Application of an improved BP neural network algorithm in intrusion detection

Chen Xuan
Cyberspace Security Institute, University of Shandong Province Key Laboratory of forensic evidence, Shandong University of Political Science and Law, Jinan, China

Abstract—Based on the analysis of the existing problems of BP neural network used in the detection system, on the basis of the traditional BP algorithm, the automatic variable rate learning method is adopted, the forgetting factor and random optimization operator are introduced, and they are used in the network intrusion detection system. The simulation results show that the improved BP neural network algorithm is fast and easy to converge. The algorithm effectively improves the detection rate, reduces the false positive rate and false negative rate, and has obvious advantages.

1. INTRODUCTION

With the development of Internet of Things, cloud computing and the advent of the era of big data, the scale of computer network is becoming larger and larger, and the communication system is becoming more and more complex. Due to the vulnerability of computer network itself and the hacker’s attack on the network, the threats and attacks on computer network are increasing [1-3]. The situation of network security is more and more serious. IDS (Intrusion Detection System) has become a key component of network security system[4]. At present, intrusion detection methods can be generally divided into two categories: misuse detection and anomaly detection. With the help of misuse detection technology, an efficient intrusion detection system can be established. This system has a high detection accuracy, but it can't do anything to the unknown intrusion activity or the variation of known intrusion activity, and it is difficult to extract the attack features, and it needs to update the feature base constantly. The advantage of anomaly detection technology is that it can detect new intrusion attacks. At present, the existing anomaly detection algorithms and models mainly include: statistical anomaly detection, anomaly detection based on neural network and anomaly detection based on data mining[5].

As an important pattern recognition method, artificial neural network has the characteristics of self-learning, self-organization and strong generalization ability [6]. In the intrusion detection system, the application of artificial neural network method can make the system better recognize known attacks, and also has the ability to detect unknown attacks. Many researchers at home and abroad use it in intrusion detection: document [7] uses the method of hybrid clustering and neural network to achieve intrusion detection; document [8] uses the randomized data based on clustering to detect botnet; document [9] uses the deep neural network for the security of the Internet of vehicles; document [10] realizes the intrusion detection based on the deep belief network. There are few researches on Intrusion Detection Based on deep neural network in China. In document [11], the application of deep neural network in big data analysis is described; in document [12], the structure dimension is reduced by two-layer restricted Boltzmann machine, the optimal representation of original data is obtained by BP neural network, and then the data is identified by SVM. However, in the anomaly intrusion detection system, the application
of standard BP algorithm has some shortcomings, such as convergence local minimum, slow learning speed, which greatly affects the performance of the intrusion detection system. Based on the improvement of the original BP neural network algorithm, this paper studies the optimized BP neural network algorithm and its application in network intrusion detection.

2. BP NEURAL NETWORK
BP neural network is a multi-layer feed-forward neural network, which includes two processes of input signal forward transmission and error back propagation. It is generally composed of three layers: input layer, hidden layer, and output layer. Neuron state only affects the next layer of neuron state. It is widely used in BP neural network prediction model. The network structure generally requires only a single hidden layer to approximate any rational function with arbitrary precision. The dimensions of the input and output vectors of the training samples respectively determine the number of neural nodes in the input and output layers of the network. The typical BP neural network structure with only a single hidden layer and a single output is shown in Fig. 1.

![Figure 1. Topological structure of the BP neural network.](image)

In Fig. 1, $x_i = (x_1, x_2, ..., x_n)$ are a set of input vectors of BP neural network; $y$ is the target output value of the network; $w_{ij}$ is the connection weight between the input layer and the hidden layer; $w_{jl}$ is the connection weight between the hidden layer and the output layer; $a_j, b$ are the node thresholds of the hidden layer and the output layer respectively. If the number of nodes in the hidden layer is $m$, then $j = 1, 2, ..., m$, in the forward transmission, the input signal vector $X_i$ is transmitted layer by layer from the input layer to the hidden layer, and finally to the output layer. It is calculated by connecting the weight vector, the threshold vector and the corresponding excitation function of each layer. The predicted output value $y$ of the output layer is obtained. If there is an error between the predicted value $y$ and the target value $y$, the error part is transferred to the reverse layer by layer, and the weight and threshold value of each layer of the network are adjusted along the direction of error reduction. Repeat the above process to make the predicted value of BP neural network approach the actual output value.

3. INTRUSION DETECTION ALGORITHM
Network intrusion detection analyzes system data. Once there is network attack and unauthorized network access, the intrusion detection system will alarm and cut off the intrusion line at the same time. The intrusion detection system shall have the activities of monitoring system and users, analyzing system and user activities, analyzing abnormal behavior patterns, identifying known attack patterns, auditing system weaknesses and structures, tracking management system audits, evaluating the integrity of system and data files, and identifying user behaviors violating security policies. At present, common attacks include unauthorized access, unauthorized access, detection, denial of service, etc. In practice, these attacks vary greatly, and intrusion detection is difficult. BP neural network has strong self-learning and self-organizing ability. After training, BP neural network will summarize and summarize the previously observed intrusion detection behavior patterns, and recognize the observed attacks and new attacks with known attack variation. Fig. 2 shows the intrusion detection process of the network.
4. IMPROVED BP NEURAL NETWORK INTRUSION DETECTION

4.1. The problems of BP neural network used in IDS
BP neural network uses distributed storage, but the traditional BP algorithm has some shortcomings, including minimal local, slow learning convergence speed, the selection of hidden layer nodes lacks theoretical support, the learned samples will be affected by the newly added samples, each sample input must have the same number of features.

In the intrusion detection, the implementation of BP neural network is mainly combined with the existing system, BP neural network and application pattern recognition system, for example, combined with expert system. In this way, BP neural network can be used as a part of the system, usually as an information filtering module or information preprocessing module. When the information is input into the system, the neural network will filter the information. In addition, the neural network can generate rules automatically, and then update the rule base and pattern base of IDS. The self-organizing and self-learning ability of BP neural network enables the trained BP neural network to summarize the previously observed intrusion detection behavior patterns. In addition to identifying the observed attacks, it can also identify new attacks, even new attacks, which are mutated from the known attacks. The advantage of this method is that it can improve the performance of intrusion detection system, but the disadvantage is that the real advantage of neural network can not be fully exploited.

4.2. Improved neural network algorithm
In signal detection, non-linear processing, pattern recognition and other fields, artificial neural network is widely used, because it has very good self-organization and self-adaptability. At the same time, its non-linear characteristics are obvious. The information is stored in distributed mode and can be processed in large-scale parallel. In essence, BP neural network algorithm belongs to the gradient algorithm of nonlinear optimization. In terms of convergence, the algorithm has shortcomings, that is to say, the learning result of the algorithm may fall into the global minimum of mean square error, or the local minimum, which causes the algorithm not to converge and makes the working mode fall into error.

The main function of intrusion detection system is to detect the behavior of intrusion computer network and computer system, including data clustering, data collection, analysis and judgment behavior, response to intrusion behavior, alarm, etc. The neurons in each layer of BP network only connect with the neurons in the adjacent layer; in each layer, there is no connection between neurons; at the same time, there is no feedback connection between neurons in each layer. After the signal is input, it is transmitted to the hidden node, and then the information is transmitted to the output node through the transformation function. After processing, the result is output. Intrusion Detection Based on neural network is based on large sample set for learning and training. Its parameters need to be updated in each iteration, which obviously increases the learning time and system resource consumption. In addition, the learning rate of this method may decrease. In this paper, the BP neural network is improved by using the automatic variable rate learning method, introducing forgetting factor and random optimization operator, and using it in network intrusion detection system.

4.2.1. Using the method of automatic variable rate learning: On the basis of gradient, the traditional BP algorithm adopts the steepest descent LMS learning problem. The learning step size is a small value, and the value is fixed, which is not conducive to network convergence. So we choose to adjust the learning rate automatically based on the gradient direction. In the gradient direction, the learning step is...
determined by the speed. If the two adjacent gradients are in the same direction, the convergence in this direction is favorable; if the two adjacent gradients are in the opposite direction, the convergence in this direction is unstable. According to this rule, the learning step length is determined by two changes of relative gradient. When the two gradients are in the same direction, the learning step increases, and the learning speed in this direction should be accelerated; when the two gradients are in the opposite direction, the learning step decreases, and the convergence speed of the whole network should be accelerated. The adaptive rate adjustment method is as follows:

$$\omega(n+1) = \omega(n) - \eta(n)D(n)$$

(1)

$$\eta(n) = \begin{cases} 1.05\eta(n-1), & \lambda > 0 \\ 0.8\eta(n-1), & \lambda < 0 \end{cases}$$

(2)

Where \(\lambda\) in (2) is the product of gradients at time \(n\) and time \(n - 1\).

4.2.2. Introducing forgetting factor: According to the change of two adjacent gradients, the learning step size algorithm is determined by adaptive variable rate learning method. Change the simple learning rate, at this time, the convergence rate cannot be fully guaranteed, but there will be no oscillation. Therefore, consider the variable rate learning method, add a quantity to the weight adjustment amount, which is proportional to the previous several times of weighting, and the weight adjustment amount is calculated by (3).

$$\Delta\omega(k+1) = \eta(k)(D(k) + \tau^1\Delta\omega(k) + \tau^2\Delta\omega(k-1) + \cdots + \tau^M\Delta\omega(k-M+1))$$

(3)

Where \(\tau\) in (3) is the forgetting factor, and the forgetting factor term is introduced. In the learning process, the effect of equivalent fine-tuning of learning rate can be explained. The function of forgetting factor is to buffer smooth and make the average direction of regulation change towards the bottom.

4.2.3. Introduce random optimization operator: After introducing the forgetting factor and adopting the automatic variable rate learning method, the BP neural network algorithm can fine tune the learning rate, but the shortcomings and limitations of BP neural network still exist. In order to further improve the BP When the network weight error iteration reaches a certain number of times, the convergence is not obvious or the system error function gradient changes several times in a row. This situation shows that the network enters into a state of fatigue and needs to be activated with the help of external driving force. When these two situations occur, the random number with the same dimension as the weight is generated, and the weight and the random number are added directly, Judge the change of system error. If the error is not reduced, continue to generate random number, modify the weight, stop when the error is reduced, and then continue to start BP algorithm from the new weight. The random optimization operator can randomly change the search direction, and the local minimum points are removed. Fig. 3 shows the improved BP algorithm flow chart.
5. SIMULATION EXPERIMENT

Intrusion detection systems for testing and evaluation require standard, reproducible and contain large amounts of intrusive data. In this simulation experiment, the DARPA data set network connection data set is selected as the experimental data. The simulation experiment in this paper is carried out on the Matlab 7.0 experiment platform to verify whether the improved BP neural network algorithm can achieve better results. This article takes 200 training samples as an example, and uses the unimproved BP algorithm network intrusion detection and the improved BP neural network algorithm network intrusion detection model to learn and train, and obtains simulation experiment results. Fig. 4 shows the training accuracy obtained by the two algorithms. From the experimental simulation results of the two algorithms, it can be seen that the improved BP neural network algorithm for intrusion detection is fast, easy to convergence, and the target accuracy is 0.02. In the specified period, the unreformed BP algorithm cannot achieve the specified target accuracy, and it is easy to fall into the local minimum. The improved BP algorithm proposed in this paper has a shorter training period, significantly shorter learning time and good effect.
The criteria for evaluating the detection model are the missing rate, false rate and detection rate, which are defined as follows:

**False Positive rate** = number of normal samples wrongly reported as intrusion / total number of normal samples

**Detection rate** = number of intrusion samples detected / total number of normal samples

**False negative rate** = 1 - (number of intrusion samples detected / total number of normal samples)

Table I shows the comparison results between the unimproved BP algorithm and the improved BP algorithm. From Table 1, it can be seen that the detection rate, false alarm rate and false alarm rate of the improved BP neural network algorithm are 95.18%, 4.21% and 4.62% respectively. The detection rate is 9.65% higher than the unimproved BP algorithm, the false positive rate is 5.22% lower than the unimproved BP algorithm, and the false negative rate is 10.92% lower than the unimproved BP algorithm.

**TABLE I. INTRUSION DETECTION RESULTS OF TWO ALGORITHMS**

| Algorithms          | Number of training iterations | Detection rate | False positive rate | False negative rate |
|---------------------|-------------------------------|----------------|---------------------|---------------------|
| Traditional BP algorithm | 500                           | 85.53%         | 9.43%               | 15.54%              |
| Improved BP algorithm | 500                           | 95.18%         | 4.21%               | 4.62%               |

6. CONCLUSION

Based on the improvement of the original BP neural network algorithm, this paper studies the improved and optimized BP neural network algorithm and its application in network intrusion detection. Based on the analysis of the existing problems of the BP neural network used in the detection system, on the basis of the traditional BP algorithm, the automatic variable rate learning method is adopted, the forgetting factor and random optimization operator are introduced, and they are used in the network intrusion detection system. Simulation results show that the improved BP neural network algorithm is fast and easy to converge, and the target accuracy is 0.02. The algorithm in this paper has obvious advantages, the detection rate of all kinds of intrusion behavior has been significantly improved, the system false Positive rate has also been reduced, the performance of the intrusion detection system has been effectively improved, and the algorithm in this paper has obvious advantages.

ACKNOWLEDGMENT

This work is the middle research result supported by the Scientific Research Project of SDUPSL under contract 2019Z02B.

Sponsorship from: A Project of Scientific Research Project of Shandong University of Political Science and Law (2019Z02B).

REFERENCES

[1] Song Ling, Chang Lei. Application of BP neural network based on mutation particle swarm optimization in intrusion detection [J]. Journal of Intelligent Systems, 2013, 8(6) : 558-563.

[2] Liu Jiankang, Xie Fu, Guo Xuexue. Research on cloud computing intrusion detection technology based on BP neural network [J]. Computer and digital engineering,2014(12) : 2357-2361.

[3] Huang Yukun. Intrusion detection technology based on BP neural network algorithm [J]. Electronic production,2015(10) : 60-62.

[4] K. Elissa, “Title of paper if known,” unpublished.

[5] R. Nicole, “Title of paper with only first word capitalized,” J. Name Stand. Abbrev., in press.

[6] Y. Yorozu, M. Hirano, K. Oka, and Y. Tagawa, “Electron spectroscopy studies on magneto-optical media and plastic substrate interface,” IEEE Transl. J. Magn. Japan, vol. 2, pp. 740–741, August 1987 [Digests 9th Annual Conf. Magnetics Japan, p. 301, 1982].

[7] M. Young, The Technical Writer's Handbook. Mill Valley, CA: University Science, 1989.
[8] Al-Jarrah Omar Y, Alhussein Omar, Yoo, Paul D. Data Randomization and Cluster-Based Partitioning for Botnet Intrusion Detection. IEEE TRANSACTIONS ON CYBERNETICS, 2016.

[9] Kang Min-Joo, Kang Je-Won. Intrusion Detection System Using Deep Neural Network for In-Vehicle Network Security. PLOS ONE 2016.

[10] Kamran Raza, Syed Hasan Adil. Intrusion Detection using Deep Belief Network. 2015.

[11] Zhang Lei, Zhang Yi. Infinite depth neural network method for big data analysis[J]. Computer research and development, 2016, 53(1):68-79.

[12] Chen Tong, Zhou Xiaohui. Deep perceptron prediction model based on BP neural network [J]. Computer and digital engineering, 2019, 47(12):2978-2981+3009.