Scalable Computing: Practice and Experience, ISSN 1895-1767, http://www.scpe.org
© 2024 SCPE. Volume 25, Issues 6, pp. 5142–5150, DOI 10.12694/scpe.v25i6.3255

EDGE COMPUTING METHOD FOR FALSE DATA INJECTION ATTACK DETECTION IN ELECTROMECHANICAL TRANSIENT SIMULATION GRID

GANG YANG,[*] YING ZHANG,[†] LILI ZHAO,[‡] LIMIN ZHANG,[§] AND NA ZHANG[¶]

Abstract. Because edge computing is close to the terminal, it has significant advantages of low latency and high-security real-time control and has huge application prospects in the current popular smart grid. Because its edge side is close to the terminal, it can also effectively avoid the risk of information leakage when control instructions or communication data are transmitted to remote cloud center servers over a long distance. However, edge devices have a greater probability of encountering false data injection attacks (FDIAs) from illegal terminals because of their proximity to terminals. The transient electromechanical situation of the smart grid due to FDIAs is analyzed under edge computing. Due to the characteristics that the status values of grid nodes have temporal correlation before and after and spatial correlation between nodes, the Long Short-Term Memory (LSTM) for training time series data is selected to predict the status values of grid nodes in advance. The FDIA detection method is also proposed based on the LSTM network. By calculating the predicted value at each historical moment and the root means square error (RMSE) of the system state estimation at that moment, the detection threshold of the scheme is calculated through the cumulative distribution function of RMSE. Simulation experiments are conducted on the Institute of Electrical and Electronics Engineers (IEEE)-14 node standard system. The detection rate is as high as 99.71%, which verifies the effectiveness of the proposed FDIA detection scheme. This paper studies the security threat of FDIA to the stable power system operation and provides theoretical analysis and practical reference for other power grid security protection strategies.

Key words: power grid, electromechanical transient, edge computing, Kalman filtering, LSTM neural network

1. Introduction.

The core national infrastructure is the most vulnerable object to network attacks, which is related to the stability and security of the whole society. The power system is the most critical infrastructure in modern society because it is the energy source of most other infrastructures [1]. With the development of information technology, the smart grid based on classic power system components and now mature information and communication technology are more convenient to operate and manage, but also particularly vulnerable. Since the 21st century, due to the attacks on information and communication networks, power grids in many parts of the world have been involved in major security threats many times [2]. In September 2019, the intranet of the Kudankulam Nuclear Power Plant in Tamil Nadu, India, was infected with malware. In April 2020, Energias de Portugal (EDP), a Portuguese multinational energy company, was attacked by Ragnar Locker's blackmail software. In June 2020, Brazilian power companies were attacked by Sodinokibi ransomware. The Venezuelan power system suffered multiple network attacks from 2019 to 2020, leading to large-scale blackouts in many places [3]. Therefore, it is particularly important to focus on strengthening the security construction of power grid facilities and the internal security protection of power enterprises. Power system state estimation can effectively guarantee the operation and control of the power system and provide accurate and real-time state information for the system. Hence, the management system can successfully perform different control and planning tasks [4]. False data injection attacks (FDIA) manipulate data without affecting system code is more difficult to detect than intrusion methods such as malware injection, leading to a greater security threat to the power grid system.

In order to ensure the safe operation of the smart grid, it is necessary to detect and defend FDIA, and scholars have conducted a lot of in-depth research on this issue. Boyaci et al. (2021) studied the detection and location of invisible FDIA in the power grid. They proposed a method based on a graphical neural network

[*] State Grid Shanxi Electric Power Company, Shanxi, Taiyuan, 030021, China (Corresponding author, GangYang81@126.com)
[†] State Grid Shanxi Electric Power Company, Shanxi, Taiyuan, 030021, China (YingZhang193@163.com)
[‡] State Grid Shanxi Electric Power Company, Shanxi, Taiyuan, 030021, China (LiliZhao8@126.com)
[§] State Grid Shanxi Electric Power Company, Shanxi, Taiyuan, 030021, China (LiminZhang7@163.com)
[¶] State Grid Shanxi Electric Power Company, Shanxi, Taiyuan, 030021, China (NaZhang72@126.com)

to identify the existence and location of FDIA. The proposed method uses an autoregressive moving average graph filter to detect and locate FDIA in power systems automatically. Many simulations and visual displays show that the proposed method is superior to the existing methods in FDIA detection and positioning [5]. Prasanna Srinivasan et al. (2021) proposed a position detection technology based on deep learning to identify FDIA continuously. False information is captured by an error data detector incorporating convolutional neural networks (CNNs). The results show that position detection can be performed in different noise and attack environments, improving the current recognition accuracy [6]. Li et al. (2021) studied the security problems of physical network systems under dynamic load change and false data injection attacks and proposed an adaptive sliding mode controller. The effectiveness of the proposed elastic defense strategy was verified through simulation [7]. Jorjani et al. (2021) implemented various methods of FDIA on the state estimator to recover the pre-attack value of the attacked grid variables based on the iterative optimization method. They proposed a framework of recovery quality index to evaluate the performance of recovery algorithms. Simulation results show that the proposed method performed satisfactorily on different test bus systems [8]. Umar and Felemban (2021) analyzed the impact of FDIA on power generation cost and the physical composition of power systems and introduced a new FDIA strategy to maximize the power generation cost. They proposed a rule-based FDIA detection and prevention mechanism for such attacks to mitigate the threat of attacks on the power system [9]. Ding et al. (2021) developed a recognition scheme based on deep learning to detect and mitigate information corruption, implemented a conditional deep belief network to analyze time series input data, and used captured features to detect FDIA. The simulation verified that the detection mechanism had good performance and was superior to other mechanisms in terms of FDIA detection accuracy and robustness [10]. Based on the research of edge computing and smart grid FDIA, this paper analyzes the attack principle of FDIAs and their impact on the power grid system. The recurrent neural network and LSTM are introduced. The advantages of the latter in time series data prediction are analyzed. Then, a state value prediction model is proposed based on LSTM neural network. Finally, the proposed FDIA detection scheme based on the LSTM network is successfully verified through simulation experiments.

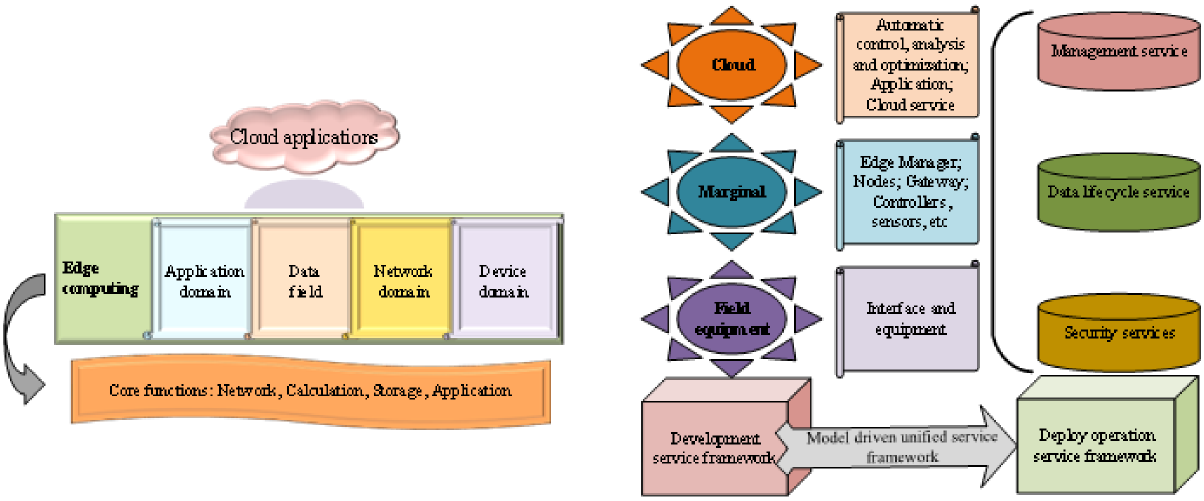
2. Method.

2.1. Edge computing. Akamai first proposed edge computing in 1998. It is between physical entities and industrial connections. It uses the open platform of the network, computing, storage, applications, and other core capabilities to provide the nearest end services. Because its applications are launched at the edge, it can respond to network services faster and has significant advantages of low latency and high-security real-time control [11]. Its core performance and architecture reference diagram are shown in Figure 2.1:

In Figure 2.1(a), because the edge server is close to the terminal device, it can provide services more quickly to ensure lower latency. On the one hand, the edge server reduces the bandwidth pressure during data upload, and on the other hand, it reduces the energy consumption of the Elastic Compute Service (ECS). Its low latency and high communication efficiency make it widely developed and applied, including the Internet of Vehicles (IoV), intelligent transportation, smart grid, and other fields [12]. In Figure 2.1(b), the problems found in edge computing are mainly in computing performance and security. Because of the complexity of the edge environment, devices deployed at the edge will be more vulnerable to attacks. Especially when one of the devices is attacked, the attacker can obtain the key information stored in it, thus causing various internal attacks. The most harmful is the false data injection attack, which will not only waste limited communication and computing resources but also seriously affect the availability of the data.

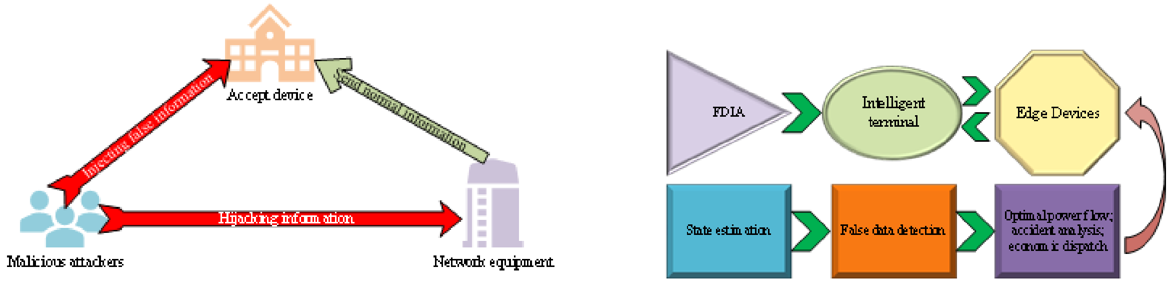
2.2. Smart grid and FDIA. Smart grid refers to the intelligentization of a power grid, which is based on a high-speed integrated two-way communication network and uses more excellent sensing and measurement, equipment, control methods, and decision support system technology to make the power grid system more reliable, safe, economical, efficient, and environmentally friendly [13]. False data injection attack FDIA is a new attack method. It has strong deception, malice, and purposefulness that can bypass traditional system detection, change and forge data in edge devices, and finally affect the calculation results and cloud decision-making. The FDIA model diagram and FDIA attack model diagram under edge computing are shown in Figure 2.2.

Figure 2.2 (a) shows the entire FDIA process. Attackers extract data from the routing of intelligent power


Cloud applications
Edge computing
Application domain
Data field
Network domain
Device domain
Core functions: Network, Calculation, Storage, Application
Cloud
Marginal
Field equipment
Automatic control, analysis and optimization; Application; Cloud service
Edge Manager; Nodes; Gateway; Controllers, sensors, etc
Interface and equipment
Management service
Data life cycle service
Security services
Development service framework
Model driven unified service framework
Deploy operation service framework

(a) Edge Computing and Core Performance (b) Reference Architecture of Edge Computing

Fig. 2.1: Edge Computing Performance and Architecture Reference Diagram

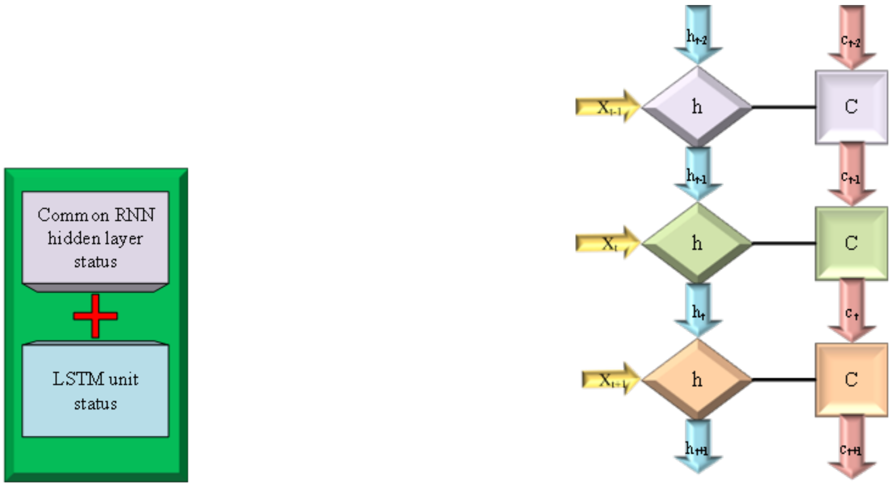


(a) FDIA process (b) FDIA model in edge computing scenario

Fig. 2.2: FDIA attack model diagram

terminals and initiate FDIA, which affects the edge devices in computing, and then affects the state estimation. FDIA can avoid bad data detection, impacting accident analysis, economic dispatch, and other decision-making schemes. In short, the process and purpose of FDIA are that the attacker tampers with the measurement data of the attacked terminal, which leads to deviation in equipment state estimation, resulting in electromechanical transient and reduced accuracy [14]. In Figure 2.2(b), in the edge scenario, FDIA can forge a lot of false data through edge devices and allow these false data to be aggregated, affecting the accuracy of the aggregation results. The edge layer will send the aggregation results to the cloud, and the cloud will make the final wrong decision because of the error aggregation results uploaded. FDIA will be more covert and destructive, bringing huge economic losses to society [15].

2.3. Deep learning and LSTM neural network. Deep learning is an important classification of machine learning. The advanced deep learning technologies are mainly CNNs and cyclic neural networks in graphics and word processing. With the development of the smart grid, deep learning technology is applied to the smart grid with huge output data, which can conduct feature extraction and result from prediction through many sample training. In the cyclic neural network model, each time series data has a hidden layer state at the



(a) LSTM hidden layer

(b) LSTM hidden layer expansion diagram

Fig. 2.3: The case of LSTM hidden layer

index position, which is sensitive to short-term input. When the interval is closer, it can retain more historical information data [16]. In addition, a state is added to the hidden layer of the LSTM neural network, which is used to retain memory for a longer time and is generally called a unit state. The hidden layer of the LSTM neural network and its expansion diagram are shown in Figure 2.3.

In Figure 2.3 (a), the LSTM hidden layer has one more unit state c, than the original recurrent neural network state h. The hidden layer is expanded according to the time dimension. At time t, LSTM has three inputs, in which the input value at time t is X_t. The output at time $t-1$ is h_{t-1}, the united state is C_{t-1}, the output at time t is h_t, and the united state is Ct. In order to control this long-term state, there must be three switches, namely the so-called door. When the output of the gate is a 0 real vector, the information representing the past time at this time is not allowed to pass. If the output is 1, it can pass completely [17]. The schematic diagram of the three-door control units of LSTM is shown in Figure 2.4.

In Figure 2.4, g represents the activation function, and there are three doors to the information in the state of the control unit c. The forgetting gate determines how much information in the cell state at the previous moment will be retained in the cell state at the current moment. The input gate determines that the input value information of the network at the current time remains in the united state currently. The final output gate is used to determine the amount of information from the unit state at the current time to the output value. The LSTM network is good at processing the state value data with obvious time series in the smart grid. Additionally, the LSTM can retain or discard historical time information in a targeted way. In particular, the closer the state value in the historical time is to the real information, and the more obvious the false information is so that it can be effectively detected. This allows it to have a good prediction effect on the state value of the smart grid. The closer its prediction of the state value is to the real state value, the more the false data will be unable to hide and will be effectively detected.

2.4. FDIA detection scheme based on LSTM. This section is based on the LSTM to train the historical state value data of nodes in the smart grid that have not been attacked by false data injection so that the next node state value can be accurately predicted. Then, false data can be detected. FDIA detection scheme based on LSTM is shown in Figure 2.5.

In Figure 2.5, the status values of each node in the distribution network are obtained, and historical status value data is generated. Then, the node state value is calculated by the system state estimation module of the distribution network system and the Newton-Raphson power flow. These data mainly include node voltage

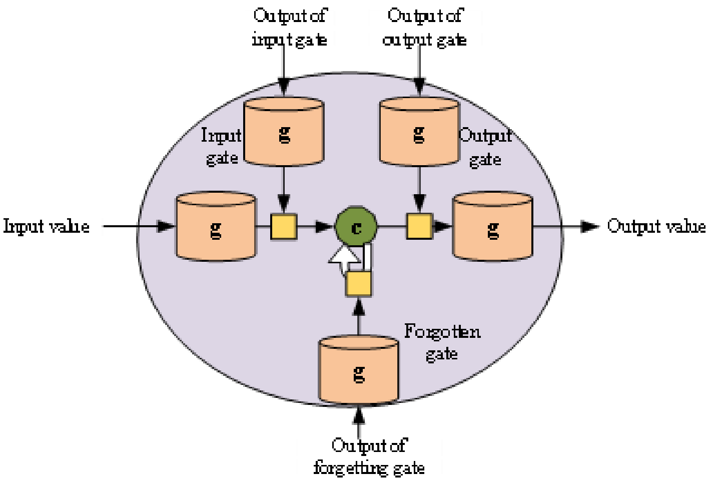


Fig. 2.4: LSTM Gating

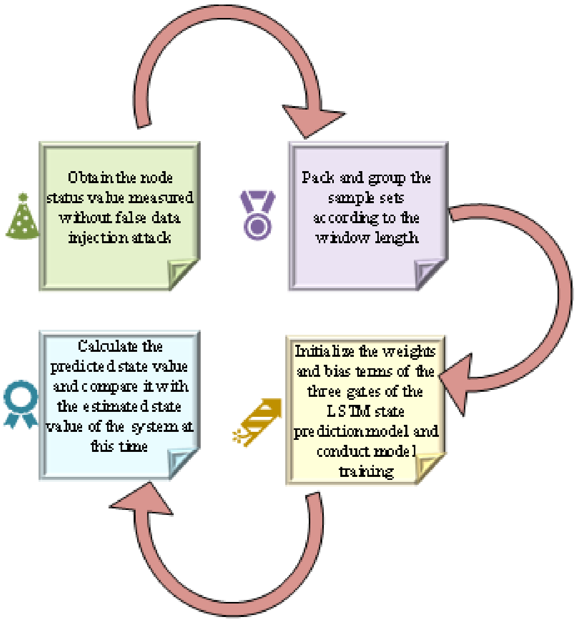

Obtain the node status value measured without false data injection attack
Pack and group the sample sets according to the window length
Calculate the predicted state value and compare it with the estimated state value of the system at this time
Initialize the weights and bias terms of the three gates of the LSTM state prediction model and conduct model training

Fig. 2.5: FDIA detection scheme flow based on LSTM

amplitude and node voltage phase angle. The historical state value data involved is a data set composed of the state values of each node at the current time and in the previous period. Next, the data set to be trained is packaged into multiple groups. The window length of the training set is determined. Then, the historical time state value of the window length is used to predict the next time state value. The LSTM state is initialized with the data to predict the weights and bias terms of the required model's input gate, forgetting gate, and output gate. The input and output samples in the training sample set are respectively used as the input and output of the LSTM state prediction model. Then, the loss value in the training process is used to realize the continuous optimization of the weight parameters, and the established LSTM state prediction model is obtained. Finally, according to the results of root mean square error (RMSE) and detection threshold comparison between the predicted value of LSTM and the estimated state value of the system state, whether a false data injection attack occurs is determined. After the results are obtained, if a false data injection attack is detected, the detection results will be fed back to the manager of the smart grid system. Then, before the system fixes the attack vulnerability, the estimated state value of the system is used as the state value at the detection time to ensure the stable operation of the smart grid. Then the next step of FDIA detection is carried out.

3. Results and discussion.

3.1. Setting of simulation experiment environment. Because the power grid's historical state value is adopted, individuals cannot obtain its real data. It is necessary to simulate the state value of the power grid when it is stable. The simulation experiment is carried out on the Institute of Electrical and Electronics Engineers (IEEE)-14 node standard system, and the network structure, line parameters, and the true values of system nodes are known. The node state value is estimated by the power system state estimation method. The simulation environment uses MatlabR2021 and MATPOWER power simulation packages. The LSTM training environment is python 3.9, tensorflow2.9.1, and Keras2.9.0.

In order to verify the performance of the improved fuzzy control P/N local path planning algorithm, the simulation experiment carried out three simulation experiments on the software of MatlabR2018a. The map scene used is a grid graph in which the obstacles in the path are marked as black areas. White areas represent the free space that the robot can move. In addition, the grid graph coordinates are refined to 10 times to improve the accuracy of simulation environment modeling. The simulation experiment conditions are set as the distribution of obstacles in the map is unknown. The simulation robot, which is regarded as a particle, simulates the motion of a differential mobile robot in the motion process. The robot can detect obstacles in the front and on the left and right sides in real-time so as to obtain the coordinates of the current robot's starting point and destination, as well as its own real-time coordinates, running speed, and angular velocity. Its initial heading angle parameter is set as 45°.

3.2. Analysis of simulation results. After the LSTM state value prediction model is trained, the sample input values of each group are transferred to the construction model to obtain the prediction values. The RMSE between the calculated prediction values and the corresponding output of this sample input is calculated. The cumulative distribution of the error is shown in Figure 3.1.

In Figure 3.1, the mean square error of the predicted value and the system estimate obtained from the LSTM state prediction model is specifically distributed between 0.014 and 0.05. So, the detection threshold can be set as 0.050, thus, false data can be detected. If the RMSE between the model's predicted value and the system's estimated value does not meet the threshold detection conditions. That is, it is inconsistent with the probability distribution of the historical RMSE. Then, it can be confirmed that the estimated value of the system is false data. That is, the grid system is attacked by false data injection. Since the LSTM state prediction model is mainly used to predict the estimated value of the system state estimation method, it will be affected by the measurement noise of the power grid. When the noise is greater, the fluctuation of its estimated value will be greater, and the prediction effect of the LSTM, on the contrary, will be weaker. Assume that when an attacker attacks the power grid with false data injection, the specific attack mode will change the state value of some nodes, which is called transient electromechanical phenomenon. When the model is set to different thresholds and attacks of different amplitudes, the final detection effect of this detection method is shown in Figure 3.2.

In Figure 3.2, no matter the size of the detection threshold, when the attack amplitude is relatively small, such as at 5%. Even if the detection threshold is set as 0.05, 87.6% of the detection results can be obtained. But for the actual attacker, if the attack amplitude is too small, the gain will not be large, so the impact of power grid fluctuation will be small, and the attacker's goal will not be achieved. Therefore, the actual attack amplitude is more than 10%. In Figure 3.2, when the attack amplitude is 15%, the detection model's detection rate is 99.71%, which can completely achieve the expected target of detection.

3.3. Comparison of results of different detection methods. In general, the measurement noise of the power grid will be large, so the attack vector constructed by attackers can easily be hidden by the measurement noise. Therefore, this paper is dedicated to detecting and analyzing state values to effectively avoid the bad

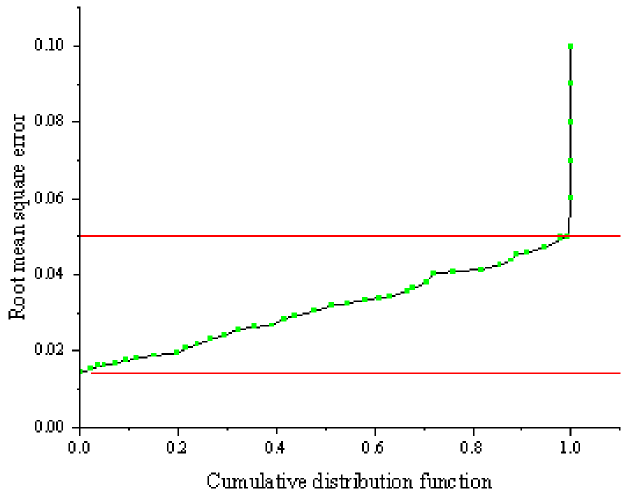
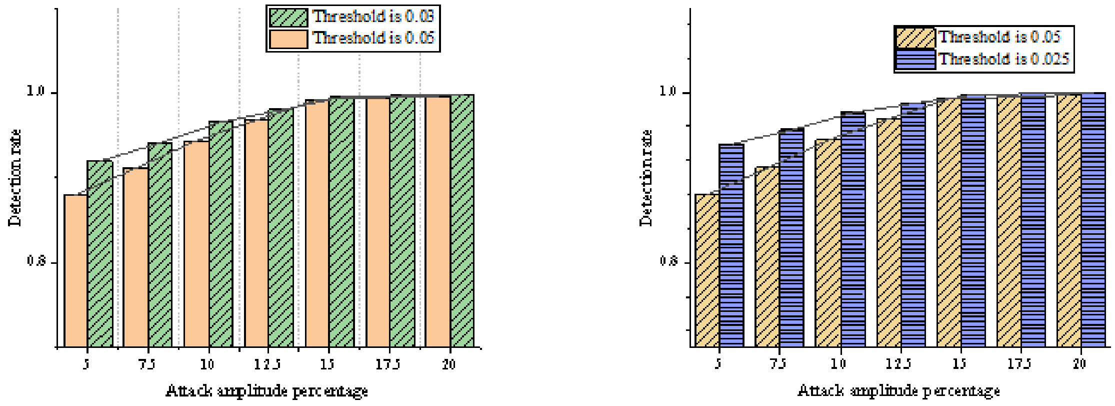


Fig. 3.1: Cumulative distribution function of RMSE of predicted value and estimated value of LSTM model



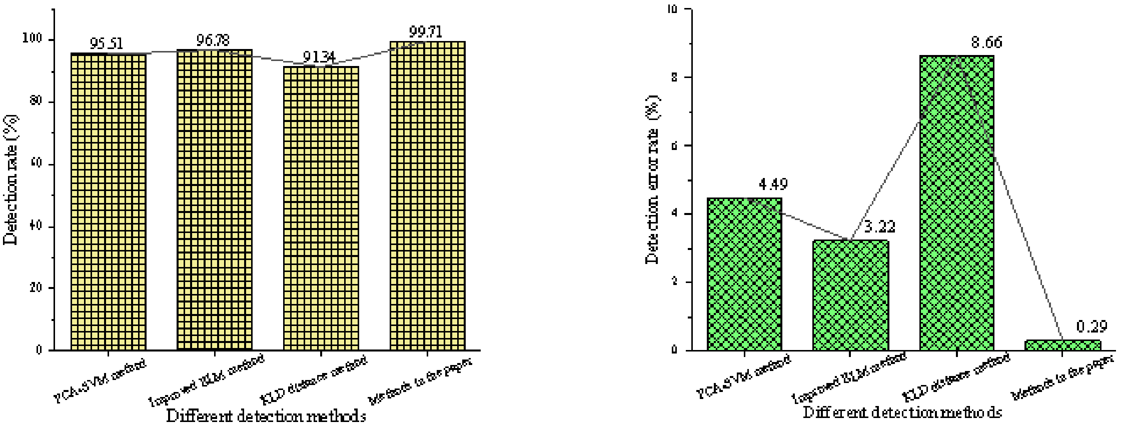
(a) Comparison of detection effects with detection thresholds of 0.03 and 0.05

(b) Comparison of detection effects with detection thresholds of 0.025 and 0.05

Fig. 3.2: Comparison of detection results under different detection thresholds

results of false data being covered up. The results of this method are compared with those of other FDIA methods, as shown in Figure 3.3.

In Figure 3.3, the proposed false data injection attack detection based on LSTM has significant advantages over other traditional detection. It not only has a higher detection rate but also has a lower false detection rate, which fully proves the progressiveness of the detection method proposed.



(a) Comparison of detection rates of different methods (b) Comparison of detection error rates of different methods

Fig. 3.3: Comparison of results of various FDIA detection methods

4. Discussion. In order to further illustrate the detection advantages of the proposed method when it is attacked by false data injection when facing an electromechanical transient simulation power grid, this paper compares and analyzes the research results with others. Li et al. (2022) proposed an FDIA detection method based on secure federation by combining Transformer, federated learning, and Paillier cryptosystem. The detection model is trained cooperatively using the joint learning framework and the data from all nodes. Data privacy is protected by keeping the data local during training. The effectiveness of this method is verified through experiments [18]. Yin et al. (2021), in the face of the false data injection attack on the FDIA of the smart grid, paid more attention to the spatial relationship between the bus/line measurement data. They proposed a microservice framework oriented to the sub-grid. They used it for FDIA detection in the AC model power system by integrating a well-designed spatio-temporal neural network [19]. Chen et al. (2022) proposed an FDIA detection method based on vector autoregression to improve the safe operation and reliable power supply in smart grid applications. It mainly combines the vector autoregression model and the measurement residuals based on infinite norms and two norms to analyze the FDIA detection under the edge computing architecture [20]. By analyzing the above detection methods and the principle of this method as well as the simulation results, the smart grid under edge computing is of great significance in FDIA attack detection. It is more suitable for FDIA attack detection under large-scale grid structures and small amounts of false data injection attacks and has higher accuracy and robustness.

5. Conclusion. False data injection attack FDIA can attack the power grid system more covertly, while the traditional detection methods cannot get effective detection. For this reason, this paper proposes a smart grid FDIA detection method based on LSTM in the face of electromechanical transient caused by attacks under edge computing. After introducing LSTM and analyzing its advantages in forecasting time series data, the proposed model has a higher detection rate and robustness. These conclusions lay a solid theoretical and practical foundation for the future development of detection algorithms. However, this paper still has the following shortcomings. Firstly, this paper studies the design based on the direct current (DC) power model. Additionally, the real nonlinear power system is linearly simplified, while the false data is only simulated and synthesized by adding Gaussian noise to the standard data. So, the final simulation detection effect is ideal. Therefore, in future work, this paper should first introduce the real data of the power grid for research and optimization. Additionally, it still needs to migrate the detection scheme to the alternating current (AC) model, simulate the different effects of various real network attacks, and develop a more active defense. Finally, this paper is hoped that the research results can provide some reference for the future FDIA detection and defense research of smart grids.

6. Acknowledgement. The study was supported by State Grid Shanxi Electric Power Company Science and Technology Project (Research and Application of New Power System Edge Intelligence Key Technology, Project No.: 52053022000B)”

REFERENCES

[1] Omitaomu, O. A., & Niu, H. (2021). Artificial intelligence techniques in smart grid: A survey. Smart Cities, 4(2), 548-568.

[2] Moreno Escobar, J. J., Morales Matamoros, O., Tejeida Padilla, R., Lina Reyes, I., & Quintana Espinosa, H. (2021). A comprehensive review on smart grids: Challenges and opportunities. Sensors, 21(21), 6978.

[3] Siniosoglou, I., Radoglou-Grammatikis, P., Efstathopoulos, G., Fouliras, P., & Sarigiannidis, P. (2021). A unified deep learning anomaly detection and classification approach for smart grid environments. IEEE Transactions on Network and Service Management, 18(2), 1137-1151.

[4] Jiang, Z., Lv, H., Li, Y., & Guo, Y. (2022). A novel application architecture of digital twin in smart grid. Journal of Ambient Intelligence and Humanized Computing, 13(8), 3819-3835.

[5] Boyaci, O., Narimani, M. R., Davis, K. R., Ismail, M., Overbye, T. J.,& Serpedin, E. (2021). Joint detection and localization of stealth false data injection attacks in smart grids using graph neural networks. IEEE Transactions on Smart Grid, 13(1), 807-819.

[6] Prasanna Srinivasan, V., Balasubadra, K., Saravanan, K., Arjun, V. S., & Malarkodi, S. (2021). Multi label deep learning classification approach for false data injection attacks in smart grid. KSII Transactions on Internet and Information Systems (TIIS), 15(6), 2168-2187.

[7] Li, J., Yang, D. F., Gao, Y. C., & Huang, X. (2021). An adaptive sliding-mode resilient control strategy in smart grid under mixed attacks. IET Control Theory & Applications, 15(15), 1971-1986.

[8] Jorjani, M., Seifi, H., Varjani, A. Y., & Delkhosh, H. (2021). An optimization-based approach to recover the detected attacked grid variables after false data injection attack. IEEE Transactions on Smart Grid, 12(6), 5322-5334.

[9] Umar, S., & Felemban, M. (2021). Rule-based detection of false data injections attacks against optimal power flow in power systems. Sensors, 21(7), 2478.

[10] Ding, Y., Ma, K., Pu, T., Wang, X., Li, R., & Zhang, D. (2021). A deep learning-based classification scheme for false data injection attack detection in power system. Electronics, 10(12), 1459.

[11] Siriwardhana, Y., Porambage, P., Liyanage, M., & Ylianttila, M. (2021). A survey on mobile augmented reality with 5G mobile edge computing: architectures, applications, and technical aspects. IEEE Communications Surveys & Tutorials, 23(2), 1160-1192.

[12] Lu, J., Chen, L., Xia, J., Zhu, F., Tang, M., Fan, C., & Ou, J. (2022). Analytical offloading design for mobile edge computing-based smart internet of vehicle. EURASIP journal on advances in signal processing, 2022(1), 1-19.

[13] Yar, H., Imran, A. S., Khan, Z. A., Sajjad, M., & Kastrati, Z. (2021). Towards smart home automation using IoT-enabled edge-computing paradigm. Sensors, 21(14), 4932.

[14] Abdurrachid, N., & Marques, J. G. (2022). Munchausen syndrome by proxy (MSBP): a review regarding perpetrators of factitious disorder imposed on another (FDIA). CNS spectrums, 27(1), 16-26.

[15] Mekruksavanich, S., & Jitpattanakul, A. (2021). Lstm networks using smartphone data for sensor-based human activity recognition in smart homes. Sensors, 21(5), 1636.

[16] Xiao, Y., Yin, H., Zhang, Y., Qi, H., Zhang, Y., & Liu, Z. (2021). A dual-stage attention-based Conv-LSTM network for spatio-temporal correlation and multivariate time series prediction. International Journal of Intelligent Systems, 36(5), 2036-2057.

[17] Boeding, M., Boswell, K., Hempel, M., Sharif, H., Lopez Jr, J., & Perumalla, K. (2022). Survey of Cybersecurity Governance, Threats, and Countermeasures for the Power Grid. Energies, 15(22), 8692.

[18] Li, Y., Wei, X., Li, Y., Dong, Z., & Shahidehpour, M. (2022). Detection of false data injection attacks in smart grid: A secure federated deep learning approach. IEEE Transactions on Smart Grid, 13(6), 4862-4872.

[19] Yin, X., Zhu, Y., & Hu, J. (2021). A subgrid-oriented privacy-preserving microservice framework based on deep neural network for false data injection attack detection in smart grids. IEEE Transactions on Industrial Informatics, 18(3), 1957-1967.

[20] Chen, Y., Hayawi, K., Zhao, Q., Mou, J., Yang, L., Tang, J., ... & Wen, H. (2022). Vector auto-regression-based false data injection attack detection method in edge computing environment. Sensors, 22(18), 6789.

Edited by: Bradha Madhavan
Special issue on: High-performance Computing Algorithms for Material Sciences
Received: Jan 29, 2024
Accepted: Mar 26, 2024