International Core Journal of Engineering Volume 5 Issue 9, 2019
ISSN: 2414-1895 DOI: 10.6919/ICJE.201908_5(9).0012

Power Information System Intrusion Detection Model Based on Deep Belief Network

Xin Wang [a], Youchan Zhu [b]

School of North China Electric Power University, Baoding 130600, China

[a]wx1164292494@163.com, [b]yc_hd@sina.com

Abstract

Network intrusion detection has become a research hotspot in the field of network space security. The grid information system is one of the infrastructures for safe and reliable operation of the grid. The protection of the grid information system is the core content of the grid company's network security construction. The biggest security problem of network security is network anomaly. In view of the defects of traditional intrusion detection methods in terms of detection speed, accuracy and complexity, a support vector machine intrusion detection model (DBN-SVM) based on deep belief network is proposed. The model uses two layers to limit the Boltzmann machine for structural dimensionality reduction, and BP neural network to inversely fine-tune the structural parameters to obtain the corresponding optimal representation of the original data. Then use the support vector machine to perform network intrusion identification on the data. The NSN-KDD data set is used to simulate the network intrusion detection of the DBN-SVM model. Experiments show that the DBN-SVM model improves the abnormal intrusion detection rate and enhances the information security of the power information system.

Keywords

Intrusion Detection;Deep Learning; Power Information System;Deep Belief Network.

1. Introduction

In recent years, cyber attacks have increased dramatically in both quantity and scale. Intrusion detection and vulnerability scanning systems have become an indispensable system for enterprise network facilities. The grid company's information system is listed as a key information infrastructure and is regarded as an important strategic resource of the country. Protecting the security of key information infrastructure has become the core content of the company's network security construction. Network intrusion detection is a technique for analyzing the status information of a protected system by collecting data packets and network audit data to discover whether there is any intrusion. By monitoring the backbone network and the core computer system in real time, detecting and identifying intrusion behaviors or attempts in the system, giving intrusion alerts, preventing intrusions in time, protecting systems and network security. In [1], the data mining AR_Tree algorithm is introduced into the power information network intrusion detection to generate the intrusion detection rule. It saves the connection information in the network transaction flow in the tree structure, and quickly mines the rules directly related to the attack in AR_Tree. The online generation of rules is implemented, which improves the efficiency of intrusion detection. In [2], for the electricity market operation system, an intrusion detection method based on artificial immune principle is proposed. This method simulates the human immune mechanism and detects the intrusion in the system by generating a detector with a genetic algorithm. The literature [3, 4] uses snort rules

ISSN: 2414-1895 DOI: 10.6919/ICJE.201908_5(9).0012

and association rules to mine the intrinsic relationship between the behavioral characteristics of network attacks and behavioral purposes to design an intrusion detection system. In [5], an intrusion detection method based on improved minimum closure spherical vector machine is proposed. This method abstracts the intrusion detection into a multi-classification problem, and improves the intrusion detection model by improving the training of the historical data samples. It uses the minimum closure ball to reduce the detection time, and uses the particle swarm optimization algorithm to dynamically search the optimal training parameters of the minimum closure ball vector machine to reduce the error of the intrusion detection model.

With the rapid development of network technology and the substantial increase of network bandwidth, the data that the power information network intrusion detection system needs to process has increased sharply. The processing speed of a single node can no longer meet the intrusion detection needs in high-speed network environment, resulting in a large number of underreporting. , affecting the accuracy and timeliness of detection.

Therefore, based on the analysis of the power information network structure, a support vector machine intrusion detection model (DBN-SVM) based on deep belief network is proposed for the defects of traditional intrusion detection methods in terms of detection speed, accuracy and complexity. The model uses two layers of restricted Boltzmann machines for structural dimensionality reduction, and uses BP neural network to inversely fine-tune structural parameters to obtain the corresponding optimal representation of the original data. Then use the support vector machine to perform network intrusion identification on the data. Simulation experiments on the NSL-KDD dataset show that the network intrusion detection using the DBN-SVM model improves the abnormal intrusion detection rate and enhances the information security of the power information system.

2. Theoretical Analysis

2.1 Power Information System Network Structure

The power information network is divided into two major regional networks according to the business and security features: the production control large area network and the management information large area network. The production control area network mainly includes real-time control and non-real-time control areas. It belongs to the power production system and uses the online operation mode of the power dispatch data network. The data exchange is high and the security requirements are high. The real-time control area includes an automated system with real-time monitoring supported by SPDnet (scheduling information network), such as dispatch automation system, phasor synchronous measurement system, distribution automation system, substation automation system, power plant automatic monitoring system, and so on. The non-real-time control area includes production operations and wholesale transaction systems that do not have control functions such as water-conditioning automation systems, energy metering systems, and power-side power market trading systems. Usually, the two areas are logically isolated, and the isolation device is a firewall. The management information area network includes the production management area and the information management area, which belong to the information management system, and the two are also isolated by adopting logic. The production management area includes a system for production management, such as a dispatch production management system, a lightning detection system, meteorological information access, and customer service supported by SPnet (Power Information Network). The information management area includes systems such as MIS and OAS [6].

It can be seen that there are two main factors that threaten the normal operation of the power system. First, various internal intrusion attacks in the area, internal personnel violations and unauthorized operations. Because the power information network is partition protection, the security level of each part is different. The production control area network has the highest security level, which is directly related to the normal operation of the power system. Therefore, there are many effective methods applied in technology. This minimizes threats such as role-based access control, PKI/PMI-based

ISSN: 2414-1895 DOI: 10.6919/ICJE.201908_5(9).0012

single sign-on, and more. The second is the various attacks on the management information network by hackers through the external Internet network. With the upgrading of the power grid, the relationship between the power information network and the Internet is getting closer and closer, and the power information network is more open and transparent, which in turn increases the number of intrusion threats. Even if there is a firewall blocking between the management information area network and the external network, the firewall does not scan the data content of the data packet because the source address, destination address, and port number of the data packet are not filtered. Prevent intrusions such as local unauthorized operations and illegal remote access. From the perspective of firewall design, it is mainly used to prevent external attacks, but it is powerless for internal attacks, and the firewall is policy-based. It implements filtering by formulating corresponding filtering rules, and uses fixed mode to prevent known attacks. rigid. Due to the complex zoning structure of the power information network and the different requirements for security, considering the intrusion detection workload of the entire power information network will be large, it is impossible to have a unified solution [7]. Therefore, the intrusion detection model is designed for the characteristics of information management area in power information network, and simulation experiments are carried out to verify the validity of the model.

2.2 Support Vector Machine Intrusion Detection Model Based on Deep Belief Network

2.2.1 How Deep Belief Networks Work

The deep belief network was proposed by Hinton et al. in 2006. It has attracted much attention as a deep learning method and has been successfully applied in the fields of object recognition and speech recognition. It learns to obtain the compression coding of the data set, which can achieve the purpose of data reduction. Structurally, the DBN consists of a multi-layered unsupervised restricted Boltzmann machine network and a supervised Back-Propagation (BP) network. The DBN is mainly divided into two steps in the process of training the model. :

(1)Separately train each layer of RBM network unsupervised separately; ensure that feature information is retained as much as possible when mapping feature vectors to different feature spaces;

(2)Set up the BP network in the last layer of the DBN, receive the output feature vector of the RBM as its input feature vector, and supervisely train the entity relationship classifier. Moreover, each layer of RBM network can only ensure that the weights in its own layer are optimal for the feature vector mapping of the layer, and the feature vector mapping of the entire DBN is not optimal, so the back propagation network also has error information from the top. Propagation to each layer of RBM, micro-tuning a DBN network. The process of RBM network training model can be regarded as the initialization of a deep BP network weight parameter, which makes DBN overcome the shortcomings of BP network which is easy to fall into local optimum and long training time due to random initialization weight parameter.

In the above training model, the first step in deep learning is called pre-training, and the second step is called fine tuning. In this paper, we construct a deep belief network model that includes two layers of RBMs, low-level RBM and high-level RBM.

2.2.2 Limiting the Boltzmann Machine

Restricting the Boltzmann machine is the core of the deep belief network. It is a two-layer neural network proposed by Hinton and Sejnowsk in 1986. The two nodes are the visible layer and the hidden unit. The whole network model is a two-part graph. Only the visible unit and the hidden unit will have edges. There will be no edge connection between the visible units and the hidden units, as shown in Figure 1 [8]. Where V(V1, V2...Vi) is a visible layer unit, indicating input data; H(H1, H2...Hj) is a hidden layer unit, and hidden layer nodes often have no practical meaning, usually machine learning automatically generates; W indicates visible The connection weight between the layer unit and the hidden layer unit. Since all V and H satisfy the Boltzmann V distribution WHV, H therefore V can get the hidden layer H through VP(H | V) when inputting HVV, and after obtaining the hidden layer H, pass P(V | H) again. Can get the visible layer. By adjusting the parameters, if the

ISSN: 2414-1895 DOI: 10.6919/ICJE.201908_5(9).0012

visible layer V1 obtained from the hidden layer is the same as the original visible layer V, then the obtained hidden layer is another expression of the visible layer.

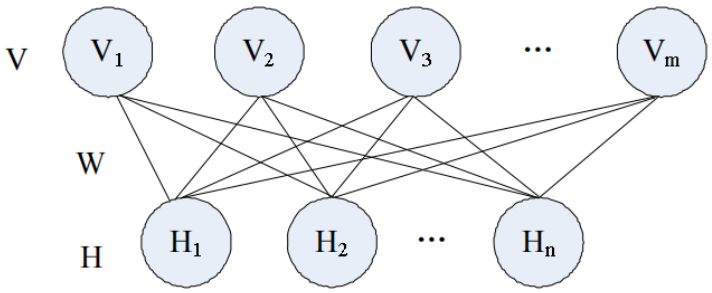

Figure 1 RBM structure diagram

2.2.3 Intrusion Detection Model Framework of Power Information System Based on Deep Belief Network

The overall framework of the power information system intrusion detection model based on the deep belief network consists of three steps:

(1)Data preprocessing. The character data in the NSL-KDD data is digitized, and the data is normalized.

(2)Through the DBN model we built, the data was trained and feature dimension reduction, and the data with excellent characteristics was extracted to prepare for the third step data classification.

(3)The(2) dimensionality reduction data obtained is used as the input of the SVM to identify the attack category.

3. Simulation and Experimental Analysis

Experimental environment: Linux-ubuntu16.04 system, tensorflow deep learning platform, pandas data analysis library.

The experimental implementation process is mainly divided into three phases: first, the data preprocessing stage, which involves digitizing and normalizing the dataset data; then the feature extraction phase, using the adaptive deep confidence network algorithm to train RBM and BP layer by layer. Fine-tuning, finding the optimal parameters, and generating the training sample distribution with the maximum probability. The final stage is to use the XGBoost algorithm in integrated learning to classify, so as to improve the detection rate and reduce the false positive rate.

This paper uses the NSL-KDD data set to evaluate our proposed DBN-SVM intrusion detection model. Among them, DBN has two uses in our experiments. First, we use DBN as the feature dimension reduction of data, and then apply SVM as a classifier to train and classify the data. In addition, we also use a single DBN as a classifier for training classification. Among them, in this experiment we use the default SVM parameter setting; DBN uses two layers of RBM structure, the number of features of RBM is 41, 13 and 4 from bottom to high, and the number of iterations is 150. And classify in different proportions of the amount of data.

(1) DBN vs SVM vs DBN-SVM

In this experiment, 20%, 40%, 60%, and 100% NSL-KDD data were extracted in SVM, DBN, and our proposed DBN-SVM model, and the accuracy and time were compared. As shown in Table 1.

Table 1 Comparison between different types of models

Training Data	SVM		DBM		DBN-SVM	
	Accuracy	Time	Accuracy	Time	Accuracy	Time
20%	82.10%	10.4s	89.61%	0.32s	90.05%	2.53s

ISSN: 2414-1895 DOI: 10.6919/ICJE.201908_5(9).0012

40%	87.59%	11.6s	89.43%	0.44s	91.51%	3.95s
60%	88.32%	20.88s	80.55%	0.56s	92.83%	5.06s
100%	89.26%	32.31s	89.61%	0.76s	93.13%	7.73s

At the beginning of the experiment, the accuracy began to rise. When the iteration reached 98 times, the accuracy of the experiment was optimal, and then began to decline. Through experimental comparison, DBN-SVM significantly improves the recognition ability of network intrusion due to the separate SVM and DBN models in terms of accuracy. In terms of runtime, DBN-SVM greatly improves processing time relative to SVM, but is slightly less than a separate DBN. In terms of overall accuracy and efficiency, DBN-SVM has outstanding advantages in this respect, greatly improving the detection capability of network intrusion.

(2) Comparison of data dimensionality reduction methods

In order to test the performance of DBN as data dimensionality reduction, NSL-KDD data is also used as the original input data, and PCA, Gain Ratio and other methods are used for comparison. The experimental comparison results given in Table 2 show that DBN as a data dimension reduction is more advantageous than other methods, and is more suitable for feature extraction tasks in high-dimensional space.

Table 2 Comparison of different data dimensionality reduction methods

Training Data	PCA	Gain Ratb	DBN
20%	68.02%	65.81%	90.05%
40%	68.89%	65.78%	91.11%
60%	71.12%	70.98%	92.83%
100%	73.23%	69.55%	93.22%

4. Conclusion

The deep belief network is a new intrusion detection model for intrusion detection. Compared with the known classification methods and feature dimension reduction methods, DBN has shown excellent performance as a classifier and feature dimension reduction. Aiming at the characteristics of power information system, this paper proposes a power information system intrusion detection model based on DBN-SVM. DBN is used for feature dimension reduction and SVM as data classifier. The experimental results of the NSL-KDD dataset show that DBN-SVM has better classification effect than SVM, and the test time is greatly improved by reducing the data. In short, the model improves the speed of intrusion detection and is a feasible and efficient intrusion detection model, which provides a new idea for power information system intrusion detection.

References

[1] Liu Xin, Sun Qiang, Yu Wei, Liu Donglan. Analysis and Research on Key Technologies of Power Information System Security[J]. Automation Technology and Application, 2019, 38(04): 63-68+76.

[2] Mu Wentao. Analysis and application of network topology algorithm for power information system [D]. North China Electric Power University (Beijing), 2017.

[3] Ding Shan. Research on key technologies of intrusion detection based on deep learning [D]. Beijing Jiaotong University, 2018.

[4]Jie Gu,Lihong Wang,Huiwen Wang,Shanshan Wang. A novel approach to intrusion detection using SVM ensemble with feature augmentation[J]. Computers & Security,2019

[5]Yang Yanqing,Zheng Kangfeng,Wu Chunhua,Yang Yixian. Improving the Classification Effectiveness of Intrusion Detection by Using Improved Conditional Variational AutoEncoder and Deep Neural Network.[J]. Sensors (Basel, Switzerland),2019,19(11).

ISSN: 2414-1895 DOI: 10.6919/ICJE.201908_5(9).0012

[6]Mirza A H, Cosan S. Computer network intrusion detection using sequential LSTM Neural Networks autoencoders[C]//2018 26th Signal Processing and Communications Applications Conference (SIU). IEEE, 2018: 1-4.

[7] Zhou Zhihua, Ji Feng. Deep Forest: Towards an Alternative to Deep Neural Networks[C]// Proceedings of the Twenty-Sixth International Joint Conference on Artificial Intelligence, 3553–3559, 2017.

[8] Xu Yin, Wang Ruilin, Liu Xiaobo, et al. Deep Forest-Based Classification of Hyperspectral Images[C]//Proceedings of the 37th Chinese Control Conference, Wuhan, China: Chinese Control Conference, 2018: 10367-10373