Advanced Science and Technology Letters
Vol.134 (CIA 2016), pp.28-34
http://dx.doi.org/10.14257/astl.2016.134.05

Based on the fusion of neural network algorithm in the application of the anomaly detection

Zhu YuanZhong

Electrical and Information Engineering Department of Beijing Polytechnic College Beijing China
Zyz107@163.com

Abstract. With the continuous expansion of network, computer network has highly unsafe factors such as hacker attacks. For efficient network anomaly detection, become the key to the healthy development of the network. A variety of sensors in the traditional neural network algorithm fusion, design a fusion of anomaly detection model, used to verify the data sets, the method is compared with the traditional single algorithm design of the detection system has better performance.

Keywords: The BP neural network; Fusion technology; Anomaly detection

1 Introduction

With the popularity of the Internet technology in the national production and living, the dependence of people on the Internet is growing. However, every coin has its two sides, the Internet technology in bring great convenience to people as well as develop the network security problem. Due to its own defects of Internet technology, as well as in various interests driven generated by the threat of hacking techniques, the security problem of network growi**n**g. The combination of data fusion is the purpose of through data, derived for more information, get the best of the coordinating role as a result, the use of multiple sensors common advantage, improve the effectiveness of the sensor system, eliminating the limitations of a single or a small number of sensors [1-2].

2 Related works

2.1 Intrusion detection technology

At present about the definition of intrusion detection mainly adopt the international computer security association about the definition of intrusion detection, intrusion detection is refers to by several key from a computer system or network nodes to collect information, and analyze the information, to find in the network or system whether there is a violation of security policy and the signs of the attack, namely to

ISSN: 2287-1233 ASTL

detect intrusion behavior. A complete the role and function of intrusion detection system are as follows: (1) monitoring, analysis of the user and the system activity.(2) auditing system configuration and weaknesses.(3) assessment of critical systems and data integrity.(4) identify attack pattern of activity.(5) statistical analysis of abnormal activities.(6) of the operating system audit trail management, user activity recognition in violation of the policy[2-4].

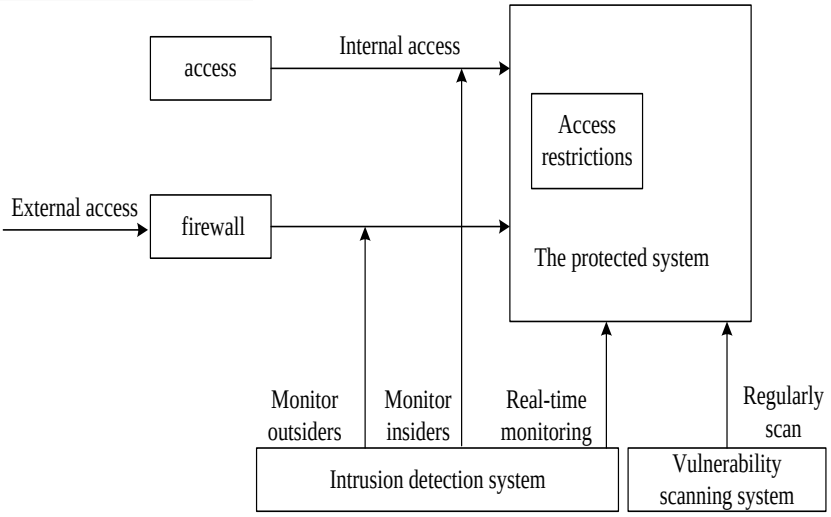

Fig. 1. The function of intrusion detection systems

At present basically has the following several kinds of common intrusion detection method

(1) pattern matching is one of the most simple misuse detection method, this method can be relatively simple pattern matching system for the current patterns of behavior to search in the pattern library, if it is found that a specific substring, argues that detected the invasion.

(2) based on contour detection method using multiple attributes to express the behavior of the system, the combination of all these attributes defined as the current of tested body contour.

(3) statistical analysis in anomaly detection is applied to the language, there are mainly four questions: can select effective measurement, statistics and generate can reflect the characteristics of the main body of the vector;Able to generate audit records according to the main body activity, and update the current main body activity session vector;Can use statistical methods to analyze data, and to assess the history of the current activity is in line with the main body behavior characteristic;Can change over time, the study main body behavior characteristic, and update the record.

(4) with some attack signature only sometimes and some attacks, the conditional probability of misuse detection technology by calculating signature under the condition of intrusion happens to judge whether there is the conditional probability of the occurrence of aggressive behavior.

(5) neural network with organizations, adaptive and self-learning ability, in dealing with some background knowledge is not clear, the environment information of a

complex situations can be very good effect, applied to the intrusion detection system can detect unknown attacks[5-6].

2.2 The BP neural network

The BP neural network is a kind of neural network learning algorithm.Composed of input layer, middle layer and output layer class type of neural network, the middle layer can be extended to multilayer.Each neuron in the connection between adjacent layers, and there is no connection between each layer of neurons, the network to learn the way the teacher teach them, when a pair of learning model for network, each neuron get the produce corresponding input connection weights of the network. Support vector machine (SVM) is put forward by Vapnik et al a classification method of study, after received widespread attention.It on the basis of statistical learning theory considering the structural risk minimization, it overcomes the defect of the traditional empirical risk minimization, on to identify the small sample problem has a unique advantage, and then get a lot of research in the field of intrusion detection applications [7-8].

2.3 Data fusion

Data fusion is through study and analysis of data from different sources, is a multi-level, multifaceted process of data processing, and the data from multiple sources are automatic detection, correlation, correlation, estimation and combination processing and so on.The classic model is mainly composed of multi-sensor data fusion, calibration, related, identify and estimate parts.Multisensor mainly complete raw data collection, the calibration ready for subsequent related and identification, the realization of the real data fusion occurs in the identification and estimation.Data fusion process can be divided into two phases, the first stage is mainly to the processing of the underlying data, namely the pixel level fusion and feature level fusion, and the result is a state, characteristics and properties, etc., the second phase of high-level data processing, namely the decision level fusion, threat, purpose and attempt to abstract results.

3 Based on the fusion of neural network algorithm

In traditional network anomaly detection model, a network connection of different characteristics in the detection of different network attacks have different influence degree. Here will take a base as calculating the weights of BP artificial neural network algorithm, namely by using BP artificial neural network as the fusion algorithm of computing engine.Final fusion decision part of the fusion center, will adopt a weighted summation method to calculate the final decision-making results.

Here to set up a based on the design idea of weights were calculated based on the BP neural network and SVM classifier fusion and fusion of BMPM network anomaly detection model, as shown in figure 2:

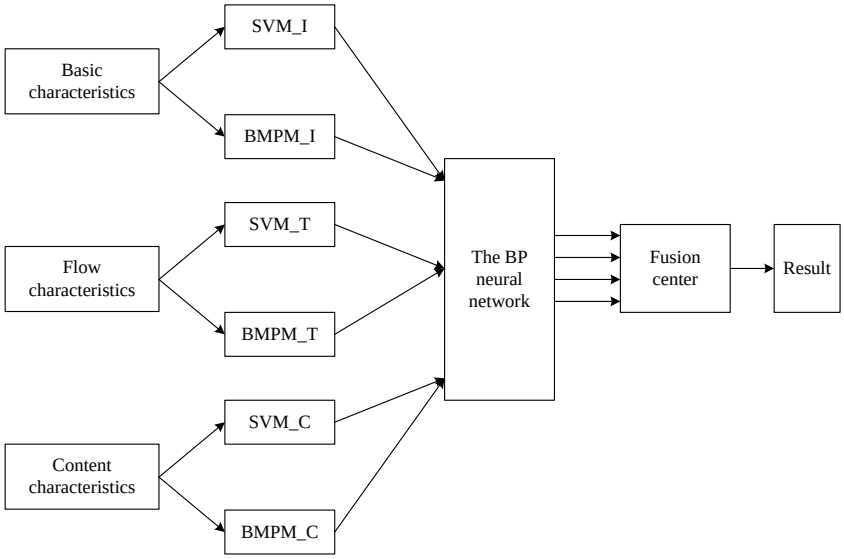

Fig. 2. The fusion of SVM and BMPM network anomaly detection model

As shown in figure 3, the model is mainly composed of three parts, the first part is for different network characteristics of early detection of the SVM and BMPM detection module, this part mainly includes the according to the characters of the early stage of the given prior network data set trained six classifier, this part of the main function is to achieve early detection, in preparation for the subsequent establishment of the BP neural network. Third part for the decision-making parts of the model, the main role of integration analysis, the results of previous processing to get the final test results.This part of the corresponding has 12 input, respectively is in the early period of the six classifier results output and the output of the BP neural network to calculate weight of the six, the final output is the final test results of the model [9-11].

4 The experiment results analysis

Experiments using 10% of KDD Cup1999 training data set, the data set includes a total of 23 different types of attacks, 326421 link records, 92373 normal connection records, each connection record is composed of 31 different attributes, 34 of them for numeric, 7 for character attributes.Test data set contains 241225 link records, 37 kinds of different types of attacks, including 14 types of attack did not appear in the training sample.At the same time, all of these attack types can be divided into the following four categories:

Dos: namely the denial of service attacks, such as the smurf, teardrop, syn flood, etc.;

Probe: namely to detect attacks, such as port scanning and vulnerability scanning;

U2R: elevated privileges, such as buffer overflow attacks, etc.;

R2L: namely remote access permissions, such as guess password attacks.

Experiment of using 10% Normal KDD Cup1999 data set, DOS, the Probe and R2L type of connecting the 4125 attack, U2R type attack connection 236.Selection of these data are for the selected data set of a variety of services, including all the network services.Experiments, such as the selection of data is divided into two, and a as the training data set, another one as a test data set, to train the fusion anomaly detection model, and to test the test data set.In order to reflect the effectiveness of the detection model in the fusion, here will use the same set of training data to train the SVM, BMPM and use the same test data set to test the SVM, BMPM and BP, and finally with the comparative analysis of monitoring results of fusion of anomaly detection model [12-15].

Table 1. The detection result of all the attacking types with SVM

Attack types	The total number of attacks	Detect attack number	Detection rate
Dos	1800	1765	0.980
Probe	1700	1692	0.995
U2R	153	142	0.928
R2L	1800	1750	0.972
Total	5453	5349	0.980

Table 2. The detection result of all the attacking types with BMPM

Attack types	The total number of attacks	Detect attack number	Detection rate
Dos	1800	1736	0.964
Probe	1700	1682	0.989
U2R	153	146	0.954
R2L	1800	1759	0.977
Total	5453	5343	0.979

Table 3. Detection rate for all types of attacks with fusion of SVM and BMPM

Attack types	The total number of attacks	Detect attack number	Detection rate
Dos	1800	1756	0.975
Probe	1700	1692	0.995
U2R	153	150	0.980
R2L	1800	1787	0.992
Total	5453	5425	0.994

Can be seen in the chart, and the SVM, BMPM compared single anomaly detection methods, such as the integration of the SVM and BMPM detection methods in keeping the detection rate of reduce the false alarm rate (SVM false-alarm rate = 1.83%, BMPM false-alarm rate = 1.26%, the integration of the SVM and BMPM false-alarm rate = 0.48%).At the same time, specific to a variety of different types of attacks on the detection, fusion method on the DOS attack types of testing, slightly

lower than the SVM detection rate and high detection rate than BMPM, namely in made a balance between two kinds of detection methods, on the three other types of attacks also played a balance SVM and BMPM high detection rate on a single attack type, low detection rate on other types of defects, this fusion model is used to detect multiple attack types with higher stability.

5 Conclusion

This paper discusses the SVM and BMPM two single anomaly detection methods by combining the BP neural network, design a fusion of anomaly detection model, and the corresponding fusion algorithm is given.By using a data set to validate, and with a single SVM and BMPM using the same experimental data for comparison, it can be seen that the anomaly detection method based on the integration of the SVM and BMPM better design of the anomaly detection system combines the advantages of SVM and BMPM at the same time, reduces the false alarm rate of the system, namely between the detection rate and false alarm rate with better balance, that is, the method to design the detection system has better performance.

References

1. Cao, S., Cao, G., Chen, K.: The Ground Objects Identification for Digital Remote Sensing Image Based on the BP Neural Network [M]// Computer Engineering and Networking. Springer International Publishing, 2014:671-677.
2. Peng, HY.: The BP neural network's GA optimization and its realization on MATLAB [C]// Control and Decision Conference (CCDC), 2013 25th Chinese. IEEE, 2013:536-539.
3. Zhang, K., Zhang, B., Qu, R.: Analysis of eight volume pulse elements based on the BP neural network[C]// Advanced Computational Intelligence (ICACI), 2015 Seventh International Conference on. IEEE, 2015.
4. Shi, T., Yuan, T., Shi, B.: Bus turnaround time prediction research based on the BP neural network [J]. Journal of Shandong Jianzhu University, 2015.
5. Li., QH, Liu, D.: Aluminum Plate Surface Defects Classification Based on the BP Neural Network [J]. Applied Mechanics & Materials, 2015, 734:543-547.
6. Benmoussat, MS., Guillaume, M., Caulier, Y., Automatic metal parts inspection: Use of thermographic images and anomaly detection algorithms [J]. Infrared Physics & Technology, 2013, 61(11):68–80.
7. Bhuyan, M H., Bhattacharyya, DK., Kalita, JK.: Network Anomaly Detection: Methods, Systems and Tools[J]. Communications Surveys & Tutorials IEEE, 2014, 16(1):303-336.
8. Lee, YJ., Yeh, YR., Wang, Y.C.F.: Anomaly Detection via Online Over-Sampling Principal Component Analysis[M]// Anomaly Detection via Online Over. IEEE, 2013:1-1.
9. Li, W., Mahadevan, V., Vasconcelos, N.: Anomaly Detection and Localization in Crowded Scenes.[J]. IEEE Transactions on Pattern Analysis & Machine Intelligence, 2013, 36(1):1.

10. Vrabič, R., Škulj, G., Butala, P.: Anomaly detection in shop floor material flow: A network theory approach [J]. CIRP Annals - Manufacturing Technology, 2013, 62(1):487–490.
11. Bhattacharyya, D.K., Kalita, JK.: Network Anomaly Detection: A Machine Learning Perspective [J]. Crc Press, 2013.
12. Poletto, MA, Ratin, A., Gorelik, A.: Aggregator for connection based anomaly detection: US, US8479057 B2 [P]. 2013.
13. Tartakovsky, A.G., Polunchenko, A.S., Sokolov, G.: Efficient Computer Network Anomaly Detection by Changepoint Detection Methods [J]. IEEE Journal of Selected Topics in Signal Processing, 2013, 7(1):4-11.
14. Angello, L., Lieuwen, T., Noble, D.R.: System and method for anomaly detection: WO, WO2013077861 A1 [P]. 2013.
15. Song, J., Takakura, H., Okabe, Y.: Toward a more practical unsupervised anomaly detection system [J]. Information Sciences, 2013, 231(9):4–14.

