Research on Power IoT Intrusion Detection Method Based on Federated Learning

Guo Xiaoyan

Abstract The development of electricity Internet of Things (IoT) is potentially accompanied by an increase in network attack invasion. With the rapid development of artificial intelligence, machine learning, deep learning and other technologies are gradually applied to intrusion detection. However, the existing artificial intelligence program is seriously dependent on data, and with the attention of the world's attention to data privacy protection, the traditional artificial intelligence algorithm causes the model effect to be unsatisfactory because it cannot guarantee a certain amount of training. In order to protect the network security of the power network, this paper proposes an intrusion detection model based on federal learning, and uses a cluster algorithm to physically deploy an edge server, and use logic regression algorithm to network data. Intrusion detection. The intrusion detection model proposed in this paper not only protects the privacy of the grid user, but also determines the accuracy and robustness of the model on the data volume due to the problem of "data island" problem.

1 Introduction

The Intrusion Detection System (IDS) is a sense of malicious users by detecting and analyzing network traffic. At present, numerous artificial intelligence algorithms are applied in the intrusion detection system, and the algorithm is in theory, but it does not consider data issues when landing. Artificial intelligence algorithms rely on data for model training. In theory, the more data, the better the model effect.

Currently, in addition to a limited number of fields, more areas are just small data, or data from poor quality, and these data are also distributed in different mechanisms.

G. Xiaoyan (✉)
State Grid Tianjin Information & Telecommunication Company Key Laboratory of Energy Big Data Simulation of Tianjin Enterprise, Tianjin, China
e-mail: 13920604365@163.com

Information and Communication Company, State Grid Tianjin Electric Power Company, Hebei District, 153 Kunwei Road, Tianjin, China

L. C. Jain et al. (eds.), *Advances in Wireless Communications and Applications*,
Smart Innovation, Systems and Technologies 299,
https://doi.org/10.1007/978-981-19-2255-8_18

In December 2016, The National Power Grid launched an application for "electric e treasure", "handle-on power", and other applications. These APPs have disclosed, involving more than 10 million, and the hazard continues to expand. The EU has introduced the first name called 《General Data Protection Regulation》 Data Privacy Protection Act. It can be seen that the company collects, shares, and analyzes data in the case of user unaware. Just 20 companies and other more than 20 enterprises such as Tencent, Huawei committed "Do not listen to personal privacy". Traditional smart grid intrusion detection models are difficult to gather a lot of data for model training to ensure model effects.

This paper proposes a smart grid intrusion detection model based on federal learning. First, clustering clients are used to cluster, and the central deployment edge server of the class is used to solve the problem of limited client computing resources. Intrusion detection. Experimental tests were performed by the IDS2017 data set, and the experiment showed that the accuracy is fitted to the traditional centralized logic regression algorithm under the condition of protecting data privacy.

2 Research Status

At present, there are three main types of intrusion detection methods at home and abroad: are based on behavioral abnormal detection methods, based on rule-based misuse detection methods, and mixed detection methods [1]. The main advantage of behavioral abnormal detection methods is very sensitive to new attack types, which is conducive to detection of new attacks, and can detect zero-day vulnerabilities; disadvantages are high training costs, complex learning behavior, and easy to produce higher false packets. Rule-based misuse detection method is to extract feature data in a large number of attack data, which will meet the data of the matching rule as an attack behavior, but the maintenance cost is relatively high, and the new attack type is not sensitive, can be carried by attack load Processing bypassing the rules match. The mixed intrusion detection method is to combine the first two types to improve the detection rate of the known intrusion type and reduce the false positive rate of future attack types.

In [2], Ren proposed a structure of a fusion zone chain and a federal learning, designed an intrusion detection algorithm for lightweight network equipment. Document [3] proposes an intrusion detection method based on a KPCA method and Support Vector Machine algorithm (SVM). Document [4] proposes an intrusion model based on internal and external convolution networks, and the accuracy and false positive rate of the modeling model are better than the baseline model. Document [5] uses depth migration technology to provide an intrusion detection algorithm for the Internet of Things, mainly identifying distributed denial services, data mobile phones, etc., and the proposed method has high classification accuracy. Literature [6] Chen improve the traditional use of signal dual profiles to improve, using the Support Vector Machine to invade the wireless device terminal, the method has a good accuracy.

Today, machine learning technology is widely used in intrusion detection systems. This paper utilizes a classification algorithm logistic regression to training sets, and obtains weights of each network eigenvalue, which predicts results.

3 Related Basics

3.1 Federated Learning

Traditional artificial intelligence algorithms require users to train data to the center server. However, the collected data may contain many privacy information, and the user may not be willing to disclose private information, or the user refuses to share data. Second, the existence of the Internet technology giants monopolizes a lot of data. This is also the cause of “data island”, causing difficult to share between the data, it is difficult to create the data value of “$1 + 1 > 2$”. Today, even the data sharing channel between the different departments of the same company is not easy to open. At the same time, the global scope has brought more challenges to data sharing on data privacy and security. The EU introduces《General Data Protection Regulation》GDPR, any organization that involves personal information will be bound by it. Facebook and Google have become the first argument after this bill takes effect.

In 2016,Google takes the lead in proposing the federal learning privacy protection framework to use mobile phone users’ local keyboard input data to predict the next prompt input of the user’s keyboard. A shared model is established between the server and the mobile terminal, so that the data “can be invisible” can be implemented in the case of mobile terminal data, and the user privacy has also reached the purpose of data utilization.

In this frame, the server first initializes the information of the model, each distributed terminal downloads the initialization model in the server, and then each distributed terminal is based on the local data set, and only the gradient information of the model is transmitted after training. The server receives the gradient information of each distributed terminal to integrate according to the proportion of the data set of each terminal. The above steps are a round of training, the training ends when the number of preset iterations or the satisfactory effect is achieved.

Suppose there are N terminals in the federal learning system, each terminal has $n_i(1 \leq i \leq N)$ sample, then the loss function of the central server is as in Eq. (1):

$$f_j(w) = \sum_{i=1}^{N} \frac{n_i}{n} F_i(w) \tag{1}$$

where $F_i(w) = \frac{1}{n_i} \sum_{j=1}^{n_i} f_j(w)$ is the loss function of the i-th terminal, $f_j(w)$ is the j-th sample of the i-th terminal Loss, w is the model parameters of the current echo.

Federal learning generally adopts a gradient decrease algorithm to minimize the loss function until the number of specified iterations or a certain model accuracy is reached.

3.2 Logistic Regression Classification Algorithm

The hypothesis function of the logistic regression [8, 9] is used to use the hypothesis function of the linear regression, so the weight vector w obtained in the former can be well shown in an impact of a feature vector to the classification result.

The hypothesis function of logistic regression is as in Eq. (2).($\boldsymbol{x}$ is the feature vector, $\boldsymbol{w}$ is the weight vector).

$$\boldsymbol{h}_{\boldsymbol{w}}(\boldsymbol{x}) = \frac{1}{1 + e^{-W_x^T}} \tag{2}$$

Loss function, such as Eq. (3) ($\boldsymbol{y}$ is the true label value, $\boldsymbol{h}$ is the predicted label value, $\boldsymbol{m}$ represents the total number of data).

$$F(w) = -\frac{1}{m}\sum_{i=1}^{m}\left[y_i * \log(h_w(x_i)) + (1 - y_i) * (1 - h_w(x_i))\right] \tag{3}$$

The gradient decrease algorithm finds a certain set of weights $\boldsymbol{w}$ make $\boldsymbol{F}(\boldsymbol{w})$ as small as possible, as in Eq. (4) ($\boldsymbol{\alpha}$ is step size).

$$w_i^j = w_i^{j-1} - a * \frac{\partial F}{\partial w_i} \tag{4}$$

4 Power IoT Intrusion Detection Algorithm Based on Federal Learning

4.1 Power IoT Intrusion Detection Algorithm Framework

The construct of intrusion detection system requires a lot of effective label data to analyze learning. For small and medium power grid units, the network data that can be collected is very limited, and tags are also required mark. This paper uses the federal machine learning framework to achieve a distributed machine learning task for more power grid units, solve the traditional “data island” problem [7], aggregate more available data. In federal learning, task participants do not need to share local

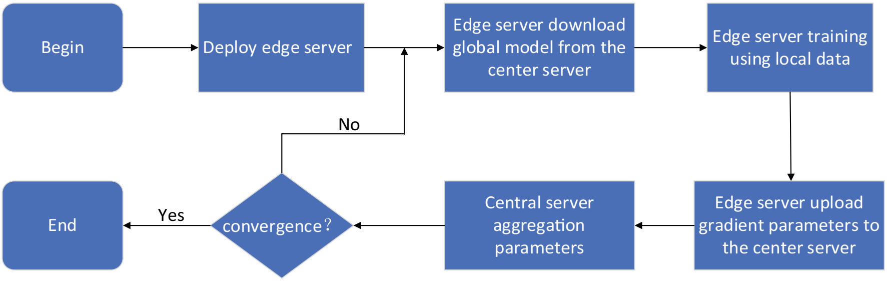
Begin
Deploy edge server
Edge server download global model from the center server
Edge server training using local data
Edge server upload gradient parameters to the center server
Central server aggregation parameters
convergence？
No
Yes
End

Fig. 1 Intrusion detection framework process scheme

data, and only need to train, only need to interact and update the iterative gradient parameters. The workflow of this framework is shown in Fig. 1.

First, in order to ensure sufficient computing power and stable communication capabilities, we deploy edge servers based on physical distance through a clustering algorithm. Secondly, the edge server collects the raw data of the power grid belonging to each terminal within its own range. Finally, the model training of the logistic regression algorithm under federated learning. The edge server uses the model aggregated by the central server in the previous round to perform a new round of model training, and then uploads local model parameters. Repeat this until convergence, and its simple process is shown in Fig. 1. The logistic regression model trained with power grid data can perform well intrusion detection and discrimination. Because it aggregates grid data of a large number of distributed nodes, theoretically the more data, the better the effect and robustness of the model.

The intrusion detection framework based on federated learning proposed in this paper mainly includes three main characters of central server, edge servers, and power users. Their respective functions are as follows:

Power User: The actual owner of network data, that is the user in the smart grid, the smart meter is responsible for collecting the user's information to the edge server.

Edge Server: Small servers deployed within a certain physical link range is to solve user-end computing, storage resource limited problems, responsible for collecting scope users to model training, and interact with the cloud server. User data does not have an edge server associated with it to a certain extent, to a certain extent, to protect data privacy.

Central Server: The role of publishing initial model, collection, integration, distribution global model, constitutes server cluster, preventing single point fault issues, ensuring normal implementation of training tasks.

The framework structure mentioned in this paper is shown in Fig. 2, mainly divided into cloud, side, and households. The cloud is a central server working layer, and the edge layer is deployed with an edge server. The user layer is the actual owner and producer of the data.

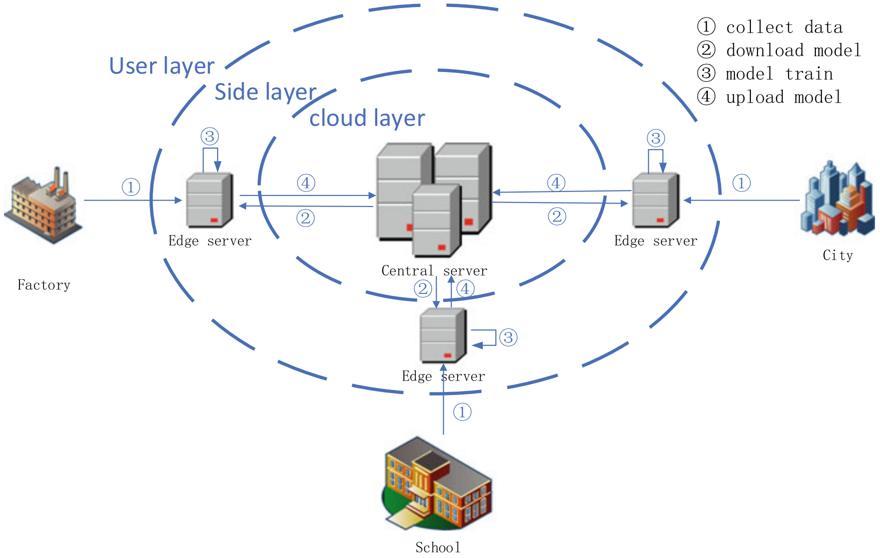

Fig. 2 Power IoT intrusion detect framework

4.2 Intrusion Detection Algorithm Experiment

Environment: cpuR7-5800H, gpu3060, Python 3.9,Windows 11.

The data set of this experiment is IDS2017, about 2,830,700 data, 81 features (including Flow Duration, Total Forward Packets, Total Backward Packets,Total Length of Forward Packets, Total Length of Backward Packets,, etc.). Randomly disrupt 2,830,700 data, extract data volume ratio of 0.01, totaling 28,307 data, and divided into training set and test set by pressing 3: 1 ratio. The data label has 11 attack prediction results such as Benign, DOS Hulk, DDoS, BOT, respectively correspond to 0, 1, …, 11, respectively.

Experiment 1: Simulate three edge nodes (three institutions or companies in reality), divide the 2,830,700 * 0.75 data is divided into 3: 3: 4, and finally according to the federal learning method data on three edge nodes Through joint training, the change in accuracy with the number of times is shown in Fig. 3.

Experiment 2: Simulate five edge nodes (five institutions or companies in reality), the proportion of 2,830,700 * 0.75 data is 2: 2: 2: 2: 2: 2: 2: 2: Finally according to federal learning methods The data of the edge node performs joint training, the change in the number of times the number of times is shown in Fig. 4.

The experimental results show that compared with the traditional single-node logic regression algorithm based on federal learning, the power-based logic regression algorithm is not only protected by user data privacy, but also accurate comparison. The accuracy of some separate training of some nodes is higher. To a certain extent, because of the "Data Lone Island", many data have been effectively utilized, making the robustness of the model better.

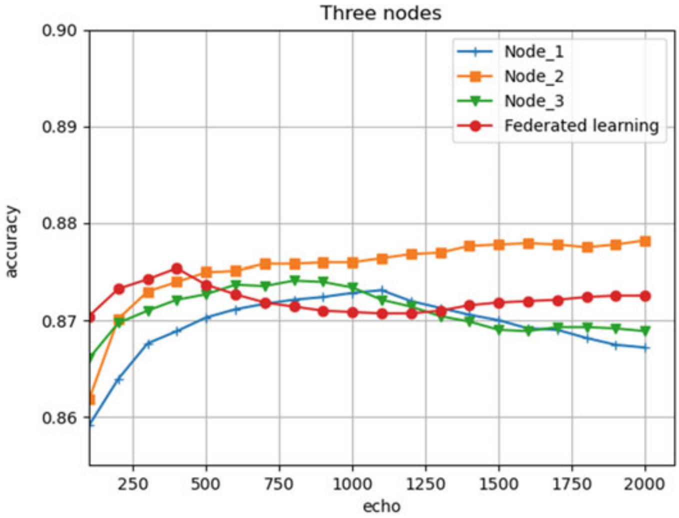

Fig. 3 Detection accuracy of three edge nodes

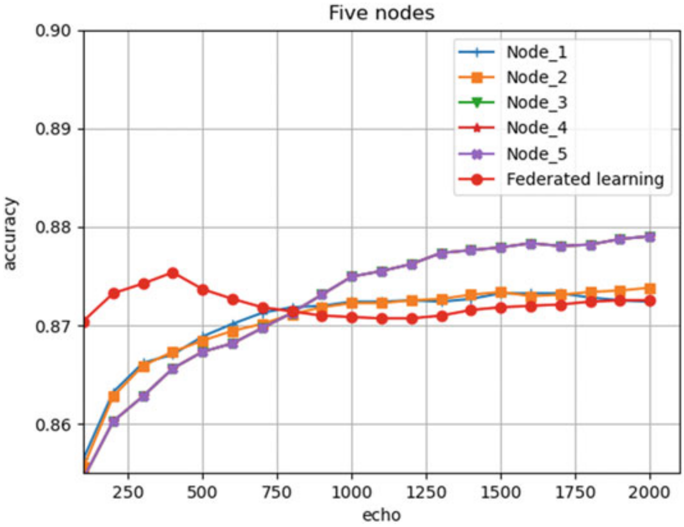

Fig. 4 Detection accuracy of five edge nodes

5 Conclusion

This paper proposes a power IoT intrusion detection method based federal learning. Federal learning as a revolutionary innovative privacy protection new paradigm, which can protect data security while user data, while protecting data security, is a unified modeling training for data information from various nodes. This paper is tested on the IDS2017 data set to achieve the expected effect. Comparing data centralized training methods, this paper does not sacrifice larger precision to achieve distributed training purposes, protecting data privacy, breaking "Data Lone Island" to a certain extent, increasing the robustness of the model Prevent it from fitting. Future work takes into account the distributed characteristics of federal learning and block chains, enabling distributed IDS, improve electricity network security, and protects residents.

References

1. Sun, Y.Z.: Application of artificial intelligence in electricity network intrusion detection. China Inform. Security **06**, 45–47 (2021)
2. Ren, T.: Network intrusion detection algorithm for fusion zone chain and federal learning. Inform. Network Security **21**(07), 27–34 (2021)
3. Shone, N., Ngoc, T.N., Phai, V.D.: A deep learning approach to network intrusion detection. IEEE Trans. Emerg. Top Computlntell. **2**(2), 41–50 (2018)
4. Wang, Y.F.: Network intrusion detection based on internal and external convolutional network. J. Beijing University of Posts Telecommunications, 1–7 (2021)
5. Zhan, L.J.: Internet invasion detection framework based on deep migration learning. Internet of Things Tech. **11**(11), 58–61 (2021)
6. Chen, Z.X.: Intrusion detection algorithm based on grid wireless device based on radio frequency fingerprint. Radio Eng. **51**(05), 352–359 (2021)
7. Yang, Q.: AI and data privacy protection: Federal learning crack. Information Security Res. **5**(11), 961–965 (2019)
8. Mao, Y.: Logical regression model based on density estimation. Automatic Chem. **40**(01), 62–72 (2014)
9. Guo, H.P.: Logical regression method for class imbalance. Pattern Identifi. Artificial Intell. **28**(08), 686–693 (2015)