International Journal of Engineering

Journal Homepage: www.ije.ir

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

P A P E R I N F O

Paper history:
Received 26 July 2020
Received 28 Februray 2021
Accepted 03 March 2021

Keywords:
Intelligent Loop Based
Artificial Neural Network
False Data Injection Attack
Smart Grid
Cyber-physical

A B S T R A C T

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 equipment's which may lead to higher fixing costs. The result and analysis of the proposed cyber detection approach help 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.

***doi**: 10.5829/ije.2021.34.05b.18*

1. 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):

- Real time monitoring
- Peak load estimation
- Forecasting
- Fast response
- Power factor improvement
- 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)

Please cite this article as: P. K. Gupta, N. K. Singh, V. Mahajan, Intrusion Detection in Cyber-physical Layer of Smart Grid using Intelligent Loop Based Artificial Neural Network Technique, International Journal of Engineering, Transactions B: Applications Vol. 34, No. 05, (2021) 1250-1259

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 loop 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 $V \in R^n$ and angle $\delta\epsilon[-\pi.\pi]^n$, where n is the number of buses. Let x is the state vector represented by the equation:

$$x = [V^a \ \delta^a \ V^b \ \delta^b \ V^c \ \delta^c]^T \tag{1}$$

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

$$V^P = [V_1^P \ V_2^P \ ....V_n^P \ ]^T \tag{2}$$

$$\delta^P = [\delta_1^P \ \delta_2^P \ ....\delta_n^P \ ]^T \tag{3}$$

Using state estimation for the n-bus system, there will be $3n$ states for voltage magnitude and $3(n\text{-}1)$ states for angle magnitude. The total states for any given system are determined by $3(2n\text{-}1)$. 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:

$$M = [P \ V \ Q]^T \tag{4}$$

where, P, V, Q are

$$P = [\,p_i^a \ \ p_i^b \ \ p_i^c \ ]^T \ \forall_i \ \in \{\varphi\} \tag{5}$$

$$V = [v_i^a \ \ v_i^b \ \ v_i^c \ ]^T \ \forall_i \ \in \{\psi\} \tag{6}$$

$$Q = [q_i^a \ \ q_i^b \ \ q_i^c \ ]^T \ \forall_i \ \in \{\varphi\} \tag{7}$$

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

$$M = h(x) + \varpi \tag{8}$$

where h *()*, represent functions relating measurements with states and ϖ 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:

$$p_i^p = \sum_{\substack{j=1 \\ j \neq i}}^{n} \sum\nolimits_{t=a\,b\,c} \begin{pmatrix} v_i^p Y_{ij}^{pt} v_i^t \cos(\ \delta_i^p - \delta_i^t - \phi_{ij}^{pt}\ ) \\ -\, v_i^p Y_{ij}^{pt} v_i^t \cos(\ \delta_i^p - \delta_i^t - \phi_{ij}^{pt}\ ) \end{pmatrix} \tag{9}$$

$$q_i^p = \sum_{\substack{j=1 \\ j \neq i}}^{n} \sum\nolimits_{t=a\,b\,c} \begin{pmatrix} v_i^p Y_{ij}^{pt} v_i^t \sin(\ \delta_i^p - \delta_i^t - \phi_{ij}^{pt}\ ) \\ -\, v_i^p Y_{ij}^{pt} v_i^t \sin(\ \delta_i^p - \delta_i^t - \phi_{ij}^{pt}\ ) \end{pmatrix} \tag{10}$$

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

$$r = z - h(.) \tag{11}$$

$$E = r^T W r \tag{12}$$

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:

$$x_k = x_{k-1} + \Delta x_{k-1} \tag{13}$$

$$\Delta x_{k-1} = (G)^{-1} H^T W r_{k-1} \tag{14}$$

$$G=H^TWH \tag{15}$$

where *H* is the Jacobian Matrix of *h(.)*. The residual vector is used to update the state's directions. The outliner 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:

$$\begin{bmatrix} V \\ \delta \end{bmatrix} = \begin{bmatrix} V_o \\ \delta_o \end{bmatrix} \tag{16}$$

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:

$$P_{\min} \le P \le P_{\max} \tag{17}$$

$$Q_{\min} \le Q \le Q_{\max} \tag{18}$$

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.

$$\begin{bmatrix} V \\ \delta \end{bmatrix} = \begin{bmatrix} V_o \\ \delta_o \end{bmatrix} + \begin{bmatrix} \Delta v \\ \Delta \delta \end{bmatrix} \tag{19}$$

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 tested 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 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.

$$e \to r \to \Delta P \tag{20}$$

Two different approach for intrusion detection process are a mismatch in overall power and mismatch in power consumed by induvial 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:

$$\Delta P \to Change\ in\ load\ combination \tag{21}$$

$$\Delta P \to \sum_{b=1\dots n}^{m=1..z} L_{bm} \tag{22}$$

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.

$$P_b = \sum_{b=1\dots n}^{m=1..z} L_{bm} \in \{Actual\ equipment\ connected\} \tag{23}$$

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

$$P \to \sum_{b=1\dots n}^{m=1..z} L_{bm} = Status\ of\ individual\ loads \tag{24}$$

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_a)* of the system is measured using the formula:

$$P_a = \frac{A_{lc} - P_{lc}}{P_{lc}} \times 100 \tag{25}$$

where A_{lc} is the actual power consumed by the load combination and P_{lc} is predicted power computation by load combination during the cyber intrusion. The

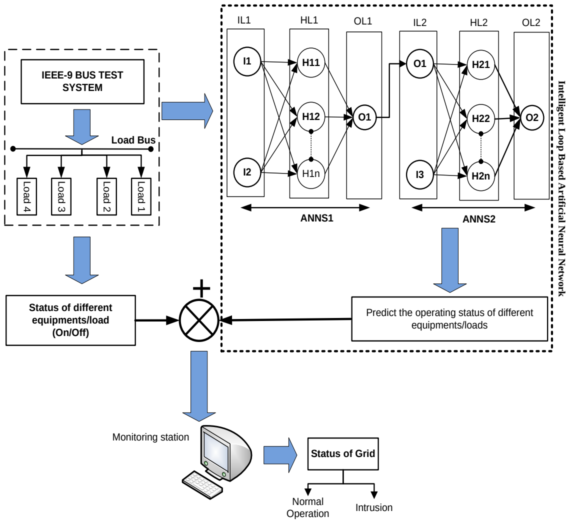

Figure 1. Basic diagram of proposed technique

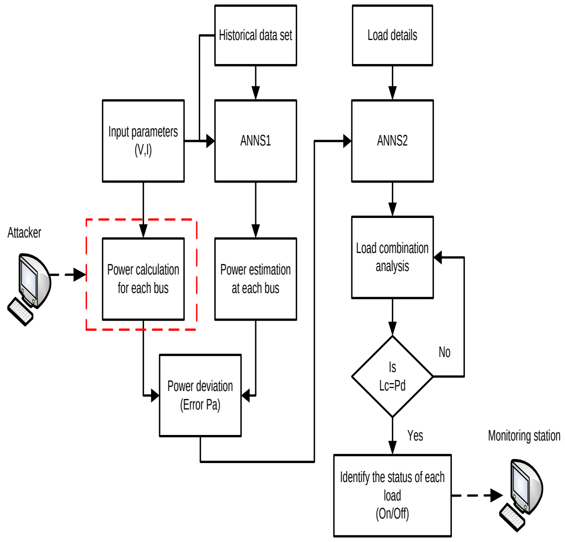
Historical data set
Load details
Input parameters (V,I)
ANNS1
ANNS2
Attacker
Power calculation for each bus
Power estimation at each bus
Load combination analysis
No
Is Lc=Pd
Power deviation (Error Pa)
Yes
Monitoring station
Identify the status of each load (On/Off)

Figure 2. Flow chart for load identification

equipment identification accuracy *(A_S)* is measured using the formula:

$$A_s = \frac{T_{on} + T_{off}}{T_{on} + T_{off} + F_{on} + F_{off}} \times 100 \qquad (26)$$

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:

$$S = \frac{T_{on}}{T_{on} + F_{off}} \times 100 \qquad (27)$$

$$P_{rec} = \frac{T_{on}}{T_{on} + F_{on}} \times 100 \qquad (28)$$

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:

$$R = \frac{T_{on}}{T_{on} + F_{off}} \times 100 \qquad (29)$$

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

$$F = \frac{2 \times R \times P_{rec}}{R + P_{rec}} \times 100 \qquad (30)$$

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

3. SIMULATION RESULTS AND DISCUSSION

3. 1. Evaluation of Proposed Technqiue

Stealth false data attack is one of the most severe attacks om 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,

TABLE 1. Load details

Bus No.	Actual Load Attached (MW)	Load Details (MW)
5	1.2	L_{51} = 0.5
		L_{52} = 0.3
		L_{53} = 0.4
6	5	L_{61} = 1.5
		L_{62} =2.5
		L_{63} =2
8	10	L_{81} =2
		L_{82} =3
		L_{83} =4
		L_{84} =1

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 reaming 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.

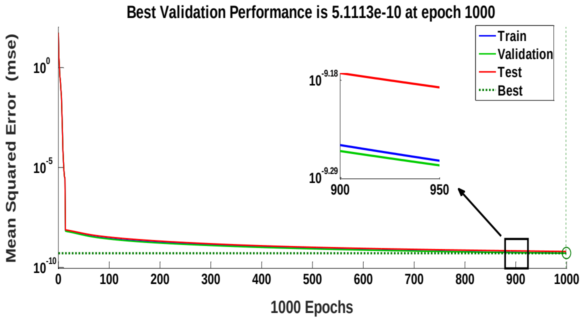

Figure 3. Mean square error of the proposed modelled

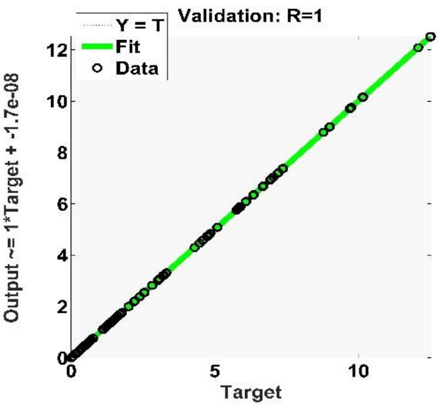

Figure 4. Validation of historical data

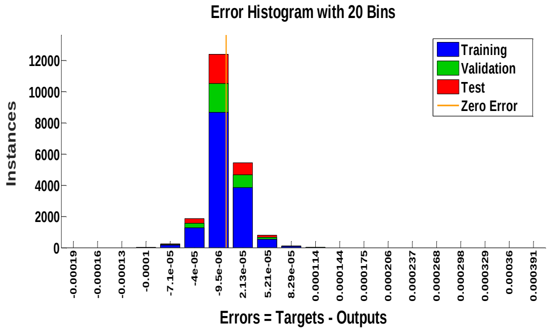

Figure 5. Error histogram

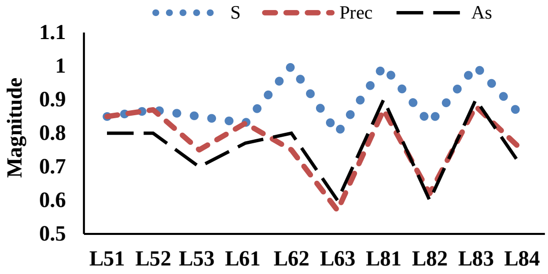

Figure 6. Sensitivity, precision and accuracy of proposed ILANN technique for individual loads

TABLE 1. Simulation result for different cases

Case No.	A_{lc} (MW)	P_{lc} (MW)	P_a (%)	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_{lc} (MW)	P_{lc} (MW)	Status of Load at control centre	ILANN Load prediction
1	16.2	15.2	L_{84} is off	L_{84} is off
2	13.2	12.5	L_{63}, L_{81} is off	L_{52}, L_{53}, L_{63}, L_{81} is off
3	13.4	12.9	L_{51}, L_{52}, L_{63}, L_{84} is off	L_{52}, L_{63}, L_{81} is off
4	12.5	11.4	L_{52}, L_{53}, L_{61}, L_{62} is off	L_{51}, L_{52}, L_{61}, L_{62}, L_{84} 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.

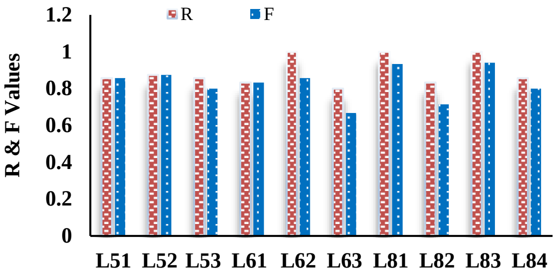

Figure 7. Recall and F-measure for different load using ILANN

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

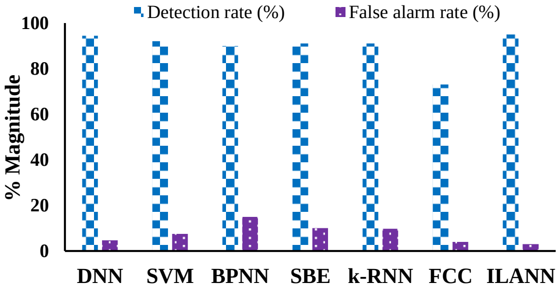

Figure 8. Comparison for detection rate and false alarm rate

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 Mohammadnezhad, 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.2020.33.12c.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.2020.33.05b.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.I., "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.2020.33.11b.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

10. Lo, C.-H. and Ansari, N., "Consumer: A novel hybrid intrusion detection system for distribution networks in smart grid", ***IEEE Transactions on Emerging Topics in Computing***, Vol. 1, No. 1, (2013), 33-44. DOI: 10.1109/TETC.2013.2274043
11. Manandhar, K., Cao, X., Hu, F. and Liu, Y., "Detection of faults and attacks including false data injection attack in smart grid using kalman filter", ***IEEE Transactions on Control of Network Systems***, Vol. 1, No. 4, (2014), 370-379. DOI: 10.1109/TETC.2013.2274043
12. Jow, J., Xiao, Y. and Han, W., "A survey of intrusion detection systems in smart grid", ***International Journal of Sensor Networks***, Vol. 23, No. 3, (2017), 170-186. DOI: 10.1504/IJSNET.2017.083410
13. Wang, Q., Tai, W., Tang, Y. and Ni, M., "Review of the false data injection attack against the cyber-physical power system", ***IET Cyber-Physical Systems: Theory & Applications***, Vol. 4, No. 2, (2019), 101-107. DOI: 10.1049/iet-cps.2018.5022
14. Singh, N.K. and Mahajan, V., "End-user privacy protection scheme from cyber intrusion in smart grid advanced metering infrastructure", ***International Journal of Critical Infrastructure Protection***, (2021), 100410. DOI: 10.1016/j.ijcip.2021.100410
15. Singh, N.K. and Mahajan, V., "Detection of cyber cascade failure in smart grid substation using advance grey wolf optimization", ***Journal of Interdisciplinary Mathematics***, Vol. 23, No. 1, (2020), 69-79. DOI: 10.1080/09720502.2020.1721664
16. Wang, G., Giannakis, G.B. and Chen, J., "Robust and scalable power system state estimation via composite optimization", ***IEEE Transactions on Smart Grid***, Vol. 10, No. 6, (2019), 6137-6147. DOI: 10.1109/TSG.2019.2897100
17. Esmalifalak, M., Nguyen, H., Zheng, R. and Han, Z., "Stealth false data injection using independent component analysis in smart grid", in 2011 IEEE International Conference on Smart Grid Communications (SmartGridComm), IEEE. 244-248. DOI: 10.1109/SmartGridComm.2011.6102326
18. Kosut, O., Jia, L., Thomas, R.J. and Tong, L., "Limiting false data attacks on power system state estimation", in 2010 44th Annual Conference on Information Sciences and Systems (CISS), IEEE. 1-6. DOI: 10.1109/SmartGridComm.2011.6102326
19. Ashok, A., Govindarasu, M. and Ajjarapu, V., "Online detection of stealthy false data injection attacks in power system state estimation", ***IEEE Transactions on Smart Grid***, Vol. 9, No. 3, (2016), 1636-1646. DOI: 10.1109/TSG.2016.2596298
20. Pan, S., Morris, T. and Adhikari, U., "Developing a hybrid intrusion detection system using data mining for power systems", ***IEEE Transactions on Smart Grid***, Vol. 6, No. 6, (2015), 3104-3113. DOI: 10.1109/TSG.2015.2409775
21. Vuković, O. and Dán, G., "Security of fully distributed power system state estimation: Detection and mitigation of data integrity attacks", ***IEEE Journal on Selected Areas in Communications***, Vol. 32, No. 7, (2014), 1500-1508. DOI: 10.1109/JSAC.2014.2332106
22. Ferragut, E.M., Laska, J., Olama, M.M. and Ozmen, O., "Real-time cyber-physical false data attack detection in smart grids using neural networks", in 2017 International Conference on Computational Science and Computational Intelligence (CSCI), IEEE. 1-6. DOI: 10.1109/CSCI.2017.1
23. Zhou, L., Ouyang, X., Ying, H., Han, L., Cheng, Y. and 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. 1-5. DOI: 10.1145/3207677.3278054
24. Ernst, J., Hamed, T. and Kremer, S., A survey and comparison of performance evaluation in intrusion detection systems, in Computer and network security essentials. 2018, Springer.555-568. DOI: 10.1007/978-3-319-58424-9_32
25. Niu, X., Li, J., Sun, J. and Tomsovic, K., "Dynamic detection of false data injection attack in smart grid using deep learning", in 2019 IEEE Power & Energy Society Innovative Smart Grid Technologies Conference (ISGT), IEEE. 1-6. DOI: 10.1109/ISGT.2019.8791598
26. Phua, C., Alahakoon, D. and Lee, V., "Minority report in fraud detection: Classification of skewed data", ***Acm Sigkdd Explorations Newsletter***, Vol. 6, No. 1, (2004), 50-59. DOI: 10.1145/1007730.1007738
27. Sundarkumar, G.G. and Ravi, V., "A novel hybrid undersampling method for mining unbalanced datasets in banking and insurance", ***Engineering Applications of Artificial Intelligence***, Vol. 37, (2015), 368-377. DOI: 10.1016/j.engappai.2014.09.019
28. Kulhare, R. and Singh, D., "Intrusion detection system based on fuzzy c means clusteringand probabilistic neural network", ***International Journal of Computer Applications***, Vol. 74, No. 2, (2013). DOI: 10.1145/3207677.3278054
29. Ren, W., Cao, J. and Wu, X., "Application of network intrusion detection based on fuzzy c-means clustering algorithm", in 2009 Third International Symposium on Intelligent Information Technology Application, IEEE. Vol. 3, 19-22. DOI: 10.1109/IITA.2009.269

Persian Abstract

چکیده

در این مقاله ، یک روش تشخیص مبتنی بر شبکه عصبی مصنوعی مبتنی بر حلقه (ILANN) برای تشخیص نفوذ سایبری در یک شبکه هوشمند در برابر حمله تزریق داده های کاذب (FDIA) پیشنهاد شده است. این روش انحراف یک سیستم را با مشخصات بار تجهیزات موجود در گره (های) سیستم مقایسه می کند و هرگونه انحراف از مقادیر از پیش تعریف شده زنگ خطر ایجاد می کند. هر ۲ میلی ثانیه (میلی ثانیه) داده های بدست آمده توسط اندازه گیری از طریق سیستم تشخیص حمله منتقل می شود ، در صورتی که انحراف به طور مداوم برای ۵ چرخه اندازه گیری یعنی برای ۱۰ میلی ثانیه باشد و با ترکیب بار مطابقت نداشته باشد، اپراتور اولین بار را دریافت می کند هشدار هشدار در صورت عدم انحراف پس از ۸ چرخه اندازه گیری ، سیستم به مرکز کنترل هشدار می دهد. حمله FDI توسط مهاجمین استفاده می شود تا عملکرد سالم شبکه هوشمند را تحت تأثیر قرار دهد. با استفاده از FDI، هکرها می توانند به طور دائمی به بسیاری از تجهیزات سیستم برق آسیب برسانند که ممکن است منجر به افزایش هزینه های رفع مشکل شود. نتیجه و تجزیه و تحلیل روش پیشنهادی تشخیص سایبری به اپراتور و مرکز کنترل کمک می کند تا نفوذ سایبری را در سناریوی شبکه هوشمند شناسایی کنند. این روش برای شناسایی حمله سایبری به سیستم تست IEEE-9 Bus با استفاده از نرم افزار MATLAB استفاده می شود.