Research on Unknown Threat Detection Method of Information System Based on Deep Learning

LingHao Zhang¹, Yunhui Liang¹, Yong Tang¹, Seng Wang¹, Chao Tang¹ and Chun Liu²*

¹ Electric Power Research Institute of State Grid Sichuan Electric Power Company, ChenDu, SiChuan, 610000, China
² State Grid SiChuan Electric Power Company Leshan Power Supply Company, LeShan, SiChuan, 614000, China
*Corresponding author’s e-mail: Liuc4271@sc.sgcc.com.cn

Abstract. Enterprise information system may be threatened and attacked at any time from the external and internal environment, so how to improve the enterprise information system from the outside world unknown threat detection is particularly important. This paper is based on the method that is applied to detecting and identifying unknown threat, so as to protect and improve the information system's safety and stability with technical support and guarantee. It can avoid the impact of unknown threat on information system security to the greatest extent.

1. Introduction

Present situations of intrusion detection. Intrusion detection technology is a supplement to the traditional security mechanism[1], which is characterized by intelligent monitoring, real-time detection and timely response, and has become the main research and development direction of network security at present. But it is difficult to cope with the large amount of data. When the detection system faces new attacks, there is no characteristic sample, so the system seems helpless when faced with new attacks. The false negative rate and false positive rate are higher. The false alarm rate and alarm rate are too high, which is the most serious problem faced by intrusion detection system. Because of the complexity of the network environment and the variety of attack methods, the intrusion detection system always has different degrees of false positives. However, a large number of missing and false reports of information will reduce the efficiency and performance of intrusion detection system, and at the same time, it will consume staff's energy and reduce sensitivity[2].

2. Common intrusion detection techniques

2.1. Detection technology based on statistical method[3].

The traditional intrusion detection technology which based on statistical method is the earliest detection method. This method holds that by observing the normal behaviour of the protection subject in the past specific time period, the "confidence interval" of the behaviour of the protection subject in the current time period can be obtained. During the protection period, the monitoring system will count the deviation produced by relevant variables, and use the deviation to judge whether there is abnormality. If the deviation exceeds the safety threshold set by the system, it means that there is abnormality. At this time, the system needs to give an alarm or make corresponding treatment.
2.2. Detection technology based on hidden Markov model
Hidden Markov Model (HMM) is good at mining the context of data, and can effectively deal with time series data. Many data in the field of network security also belong to time series data, such as system call sequence, operation command sequence and so on. The key point of HMM is to determine the hidden parameters of the process from the observable data, and then use these parameters for further analysis, such as pattern recognition. HMM is widely used in the field of network security. The normal behaviour training module trains the normal behaviour data collected in the system, in order to form an HMM model that can describe the normal behaviour. While the anomaly detection module compares the real-time data in the system the HMM of normal events to judge whether abnormal behaviour occurs.

2.3. Detection technology based on support vector machine
In recent years, many researchers have also applied SVM to intrusion detection. The essence of this method is to construct the optimal hyperplane among different types of samples by using support vectors, and take this optimal hyperplane as the segmentation plane of sample data.

2.4. Detection technology based on neural network
Neural network can effectively deal with the input data nonlinearly, and learn the potential knowledge in the original data by transmitting information layer by layer, which is widely used in pattern recognition, function approximations and other fields[4]. Intrusion detection needs to identify whether the input data is abnormal information, which is also a classification problem in essence.

2.5. Detection technology based on deep learning
Deep learning is used in intrusion detection system to improve the feature recognition performance of intrusion detection model.

3. Deep learning related technologies

3.1. Composition of neurons
The basic calculation unit of depth is a single neuron, and the composition of neurons is shown in the following figure[5]:

![Neuronal structure](image)

The inputs of neurons are x1, x2, x3 and x4. Output is Hw, b(x)=f(WTX), where f is the activation function of neurons, and the common activation functions are Sigmoid function, Tanh function and ReLU function.

Sigmoid function: \( f(x) = \frac{1}{1+e^{-x}} \)

Tanh function: \( f(x) = \frac{e^x - e^{-x}}{e^x + e^{-x}} \)

ReLU function: \( f(x) = \max(0, x) \)
Deep learning generally includes multi-layer neural networks. Learning and training from big data sets can make intelligent identification and accurate prediction of new data samples, the multi-layer network structure of deep learning model can express complex functions more effectively, thus learn more accurate features. Deep neural network algorithm divided into three parts: input layer, hidden layer and output layer. The excellent feature learning process of deep learning depends on the effective training methods of deep learning. There are many ways to realize deep learning, but they all have three characteristics in common, which are deep-level, nonlinear and layer-by-layer feature extraction. Training multi-layer neural network nodes at the same time will lead to higher time and space complexity, and the deviation caused by hierarchical learning will also be transmitted between layers.

3.2. Training methods of deep learning

![Training methods of deep learning](image)

3.2.1. Bottom-up unsupervised learning
Firstly, data types are separated from data labels, and unsupervised learning without labels is carried out. The data sets are gradually be input into the deep neural network structure from the input layer, these unlabelled data are used to train the neural network unsupervised layer by layer, and the output of the previous layer is taken as the input of the next layer. This method is also called greedy training method; by training in turn with this method, we can get the parameters of each layer.

3.2.2. Supervised fine-tuning from top to bottom
After the previous bottom-up unsupervised learning, train the neural network from top to bottom by the labelled data. The first step of the bottom-up unsupervised learning process can only ensure that the weight matrix of each layer is locally optimal rather than globally optimal, so the second step of supervised learning is needed, which adjusts the output error from top to bottom and fine-tunes the parameters of each layer to achieve global optimization.

3.3. Intrusion detection model
The whole models divided into three parts: data pre-processor, feature selector and deep neural network classifier, among which the deep neural network classifier is the core module of the whole model.

![Detection model](image)
3.3.1. The data preprocessor respectively
The data pre-processor respectively reads the training data set, the test data set and their respective categories, and then performs normalization processing. The main goal of data pre-processor is to normalize network traffic data. Specifically, the training set data and the test set data are loaded separately, and then the abnormal data in them are detected and processed. Such as clearing the lost or wrong data, adding, inserting and deleting irrelevant data, and finally grouping and transforming the data to obtain new and meaningful new data.

3.3.2. The feature selector
The feature selector reduces the dimension of the pre-processed training set data and test set data, removes redundant data, and forms a network traffic data feature set. The feature selector data enters the feature selector after pre-processing. The function of feature selector is to create new data features according to the original data set of network traffic.

3.3.3. Load the data features and categories of the training set into the deep neural network classifier
The work flows of classifier is as follows: 1, Load training data and test data into the classifier of this model, where training data enter the training module of deep neural network classifier and test data enter the testing module of deep neural network classifier. 2, After the training data is trained by the deep neural network classifier, the effective results are obtained, then the test data are loaded, and then the classification of the test data set is predicted according to the effective training results. Get the prediction result, that is, complete the classification prediction process once. 3, The loaded test set category markers are compared with the predicted values of the deep neural network classifier, and the model performance is evaluated according to the confusion matrix and other methods.

4. Applying deep learning method to detect threats

4.1. Style and spacing

The project adopts distributed deployment, and the deployment situation is as follows

![Frame structure](image)

Figure 4: Frame structure

A set of network intelligent defence management and control platform, consisting of two high-end devices, which be deployed next to the core switch of the headquarters, and is deployed in the dual-machine hot standby mode. Each branch deployed a set of network intelligent defence management and control platform, which was composed of two middles and low-end devices, and deployed in dual-
machine hot standby mode. The network intelligent defence equipment receives the network traffic through the port mirroring mode, and realizes the admission control and abnormal/malicious behaviour detection of the local terminal. The headquarters and branches adopt intelligent phantom technology, actively capture abnormal/malicious behaviours, and control by linkage admission.

4.2. Platform function[6]
Sections should be numbered with a dot following the number and then separated by a single space:

![Functional composition of platform](image)

4.2.1. Accurate identification and classification management of equipment
Intelligent acquisition: Intelligent acquisition of equipment information based on active and passive information acquisition technology. Intelligent identification: Intelligent identification of equipment types and manufacturers based on equipment portrait technology.

4.2.2. Intelligent access management
Support intelligent access based on AD domain, Email and fingerprint. Authentication methods support LDAP/RADIUS/AD, etc.

4.2.3. Access compliance testing:
Software compliance detection, configuration compliance detection, anonymous detection, NAT equipment detection, illegal sharing, equipment access time check and Telnet compliance check.

4.2.4. Attack behavior detection
C&C attack, DoS attack, brute force crack, ransomware, botnet, worm, Trojan horse attack, network scanning, Shellcode attack, malware attack, privilege crack attack, video voice protocol attacks, etc. Equipment counterfeiting, abnormal connection, abnormal traffic, abnormal protocol and abnormal online time.

4.2.5. Vulnerability detection
Weak password detection, vulnerability detection and patch installation detection.

4.2.6. Anomaly behavior detection mainly applies deep learning method to detect unknown attacks
Automatically learn the connection relationship between devices in the network and the behaviour of accessing the Internet, automatically construct the normal access behaviour pattern of users, and intelligently discover abnormal connections. When abnormal connection is be found, the system will give an alarm or block automatically.
Automatically learn the traffic behaviour characteristics between devices in the network and the traffic characteristics of accessing the Internet[7, 8]. When the traffic is abnormal in a certain period, the system will give an alarm or automatically block it.

Discover abnormal protocol access in time. Learn the online time of equipment automatically, and give an alarm or block immediately if the online time of equipment is abnormal.

For devices with relatively fixed access, positions, such as servers, dumb terminal devices, IoT devices, etc., once it found that the access position of the devices changes, it would immediately alarm or block them.

Using the combination of machine learning and threat intelligence, analyse the suspicious degree of domain names, and immediately alarm or block malicious domain names.

Discovering unknown attacks, finding attacks by trapping, and capturing them without knowing the attack types.

Discover unknown attacks through deep learning methods, including portrait discovery, association analysis, suspicious domain name analysis, etc.

Flow analysis: Support to display real-time traffic, total traffic analysis, active session analysis, host traffic analysis, network segment list, and support Internet traffic map.

4.2.7. Risk disposal and visual management
Intelligent disposal. for risky equipment, the system can intelligently dispose of it in the following ways according to the change of safety factor: active alarm, network control and third party interface

Visual management. show the risk status of the whole network: the system can show the risk status of the equipment and the whole network qualitatively or quantitatively according to the severity and distribution of abnormal behaviour, attack behaviour, compliance and vulnerability of the equipment.

5. Conclusion
The application of deep learning technology can effectively improve the success rate of information system in identifying known threats and unknown threats, and provide technical support and guarantee for ensuring and improving the safe and stable operation of information systems, so as to avoid the impact of unknown threats on the security of information systems to the greatest extent.

Acknowledgments
This work was supported by the State Grid SiChuan Electric Power Company of China (Project Name: Research and platform development of full flow Advanced Sustainable threat intelligent analysis technology based on deep learning).

References
[1] Yang,KM. Intrusion Detection Based on Deep Learning[D], Beijing Jiaotong University,2015
[2] Li,C. (2017). Analysis on Threat Intelligence in Big Data Environment[J], Journal of Intelligence, 36: 24-30.
[3] Yang,C. Research on Intrusion Detection Technology Based on Deep Learning[D], Xidian University, 2019
[4] Jia,F. Intrusion Detection Algorithm Based on Convolutional Neural Network[J], Transaction of Beijing Institute of Technology, 2017,37: 1271-1275.
[5] Ding,S. Research on the Key Technology of Intrusion Detection Based on Deep Learning[D], Beijing Jiaotong University, 2018
[6] Li,ZH. Reflection on the Protection of Electric Power Information Network under the New Threat of Security[J], 2017,Digital Technology & Application: 192-193.
[7] Shi,QF. Research and Implementation of Unknown Threat Detection Technology Based on Behavior[D], Xidian University,2018
[8] Huang, XL. Unknown Network Threats Detection Based on Deep Learning[D], University of Chinese Academy of Sciences, 2020