Application and Research of Deep Neural Network Model in Computer Network Intrusion Detection

Tuqian Zhang

College of Science and Technology, Xinjiang Agricultural University, Urumqi, China,

Keywords: Deep neural network, Computer, Network intrusion, Application.

Abstract: With the rapid development of information technology, the neural network model has developed rapidly in recent years. At the same time, the high latitude and non-linear characteristics of computer network data make the network intrusion detection work difficult to break through, and the network security problem has become the focus of problems in all walks of life. In this context, this paper deeply analyzes the characteristics of deep neural network and network intrusion detection, and constructs an intrusion detection model based on deep neural network by using functions such as ReLU activation function and cross entropy loss. The experimental results show that the influence of network parameter selection on the experimental results is small, and the experimental results of the spindle-shaped network structure are better than the pyramidal network structure.

1. Research Background

1.1 Literature review

Xu Zhenhua believes that the computer intrusion detection model based on artificial neural network can effectively guarantee the security of computer network system and prevent the occurrence of network intrusion events (Xu, 2016). Zhang Shaoqi and other scholars have suggested that preventing and identifying intrusion activities is the most challenging task in computer network security. Therefore, they studied computer intrusion detection based on the classification method of deep neural network. It was found that in computer intrusion detection, the method of deep neural network can obtain more accurate detection results (Zhang et al, 2017). Cui Wei and other scholars have studied the computer network security problem against the traditional BP neural network. Moreover, the differential BP algorithm is used to optimize the threshold and weight of the traditional BP neural network (Cui et al, 2018). Liu Yuefeng and other scholars applied convolutional neural networks in computer network intrusion detection to achieve the purpose of high-accuracy identification of network attacks. The results show that compared with the traditional method, this method can reduce the false detection rate of intrusion detection by 0.5% on average and has high precision (Liu et al, 2018). Yang Yingen and Wang Zhongyang used the deep neural network as the starting point to study the intrusion detection technology in computer network security, and proposed the LSTM-RESNET intrusion detection model with neural network training and data processing as the main components. The research results show that LSTM-RESNET has good attack detection capability and good stability (Yang and Wang, 2019). Lu Zhi said that computer security issues were studied from three aspects: expert system, multi-agent system and neural network system. The research results show that in the computer network security management work, the expert system can effectively improve the intelligence of the computer system. Multi-agent systems can improve the system's defense capabilities and network situational awareness. The neural network can effectively reduce the false detection rate of the system and improve the system intrusion detection capability (Lv, 2019).

1.2 Purpose of research

With the development of communication technology and computer networks, computers have become an important tool for information exchange and sharing. While computer networks bring

  DOI: 10.25236/scmc.2019.075

convenience to people's lives and production, they also bring many personal information security issues. For example, citizens' personal information leaks, data from important state agencies are attacked, and corporate data information is lost. There are many reasons for these network security issues, such as hacking, inadequate network management, security vulnerabilities in software, and so on. Based on this, this paper expounds the deep neural network and network intrusion detection from the theoretical level, and constructs the deep neural network detection model. Finally, it deeply explores the application of the bad depth neural network model in computer network intrusion detection, in order to be computer network security. The solution to the problem provides a useful reference.

2. Theoretical Overview

2.1 Deep neural network

The neural network algorithm was proposed by mathematicians and neurophysiologists. It was originally a conjecture on the laws of human nerves. Based on this conjecture, a neural network was constructed to simulate the operation of human neurons (Wang et al, 2018). This concept proposes an initial stage. Due to the instability and range limitations of the neural network algorithm when solving problems, it has not been rapidly developed. With the tremendous increase in computer computing power, neural networks have been re-emphasized and developed in recent years. In short, the specific operation of the neural network can be understood as follows. First, create M hidden layers and establish a connection between the hidden layer and the input layer in turn. For each hidden node, select the activation function to solve the weight and bias value of each connection point and corresponding node respectively. The neural network operation mode is shown in Figure 1.

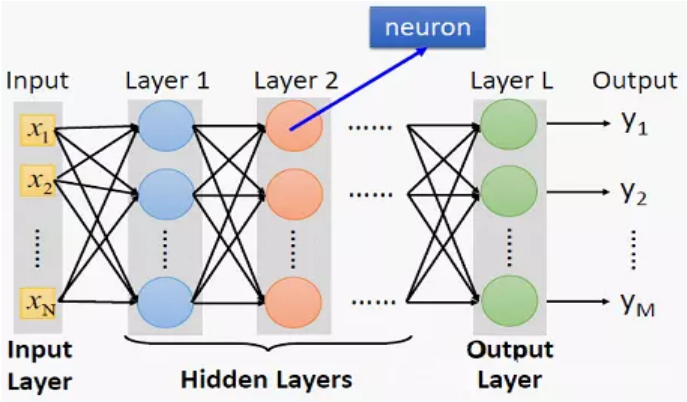

Figure 1.Neural Network Operating Mode

2.2 Network intrusion detection

Computer network intrusion detection is a technical means to determine whether there is abnormal operation in the current network by extracting and classifying network data. In simple terms, it can be understood as a safe means of preventing cyber attacks (He et al, 2016). The process of intrusion detection can be roughly divided into three parts, namely data extraction, data analysis and data response. In the data extraction phase, the data is extracted by using network datagrams, undesired behaviors in the execution program, system logs, etc., and is simply filtered to extract key information such as user activity status and behavior. In the data analysis phase, the extracted data is transmitted to the network intrusion detection engine to analyze the reality represented by the data. The logic of the network intrusion engine is to compare and analyze the extracted data with the data already stored in the knowledge base through the statistical data. In the engine's knowledge base, it contains the system misuse pattern, the network intrusion description, and the attribute description when the system is in normal use. In the data response phase, based on the results of the comparative analysis, the corresponding system response is performed, such as closing the network connection, terminating the process, and issuing an alarm to the operator. To

provide uniform management of different intrusion detection systems, the University of California has proposed a common intrusion detection system. The system defines a standard language for expressing detection information, and logically divides the intrusion detection system into task-oriented components and newly defines communication protocols between components. According to this set of specifications, the intrusion detection system is divided into four components, namely event generator, event analyzer, event database and response unit.

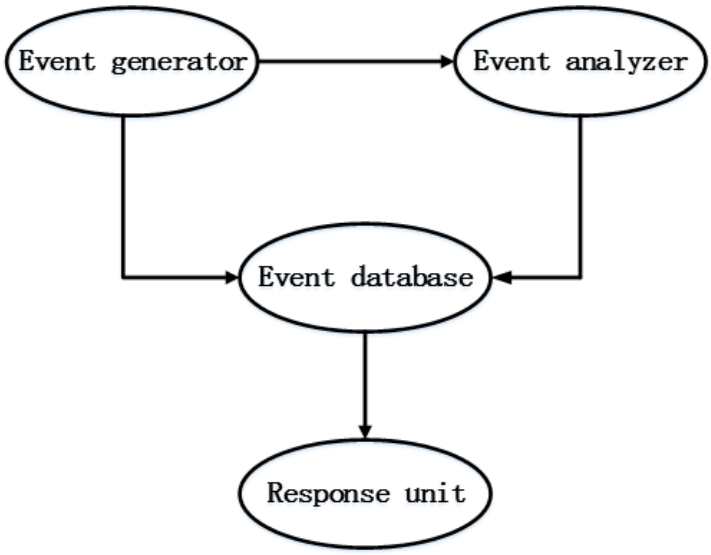

Figure 2.Network Intrusion Monitoring System

3. Construction of Deep Neural Network Detection Model

3.1 Algorithm research

The deep neural network is also called the multi-layer feedforward neural network. The perceptron is the simplest neural network, which consists of the input layer and the output layer, and the deep neural network also adds a hidden layer. Define each neuron input as: $\beta = \sum_i w_i \alpha_i$,and the output is $\chi = f(\beta - \theta)$ .Where w_i is the connection between the neuron and the first neuron in the upper layer network. is the output of the upper layer network and the first neuron. θ is the stimulus threshold. f is the activation function corresponding to the neuron. f has a wide selection range. Commonly there are ReLU functions, tanh functions, and Sigmoid functions. At the same time, each network also has an objective function that needs to be optimized, as shown in Equation 1:

$$L = \frac{1}{m} \sum_{x_{i \in X}} loss(y_i', y_i) \tag{1}$$

Where loss is a loss function, representing the error. $x_i = (x_{i1}, x_{i2}, ...x_{in}) \in R^n$ represents the sample i feature vector. y_i is the expected output vector of sample i,and y_i' represents the actual output vector corresponding to sample i. The goal of applying the neural network algorithm is to obtain the neuron threshold and the connection weight in the network structure, and the average error of the objective function is minimized.

3.2 Neural network structure and intrusion detection model design

The main feature of the deep neural network topology designed in this paper is that before the classification network, the independent component extraction layer and the whitening layer are set, and the features of the high-dimensional space with the current linear correlation action are mapped into independent features in the low-dimensional space, and then used. The resulting low-

dimensional feature set and tag train deep neural network structures.

In the independent component extraction layer and the whitening layer, the neuron threshold is set to 0, and the activation function is y=x. The goal of establishing a whitening layer is to find a linear sub-control that minimizes the Euclidean distance between the spatial feature and the original feature. The goal of the independent component extraction layer is to approximate the negative entropy maximization. Specifically, in the recognition layer, the loss function uses the cross-entropy loss function, inputs the probability of each category, selects the result with the highest probability, and attaches a label as the response result.

The intrusion detection system based on the deep neural network model constructed in this paper is shown in Figure 3. The overall system consists of three modules, the first is the data collection module, which is mainly responsible for capturing the package and obtaining the connection feature value; the second is the processing module, which supports data normalization and attribute numerical processing; It is responsible for analyzing the connection characteristics, determining whether it is an intrusion, and transmitting the intrusion discrimination result to the corresponding response unit.

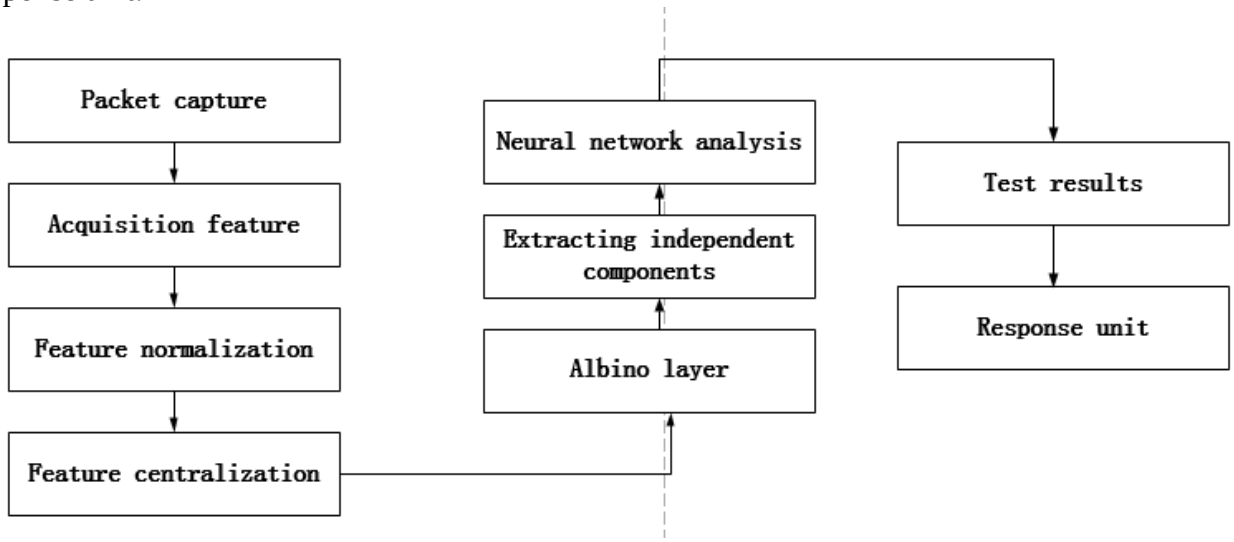

Figure 3.Intrusion Detection System based on Deep Neural Network

4. Application of Deep Neural Network Model in Computer Network Intrusion Detection

4.1 Data preprocessing

In the field of computer network security intrusion detection, KDD99 is a classic data set. In this data set, each anomalous or normal record that is marked has a 41-dimensional feature, a 3-dimensional symbol feature and a 38-dimensional digital feature. Because the CNN input data is required to be floating point data, the range is between 0-1. Therefore, data needs to be preprocessed during intrusion detection. The data preprocessing work studied in this paper will be carried out through MATLAB software, which mainly includes two processing stages.

The first is the digitization of symbolic features. At this stage, it is first necessary to perform binary digital feature conversion on the 3-dimensional symbol feature. The 3-dimensional symbol features mainly include connection errors or correct status flags and network service types. The network service type includes the target host and protocol type. In this study, this paper carries out binary digital feature conversion for three protocol types, ICMP, UDP and TCP. The resulting binary digital feature vectors are $ICMU\{0,0,1\}$, $UDP\{0,1,1\}$, and $TCP\{1,0,0\}$, respectively. Because the stateful flag feature can be extended to a 11-dimensional binary feature; the service type feature can be extended to a 70-dimensional binary feature. Therefore, the KDD99 classic data set can be extended from a 41-dimensional feature to a 122-dimensional feature.

The second is the normalization of digital features. In the CNN model, the required range of input data is 0-1, so all data needs to be normalized during intrusion detection. The main formula is

as follows:

$$y = \frac{y - M_{\min}}{M_{\max} - M_{\min}}$$

Where y represents the data value to be normalized, $M_{\max}$ represents the largest number in a dimension, and $M_{\min}$ represents the smallest number in a dimension. This paper uses the "10% KDD" data in the KDD99 classic dataset for network training, using the data marked correctly for testing. Finally, the test set data and the training set data are uniformly preprocessed, and the obtained data is the input data that satisfies the system requirements.

4.2 Deep neural network experimental process

In the experiment using the deep neural network model, this paper uses a four-layer network structure. This can deepen the number of layers, so that the data features are fully trained, and the training time is too long due to the data layer being too deep. At the same time, in the model selected in this paper, there are also three hidden layers. In the process of selecting network parameters, the output data layer dimension selected in this paper is 5, and the input data layer dimension is 122.

In the training process of DNN model, the loss function selected in this paper is cross entropy. Compared with the variance loss function, the cross entropy can effectively overcome the problem that the weight update speed is too slow. When the error generated is small, the weight update speed will be slower. When the resulting error is large, the update weight will be faster.

In the DNN model training process, the output layer parameter selected in this paper is 0.5. At the beginning of the training, half of the hidden layer units are randomly hidden and the output layer and the input layer are kept unchanged. At the same time, the neural network weight value is updated according to the BP algorithm. This is the first iteration of the update process. When the iteration is updated for the second time, the method does not change, but the hidden hidden layer unit is replaced with the other half. Follow this method in order, until the end of the training. This neural network that performs only half of the hidden layer unit training is called a half network. During the training process, most of the network can get the correct classification results. A small number of erroneous results have less impact on the final experimental results.

4.3 Experimental results

Through experimental research, it is known that among the influencing factors of experimental results, the influence of network parameter selection is small. The experimental results of the pyramid-type network structure are worse than those of the spindle-type network structure. In the KDD99 dataset, there are a total of 250,429 total data, and there are 60,582 normal data, which is much smaller than the attack data. Therefore, it can be concluded that the false positive rate in the experiment is less than the false negative rate. In actual computer networks, the attack data is less than the normal data. Therefore, the actual computer network false positive rate should be much larger than the false negative rate.

References

[1] Xu Z.H.(2016).Research on Improved Algorithm of Distributed Intrusion Detection Model Based on BP Neural Network, Network Security Technology and Application, 16 (2), 77-78.

[2] Zhang S.W., Yang H.L., Zhou F.(2017). Research on Intrusion Detection Method Based on Artificial Neural Network, Journal of Beijing Printing University, 25(07), 142-143+163.

[3] Cui K., Fu L.X., Zhang Y., et al.(2018). Application of BP Neural Network Based on DE Optimization in Intrusion Detection, Software Guide, 17 (07), 177-179+183.

[4] Liu Y.F., Wang C., Zhang Y.B., et al. (2018). Deep Convolution Neural Network Model for Network Intrusion Detection System, Journal of Inner Mongolia University of Science and

Technology, 37 (01), 62-67.

[5] Yang Y.G., Wang Z.Y. (2019). Intrusion Detection Technology based on Deep Neural Network, Network Security Technology and Application, 19 (04), 40-44.

[6] Lv Z.W.(2019).Application of Artificial Intelligence System in Computer Network Security Management, Radio and TV University, 41(01), 16-19+27.

[7] Wang Y., Feng X.N., Qian T.Y., et al.(2018). Camouflage User Intrusion Detection based on CNN and LSTM Deep Networks, Computer Science and Exploration, 12 (4), 575-585.

[8] He Y., Wei C.Q., Lu Y.H. (2016). Text Emotional Analysis based on Deep Neural Network and Topic Model --- Taking the Survey of Tourist Satisfaction of Shanghai Disney Scenic Spot as an Example, Statistical Science and Practice, 35 (12), 17-21.