Intrusion Detection Localization Method of Large Association Embedded Network Equipment

Lang Liao[1,a], Zhu Zhenjia[1,a]

[1]Shenzhen Institute of Information Technology,ShenZhen GuangDong 518172,China

[a]22900699@qq.com

Keywords: intrusion detection; association embedded network; neural network

Abstract. The method of intrusion detection of embedded network equipment in large assoc iation is researched. In the process of large-scale embedded network device associated intrus ion detection, the intrusion detection results of network equipment directly affect the stabilit y and security of the network. For this, an intrusion detection method of large-scale embed ded network device is proposed based on improved ART2. When there are amount of mem ory models in artificial neural network, effective organization for learning the model can be carried out, and improve the detection efficiency, the judgment condition adjustment is red uced by linear combination of amplitude and phase, the cluster size difference is reduced, t hus, the network intrusion detection and positioning of device are completed. The experimen t results show that, by using the improved ART2 algorithm for large embedded network de vice intrusion detection, it can simplify the training set, shorten the detection time, the accu racy of detection is improved.

Introduction

With the development and popularization of network technology, large association embedded network has become the focus in the field of network application object. Network security has been paid more and more attention[1-3]. The intrusion detection of embedded network equipment in large correlation is very important, the intrusion detection has become the core problem of network research field, so it has received great attention. At present, the mainstream intrusion detection methods of large association embedded network devices include ant colony detection method, detection method based on immune genetic algorithm, and the detection method based on neural network algorithm. Among them, the most commonly used method is the intrusion detection algorithm based on neural network algorithm, it is used for intrusion detection of large association embedded network devices, and it has obtained good results, the effective detection of large embedded network device associated intrusion can safeguard information security, it plays an irreplaceable role, therefore, it has obtained attention of the relevant experts, it has a very broad development potential[4-7].

Principle of intrusion detection and localization of large embedded network devices based on Improved ART2

As a competitive neural network, adaptive resonance theory (ART) is proposed to solve the instability problem in the process learning, ART can make the artificial neural network accept the new mode, when the state is not related to patterns of response, it can ensure the stability of the current network. The intrusion detection based on improved ART2 algorithm can complete embedded network equipment in large association, the detailed process is shown as follows:

In the process of large embedded network intrusion detection positioning, learning rules of ART network is divided into two parts: 1. For the L1-L2 connection; 2. the connection for L2-Ll. The two part have different effects, among them, it is the normal operating mode to identify large association of embedded network, the instar learning process is used to identify large association normal peration, it is a normal mode of operation using the outstar learning process, it repeats the

detection process, and the large association of embedded network is constructed. At the same time, update the step 1 and step 2. When the input model and the expectation of large embedded network equipment intrusion detection values match together, update the W1:2 and W2:1 by adjusting the control subsystem. The matching process and subsequent adaptation process is called as resonance. The core of the whole network structure is to adjust the subsystem, its role is expected to determine the value of L2-L1 and the input pattern matching degree. According to the determination result, intrusion detection and location of large associated embedded network equipment is realized. Calculation equation for adjustment subsystem is shown as:

$$\varepsilon \frac{dn^0(t)}{dt} = -n^0(t) + \left({}^{+}b^0 - n^0(t)\right)\left\{{}^{+}W^0 p\right\} - \left(n^0(t) + {}^{-}b^0\right)\left\{{}^{-}W^0 a^1\right\} \tag{1}$$

Inhibitory inputs can be written as:

$${}^{+}W^0 a^1 = [\beta, \beta, \ldots, \beta] a^1 = \beta \sum_{j=1}^{s^1} a_j^1(t) = \beta \left\| a^1 \right\|^2 \tag{2}$$

When the excitation input is greater than the inhibitory input, adjust ART network subsystem of the large association large association, the ART network subsystem will be driven, the steady state operation is taken as following:

$$\begin{aligned} 0 &= -n^0 + \left({}^{+}b^0 - n^0\right)\left\{\alpha \left\| p \right\|^2\right\} - \left(n^0 + {}^{-}b^0\right)\left\{\beta \left\| \alpha^1 \right\|^2\right\} \\ &= -\left(1 + \alpha \left\| p \right\|^2 + \beta \left\| \alpha^1 \right\|^2\right) n^0 + {}^{+}b^0 \left(\alpha \left\| p \right\|^2\right) - {}^{-}b^0 \left(\beta \left\| \alpha^1 \right\|^2\right) \end{aligned} \tag{3}$$

It can be solved as:

$$n^0 = \frac{{}^{+}b^0 \left(\alpha \left\| p \right\|^2\right) - {}^{-}b^0 \left(\beta \left\| \alpha^1 \right\|^2\right)}{\left(1 + \alpha \left\| p \right\|^2 + \beta \left\| \alpha^1 \right\|^2\right)} \tag{4}$$

In the formula, it will lead to the second layer reset condition, $\rho = \alpha / \beta$ is named as intrusion alert parameter for the large association embedded network equipment, when the intrusion alert parameter is close to 1, and α^1 is not close to P, it will cause the reset. When the intrusion alert parameter is close to 0, it will prevent the reset.

The input pattern is mapped into the interval $\left[\frac{1}{n}\sum_{i=1}^{n} x_i,\ MAX\right]$, the vector X_S' is obtained. The corresponding denoised vector is WS′, XS′ and WS′ are compared. According to the comparison results, it can realize large association of embedded network intrusion detection and location.

Experiment results and analysis

In order to verify the validity of this algorithm, we need for an experiment, in this experiment, large number of normal data and different types of intrusion data sets in KDDCup99 are taken as sample, the selection of samples are representative. In the data set, it has 20 dimensional attributes and a decision attribute. The 20 dimensional attributes are divided into 4 feature subsets, the decision attribute is divided into Normal DOS attack, Probing attack, U2R attack and R2L5 classes.

By using the improved algorithm for simulation, the large-scale embedded network device associated intrusion detection is obtained, the experimental data are taken with reduction processing, and features of the intrusion data are extracted, the results and process are described as follows:

Table 1 Feature data table of network equipment intrusion

Feature name	Feature attribute
duration	Cost time of network connection process
flag	State of the network connection
protocol_type	Protocol type

dst_bytes	Since the number of all the characters, transmitted to the source address destination address
src_bytes	Since the source address is transmitted to all the characters of the target address

Table 2 Flow features of time window

Feature name	Feature attribute
srv_count	The number of connected to the same server
count	The number of connected with the same host
srv_diff_host_rate	For same connection service, the number of connected to different hosts
land	The source and destination ports or host is the same, if same,it is 1, else 0

Table 3 Flow features based on the target host

Feature name	Feature attribute
dst_host_count	Number of the same host and the destination host is connected
dst_host_srv_count	Number of the same host machine is connected with the other host
dst_host_same_srv_rate	Same host is already connected state accounts for the proportion in all host
dst_host_diff_srv_rate	Same proportion accounted for the host state in all host and connect different host
dst_host_same_src_port_rate	Connection object end host with the same host proportion in all host
dst_host_srv_diff_host_rate	Proportion in connect to the target host end host and different all host

Table 4 Feature attributes based on content

Feature name	Feature attribute
num_root	Number of visits
logged_in	Success for legend and display 1, else 0
root_shell	Have access 1,else 0
Is_host_login	Belong to host, legend is 1, else 0
Is_guest_login	Belong to guest, legend i1, else 0

By the experiment, we can lean that the improved algorithm is taken based on feature selection, the number of features can be selected, characteristics of each data are less than the number of features, , therefore, the improved algorithm can greatly enhance the real-time performance, the detection performance of embedded network intrusion is improved greatly.

The improved algorithm is applied in intrusion detection and location, the detection results are shown in Figure 1.

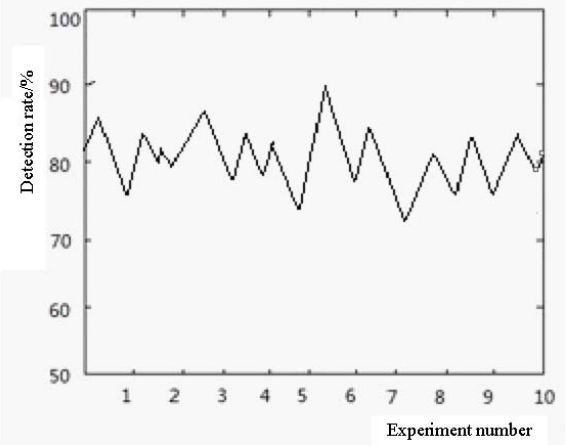

Figure 1 Detection rate of improved algorithm

From the above figure, it can be obtained that intrusion detection algorithm are used in large association embedded network equipment, the detection rate is relatively high, it can satisfy the security demand, the actual demand of stable operation can be satisfied.

Conclusions

In this paper, the method of intrusion detection of embedded network equipment in large association is researched. In the process of large-scale embedded network device associated intrusion detection, the intrusion detection results of network equipment directly affect the stability and security of the network. For this, an intrusion detection method of large-scale embedded network device is proposed based on improved ART2. When there are amount of memory models in artificial neural network, effective organization for learning the model can be carried out, and improve the detection efficiency, the judgment condition adjustment is reduced by linear combination of amplitude and phase, the cluster size difference is reduced, thus, the network intrusion detection and positioning of device are completed. The experiment results show that, by using the improved ART2 algorithm for large embedded network device intrusion detection, it can simplify the training set, shorten the detection time, the accuracy of detection is improved. It has good application value in practice.

Acknowledgrments

A Research of Semantic Analysis Based MultiPlatform System for Resolving SQL Code. No.YB201014,Research project of ShenZhen Institute of Information Techology

References

[1] Song Minghong,Yu Huafeng,Chen Haiyan. Application of Improved Quantum Evolutiona ry Algorithm in Computer Network's Routing Choice[J]. Bulletin of Science and Technolog y, 2014,30(1):170-173.

[2] GUO Xiao-yan. Simulation and Analysis on Uncertain Attenuation Property of Underwat er Acoustic Signal for Oil Field Pipe[J]. Computer Simulation, 2014,31(3):118-121.

[3] Yan We, Nan Yang. An Improved Algorithm for Network Intrusion Detection Based on SVM[J]. Bulletin of Science and Technology. 2012; 28(10): 158-162.

[4] DENG Bing1, TAO Ran, PING Dian-fa, MA Lu. Moving-Target-Detection Algorithm w ith Compensation for Doppler Migration Based on FRFT[J]. ACTA ARMAMENTARII, 200 9, 30(10)：1034-1039.

[5] Wang An,Jiao Meipeng,Zhang Xiaodong. Investigation of Spectrum Correction Algorithm for Detection of Domestic 18 kinds of Information Frequency-shift Signal[J]. Computer Si mulation, 2012.2.11-12.

[6] Abusalah L, Khokhar A, Guizani M. A survey of secure mobile Ad Hoc routing protoc ols[J]. IEEE Communications Surveys&Tutorials, 2008,10(4):78-93.

[7] Varadharajan V, Shankaran R, Hitchens M. Security for cluster based Ad Hoc networks [J].Computer Communication, 2004,27(5):488-501.