IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received March 2, 2019, accepted March 10, 2019, date of publication March 26, 2019, date of current version April 13, 2019.

Digital Object Identifier 10.1109/ACCESS.2019.2905812

Research on Detection and Defense Mechanisms of DoS Attacks Based on BP Neural Network and Game Theory

LIJUN GAO[1], YANTING LI[1], LU ZHANG[1], FENG LIN[1], AND MAODE MA[2], (Senior Member, IEEE)

[1]Department of Computer Science and Technology, Shenyang Aerospace University, Shenyang 110136, China
[2]School of Electrical and Electronic Engineering, Nanyang Technological University, Singapore 639798

Corresponding author: Yanting Li (liyantinglovely@163.com)

This work was supported in part by the Aerospace Science Foundation under Grant 20158054008 and Grant 20148001001.

ABSTRACT DoS (Denial of Service) attacks are becoming one of the most serious security threats to global networks. We analyze the existing DoS detection methods and defense mechanisms in depth. In this paper, BP (back propagation) neural networks and game theory are introduced to design detection methods and defense mechanisms for the DoS attacks. The BP neural network DoS attacks detection model uses KDDCUP99 as the dataset and selects multiple feature vectors from the dataset that can efficiently identify DoS attacks by large-scale training, which improves the accuracy of detecting DoS attacks to 99.977%. Furthermore, we use game theory to perform secondary analysis on DoS attacks that are not recognized by the neural network model, so that the detection rate of Dos attacks increases from 99.97% to 99.998%. Finally, we propose a DoS attacks defense strategy based on game theory. The simulation results show that the proposed detection method and defense strategy are effective for DoS attacks.

INDEX TERMS DoS attacks, security, game theory, BP neural network.

I. INTRODUCTION

In 2010, the security annual report of global internet infrastructure released by Arbor Networks showed that the DDoS (Distributed Denial of Service) attack scale exceeded 453.8Gbps for the first time [1]. DoS (Denial of Service) attacks are becoming more and more professional, which has caused great harm to the global network. The detection and defense technologies for DoS attacks are becoming a research hotspot in the field of network security.

The detection model for DoS attacks based on BP (back propagation) neural network has been introduced in [2], which divided the attack types into known (such as imap, nmap, warezaster and land) and unknown (such as smurf, ipsweep, back and Neptune) to train and test respectively. Analysis shows that the model is not ideal to detect two typical Dos attacks smurf and Neptune. The KDDCUP99 dataset and eleven training functions are used to test the effect of BP neural network in intrusion detection for Dos attack in [3]. The detection accuracy of the resilient back propagation algorithm can reach 97.04%. Literature [4] improves the accuracy of the DoS attacks to 97.3% by using RBF (Radical Basis Function) and MLP (Multi-Layer Perceptron) neural network on KDDCUP99 dataset. A two-stage BP neural network intrusion detection algorithm has been proposed in [6]. The same neural network model is used in both phases, but the input fields are different. The model not only reduces the system burden, but also improves the detection accuracy to 99.4%. Literature [7] also uses the two-stage detection method, which combines SVM (Support Vector Machine) and BP neural network to improve the detection accuracy to 99.95%. However, the two-stage detection method does not fully consider the false detection rate in the first detection phase, so that a large amount of attack traffic is mistaken for legal traffic at this stage. A multi-level detection model has been introduced in [8], which is based on the mechanism of the division of labor. The Fuzzy-C-mean clustering, ANN (artificial neural network) and SVM of the model undertake the role of data partitioning, data training and detection respectively. The correct rate of the detecting model

The associate editor coordinating the review of this manuscript and approving it for publication was Jiafeng Xie.

for DoS attacks can reach 99.66%. The protocol proposed in [10] trained BP neural network according to CPU state, data length and request rate. The advantage is that the input attributes are small and the model is simple. However, 96.2% detection rate is not ideal. Literature [11] used the hole-black algorithm to optimize the neural network output function. During the experiment, all the KDD99 attributes were used as input. The experimental results show that the detection rate of DoS attacks is 96.3%. The model in [12] used three BP network structures to detect three common protocols in DoS attacks. They used the data packets generated by the real environment as the experimental dataset, and the correct rate was 98%. The drawback is that the model cannot detect other communication protocols, and as the detection model increases, the training cost increases. Below is some research targeted on feature choices. Literature [13] proposed a DoS attack detection framework based on KDD-NSL dataset. It uses a simplified data set with nine basic attributes and a complete data set with 41 attributes for experimentation. And the experimental results are 93.7852% and 97.2372% respectively. But the model is very complicated because each hidden layer contains 100 nodes. Literature [14] filtered the attributes according to the information gain ratio. The maximum accuracy gained is 98.02% with C4.5 algorithm, and the features number is reduced to 11. In addition to neural network detection algorithms, game theory is also widely used in defense strategies for DoS attacks. A dynamic game method has been proposed in [15] to avoid DoS attacks, in which the defenders use deception to obtain the maximum benefit. The defender uses the honeypot system to confuse the attacker to attract the attack traffic and consumes the attack cost. Furthermore, the defender performs a game based on the complete Bayesian balance theory, and adjusts the communication strategy according to the acquired information to enhance the resistance of the DoS attacks. The protocol in [16] used dynamic game models to resist botnet DDoS attacks. The attacker decides whether to increase the number of participating zombie hosts according to the attack quality. The defender decides whether to start the defense mechanism according to the network load capacity. The experimental results show that the scheme can increase the exposure of the zombie host while ensuring the benefits of the defender. However, the main problem of this scheme is that there is no actual evaluation method for the parameter γ (connection suspiciousness). Literature [17] designed optimization strategies based on specific circumstances. The model adopts a static game method, which is not conducive to update the strategy in real time when the system environment changes. The dynamic game and the static game method are combined in [18], which uses the static game model to set a fixed prior probability for the opponent. In the attack and defense process, the defender uses the dynamic game model to update the trust degree in real time according to the opponent's behavior. All the schemes mentioned above adopt non-cooperative game models. Literature [19] gave a method to make the strategy with the cooperation of both defender and attacker. The attacker determines the distribution and means, the defender determines the detection threshold. In the game progress, both defender and attacker negotiate many times according to their interests and purposes. Analysis shows that the model is too ideal and the practical effect is not good. The protocol in [20] used game means to determine whether to enable IDS (intrusion detection systems) to reduce the resource consumption caused by IDS. Literature [21] calculates the benefits according to the statistics data in the specific network environment to improve the performance and fault tolerance. But the author did not give the data statistics method.

In this paper, we analyze the existing DoS detection methods and defense mechanisms in depth and then propose a DoS attacks intelligent detection/defense system. The contributions and innovations of this paper include four aspects: (1) BP neural network and game theory are introduced to design detection methods and defense mechanisms for DOS attacks; (2) we propose two key parameters, e (evaluation coefficient) and JR (normal traffic judgment rate). At the first stage, the results of neural network calculation are used as evaluation parameters in DoS defense scheme, and then we explained why these two parameters are introduced and how to increase the detection rate. So far, no similar applications have been found in other papers; (3) the features of KDDCUP99 dataset are simplified according to the attack type to reduce the burden of the detection system; (4) the main contribution of the scheme is that the detection rate of DoS attack is improved with the two phases' model. The detection accuracy for DoS attack was improved to 99.998%.

In this paper, we focused on designing the model to reduce the burden of the detection system and improving the detection rate of Dos attacks. And the experimental results are ideal. In addition, the key parameters proposed based on BP neural network also have research value in other classification or prediction fields.

The remainder of this paper is arranged as follows. In section II, we introduce the BP neural network, dataset, and evaluation values mentioned in this paper. Then we introduce the overall architecture of the proposed system in section III and introduce the important parts of this system respectively in section IV and V. In section IV introduce the detection model based on BP neural network and give the experimental process and the results analysis. In section V, we introduce the defense model and describe the related parameters, defense strategy and the experiment results. Finally, we give a conclusion section V and make a plan for future work.

II. PREPARATORY WORKS

A. BP NEURAL NETWORK

The back propagation [22] algorithm proposed by Rumelhart in 1986 is widely used in multilayer feedforward neural network. The BP neural network is a fully connected multilayer feedforward neural network which uses the error back propagation algorithm. It contains input layer, hidden layer,

and output layer. And the neurons in each hidden layer and the output layer have their own thresholds.

Training of BP neural network is a supervised learning process, which is divided into two stages: information forward propagation and error back propagation. In the forward propagation phase, both the hidden layer and the output layer calculate the output result according to the input, connection weight, threshold, and the functions of the previous layer.

If there is a BP neural network model with two hidden layers (the hidden layers have j and l modes, output layer has k nodes) and the input is x_i ($i = 1, 2, 3 \ldots$), the output of the first hidden layer is as follow:

$$a_j = f_1\left(\sum_i \omega_{ij} x_i - \varepsilon_j\right) \tag{1}$$

In equation (1), $f_1(\cdot)$ is the transfer function for this layer. We use the ω denotes the weight between the input layer and the hidden layer and the ε represents the threshold of the first hidden layer.

Similarly, the output of the second hidden layer is as follow:

$$b_l = f_2\left(\sum_j \varphi_{jl} a_j - \mu_l\right) \tag{2}$$

In equation (2), $f_2(\cdot)$ is the transfer function for this layer. We use the φ denotes the weight between the two hidden layers and the μ represents the threshold of the second hidden layer.

Finally, the output of the output layer is as equation (3).

$$y_k = f_3(\sum_l \sigma_{jl} b_l - \vartheta_k) \tag{3}$$

Similarly, $f_3(\cdot)$ is the transfer function for output layer. We use the ω denotes the weight between the input layer and the hidden layer and the ε represents the threshold of the first hidden layer.

After getting the result of the output layer. The error is calculated based on the expected output. Assuming the input sample is p, the expected output is E_p, and the actual output is Y_p. The error of the output layer of p is as follow:

$$E_p = \frac{1}{2}\sum_k (y_{pk} - Y_{pk})^2 \tag{4}$$

After obtaining the mean square error, the training process of the BP neural network enters the second phase, the error back propagation phase. At this point, the BP neural network performs error reversal adjustment based on whether the mean square error is expected. The parameters of the first round are performed as follows:

1) Give error E_p and learning rate η;

2) Calculate the gradient terms of output layer and hidden layers: δ, ξ_1, ξ_2;

3) calculate the adjustment range of each parameter: $\Delta\varepsilon, \Delta\mu, \Delta\vartheta, \Delta\omega, \Delta\varphi, \Delta\sigma$;

4) The weight and the threshold are adjusted in the same way as "$A + \Delta A \rightarrow A$".

The back propagation method adjusts the threshold and the weight according to the above steps from the output layer to the previous layer to reduce the output error. If the error reaches the expected goal, the training is over.

During the training of BP neural network, the training function, transfer functions and performance function are very important. Therefore, choosing the right training method is the key problem. A BP neural network with two hidden layers is proposed to detect DoS attacks, distinguish legitimate traffic and illegal traffic. The detailed experimental process and parameters chosen will be described in detail in Section IV.

B. KDD CUP 99 DATASET [23]

The KDD CUP 99 is a generic dataset for network security. It contains 22 attack types and one normal type. The kddcup_data_10_percent dataset has approximately 500,000 records. Each record is represented by 41 attributes. Together with the final flag attribute, there are 42 attributes. These attributes are used to represent the basic feature, content feature, and traffic feature of network connection. In this paper, we only focus on DoS attack, and there are six types that belong to DoS attack in dataset, they are PoD, Land, Smurf, Teardrop, Back and Neptune. We briefly describe these types of attack as follows:

1) PoD (Ping of Death): In the TCP/IP system, the maximum size of legal packet is 65535 bytes. If the attacker deliberately sends IP packets larger than that, the receiver will crash because of buffer overflow;

2) Land: This attack uses an empty connection where both the source and destination addresses are its own IP addresses. The attacked computer will continually responds to itself and consuming system resources until it crashes;

3) Neptune: This attack is synonymous with SYN Flood and it is a typical type of DoS attack. The attacker exploits the flaws in the TCP protocol and sends a large number of bogus TCP connection requests. Then the attacked sever cannot respond to normal requests because the TCP connection resource is exhausted;

4) Back: This attack is also a flood attack similar to Neptune's principle;

5) Smurf: This attack combines IP spoofing with echo request of ICMP protocol. The attacker will flood the target system with massive network traffic and then the target system will cannot provide services to normal users;

6) Teardrop: The attacker carries out this attack by sending abnormal fragmented packets to target system. And then the receiver will crash when these packets cannot be reassembled because the packets overlap one another.

In this paper, we select the appropriate features of these attacks and use the corresponding data for experimental.

C. EVALUATION OF EXPERIMENT RESULTS

In this paper, we conduct two stages of experiment and adopt several numerical values to evaluate the experimental results.

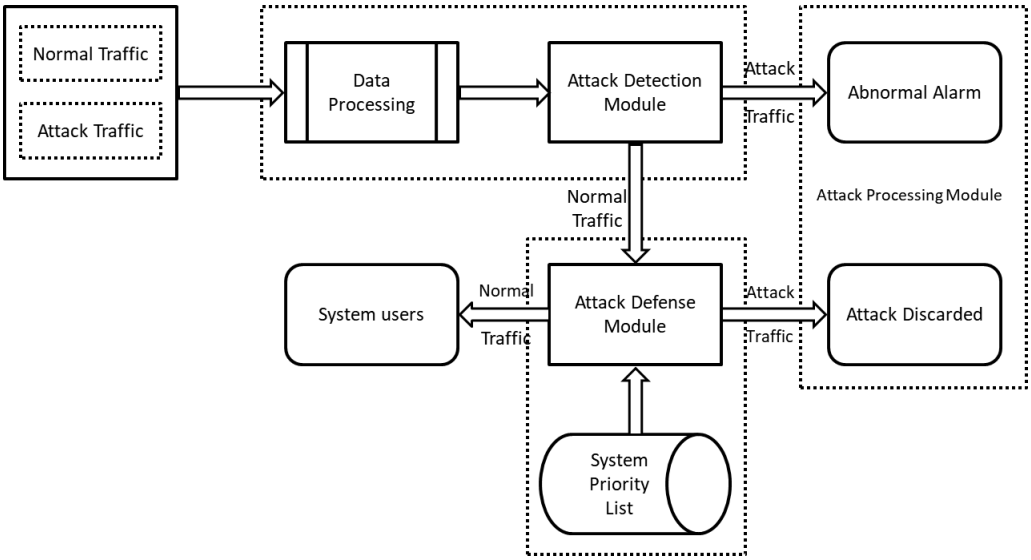


FIGURE 1. The overall structure diagram of system.

We listed these values and giving the method of calculation as follows:

1) ARR

ARR is the attack rejection rate which only used in defense stage and its calculation method is as equation (5).

$$ARR = \frac{rejection\ number\ of\ attack}{wrong\ number\ of\ attack\ in\ detection\ stage} \tag{5}$$

2) ADR

ADR is the attack detection rate and it is used in both two experiments. ADR is calculated according to the equation (6) in the first stage and .according to the equation (7) in the second stage.

$$ADR = \frac{correct\ number\ of\ attack}{total\ number\ of\ attack} \tag{6}$$

$$ADR = \frac{correct\ number\ of\ attack + wrong\ number\ of\ attack \times ARR}{total\ number\ of\ attack} \tag{7}$$

3) ANDR

ANDR is the actual normal data ratio and it is an important parameter in both two experiment and defense strategy. Its calculation method is as equation (8).

$$ANDR = \frac{correct\ number\ of\ normal}{correct\ number\ of\ normal + wrong\ number\ of\ normal} \tag{8}$$

III. INTELLIGENT DETECTION/DEFENSE SYSTEM

In this paper, we propose an intelligent detection/defense system based on BP neural network and dynamic game theory for DoS attacks. The system includes three modules: attack detection module, attack defense module and attack processing module. The overall structure of the system is shown in Figure 1.

The system takes the traffic of DoS attacks and the traffic of legitimate user as input. Then, the two types of traffic are analyzed and judged by the attack detection module and the attack defense module, and the results are used as a reference for the processing module. The basic functions of each module are as follows:

1) Attack detection module: The module includes two parts: data processing and attack detection. Data processing is used to analyze the traffic characteristics required for detection, and twelve eigenvalues are generated as input for the attack detection phase. In the attack detection phase, the BP neural network model trained is used to divide the input traffic into attack traffic and legal traffic. In addition, the evaluation coefficients are added to determine the legal traffic. Finally, the attack detection module transmits the legal traffic determination result and the evaluation coefficients to the attack defense module. The evaluation coefficients refer to the intermediate value generated during the neural network detection module, which is significant for legality detection of traffic;

2) Attack defense module: The attack defense phase uses a dynamic game strategy to filter attack traffic based on the traffic credibility (calculated from the evaluation coefficients and the system priority) and the detection rules. At the same time, the defense module can adjust the decision rules according to the attack and defense status. The dynamic adjustment strategy is given in section V. Eventually, the attack defense module receives the legitimate traffic and transmits it to the user;

3) Attack processing module: This module is used to process the attack traffic sent from the attack detection module

TABLE 1. The filtering results of features.

Attack types	Name of features	value
POD	protocol_type	ICMP
	Service	ecr_i
		tim_i
	src_bytes	564
		1480
Land	land	1
Smurf	service	ecr_i
	src_bytes	520
		1032
Teardrop	protocol_type	UDP
	service	private
	src_bytes	28

and the attack defense module, and make different responses according to different sources. When the attack traffic is received from the attack detection module, the system will send an abnormal alarm to remind the user of the attack. When the attack traffic comes from the attack defense module, the system will discard it directly without warning.

IV. DETECTION MODEL BASED ON BP NEURAL NETWORK

In this section, the neural network model based on back propagation is used to train and test the selected experimental data. And then, the optimized neural network model is established by adjusting the number of hidden layers and the number of neurons in each layer according to the experimental results.

A. DATA SELECTING AND PREPROCESSING

Each feature has different meanings for detecting different types of attacks in KDD CUP 99 dataset. Because this paper is aimed at analyzing DoS attacks, we only filter the attributes related to DoS attacks.

The different attack types correspond to different feature fields. First, the feature fields are filtered according to the types of attacks. The screening results are shown in Table 1.

As can be seen from Table 1, more than 99.5% DoS attacks of PoD, Smurf, Teardrop and Land can be screened intuitively with the four fields: protocol_type, service, src_bytes and land.

The other two attacks, back attacks and neptune attacks, have no significant feature fields. However, the connection number of neptune attacks is very large. After removing the fixed fields, we select another 8 fields as input of the experiment according to the DoS attack features. Finally, the selected 12 feature fields are: protocol_type, service, flag, duration, src_bytes, dst_bytes, land, count, sry_count, dst_host_count, dst_host_same_src_port_rate and dst_host_srv_diff_host_rate. Since the values of the first three fields are non-numeric, they cannot be used as the input of the neural network directly. We will replace it according to certain rules, and replacement method is as follows:

a. Protocol_type: The field indicates the protocol type. There are three values: TCP, UDP, and ICMP. We use ICMP=1, TCP=6, UDP=17 to mark the three protocol types.

b. Service: This field indicates the service type of the target host. There are 70 service types. We use Ftp=21, bgp=179, smtp=25, telnet=23 to mark the server port number of different types;

c. Flag: This field indicates that the connection status is normal or incorrect. We mark the 11 flags with numbers, such as SF=0, S1=1, REJ=100;

Firstly, we randomly selected 119476 DoS attacks data as the training sample set according to the attack type, including 1682 back attacks, 14 land attacks, 32987 neptune attacks, 82 POD attacks, 84848 smurf attacks, and 317 teardrop attacks. Secondly, we use the same method to extract another 29,870 DoS attack data as a test sample set, in a ratio of 4:1, including 421 Back attacks, 3 land attacks, 8225 neptune attacks, 20 POD attacks, and 21121 smurf attacks and 80 teardrop attacks. Finally, we extracted 56980 and 14245 normal data for neural network training and testing respectively.

B. EXPERIMENTAL AND RESULT ANALYSIS

We select 12 feature fields as the input of the neural network according to the analysis results in part B of this section. If the output is equal to 1, it is attack data. If the output is equal to 0, it is legal data. The proposed neural network model has one input layer (12 nodes), one output layer (1 node, the result is 0 or 1) and one or more hidden layers. We select 119476 attack data and 56980 legal data to train the BP neural network, and use MATLAB R2016 as the simulation tool. Single, double and triple layer neural network are used in the training, and the number of nodes in each layer is also dynamically adjusted. We will test the neural network model with 29870 attack data and 14245 legal data when each network model ends training. The experimental results of neural network with different hidden layers and different number of nodes are shown in Figure 2. And we listed the used structures and their correct rate in x-axis. The (a, b, c) format is used to represent the hidden layer structure of the neural network, where a is the number of nodes in the first layer, b is the number of nodes in the second layer, and c is the number of nodes in the third layer.

The experimental results show that when the BP neural network has two hidden layers, the node number in the first layer is 15, and the node number in the second layer is 5, the detection accuracy rate is the highest 99.977%. So we decided to use the BP neural network model of this structure. The final structure of our model is shown in Figure 3, and the related parameters are listed in Table 2.

In the final BP neural network model, we use the Levenberg-Marquardt algorithm as the training function. This algorithm is combined the advantages of Gauss-Newton and Steepest Descent algorithms. And [6] gave a comparison among Resilient Backpropagation, Levenberg-Marquardt and Radial Basis Function, the results proved the

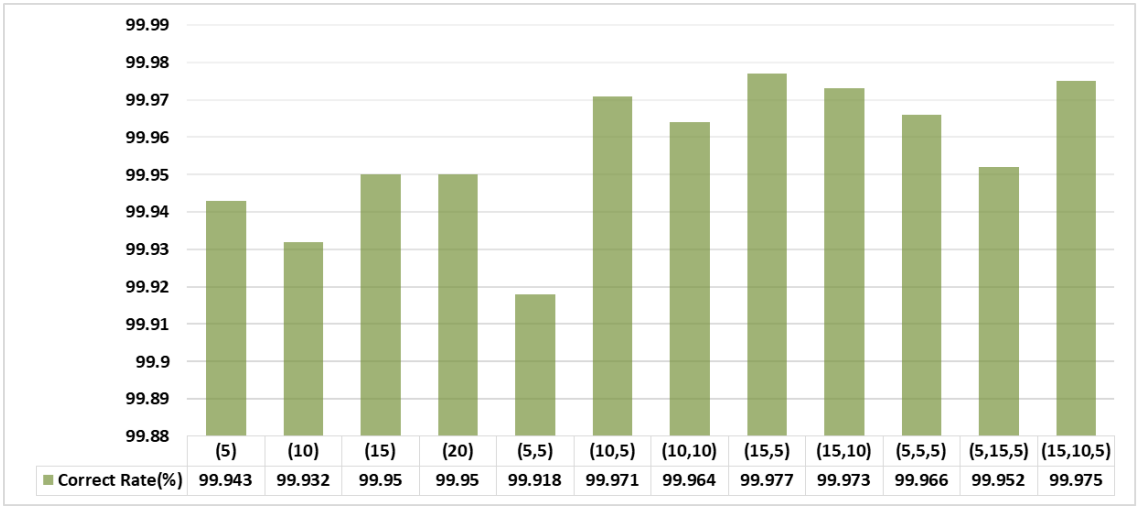


FIGURE 2. Experimental results of every BP neural network model.

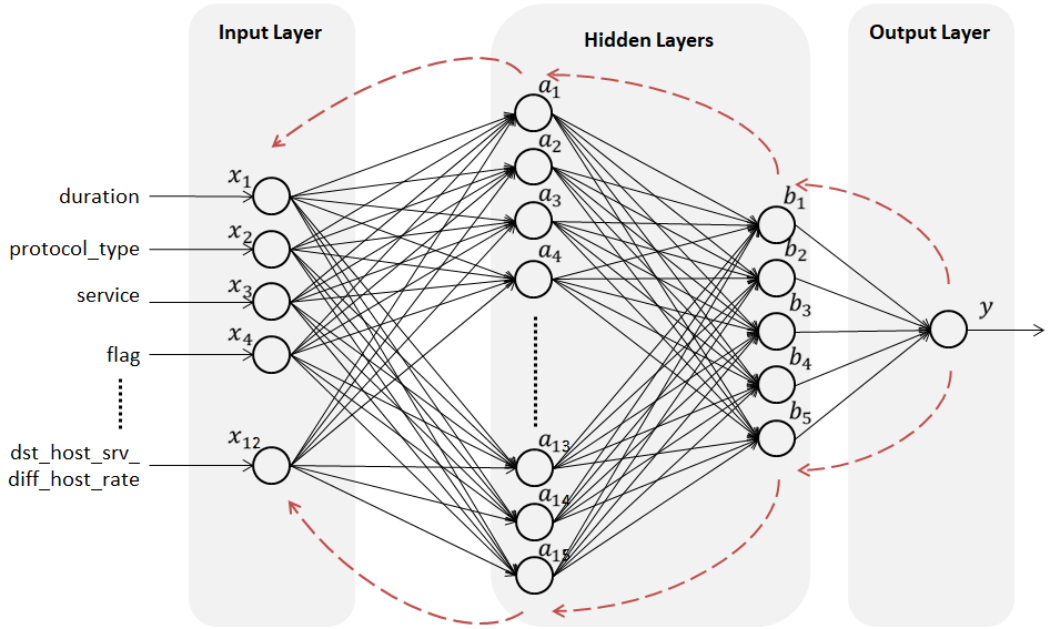


FIGURE 3. Final structure of BP neural network.

Levenberg-Marquardt algorithm had a better performance in detection rate. According to the characteristics of this algorithm, the learning rate parameter Mu should be kept relatively small, so we set the initial value of Mu to 0.001, and we adopt the default values for Decrease Ratio and Increase Ratio in MATLAB. Otherwise, we use the transfer function tansig for both hidden and output layers. This function converges faster than sigmod and we normalized the values before training in order to prevent the function from reaching saturation. For our network, the equations for output of each layer are same as equation (1), (2), and (3). And we specify the number of nodes in each layer ($i = 12, j = 15, l = 5,$ and $k = 1$). Finally, we use 0.5 as the threshold in the BP neural network model. And if the result is not less than 0.5, the output is 1, otherwise the output is 0. The experimental results also show that the setup is suitable.

We compared this result with the existing research. The comparison is shown in Table 3. The statistical results of the detection rate are shown in Figure 4 according to the year. In table 3, the research scheme of [3], [8], and [9] have high detection rate relatively, but [3] used 30 features and [9] used 35 features. In our scheme, we used only 12 features as the inputs. In addition, we only use a simple BP neural network, but [8] used a multi-level detection model

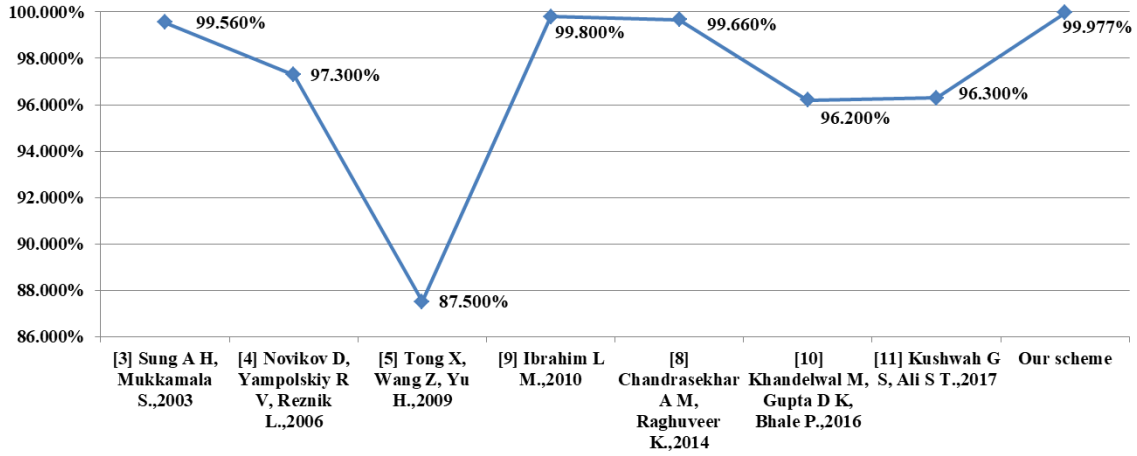


FIGURE 4. Comparison between our scheme and other schemes.

TABLE 2. BP neural network parameters.

Training Function	Levenberg-Marquardt
TransferFcn	tansig
Performance Function	Mean Squared Error
Mu Decrease Ratio	0.1
Mu Increase Ratio	10
Mu	0.001
Maximum Validation Checks	6

TABLE 3. Comparison between our scheme and other schemes.

Research Scheme	Type of model	dataset	Detection rate for DoS
[3] Sung A H, Mukkamala S.,2003	SVM	KDDCUP99	99.56%
[4] Novikov D, Yampolskiy R V, Reznik L.,2006	RBF	KDDCUP99	97.3%
[5] Tong X, Wang Z, Yu H.,2009	RBF/Elman	DARPA	87.5%
[9] Ibrahim L M.,2010	DTDNN	KDDCUP99	99.8%
[8] Chandrasekhar A M, Raghuveer K.,2014	FCM Clustering ANN SVM	KDDCUP99	99.66%
[10] Khandelwal M, Gupta D K, Bhale P.,2016	BP neural network	Simulation traffic	96.2%
[11] Kushwah G S, Ali S T.,2017	Black-hole optimized ANN	KDDCUP99	96.3%
Our scheme	BP neural network	KDDCUP99	99.977%

including Fuzzy-C-mean clustering, ANN and SVM. So, the comparison shows that the detection rate for DoS attacks is significantly improved with our scheme. And the proposed neural network model is simple with few input attributes. Of course, since we use a standard dataset KDD CUP 99, this is also a reason for the high accuracy. However, we chose the similar schemes for comparison. Therefore, there are obvious advantages in training efficiency and detection efficiency.

In order to further analyze the test results, we counted the various test results in detail, as shown in Table 4. According to the data in Table 4, we obtained the *ADR* and *ANDR* according to the equation (6) and (8), which are 99.97% and 99.937% respectively. The *ADR* of this model is 99.970%, that is, there is still attack traffic which is mistaken for legal traffic. As we all know, DoS attacks traffic is very large, so there are still a lot of missing net fish after the detection. To solve the problem, a defense strategy based on game theory is proposed to reduce the throughput rate of attack traffic to protect users to the maximum extent.

V. DEFENSE MODEL BASED ON GAME THEORY

Game theory is a mathematical method for describing and solving game problems. The main research question is both parties with conflicts of interest how to choose their respective strategies or behaviors under certain conditions. The choice can be one or many times, namely static game and dynamic game. According to whether there is a cooperative relationship between the two parties, it can be divided into cooperative game and non-cooperative game. In the network attack and defense process, there are two entities: the attacker and the defender. They adopt corresponding attack and defense strategies according to their own system conditions, which is very similar to game theory. Therefore, game theory model can be used to design attack and defense strategy. Based on the detection model proposed above, we design a second dynamic screening model to reduce the false positive rate of attack traffic. Firstly, the defense scheme proposes the concept of the evaluation coefficient (e) based on the previous

TABLE 4. Statistical table of the optimal network model test results.

Type of attack	Number of training data	Number of testing data	Number of correct	Number of wrong	Correct rate (%)
Normal	56980	14245	14244	1	99.993
Attack	119476	29870	29861	9	99.970
Back	1682	421	421	0	100
Land	14	3	3	0	100
Neptune	32897	8225	8222	3	99.964
POD	82	20	18	2	90
Smurf	84484	21121	21120	1	99.995
Teardrop	317	80	77	3	96.25
Total	176456	44115	44105	10	99.977

BP neural network detection results, and gives the calculation method of the credibility evaluation value (C). In the defense process, the dynamic game adjustment of the defense strategy is realized by comparing the connection acceptance rate (PR) with the legal judgment rate (JR). Finally, the benefits of both the attacker and defender, the ratio of the rejected attack traffic and the legitimate traffic are used to identify the defense effect.

A. BENEFIT OF ATTACKER AND DEFENDER

The method of the benefit calculation of the attacker and defender is as follows and the notations used in this section are listed in Table 5.

1) BENEFIT OF ATTACKER

The purpose of DoS attacks is to encroach on the resources of legitimate users, so that the defender has no chance to handle the request of the legitimate user or cause the system to crash. During the attack process, the attacker's benefits involve five parts, which will be introduced in turn.

a: THE RATIO OF ATTACK PACKETS TO TOTAL PACKETS

When attacking, the attacker sends a large number of attack packets, which are mixed with the legitimate packets and cause a lot of extra bandwidth consumption. It can be seen that if the ratio of attack packets to total packets increases, the more defense bandwidth is consumed by the attacker, the more positive benefit the attacker obtains. The calculation method is:

$$X_1 = \frac{N_a}{N_n + N_a} \tag{9}$$

In equation (9), N_a represents the number of attack packets and N_n represents the number of normal packets. Obviously, this calculation method only takes into account the current defense stage. But in fact, there are 99.970% attack packets that have been rejected during the detection phase of the BP neural network model. After considering the detection and defense stages, its calculation method is:

$$X_1 = \frac{N_a/R_{ap}}{N_n/R_{np} + N_a/R_{ap}} \tag{10}$$

In equation (10), R_{ap} is the pass rate of attack packets in the detection module and R_{np} is the pass rate of normal packets in the detection module.

TABLE 5. The notations and their meanings.

N_a	the number of attack packets
N_n	the number of normal packets
R_{ap}	the pass rate of attack packets in the detection module
R_{np}	the pass rate of normal packets in the detection module
N_{nd}	the number of normal packets that are denied in defense module
N_{ad}	the number of attack packets that are denied in defense module
a	the number of attack nodes
$E(a)$	the expected transmission rate of each attack node
N_{ap}	the number of the attack packets received in the defense strategy
t	the average service time of the system
T	the time complexity of the defense strategy
O	the space complexity of the defense strategy
ω_i, φ_i	the ith weight of the benefits for attacker or defender
X_i, Y_i	the ith benefit of the attacker or defender
U_a, U_d	the total benefit of the attacker or defender

b: THE DENIAL RATE OF NORMAL PACKETS

There is a possibility of misjudgment in the defense strategy, in which case the legitimate packets will be discarded. This is what the attacker wants to see, so the discard rate of legitimate packets is also the positive benefit of the attacker. Its calculation method is:

$$X_2 = \frac{N_{nd}}{N_n} \tag{11}$$

In equation (11), N_{nd} represents the number of normal packets denied in defense module.

At the same time, It's possible that the legitimate data packets are misidentified as illegal in detection model. In section IV, the false rate is calculated based on the experimental results. Considering the detection and defense stages, the calculation method becomes the following equation:

$$X_2 = \frac{\frac{N_n}{R_{np}} * (1 - R_{np}) + N_{nd}}{N_n/R_{np}} \tag{12}$$

c: THE DENIAL RATE OF ATTACK PACKETS

The main purpose of the defense scheme is to discard attack packets, which is a negative benefit for the attacker. The calculation method becomes the following equation:

$$X_3 = \frac{N_{ad}}{N_a} \tag{13}$$

In equation (13), N_{ad} represents the number of attack packets that is denied in defense module.

d: THE AMOUNT OF ATTACKER'S BANDWIDTH CONSUMED BY ITSELF

When attacking, the attacker sends a large number of attack packets. It not only consumes the defender's bandwidth, but also consumes the attacker's. So it is a negative benefit for the attacker. The calculation method is:

$$X_4 = a \cdot E(a) \tag{14}$$

In equation (14), a represents the number of attack nodes and $E(a)$ is the expected transmission rate of each attack node.

e: THE TOTAL SERVICE TIME CONSUMED BY THE ATTACKER

$$X_5 = N_{ap} \cdot t \tag{15}$$

In equation (15), N_{ap} is the number of the attack packets received in the defense strategy, t is the average service time of the system. From the above, the benefit of the attacker in the defense phase is:

$$U_a = \omega_1 X_1 + \omega_2 X_2 - \omega_3 X_3 - \omega_4 X_4 + \omega_5 X_5 \tag{16}$$

In equation (16), ω_1, ω_2, ω_3, ω_4, ω_5 are the weight of the corresponding benefits.

2) BENEFIT OF DEFENDER

The purpose of the DoS attack defense strategy is to identify suspicious user requests to refuse or reduce the service time and service number to ensure the rights of legitimate users. In the defense process, the benefits of the defender also include five parts, which will be introduced in turn.

a: THE RATIO OF NORMAL PACKETS TO TOTAL PACKETS

When there is no attack, all the packets in the network are legitimate packets. However, the ratio of normal packets will reduce due to the attack traffic, which means that the defender's benefits are proportional to the ratio of the legitimate packet to the total packet. This is the positive benefit for the defender. Its calculation method is:

$$Y_1 = \frac{N_n}{N_n + N_a} \tag{17}$$

Obviously, same as the attacker's benefit, the calculation method only takes into account the current defense stage. But in fact, there are a small number of normal packets that have been rejected during the detection phase of the BP neural network model. After considering the detection phase and the defense phase, the calculation method becomes the following equation:

$$Y_1 = \frac{N_n/R_{np}}{N_n/R_{np} + N_a/R_{ap}} \tag{18}$$

In equation (18), R_{ap} is the pass rate of attack packets in the detection module and R_{np} is the pass rate of normal packets in the detection module.

b: THE DENIAL RATE OF ATTACK PACKETS

The discard rate calculation method of the legal data packets is consistent with X_2. It is the positive benefit for the defender. Its calculation method is:

$$Y_2 = \frac{N_{ad}}{N_a} \tag{19}$$

Similarly, after considering the detection and defense modules, the calculation method becomes the following equation:

$$Y_2 = \frac{\frac{N_a}{R_{ap}} * (1 - R_{ap}) + N_{ad}}{N_a/R_{ap}} \tag{20}$$

c: THE DENIAL RATE OF NORMAL PACKETS

The denial rate calculation method of normal packets is consistent with X_3. It is the positive benefit for the defender. The calculation method is:

$$Y_3 = \frac{N_{nd}}{N_n} \tag{21}$$

In the same way, after comprehensive consideration of the detection and defense stages, the calculation method becomes the following equation:

$$Y_3 = \frac{\frac{N_n}{R_{np}} * (1 - R_{np}) + N_{nd}}{N_n/R_{np}} \tag{22}$$

d: THE COST OF IMPLEMENTING THE DEFENSE STRATEGY

The defense strategy will consume the time and space of the defender, which is proportional to the number of packets. Therefore, the consumption of the defense strategy is a negative benefit of the defender, and its calculation method is:

$$Y_4 = (T + O) \cdot (N_n + N_a) \tag{23}$$

In equation (23), T and O represent the time and space complexity of the defense strategy respectively.

e: TOTAL SERVICE TIME CONSUMED BY THE ATTACKER

The calculation method of the total service time consumed by attacker is consistent with X_5, and it is a negative benefit of the defender, and its calculation method is:

$$Y_5 = N_{ap} \cdot t \tag{24}$$

In summary, the benefit of the defender is:

$$U_d = \varphi_1 Y_1 + \varphi_2 Y_2 - \varphi_3 Y_3 - \varphi_4 Y_4 + \varphi_5 Y_5 \tag{25}$$

In equation (25), φ_1, φ_2, φ_3, φ_4, φ_5 are the weight of the corresponding benefits.

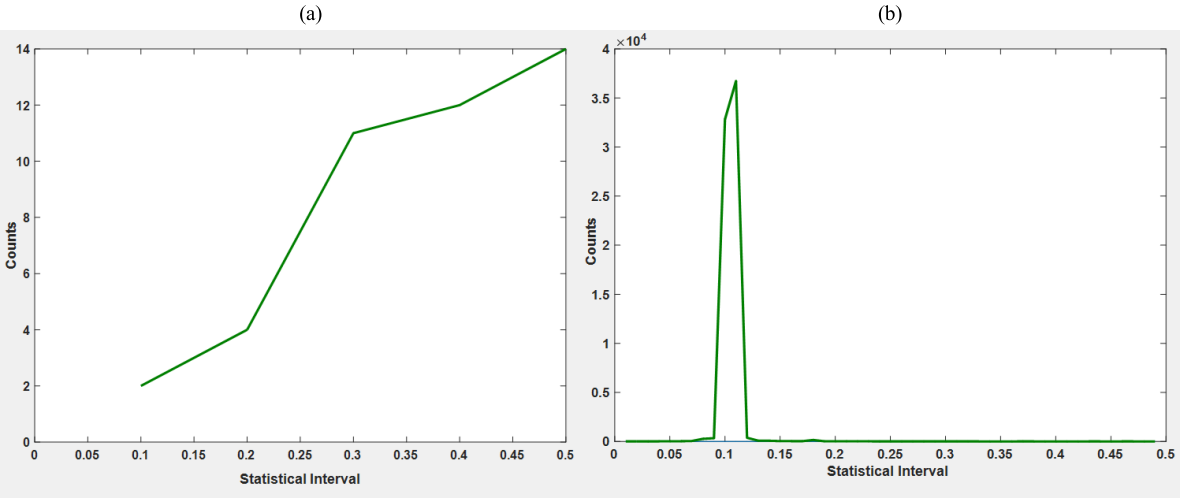


FIGURE 5. Distribution of the actual output result with values less than 0.5. (a) Actual attack data. (b) Actual normal data.

B. THE SCHEME OF DEFENSE

1) THE CREDIBILITY EVALUATION VALUE (C)

The (C) is used to evaluate the credibility of the user request, which is calculated by the evaluation coefficient (e) and the system priority (p).

a: EVALUATION COEFFICIENT (e)

In fact, evaluation coefficient (e) is the actual output calculated by BP neural network. We use 0.5 as the threshold in the BP neural network model. And if the result is not less than 0.5, the output is 1, otherwise the output is 0. In other words, the output value which is determined to be a legitimate traffic packet is less than 0.5. The segmentation statistics of the output values of legal traffic are shown in Table 6 and Figure 6.

The statistical results in Table 6 show that when the output threshold is 0.12, the ratio of normal flow is 99.8%. If the threshold is raised to 0.2, the ratio of normal flow will increase to 99.8%. Less than 14% of attack traffic are misidentified as legitimate traffic when the threshold is 0.2. Similarly, the segmentation statistics are given in Figure 5. It is easy to find that the outputs of legitimate traffic are mostly concentrated between 0.08 and 0.12, while the outputs of attack traffic tend to be 0.5. The results show that the closer the output result is to 0.5, the easier it is to be judged as the legitimate traffic in the neural network detection stage. After the analysis, the concept of the evaluation coefficient is proposed, denoted as e, e is always less than 0.5. Moreover, the closer the evaluation coefficient is to 0.5, the lower the reliability of the connection. The evaluation coefficient e links the detection model of the neural network with the defense scheme based on the game theory, and provides an important reference for designing the defense scheme.

TABLE 6. Statistical of the actual output result with values.

Range	Actual Normal Data Ratio	Actual Attack Data Ratio
<0.12	99.197%	6.977%
(0.12,0.2)	0.608%	6.977%
(0.2,0.5)	0.176%	86.047%

b: SYSTEM PRIORITY (p)

The system priority is set by the defender. It can be dynamically adjusted based on the number of user connection requests. Furthermore, the connection request is sorted to generate a request queue according to the priority. We divide the adjustment of priority p into two parts:

i. Request processing: When there is a user request, the system queries the corresponding priority according to the user information, and then adjusts the priority according to the requested quantity within T time;

ii. Periodic adjustment: The system will periodically traverse the system priority list at the time interval of T. If there is no connection request received within T time, its priority is raised.

2) INTELLIGENT DEFENSE SCHEME

The defense scheme is based on the previous BP neural network detection model. The defense system determines whether the user connection request is accepted according to the credibility (C) and the decision criterion (J). The defense rules are also dynamically adjusted based on the legal traffic rate (JR). The judgment rules (J), the legal judgment rate (JR), and the defense strategy are defined as follows.

a: JUDGMENT RULES (J) AND LEGAL JUDGMENT RATE (JR)

The legal judgment rate (JR) is a constant, which comes from the experimental results of the neural network

detection model in section IV. We have calculated the *ANDR* in section IV, which represents the ratio of actual legal traffic to detecting legitimate traffic. It will be introduced into the defense strategy as a reference for dynamic adjustment. When the ratio of the connection request accepted by the defense system is larger than *JR*, it is believed that the accepted request number by the system has been exceeds the number of the actual legitimate request, that is, attacker's requests have been accepted by defender. It is necessary to strengthen the defense strategy and make the judgment standard stricter. Therefore, the judgment rules (J), as a threshold for judging whether the request is acceptable. It can be dynamically adjusted according to the current defense results.

b: DEFENSE STRATEGY

When the connection requests are sent by normal users or attacker, they enter the DoS attack detection model firstly. If the connection request passes the detection model, it will enter the defense model to accept the second determination. Each connection request passed the DoS attack detection model has own evaluation coefficient (e) and related request information. The corresponding system priority (p) can be obtained according to the IP address, and then the credibility (C) can be calculated based on the evaluation coefficient (e) and the system priority (p). Finally, the defense system decides whether to accept the connection request based on the judgment rules (J). At the same time, according to the acceptance rate, the defense system will make a dynamic adjustment for the judgment rules (J) after each time decision. The connection acceptance rate is the ratio of the number of connections accepted by the defense system to the number of processed connections. The defense system will make the judgment standard stricter to strengthen defense capabilities when the acceptance rate exceeds the judgment criteria (J). The process of defense strategy is shown in figure 6.

C. EXPERIMENTAL AND RESULT ANALYSIS

In this section, the simulation experiment is performed according to established defense strategy and parameters by MATLAB R2016. During the experiment, the ratio of normal data to attack data in the input dataset is equivalent to the neural network detection phase, which is beneficial to ensure the seamless connection between the detection model and the defense model to increase the credibility of the detection results. After the simulation, we made a statistical analysis in four aspects: attack rejection rate (*ARR*) in defense stage, attack detection rate (*ADR*) in detection and defense stages, actual normal data ratio (*ANDR*), and benefits of attacker and defender. The experimental results show that the model parameters are reasonable, and the defense results have been greatly improved compared to the first stage. The attack traffic rejection rate in the defense phase is shown in Figure 7. If the defense policy is not used, the attack traffic in this phase will be fully accepted (rejection rate is 0%). After using the

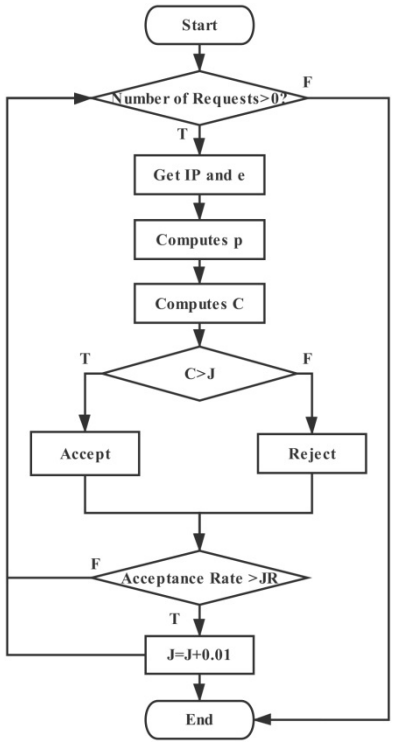


FIGURE 6. The flow chart of defense strategy.

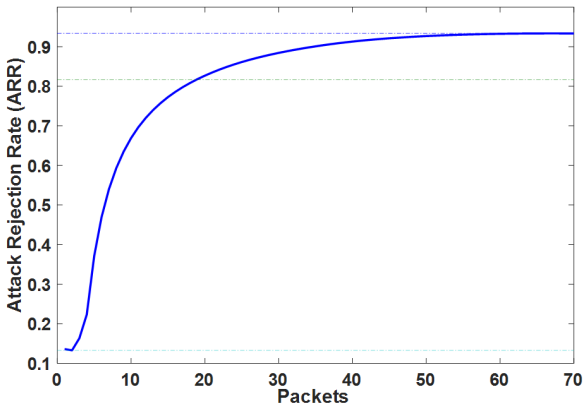


FIGURE 7. The change of ARR in defense stage.

defense strategy, the average ARR in this stage can reach 81.63% and stabilize at 93.36%.

The experimental data of neural network detection phase and game theory defense phase showed that the attack detection rate increased from 99.97% in the first phase to 99.998%. The change in the benefits of attacker and defender is shown in Figure 8.

After introducing the two-stage detection and defense model the rejection rate of attack traffic has increased, which leads to a significant increase in the pass rate of the legitimate traffic. In addition, the benefits of the attacker continue decreasing; the benefits of the defender grow steadily. It can be seen that the model we designed has achieved the expected results.

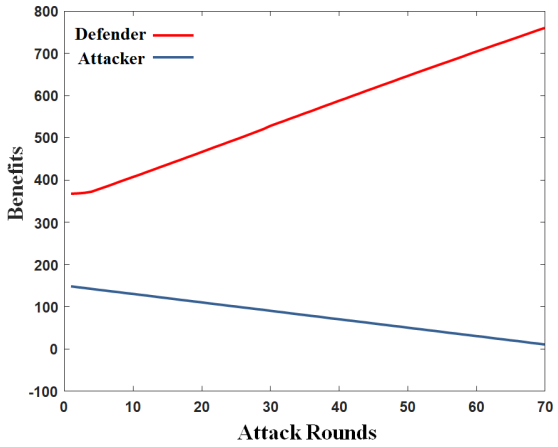


FIGURE 8. The benefits on attacker and defender.

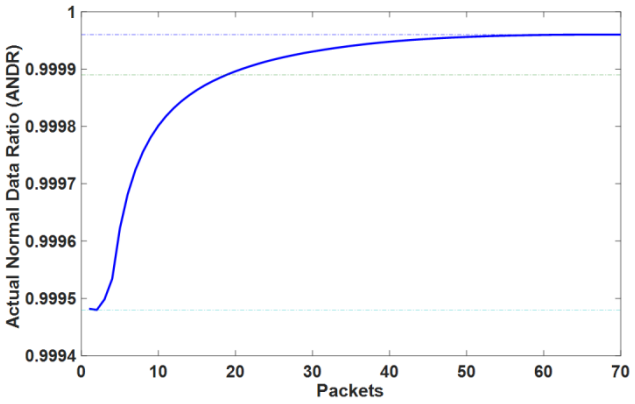


FIGURE 9. The change of ANDR in defense stage.

Figure 9 shows the change in the ratio of the legal traffic. The simulation results clearly show that after using the defense strategy, the ratio of the normal data entering the system increases from 99.937% in the first stage to 99.95%, and finally stabilize at 99.997%.

Of course, we only did the experiments in the simulation environment, so the effect of our scheme in the actual environment needs to be further confirmed and this is one of our future works.

VI. CONCLUSION AND FUTURE WORKS

In this paper, we analyzed the existing achievements of DoS attacks detection model. Furthermore, a DoS attacks intelligent detection/defense system is proposed. The system took the DoS attack traffic and the normal traffic as input, and then the two-stage model has been performed. In the first stage, the DoS attacks detection model based on the BP neural networks has been improved the detection accuracy of the DoS attacks to 99.977%. In the second phase, the dynamic defense strategy based on game theory has been employed to increase the detection rate of the DoS attacks to 99.998%. Finally, the simulation results show the model parameters, such as the evaluation coefficient (e) and the legal judgment rate (JR), are reasonable and the proposed scheme is efficient.

In this paper, the main contributions have four aspects: (1) the comprehensive use of BP neural network and game theory; (2) proposed two key parameters based on BP neural networks; (3) the number of required features was reduced to twelve; (4) the detection accuracy for DoS attack was improved to 99.998%. However, we only carried out the experiment in the simulation environment and used the sorted dataset at the same time. So the effect of the scheme needs to be further verified in the real environment and this is one of our future works. In addition, we will continue to study how to reduce the computational complexity and the number of features in the follow-up. And we also try to apply the proposed key parameters in other classification or prediction fields.

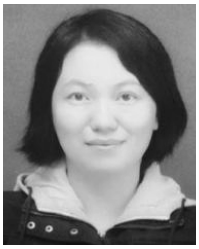
REFERENCES

[1] B. Botezatu, *Anatomy of a Botnet*. Burlington, NJ, USA: Burlington, 2010.
[2] V. Muthukkumarasamy and R. Birkely, "An intelligent intrusion detection system based on neural network," *J. Neurosci. Methods*, vol. 152, pp. 221–227, Jan. 2014.
[3] S. Mukkamala and A. Sung, "Feature selection for intrusion detection with neural networks and support vector machines," *Transp. Res. Rec., J. Transp. Res. Board*, vol. 1822, pp. 98–189, Jan. 2003.
[4] D. Novikov, R. V. Yampolskiy, and L. Reznik, "Anomaly detection based intrusion detection," in *Proc. 3rd Int. Conf. Inf. Technol., New Gener. (ITNG)*, Las Vegas, NV, USA, 2006, pp. 420–425.
[5] X. Tong, Z. Wang, and H. Yu, "A research using hybrid RBF/Elman neural networks for intrusion detection system secure model," *Comput. Phys. Commun.*, vol. 180, no. 10, pp. 1795–1801, 2009.
[6] A. Yousef, G. Kvascev, S. Gajin, and Z. Jovanovic, "Flow-based anomaly intrusion detection system using two neural network stages," *Comput. Sci. Inf. Syst.*, vol. 11, no. 2, pp. 601–622, 2014.
[7] J. Hussain, S. Lalmuanawma, and L. Chhakchhuak, "A two-stage hybrid classification technique for network intrusion detection system," *Int. J. Comput. Intell. Syst.*, vol. 9, no. 5, pp. 863–875, 2016.
[8] A. M. Chandrasekhar and K. Raghuveer, "Confederation of FCM clustering, ANN and SVM techniques to implement hybrid NIDS using corrected KDD cup 99 dataset," in *Proc. Int. Conf. Commun. Signal Process.*, Melmaruvathur, India, 2014, pp. 672–676.
[9] L. M. Ibrahim, "Anomaly network intrusion detection system based on distributed time-delay neural network (DTDNN)," *J. Eng. Sci. Technol.*, vol. 5, no. 4, pp. 457–471, 2010.
[10] M. Khandelwal, D. K. Gupta, and P. Bhale, "DoS attack detection technique using back propagation neural network," in *Proc. Int. Conf. Adv. Comput., Commun. Inform. (ICACCI)*, Jaipur, India, 2016, pp. 1064–1068.
[11] G. S. Kushwah and S. T. Ali, "Detecting DDoS attacks in cloud computing using ANN and black hole optimization," in *Proc. Int. Conf. Telecommun. Netw.*, Noida, India, 2017, pp. 1–5.
[12] A. Saied, R. E. Overill, and T. Radzik, "Detection of known and unknown DDoS attacks using artificial neural networks," *Neurocomputing*, vol. 172, pp. 385–393, Jan. 2016.
[13] K. Amarasinghe, K. Kenney, and M. Manic, "Toward explainable deep neural network based anomaly detection," in *Proc. Int. Conf. Hum. Syst. Interact.*, Gdansk, Poland, 2018, pp. 311–317.
[14] S. Dongre and M. Chawla, "Analysis of feature selection techniques for denial of service (DoS) attacks," in *Proc. Int. Conf. Recent Adv. Inf. Technol.*, Dhanbad, India, 2018, pp. 1–4.
[15] H. Çeker, J. Zhuang, S. Upadhyaya, Q. D. La, and B.-H. Soong, "Deception-based game theoretical approach to mitigate DoS attacks," in *Proc. Int. Conf. Decis. Game Theory Secur.*, New York, NY, USA, 2016, pp. 18–38.
[16] Y. Wang, J. Ma, L. Zhang, W. Ji, D. Lu, and X. Hei, "Dynamic game model of botnet DDoS attack and defense," *Secur. Commun. Netw.*, vol. 9, no. 16, pp. 3127–3140, 2016.
[17] H. Zhang, J. Wang, D. Yu, J. Han, and T. Li, "Active defense strategy selection based on static Bayesian game," in *Proc. 3rd Int. Conf. Cyberspace Technol.*, Beijing, China, 2015, pp. 1–7.

[18] Y. Liu, C. Comaniciu, and H. Man, "A Bayesian game approach for intrusion detection in wireless ad hoc networks," in *Proc. Workshop Game Theory Commun. Netw.*, Pisa, Italy, 2006, Art. no. 4.
[19] H. Wu and W. Wang, "A game theory based collaborative security detection method for Internet of Things systems," *IEEE Trans. Inf. Forensics Security*, vol. 13, no. 6, pp. 1432–1445, Jun. 2018.
[20] Y. Ma, H. Cao, and J. Ma, "The intrusion detection method based on game theory in wireless sensor network," in *Proc. 1st IEEE Int. Conf. Ubi-Media Comput.*, Lanzhou, China, Jul./Aug. 2008, pp. 326–331.
[21] A. A. Titorenko and D. E. Goncharov, "Influence of DoS attacks on intrusion detection systems," in *Proc. IEEE Conf. Russian Young Researchers Electr. Electron. Eng. (EIConRus)*, Moscow, Russia, Jan./Feb. 2018, pp. 144–146.
[22] D. E. Rumelhart, G. E. Hinton, and R. J. Williams, "Learning representations by back-propagating errors," *Nature*, vol. 323, pp. 533–536, Oct. 1986.
[23] *KDDCUP1999*. Available at:. [Online]. Available: http://kdd.ics.uci.edu/databases/

LIJUN GAO received the B.Sc. and M.Sc. degrees from the Department of Computer Science and Technology, Shenyang Aerospace University, in 2000 and 2007, respectively, where he has been an Associate Professor, since 2005. He has extensive research interests, including computing networks and information security.

YANTING LI is currently pursuing the master's degree with Shenyang Aerospace University, China. She majors in network information security technology. Her research interests include cryptography, detection, and defense of network attacks.



LU ZHANG received the B.Sc. degree from the Department of Computer Science and Technology, Shenyang Aerospace University, in 2006, where she has been a Lecturer, since 2003. She has extensive research interests, including wireless networking and wireless network security.

FENG LIN received the B.E. degree from Northeastern University, in 1985, the M.E. degree from the Shenyang University of Technology, in 1987, and the Ph.D. degree from the Shenyang University of Technology, in 2003. He is currently a Professor with Shenyang Aerospace University. He has extensive research interests, including computing networks and information security.

MAODE MA received the B.E. degree from Tsinghua University, in 1982, the M.E. degree from Tianjin University, in 1991, and the Ph.D. degree in computer science from The Hong Kong University of Science and Technology, in 1999. He is currently an Associate Professor with the School of Electrical and Electronic Engineering, Nanyang Technological University, Singapore. He has extensive research interests, including wireless networking and network security. He has led and/or participated in around 20 research projects funded by the government, industry, military, and universities in various countries.He has been a member of the Technical Program Committees for over 120 international conferences. He is a Senior Member of the IEEE Communication Society and the IEEE Education Society. He has been the General Chair, Technical Symposium Chair, Tutorial Chair, Publication Chair, Publicity Chair, and Session Chair for over 50 international conferences. He has more than 200 international academic publications. He currently serves as the Editor-in-Chief for the *International Journal of Electronic Transport*. He also serves as a Senior Editor for the IEEE COMMUNICATIONS SURVEYS AND TUTORIALS, and an Associate Editor for the *International Journal of Network and Computer Applications*, the *International Journal of Security and Communication Networks*, the *International Journal of Wireless Communications and Mobile Computing*, and the *International Journal of Communication Systems*. Moreover, he was an Associate Editor of the IEEE COMMUNICATIONS LETTERS, from 2003 to 2011.