A Network Intrusion Detection System Architecture Based on Snort and Computational Intelligence

Tao Liu [1, a], Da Zhang [1,b]

[1] North China Electric Power University, 071003 Baoding, China

[a]taoliu@ncepu.edu.cn, [b]zhangda1215@163.com

Abstract: With the rapid development of network technology, network attack tools are becoming more and more specialized, hence network intrusion detection becoming greatly difficult, and computational intelligence with its unique advantages in intrusion detection plays more and more important role. On the basis of the detailed analysis of the characteristics of misuse and anomaly detection technology, this paper proposed a network intrusion detection system model based on snort and computational intelligence, which mainly improved the abnormal detection module based on BP neural network, and the KDDCUP99 data set is used to train the BP neural network to carry out the test. The experimental result shows superior performance in terms of both real-time and detection rate via identifying malicious behavior in high speed network traffic.

Keywords: Network Intrusion Detection, Computational Intelligence, Artificial Neural Network, Snort, Anomaly detection, Misuse detection.

1 Introduction

In recent years, many advanced network attack methods usually tend to conceal and complicated, traditional intrusion protection technology such as firewall and access control that can no longer be all-round protection network security. When faced with a new type of attack, these technology is useless, even without protection. Intrusion detection system (IDS), which is an integral part of network security, playing a vital role in the network attack detection. However, intrusion detection is also facing some problems, such as high speed of network traffic, data distribution is not balanced, difficult to determine the decision boundary between normal and abnormal behavior, difficult to adapt to changing conditions and so on [1]. At present, artificial intelligence and machine learning bring a new field of intrusion detection. But they have shown limitations in achieving high detection accuracy and fast processing times, when confronted with new requirements. Computational intelligence is a good compensate for the limitations of these two approaches. In this paper, we proposed a network intrusion detection method based on hybrid SANN to detect network attacks.

The rest of this paper is organized as follows. We briefly start with reviewing on the related work of intrusion detection in section 2. In section 3, we illustrate the proposed framework of model, explain principles and working procedures. Then, the experimental results and analysis by means of processing the intrusion detection dataset are shown in section 4. Finally, a conclusion is drawn in section 5.

2 Related Work

Computational intelligence technology is widely used in the research of network intrusion detection. In the process of research, it was found that a single artificial neural network technology has been unable to meet the needs of the current intrusion detection system. The Back Propagation (BP) network structure is improved by the improved ant colony algorithm in the literature [2]. Although these improvements have well conquered the long convergence speed and premature problem, but the computation of the improved algorithm is relatively large, it is not easy to deal with large scale network problems. Chen et al. [3] proposed a detection model based on neural network and decision tree, which is combined with the evolutionary algorithm and the particle swarm optimization (PSO) algorithm. Experimental results show that the proposed method has higher accuracy. Modi C N et al. [4] proposed a network intrusion detection system framework based on Bias classifier and Snort in cloud computing environment, this model can achieve the complementary effect by using anomaly detection and misuse detection techniques. Experiments show that the proposed method has higher detection rate and lower false alarm rate, but it is likely to increase the computational cost. Song et al. [5] proposed a hybrid detection method based on BP neural network with dynamic change of learning rate and simulated annealing algorithm. Experimental results show that this method is effective in reducing the training steps.

As mentioned above, the hybrid artificial neural network has become a trend in the research of intrusion detection. In this paper, according to the practical application, combined with computational intelligence methods, to build an intrusion detection system architecture which is suitable for the actual network.

3 The Architecture Design

In this section, we propose a hybrid network intrusion detection framework based on snort-online and BPNN, called SANN, system model frame shown in Figure 1.

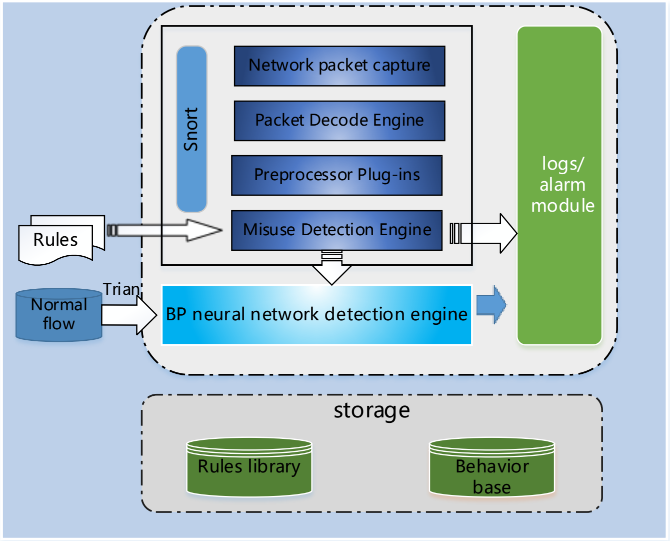

Figure 1 Hybrid network intrusion detection framework

Intrusion detection system model is designed in this paper, combined with the advantages of misuse detection and anomaly detection technology, instead of the single detection technology. As shown in figure 2, it includes misuse detection module based on snort, anomaly detection module based on the improved BP neural network, alarm log module and storage module. Storage module mainly storage network events, mainly includes two parts: rule library and characteristics of the normal flow. Rule library (known attack) is used by the Snort to detect known malicious attacks, and traffic characteristics (normal network traffic) used for BP neural network detector. Detailed testing process as depicted in figure 2.

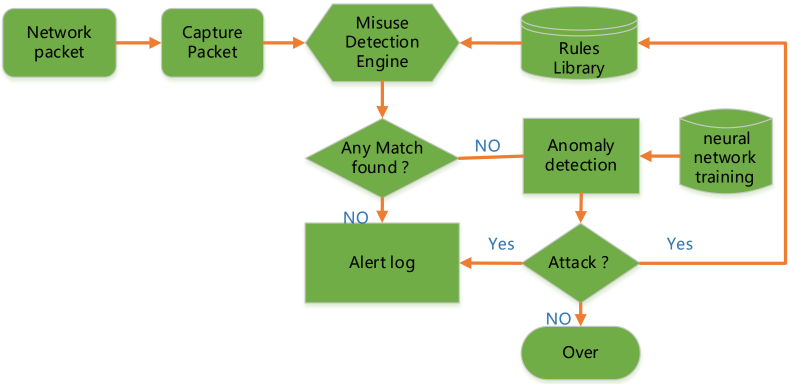

Figure2 The flow of system operation

When detecting, matching the characteristic of network traffic with the rule library, once matched, we considered it is an intrusion behavior, in this way, the known malicious attacks can be detected rapidly and accurately. Once found malicious behaviours, will immediately alert, when don't match, the data packets will send to the anomaly detection module, if discovery it is unusual, and alarm, at the same time to save the network events into the feature library; if not, then add data to the training set in the database, to ensure the real-time update of the database. It is able to accurately detect known attacks, but also can discover the new, unknown attacks, and achieve the goal of all-round protect the network security.

3.1 Anomaly detection module based on improved BP neural network

In this paper, we use the feedforward neural network of BP algorithm to construct the anomaly detection module, and carries on the corresponding improvements. The BP neural network structure can be divided into input layer, hidden layer and output layer. Each layer in the network is composed of multiple neurons which can perform parallel computing. In three layer network model, for example, as shown in figure 3, x represents the input vector and y represent the output vector, ω and v represent respectively the connection weight matrix of each node between two layers. Hidden layer can be a layer or multi-layer. After the signal is input through the hidden layer to output layer, the resulting output information after the processing of each layer [6].

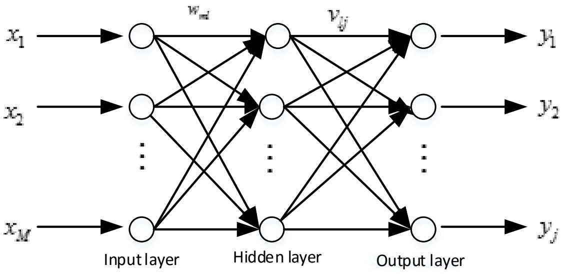

Figure 3. Three layer structure of neural network

The output of hidden layer nodes: $$h_l = f_1\left(\sum_{m=1}^{M}\omega_{ml}x_{ml} - \vartheta_l\right) \quad (1)$$

The output of the output layer nodes: $$o_j = f_2\left(\sum_{l=1}^{L}v_{lj}h_l - \theta_j\right) \quad (2)$$

Incentive function is: $$f(x) = \frac{1}{1+e^x} \quad (3)$$

The output value will be compared with the target, in this study, error function is expressed as follows [7]:

$$E = \frac{1}{2p}\sum_{p}\sum_{k}\left(t_{pk} - o_{pk}\right)^2 \tag{4}$$

Where p is the number of training samples, k is the number of neurons in input layer, t_{pk} and o_{pk} are the target value and the output value, respectively. Network error E is a function about the weight and threshold of each layer. In consequence, it can modify the error by adjusting the weights and threshold. The weights and threshold values change as follows:

$$w_{ml}\left(n+1\right) = w_{ml}\left(n\right) + \Delta w_{ml} \qquad \vartheta_l\left(n+1\right) = \vartheta_l(n) + \Delta\vartheta_l \tag{5}$$

Where $\Delta w_{ml} = \eta\frac{\partial E}{\partial w_{ml}}$, $\Delta\vartheta_l = \eta\frac{\partial E}{\partial\vartheta_l}$, η is the learning rate.

In order to increase the convergence speed, speed training, at the same time to prevent the BP neural network into a local minimum, using the adaptive learning rate [8], increase the momentum factor, α is momentum factor.

$$w_{ml}\left(n+1\right) = w_{ml}\left(n\right) + \eta(n)\partial E\left(n\right)/\partial w\left(n\right) + \alpha\Delta w_{ml}\left(n\right) \qquad \alpha \in \left(0,1\right) \tag{6}$$

In addition, we noticed when the input absolute value of network is larger, will fall into the activation function of virtual saturation area, the function derivative values close to 0, the network weights update is also close to 0, the weights of the fixed speed almost ground to a halt, and tremendously time-consuming. To improve this kind of problem, put forward the improvement activation function, avoid the generation of local convergence phenomenon. Therefore on the excitation function introducing new coefficient, *λ, β*, function is described as follows:

$$f(x,\lambda,\beta) = \frac{1}{1+ae^{-\lambda(x-\beta)}} - a \tag{7}$$

Where the factor a decides the range of the excitation function, it is an adjustable parameters for our neural model. λ is the steepness factor, the λ more greater, the images of *f(x, λ, β)* more steep. β is used to adjust the horizontal position of *f(x, λ, β)*. During the network error reverse, λ and β will be revised according to the error signal, it can not only improve the neuron adaptive ability, but also will significantly accelerate the convergence of the algorithm. The modified activation function will be used in this paper.

5 Experiment Design and Result Analysis

As we all know, Snort has the capability of detecting the known attacks, its detection accuracy depends on the completeness of the rules. Therefore, Our experiment mainly verify the anomaly detection module. We have used KDDCUP99 intrusion detection dataset [9] as training data and testing data for BPNN classifier. We randomly select 8067 records as training data, 8000 data as the testing data, Table 1 shows detailed information about the number of the data that used during the experiment.

Table 1 data distribution of training set and testing set

Connection type	Training dataset	Training dataset
Normal	1591	2000
DOS	6209	5000
Probe	67	500

U2R	22	100
R2L	178	400

A Feature Selection

The KDDCUP99 dataset includes a set of 41 features derived from each connection and a label which specifies the status of connection records as either normal or specific attack type. In order to improve the performance of the BP neural network, WEKA [11] is used to analy the 41 features, and found that the 7, 8, 9, 10, 11, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22 have little influence on the result of the detection .So we will delete the above 15 characteristics, select other 26 key features as input, in order to achieve the purpose of the feature dimension reduction. Reducing the feature dimension can effectively reduce the time required for training and testing, improve the detection efficiency.

B Evaluation Standard

The performance evaluation of Intrusion detection system is mainly based on the detection rate, accuracy, the rate of false positives, the precision and Recall, F - Score and training time. In this paper, accuracy, detection rate and false alarm rate are used to evaluate the performance of anomaly detection module, the specific formula as follows:

$$\begin{aligned} &Accuracy=\frac{TN+TP}{TN+TP+FN+FP} \\ &Detection\quad \mathrm{Rate}=\frac{TP}{TP+FN} \\ &False\quad alarm\quad rate=\frac{FP}{TN+FP} \end{aligned} \tag{9}$$

Where, TP, TN, FP and FN is true positives, true negatives, false positives and false negatives.

C Results and Discussion

In this experiment, the input layer node number is 26, it is because we have chosen 26 features. The number of hidden layer nodes, we use the formula $n=(a+b)^{\frac{1}{2}}+\alpha$, $1<\alpha<10$ to determine, where a is the number of input nodes, b is the number of output nodes. Activation function using our improved function, formula (7). In the training phase of mean square error(MSE) is set to 0.001. Learning rate is 0.01, the momentum factor is 0.9. We compare the result of the experiment with other famous classification method such as decision tree, bayes classification method. We use the data mining tool WEKA to carry out the experiment, the results are shown in Table 2.

Table 2 The experimental results with different model

	Decision tree	Bayes	BP	Improved BP
accuracy (%)	98.44	91.82	97.91	99.10
detection rate (%)	98.64	99.23	97.59	99.07
false alarm rate (%)	2.39	38.53	1.82	0.82

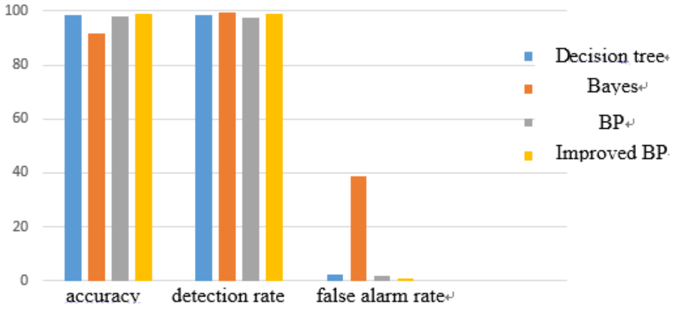

Figure 4. Comparison of experimental results

As shown by the Table2 and Fig4, the improved BP neural network improves the detecting accuracy, and reached 99.1%, and the detection rate is higher than the decision tree and BP neural network, respectively 0.43% and 1.48%, but 0.16% lower when compared with bayesian classifier, this is because the bayesian uses prior probability to classify, so is somewhat higher in the detection rate, and the false alarm rate of bayesian classifier reached 38.53%, far greater than 0.82% of this article. Relatively, the method of this paper is to obtain high detection accuracy and detection rate , but the rate of false positives only is 0.82%, able to meet the needs of intrusion detection.

6 Conclusion

On the basis of analyzing the misuse detection and anomaly detection, this paper proposed a hybrid intrusion detection model, which uses the Snort lightweight intrusion detection system to construct the misuse detection module, and the improved BP neural network is used to construct the anomaly detection module. The intrusion detection model can quickly detect known network intrusion behavior, at the same time, to be able to accurately find the unknown, a new type of network attacks behavior. The experimental results show that the model has higher detection performance.

Acknowledgments. This work is partially supported by National Natural Science Foundation of China (No. 61302105、No. 61302163), and the Fundamental Research Funds for the Central Universities (No. 2014MS99).

References

[1] Wu S X, Banzhaf W. The use of computational intelligence in intrusion detection systems: A review[J]. Applied Soft Computing, 2010, 10(1): 1-35.

[2] Wang L, Wang D Q, Ding N． Research on BP neural network optimal method based on improved ant colony algorithm[C]// Proceedings of 2010 Second International Conference on Computer Engineering and Applications. Washington DC:IEEE Society Computer, 2010:117-121.

[3] Chen Y H, Abraham A, Yang B. Hybrid flexible neural‐tree‐based intrusion detection systems[J]. International Journal of Intelligent Systems, 2007, 22(4): 337-352.

[4] Modi C N, Patel D R, Patel A, et al. Bayesian Classifier and Snort based network intrusion detection system in cloud computing[C]//Computing Communication & Networking Technologies (ICCCNT), 2012 Third International Conference on. IEEE, 2012: 1-7.

[5] Song G J, Zhang J L, Sun Z L. The research of dynamic change learning rate strategy in BP neural network and application in network intrusion detection[C]//Innovative Computing Information and Control, 2008. ICICIC'08. 3rd International Conference on. IEEE,2008: 513-513.

[6] Xu S, Huang C T, Matthews M. Security issues in privacy and key management protocols of IEEE 802.16[C]//Proceedings of the 44th Annual Southeast Regional Conference．New York：ACM Press，2006：113-118

[7] Li H G, Lu H, Li G. An Improving Method of BP Neural Network and Its Application [1]. Engineering Science, l 009-1742 (2005) 05-0063-03

[8] KDD Cup 99 training data set Available:
http://kdd.ics.uci.edu/databases/kddcup99/kddcup99.html. (2011).

[9] Weka. Weka Program Available: www.cs.waikato.ac.nz/ml/weka,(2011).