Network Intrusion Detection Method Based on Agent and SVM

Guan Xiaoqing
Beijing Vocational College
of Electronic Science
Beijing 100026,P.R. China
Email: guanxiaoqbm@163.com

Guo Hebin
Northern Beijing Vocational
Education Institute
Beijing 101400, P.R. China

Chen Luyi
Beijing Vocational College
of Electronic Science
Beijing 100026, P.R. China

***Abstract*—It is necessary to study a kind of network intrusion detection method which realizes faster attack detection and response. In order to improve the network intrusion detection precision further, Network intrusion detection method based on Agent and SVM is proposed to recognize the intrusion types in the paper. The network intrusion detection system based Agent and SVM are created. Then, network Intrusion detection model based on SVM is gained, and the process of intrusion detection by SVM is given. The experimental results demonstrate that the presented method in this paper is better than artificial neural network.**

Keywords- network; intrusion detection; support vector machine; Agent

I. Introduction

With the development of Internet applications, network intrusion is more and more serious. The anomaly network intrusion detection is a very important part of network security[1-3]. So it is necessary to study a kind of network intrusion detection method which realizes faster attack detection and response. At present, there are many intrusion detection methods available. In these intrusion detection methods, artificial neural network (ANN) is data mining approach which is commonly taken in intrusion detection. Artificial neural network includes the processing elements interconnected and transform a set of inputs to a set of desired outputs. In order to improve the network intrusion detection precision further, support vector machine network intrusion detection method is used here. Support vector machine abbreviated as SVM is a kind of learning method which finds global optimum solutions for classification problem with non-linear. Thus, Network intrusion detection method based on Agent[4,5] and SVM is proposed to recognize the intrusion types in the paper. The network intrusion detection system based Agent and SVM are created, which is composed of acquisition module of data packet, intrusion detection Agent and management Agent. Then, network Intrusion detection model based on SVM is gained, and the process of intrusion detection by SVM is given.

II. Support Vector Machine

The machine achieves this desirable property on the basis of the principle of structural risk minimization principle.

Let us consider a training set $\{x_i, y_i\}_{i=1}^n$, where x_i represents the n-dimensional input feature vector, $y_i \in \{+1, -1\}$ represents the target output. The target output $y_i = 1$ represents the positive group and the target output $y_i = -1$ represents the negative group.

Decision surface in the form of hyperplane is defined as $w \cdot x + b = 0$, where ***w*** is the weight vector and *b* is the bias.

The quadratic optimization problem is defined as:

Min

$$\frac{1}{2}\|w\|^2 \tag{1}$$

S.t.

$$y_i(w \cdot x_i + b) \ge 1$$

The positive slack variables ξ_i are introduced, the optimization problem can be reformulated as:

Min

$$\frac{1}{2}\|w\|^2 + C\sum_{i=1}^{n}\xi_i \tag{2}$$

S.t.

$$y_i(w \cdot x_i + b) \ge 1 - \xi_i$$

$$\xi_i \ge 0$$

where C is called the regularization parameter.

Lagrange multipliers α_i are introduced, and the decision function is defined as:

$$f(x) = sign(\sum_{i=1}^{m}\alpha_i y_i k(x_i, x_j)) + b) \tag{3}$$

where $k(x_i, x_j) = \varphi(x_i)\varphi(x_j)$ is defined as kernel function, which can map the input data to a higher dimensional space.

III. Network Intrusion Detection Sysytem Based On Agent And Svm

Structure of Network Intrusion Detection System

The description of the system structure and agents cooperation scheme is shown in Fig.1. The network intrusion

978-1-4244-5265-1/10/$26.00 ©2010 IEEE

detection system is composed of acquisition module of data packet, intrusion detection Agent and management Agent. Acquisition module of data packet is used to gain network data. Intrusion detection Agent which is the core module of network intrusion detection system is used to detect the network abnormal intrusion. Intrusion detection model based on support vector machine is applied to recognize the intrusion types. Management Agent is a higher-level component of network intrusion detection system, which is mainly used to coordinate the work of the intrusion detection Agents, and manage the entire system.

Network Intrusion Detection Model Based on SVM

SVM intrusion detection model is the core of the entire intrusion detection system. In the paper, four main intrusion types including DOS,R2L,U2R and Probing are used to test the proposed model. Then, four SVM classifiers are applied to recognize them, among which SVM1 is used to recognize normal state from the other states, when the output of SVM1 is '1', the results indicate that the system is normal, otherwise the results indicate that system encounters intrusion; SVM2 is used to recognize DOS intrusion state from R2L,U2R and Probing intrusion states, when the output of SVM1 is '1', the results indicate that the system encounters DOS intrusion, otherwise the results indicate that system encounters R2L,U2R or Probing intrusion; SVM3 is used to recognize R2L intrusion state from U2R and Probing intrusion state, when the output of SVM1 is '1', the results indicate that the system encounters R2L intrusion, otherwise the results indicate that system encounters U2R or Probing intrusion; SVM4 is used to recognize U2R intrusion state from probing intrusion state, when the output of SVM1 is '1', the results indicate that the system encounters U2R intrusion, otherwise the results indicate that system encounters Probing intrusion.

The Process of Intrusion Detection by SVM

The process of intrusion detection by SVM is given in Fig.3. Feature extraction is gained firstly, and the data are divided into training samples and testing samples, among which training samples are used to create SVM detection model and testing samples are used to gain detection precision of SVM detection model.

IV. Experiment Research

KDDCUP99 database of MIT Lincoln Laboratory are applied to research the detection ability of SVM network intrusion detection model here. Four SVMs constitute the detection model of this paper. The training sets are composed of 300 normal samples and 200 intrusion samples from DOS data sets, U2R data sets, R2L data sets and Probing Probe in KDDCUP99 database. The testing sets are composed of 200 normal samples and 150 intrusion samples from DOS data sets, U2R data sets, R2L data sets and Probing Probe in KDDCUP99 database. The testing results are given in Tab.1.The detection precision of SVM network intrusion detection model is 0.9457, but detection precision of BP neural network (abbreviated as BPNN) network intrusion detection model is 0.8771.So SVM network intrusion detection model is applied here.

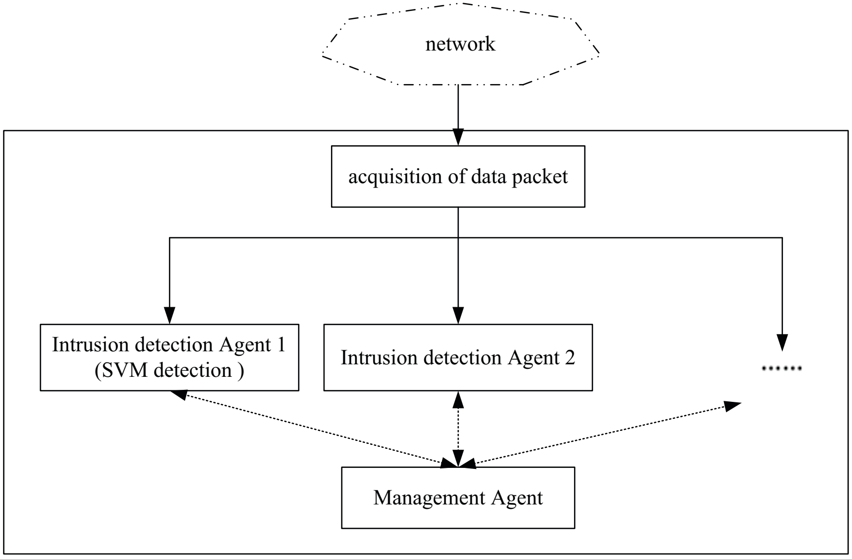
network
acquisition of data packet
Intrusion detection Agent 1 (SVM detection)
Intrusion detection Agent 2
......
Management Agent

Figure 1. Network intrusion detection system

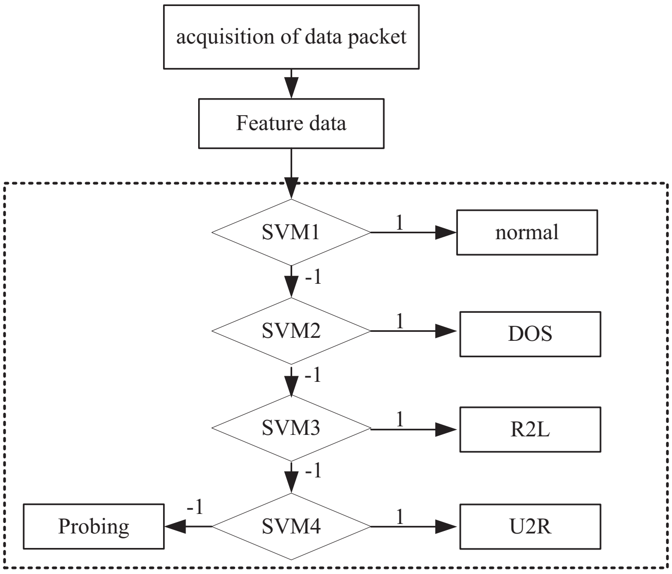

Figure 2. Network intrusion detection model

V. CONCLUSION

Network intrusion detection method based on Agent and SVM is proposed to recognize the intrusion types in the paper. The network intrusion detection system based Agent and SVM are created, which is composed of acquisition module of data packet, intrusion detection Agent and management Agent. KDDCUP99 database of MIT Lincoln Laboratory are applied to research the detection ability of SVM network intrusion detection model here. Four SVMs constitute the detection model of this paper. The detection precision of SVM network intrusion detection model is 0.9457, but detection precision of BPNN network intrusion detection model is 0.8771. It is indicated that the experimental results demonstrate that the presented method in this paper is better than artificial neural network.

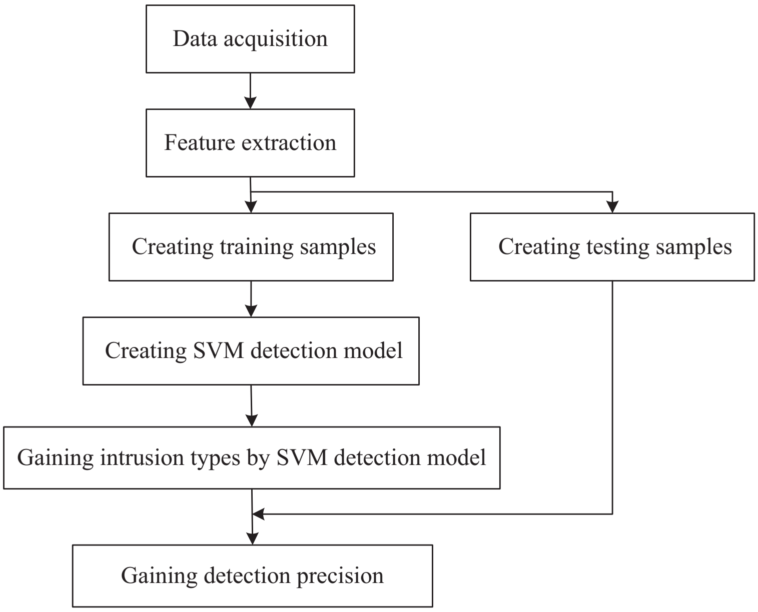
Data acquisition
Feature extraction
Creating training samples
Creating testing samples
Creating SVM detection model
Gaining intrusion types by SVM detection model
Gaining detection precision

Figure 3. The process of intrusion detection by SVM

TABLE I COMPARISON OF THE DETECTION RESULTS BETWEEN SVM AND BPNN

algorithm	total number /the number of error categorization	detection accuracy
SVM	350/331	0.9457
BP	350/307	0.8771

REFERENCES

[1] Richard P. Lippmann, Robert K. Cunningham, “Improving intrusion detection performance using keyword selection and neural networks”, Computer Networks, 2000, vol.34,no.4,pp.597-603.

[2] Lih-Chyau Wuu, Chi-Hsiang Hung, Sout-Fong Chen, “Building intrusion pattern miner for Snort network intrusion detection system”, Journal of Systems and Software, 2007, vol.80, no.10,pp.1699-1715.

[3] Giorgio Giacinto, Roberto Perdisci, Mauro Del Rio, Fabio Roli, “Intrusion detection in computer networks by a modular ensemble of one-class classifiers”, Information Fusion,2008,vol.9,no.1, pp.69-82.

[4] Azzedine Boukerche, Renato B. Machado, Kathia R.L. Jucá, João Bosco M. Sobral, Mirela S.M.A. Notare, “An agent based and biological inspired real-time intrusion detection and security model for computer network operations”,Computer Communications, 2007,vol.30,no.13,pp.2649-2660.

[5] Agustín Orfila, Javier Carbó, Arturo Ribagorda, “Autonomous decision on intrusion detection with trained BDI agents”, Computer Communications, 2008,vol.31,no.9,pp.1803-1813.