a large number of communication sensors deployed in the smart grid has made cybersecurity a critical challenge for engineers [4]. Thus, ensuring security is imperative for smart grid infrastructure [5]. Although enormous research has been published, such as intrusion detection using the weight trust method, using advance cryptographic, and Intrusion Detection Techniques (IDT), despite different countermeasures smart grid still remain vulnerable to different intrusions [6-9].
  - To prevent intrusion, the smart grid confides on classical security strategy which includes firewall and password protection. Intrusion detection Mechanism (IDM) is capable to generate alarms for viable intrusions via constantly monitoring operations [10, 11]. Although there are several research on well-known IDS in system safety, limited effort has been made especially to the smart grid [12, 13]. Generally, two types of IDM system is used named as: data sourced based and detection based

*Corresponding Author Institutional Email: vmahajan@eed.svnit.ac.in

(V. Mahajan)
method. The majority of industries preferred the detection-based type because of its accuracy and simplicity [14, 15]. This simplicity attracts intruders to perform stealth attacks. The attackers may induce false data which may confuse the operator in their decision making which leads to economic loss [16]. Manandhar et al. [11] have done an extensive investigation of different false data injection attacks. Recently, the method of FDIA has been attracting the attention of engineers and researchers. The FDIA impacts the state estimation by manipulating data [17-19]. In some cases the true digital value of instruments at substation and control centre due to which false operation may occur like the false operation of breakers. In general FDIA targets analog measurement from the power system mainly bus voltage, bus power injection and digital data of switches and breakers [20, 21].

In this paper, a neural network is modelled which continuously monitors the grid energy consumption. Energy consumption totally depends on the load attached to the system, so the proposed technique identifies the equipment connected in the system through intelligent feedback. Each equipment has its own power rating, accordingly the system estimate the combination of equipment contributing as load. In case if the load variation matches with the equipment on/off status means no intrusion and the system is working properly, otherwise the system is under fault condition or under the cyber-attack scenario. The main contributions of this paper are three-fold:

1. The proposed model is so effective that it can identify the stealth FDIA, which may easily pass through other Intrusion Detection Techniques (IDT).
2. In the case of a non-stealth attack if the power deviation is for more than 8 cycles then the operator gets an unhealthy alarm.
3. The load combination results can be used for energy management/load shedding during unhealthy operations.

2. SYSTEM MODELLING AND DESCRIPTION

2.1. Attack Strategy

In the power system, bus voltage and its corresponding phase angle are used to represent the state with magnitude $V \in \mathbb{R}^n$ and angle $\delta \in [-\pi, \pi]$, where $n$ is the number of buses. Let $x$ is the state vector represented by the equation:

$$x = [V^a \delta^a V^b \delta^b V^c \delta^c]^T$$

where $a, b, c$ represents three-phase. For a given power system the measurement vectors are stated as:

$$V^p = [V_1^p \quad V_2^p \quad \ldots \ldots \quad V_n^p]^T$$

$$\delta^p = [\delta_1^p \quad \delta_2^p \quad \ldots \quad \delta_n^p]^T$$

Using state estimation for the $n$-bus system, there will be $3n$ states for voltage magnitude and $(3(n-1))$ states for angle magnitude. The total states for any given system are determined by $(3(2n-1))$. To monitor the buses three types of measurements are considered: injected power, voltage magnitude and reactive power injection. The measurement vector $M$ is given by the equation:

$$M = [P \ V \ Q]^T$$

where, $P, V, Q$ are

$$P = [p_1^a \quad p_1^b \quad p_1^c]^T$$

$$V = [v_1^a \quad v_1^b \quad v_1^c]^T$$

$$Q = [q_1^a \quad q_1^b \quad q_1^c]^T$$

In Equation (5) $\varphi$ denotes a set of nodes with power measurement and $\psi$ is the set of nodes with voltage measurement. A simple relation between different elements in the measurements can be written as:

$$M = h(x) + \sigma$$

where $h(\cdot)$, represent functions relating measurements with states and $\sigma$ indicates noise present in the system. The relation for the active and reactive power measurement at the bus may be given in terms of states as follow:

$$p_i^a = \sum_{j=1}^{n} \sum_{r=1}^{m} \left( v_i^a v_j^a \cos(\delta_i^a - \delta_j^a - \phi_i^a) - v_i^b v_j^b \cos(\delta_i^b - \delta_j^b - \phi_i^b) \right)$$

$$q_i^a = \sum_{j=1}^{n} \sum_{r=1}^{m} \left( v_i^a v_j^a \sin(\delta_i^a - \delta_j^a - \phi_i^a) - v_i^b v_j^b \sin(\delta_i^b - \delta_j^b - \phi_i^b) \right)$$

For each bus, power injection is present in polar form, where $Y$ represents admittance and $\phi$ represents the corresponding admittance angle. The error deviation in the states can be calculate using the weight means square:

$$r = z - h(\cdot)$$

$$E = r^T Wr$$

In Equations (11) and (12) $r$ represent a residual vector, $E$ is the objective function, and $W$ is the measurement weight matrix. The error and the noise can be modelled as:

$$x_k = x_{k-1} + \Delta x_{k-1}$$

$$\Delta x_{k-1} = (G)^{-1} H^T W r_{k-1}$$
where \( H \) is the Jacobian Matrix of \( h(\cdot) \). The residual vector is used to update the state’s directions. The outlier of the residual vector a scalar function whose value should be below the threshold, otherwise the system contains false data. Many machine learning approaches can sense non-possible states solutions using physical relationships such as Kirchhoff’s Current Law (KCL) and Kirchhoff’s Voltage Law (KVL). Thus to make the FDIA more stealthy, the injected false data in this paper follows KCL and KCL in the region of attack. For constructing a stealth attack vector the initial states variable is considered as:

\[
\mathbf{V} = \begin{bmatrix} V_o \\ \delta_o \end{bmatrix}
\]

Now determine if the constraints are satisfied. In case there is some mismatch the go to the next step by checking the limits of the constraints:

\[
P_{\text{max}} \leq P \leq P_{\text{max}}
\]

(17)

\[
Q_{\text{max}} \leq Q \leq Q_{\text{max}}
\]

(18)

The attacker must control and inject the power flow to minimize the detection of power mismatch. The load pattern is maintained by updating the state variables.

\[
\mathbf{V} = \begin{bmatrix} V_o \\ \delta_o \end{bmatrix} + \Delta \mathbf{V}
\]

(19)

Using the above equations attackers can easily able to inject stealth FDIA into the power system. In the next section, the Intelligent Loop Based Artificial Neural Network (ILANN) for false data detection is presented.

2. 2. ILANN System Modelling

In this section, an overview of the proposed technique for detecting false data injection is shown in Figure 1. The proposed technique mainly consists of two Artificial Neural Network Stage (ANNS) and a loop that compares the test results with the real-time scenario data. The ANNS consists of two neural networks such that the output of ANNS1 is acting as input for ANNS2. For the ANNS-1, voltages (Input-I1) and current (Input-I2) measurements are used to estimate the bus output (Output-O1) i.e power delivery through the corresponding bus. The output of ANNS-1 acts as the first input of ANNS-2. The other input (Input-I3) for ANNS-2 consists of different load details connected to particular buses.

According to the power consumption the load pattern is estimated which is compared with the actual reading of the system using the loop associate with the ANN system. As stealth FDIA has no fixed pattern and can be injected at any time to make the system unhealthy. For training neurons, estimation is performed for different conditions with and without FDIA. In the first stage of ANN, the residual vector is saved. Using this vector the power deviation is monitored, and error \( (e) \) is estimated for different conditions with and without FDIA. In the first stage of ANN the residual vector is saved. Using this vector the power deviation is monitored, and error \( (e) \) is estimated.

\[
e \rightarrow r \rightarrow \Delta P
\]

(20)

Two different approach for intrusion detection process are a mismatch in overall power and mismatch in power consumed by indivual equipment (Load). The second approach is more appropriate for stealth FDIA. This is because during normal fault the overall power mismatch occurs which may lead to wrong interpretation. So the main characteristic of the ILANN model is, it uses individual load consumption data to predict the cyber intrusion due to FDIA. The change in load combination is given by:

\[
\Delta P \rightarrow \text{Change in load combination}
\]

(21)

\[
\Delta P \rightarrow \sum_{b=1,..,a} L_{b_m}
\]

(22)

where \( b \) denotes bus number and \( m \) denotes load number. The exchange of power to different loads must be satisfied and the load must respond accordingly.

\[P_e = \sum_{b=1,..,a} L_{b_m} \in \{\text{Actual equipment connected}\}
\]

(23)

Through the feedback loop, the bus load combination is compared with the control centre load status.

\[P \rightarrow \sum_{b=1,..,a} L_{b_m} = \text{Status of individual loads}
\]

(24)

Figure 2 shows the flow chart of the proposed technique. In the first step, the ANNS-1 gets input details which include voltage and current associated with each bus. Also, the second input consists of historical past data accomplice with each bus. In the next stage, the power deviation for each bus is calculated. With the help of ANNS-2, the ILANN predict the possible combination of active load connected to each load bus.

This load combination is rechecked with the control centre through the feedback loop. Through control centre status of the individual load is acquired and compare with the predicted equipment status. If both are the same with high accuracy means the system is healthy otherwise the presence of the wrong status data. The wrong status is due to malicious information put by the attackers after getting the system access. The % power error \( (P_e) \) of the system is measured using the formula:

\[
P_e = \frac{A_k - P_{i_k}}{P_{i_k}} \times 100
\]

(25)

where \( A_k \) is the actual power consumed by the load combination and \( P_{i_k} \) is predicted power computation by load combination during the cyber intrusion. The
equipment identification accuracy ($A_e$) is measured using the formula:

$$A_e = \frac{T_{on} + T_{off}}{T_{on} + T_{off} + F_{on} + F_{off}} \times 100$$

(26)

where $T_{on}$ means the number of time load is correctly classified as on; $T_{off}$ means the number of time load is correctly classified as off; $F_{on}$ indicates the number of time load is incorrectly classified as on; $F_{off}$ inverse of $T_{off}$. In similar manner sensitivity ($S$) and precision ($P_{rec}$) can be evaluated as:

$$S = \frac{T_{on}}{T_{on} + F_{off}} \times 100$$

(27)

$$P_{rec} = \frac{T_{on}}{T_{on} + F_{off}} \times 100$$

(28)

In case of a non-stealth attack, the power deviation will be monitored and if it crosses the threshold value of the time limit the operator will get an alarm. To evaluate the proposed model ability to recognize attack, recall/detection rate ($R$) is calculated using the equation given below:

$$R = \frac{T_{on}}{T_{on} + F_{off}} \times 100$$

(29)

Using Equations (27) and (28) F-measure ($F$) is defined as:

$$F = \frac{2 \times R \times P_{rec}}{R + P_{rec}} \times 100$$

(30)

F-measure highlights the performance of the system during the cyber intrusion.

3. SIMULATION RESULTS AND DISCUSSION

3.1 Evaluation of Proposed Technique

Stealth false data attack is one of the most severe attacks on the power system. The IEEE-9 bus test system is used to examine the proposed method. To investigate the method, some details are discussed. Each load bus is connected with more than 2 loads. The details of the load on different buses are given in Table 1. To check the accuracy of the proposed method four cases are considered as follow:

1. **Case 1:** No FDIA
2. **Case 2:** Stealth FDIA on bus no. 6 and 8
3. **Case 3:** Stealth FDIA on all the load bus
4. **Case 4:** Non-stealth FDIA on all the buses

To train and test the proposed technique, a dataset of historical data is provided. As, mentioned residual error,

| Bus No. | Actual Load Attached (MW) | Load Details (MW) |
|---------|----------------------------|-------------------|
| 5       | 1.2                        | $L_{o1} = 0.5$    |
| 5       | 1.2                        | $L_{o2} = 0.3$    |
| 6       | 5                          | $L_{o2} = 2$      |
| 6       | 5                          | $L_{o2} = 2.5$    |
| 8       | 10                         | $L_{o2} = 4$      |
| 8       | 10                         | $L_{o2} = 3$      |
state variables and state estimation are computed by using load profile and generation units. Figures 3-6 depict the performance of the proposed method with 30 Neurons each for ANNS1 and ANNS2. The mean square error shown in the figure indicates the value predicted by the model is very close to the actual observed values. During the training phase, the active and reactive power consumption of the individual load is recorded and saved. Figure 3, as indicated by the training best epoch, shows the best results at 1000. The training, testing and validation of data are very accurate as shown in Figure 4. Figure 5 shows the error histogram with 70% data used for training, 15% is used to validate and the remaining 15% used for a completely independent test. Table 2 highlights the detection time for stealth/non-stealth FDIA. The prediction of load combination by ILANN is given in Table 3. It can be observed that for cases 2, 3 and 4 the on/off status of ILANN is not matching with control centre status. So it can be concluded that in the above-said cases the system is under FDIA. The sensitivity, precision and accuracy of the proposed ILANN technique are shown in Figure 6 for each load.

In case 1 detection time is not applicable although the change in system parameter was detected at a period of 5.32 s. A very little deviation in ILANN prediction is due to small loads. Its accuracy may increase with a loads with a large difference in its’s capacity.

![Figure 3](image3)  Mean square error of the proposed modelled

![Figure 4](image4)  Validation of historical data

![Figure 5](image5)  Error histogram

![Figure 6](image6)  Sensitivity, precision and accuracy of proposed ILANN technique for individual loads

### Table 1. Simulation result for different cases

| Case No. | $A_s$ (MW) | $P_s$ (MW) | $P_r$ (%) | Detection time of FDIA (Sec) |
|----------|------------|------------|-----------|-----------------------------|
| 1        | 16.2       | 15.2       | 6.17      | NA                          |
| 2        | 13.2       | 12.5       | 5.30      | 3.64                        |
| 3        | 13.4       | 12.9       | 3.73      | 3.87                        |
| 4        | 12.5       | 11.4       | 8.8       | 9.12                        |

### Table 2. ILANN prediction

| Case No. | $A_s$ (MW) | $P_s$ (MW) | Status of Load at control centre | ILANN Load Prediction |
|----------|------------|------------|---------------------------------|-----------------------|
| 1        | 16.2       | 15.2       | $L_{on}$ is off                 | $L_{off}$ is off       |
| 2        | 13.2       | 12.5       | $L_{off}$, $L_{on}$ is off      | $L_{off}$, $L_{on}$, $L_{on}$, $L_{off}$ is off |
| 3        | 13.4       | 12.9       | $L_{off}$, $L_{on}$, $L_{on}$, $L_{off}$ is off | $L_{off}$, $L_{on}$, $L_{on}$, $L_{off}$ is off |
| 4        | 12.5       | 11.4       | $L_{off}$, $L_{on}$, $L_{on}$, $L_{off}$ is off | $L_{off}$, $L_{on}$, $L_{on}$, $L_{off}$ is off |

From Table 2 it is clear that nodes having more load connection required a little more time to detect FDIA. The performance metrics $R$ and $F$ of ILANN are shown in Figure 7. It can be observed that the range is between 80-95%, indicating desired performance.
3.2. Comparison With Existing Technique

This section compares the ILANN technique with a few existing techniques stated in Table 4. All the comparison is based on the data/sample used by the system during the detection process. Overall, the accuracy of system is around 97% (for multiple load combination its 76%) making it efficient and accurate. Comparing with detection rate and false alarm rate, the ILANN prove to be the most trusted method as shown in Figure 8.

**Figure 7.** Recall and F-measure for different load using ILANN

**Table 3.** Comparison of ILANN with existing techniques

| Method                        | Parameter                      | Accuracy (%) |
|-------------------------------|--------------------------------|--------------|
| Single Sensor Score (SSS) [22] | Sensor data streams            | 3.2          |
| Deep Neural Network (DNN) [23] | Data samples                   | 70           |
| Support Vector Machine (SVM) [22, 24] | Data samples                 | 45-60        |
| Back Propagation Neural Network (BPNN) [25] | Sensor data streams      | 82           |
| Stacking-Bagging Ensemble (SBE) [26] | System data                  | 60           |
| k-RNN and OCSVM [27]          | Sample data from sensors      | 60.61        |
| Fuzzy C-Means Clustering (FCC) [28] [29] | Sample data                  | 75           |
| Proposed ILANN                | Node and load data sample     | 97           |

**Figure 8.** Comparison for detection rate and false alarm rate

4. CONCLUSION

The artificial neural network provides several advantages in the detection of FDIA. In this paper, ILANN is introduced using the concept of ANN to detect stealth/non-stealth false injection attacks. The proposed method is implemented in the IEEE-9 bus system with the help of MATLAB software. After having prepared enough historical information for the power system an ILANN is developed to train, test, and update the system for intrusion detection. The feedback comparison gives better results with a low chance of failure. The ability of ILANN is tested to predict the status of load which can be compared with the actual status and deviation can be noted. This deviation can be due to load change or due to cyber intrusion. From the results, the overall performance of the system is high with 97% of accuracy.

The simulation result shows the sensitivity, precision, and accuracy of the proposed method for load detection is high. It can be implemented on large-scale power systems to train individual subsections for monitoring against FDIA.

5. REFERENCES

1. Mansouri, H.R., Mozafari, B., Soleymani, S. and Mohammadnejad, H., "A new optimal distributed strategy to mitigate the phase imbalance in smart grids", *International Journal of Engineering*, Vol. 33, No. 12, (2020), 2489-2495. DOI: 10.5829/ije.2020.33.12.08.

2. Singh, N.K. and Mahajan, V., "Analysis and evaluation of cyber-attack impact on critical power system infrastructure", *Smart Science*, (2021), 1-13. DOI: 10.1080/23080477.2020.1861502

3. Sunitha, R. and Chandrikab, J., "Evolutionary computing assisted wireless sensor network mining for qos-centric and energy-efficient routing protocol", *International Journal of Engineering*, Vol. 33, No. 5, (2020), 791-797. DOI: 10.5829/ije.2020.33.05.10.

4. Wang, W. and Lu, Z., "Cyber security in the smart grid: Survey and challenges", *Computer Networks*, Vol. 57, No. 5, (2013), 1344-1371. DOI: 10.1016/j.comnet.2012.12.017

5. Sou, K.C., Sandberg, H. and Johansson, K.H., "On the exact solution to a smart grid cyber-security analysis problem", *IEEE Transactions on Smart Grid*, Vol. 4, No. 2, (2013), 856-865. DOI: 10.1109/TSG.2012.2230199

6. Alfantookh, A.A., "Dos attacks intelligent detection using neural networks", *Journal of King Saud University-Computer and Information Sciences*, Vol. 18, (2006), 31-51. DOI: 10.1016/S1319-1578(06)80002-9

7. Kwon, Y., Kim, H.K., Lim, Y.H. and Lim, J.L., "A behavior-based intrusion detection technique for smart grid infrastructure", in 2015 IEEE Eindhoven PowerTech, IEEE. 1-6. DOI: 10.1109/PTC.2015.7232339

8. Zhang, J., Ai, Z., Guo, L. and Cui, X., "Reliability evaluation of a disaster airflow emergency control system based on bayesian networks", *International Journal of Engineering*, Vol. 33, No. 11, (2020), 2416-2424. DOI: 10.5829/ije.2020.33.11.32.

9. Singh, N.K., Gupta, P.K. and Mahajan, V., "Intrusion detection in wireless network of smart grid using intelligent trust-weight method", *Smart Science*, Vol. 8, No. 3, (2020), 152-162. DOI: 10.1080/23080477.2020.1805679
چکیده

در این مقاله، یک روش تشخیص فنود سایبری در یک شبکه هوشمند در بر اثر حمله تریک داده (ILANN) برای تشخیص فنود سایبری در یک شبکه هوشمند در بر اثر حمله تریک داده (FDIA) و نفوذ سایبری در شبکه هوشمند نیز ارائه می‌شود. به طور کلی، این روش بر اساس مدل‌سازی بر اساس فکری و سیستم‌های هوشمند مبتنی بر الگوریتم فشرده سازی (ICA) و سیستم‌های هوشمند مبتنی بر الگوریتم فشرده سازی (ICA) است. این روش جهت تشخیص حمله‌های سایبری در شبکه هوشمند می‌تواند به عنوان یک روش با کیفیت و بهینه‌سازی سیستم‌های هوشمند معمول در شبکه‌های هوشمند کاربردی باشد.