The algorithm design of anti-attack performance testing software in large network

Zhang Ling

Shangqiu Medical College, Shangqiu Henan 476100, China

Keywords: large network; network environment; anti-attack performance

Abstract. This paper studied anti-attack performance testing methods in large network. Anti-attack performance testing process in large networks is different from traditional testing process, which mainly features harbinger attacks, lacking precise characteristic information of determining the attack act. Point to point structure limit characteristics connections, traditional detection method focuses on fixed feature information directly linked to take anti-attack performance testing, once lost contact feature will cause the detection inaccuracy. In order to avoid these shortcomings, this paper proposed an anti-attack performance testing method in large networks based on fuzzy C-means clustering algorithm. Collected relevant data to extract and analysis sample characteristics, the use of fuzzy C-means clustering method for classification of data for further calculations, to gain abnormal behavior pattern data to complete anti-attack performance testing in large network. Experimental results showed that using the proposed algorithm for anti-attack performance testing in large network could greatly improve the accuracy of detection, so as to effectively maintain a large network security, and to provide users with good network environment.

Introduction

With the constantly updated of network technology and range expanding of network applications, network security issues have received more and more attention [1]. Large-scale network is a mainstream network form. Assuming a large network security threats, the network user information and network resources will be destroyed [2]. Therefore, the detection method of anti- attack performance in large-scale network has become a mainstream needed research method in network [3]. At this stage, the main anti-attack performance detection method in large networks include the anti-attack performance detection algorithm based on principal component analysis of large networks, anti-attack performance testing method based on quantum neural network algorithm in large networks and anti-attack performance detection method based on ant colony algorithm Large network [4]. Among them, the most commonly used method is based on the quantum neural network algorithm method in large networks [5]. Due to anti-attack performance testing method in large network has a very broad space for development. Therefore, it is able to get attentions of many scholars, and have become hotspot research [6].

Anti-attack performance testing process for large networks is different from traditional inspection process, which mainly features harbinger attacks, lacking precise characteristic information of determining attack act, point to point structure limit the contact between features. Traditional detection method focuses on contact between stationary feature information for anti-attack performance testing, once lost contact feature will cause the detection inaccuracy.

In order to avoid the above defects of traditional algorithms, we propose a method for anti-attack performance testing in large network based on fuzzy C-means clustering algorithm. Collected relevant data of sample characteristics to extract and analysis, using fuzzy C-means clustering method for classification of data for further calculations, to gain the behavior patterns of attack data to complete anti-attack performance testing in large network. Experimental results show that using the proposed algorithm for anti-attack performance testing in large network can greatly improve the accuracy of detection, so as to effectively maintain a large network security, and to provide users with good network environment.

Principle of anti-attack performance detection in large networks

Using quantum neural network algorithm can detect anti-attack performance in large-scale networks, to provide users with good network environment. The steps are as follows:

Set in a large network, the size of all user data including network operations can be used to describe by $r = 500$, the population at large networks anti-attack during performance testing iterative processing times can be used to describe the maximum value $I_{\max} = 100$. These data were cross-user network operation processing and mutation processing, can obtain an initial population of anti-attack performance testing in a large network.

For large-scale network operation data crossover and mutation processing, you can get a large population of new network operating characteristic composition.

In a large network of anti-attack performance testing, the set of all anomalies can be formed $U = \{(z_1, a_1, v(z_1)), \cdots, (z_n, a_n, w(z_n))\}$, where, $z_l \in T^q$, $w(z_l) \in \{-1,1\}$, $\omega \le w(z_l) \le 1$, ω is running state of a large network, $x(z_l)$ is the membership of the major network operating characteristics, ζ_l is the coefficient variation of a network feature.

According to the following formula, it can describe for large networks operating characteristic classification problem:

$$\begin{cases} \min\limits_{y,d,\zeta} \frac{1}{2}\|y\|^2 + E\sum\limits_{l=1}^{n} w(z_l)\zeta_l \\ s.t. \quad a_l((y \cdot z_l) + d) + \zeta_l \ge 1 \\ \qquad \zeta_l \ge 0, l = 1, 2, \cdots, n \end{cases} \tag{1}$$

Among them, $E > 0$ is penalty factor of anti-attack performance testing in large network, $\zeta = (\zeta_1, \zeta_2, \cdots, \zeta_l)^T$, $w(z_l)$ is the degree of membership network operating data.

To solve the above-mentioned problems of the detection of anti-attack performance in large networks, the desired results is $\chi' = (\chi_1', \chi_2', \cdots, \chi_n')^T$, to obtain the following anti-attack performance testing in large networks function:

$$\begin{aligned} h(z) &= \operatorname{sgn}\{\sum_{l=1}^{n} \chi_l^* a_l M(z, z_l) + d^*\} \\ d^* &= a_k - \sum_{l=1}^{n} a_l \chi_l M(z_l, z_k) \quad k \in \{k \mid 0 < \chi_k^* < w(z_l)E\} \end{aligned} \tag{2}$$

According to the method above, it can take anti-attack performance testing in large networks. However, in the detection process, due to the characteristics of the network is harbinger features, and no actual contact between features, resulting in too little contact between the characteristics of the network anti-attack, which cannot get fixed feature information based on the characteristic behavior, thereby reducing the accuracy of anti-attack performance detection in large network.

Related principles of anti-attack performance optimization testing method in large networks

Attack act sample data feature extraction in large-scale network. Under a large network environment, anti-attack performance testing needs to establish normal behavior profile and extract normal samples feature vector data. Both exhibited typical feature of normal behavior of the system or user also enables obtaining optimization data. Feature extraction method is showed as follows:

Set-dimensional vector can use a weighted sum of basis vectors description:

$$x = \sum_{i=1}^{n} a_i \times \varphi_i \tag{3}$$

In the formula φ_i represents the basis vectors, a_i represents a weighting coefficient. Set basis vectors orthogonal vectors:

$$\varphi_i^T \varphi_j = \begin{cases} 1, i = j \\ 0, i \ne j \end{cases} \tag{4}$$

In the formula, φ described as an orthogonal matrix, then $\varphi_i^T \varphi_j = I$, I is the identity matrix.

Before the conversion of $y = A^t x$, set up a known large network of anti-attack program and normal procedure mode's total mean vector as the new coordinate origin, $E[x] = 0$, then obtained the following formula:

$$b_j = E[a_j] = E[\varphi_j^t x] = \varphi_j^t E[x] = 0 \tag{5}$$

The above mean square error is convert to:

$$\varepsilon^2 = \sum_{j=m+1}^{n} E\left[a_j^2\right] = \sum_{j=m+1}^{n} E\left[(\varphi_j^T\ x)(\varphi_j^T x)^T\right] =$$

$$\sum_{j=m+1}^{n} E\left[(\varphi_j^T x x^T \varphi_j^T)\right] = \sum_{j=m+1}^{n} \varphi_j^T\ R\varphi_j = \sum_{j=m+1}^{n} \lambda_j \tag{6}$$

From the foregoing, λ_j is the j feature of the autocorrelation matrix R of x; φ_j is the corresponding λ_j eigenvectors.

By the above method, it can extract the sample characteristics of large networks to provide data support for effectively identify attacks.

Realization of anti-attack behavior detection in large network. According to the acquired characteristics attacking data in large network, using fuzzy C-means clustering algorithm to complete the detection of attacking behavior, enabling detection of anti-attack capability in large network, follow these steps:

(1) Initialization of acquired data sets: sample data set is divided into $C_{\max} - 1$ different clusters, and the number is C_k. Calculate the C_k corresponding initial cluster centers;

(2) Do chromosome coding process to the C_k corresponding cluster centers in (1), to become the initial population.

(3) The use of fuzzy C-means clustering algorithm for individual populations corresponding correlation operation, access the value of U_{ck} and V_{ck}, thereby performing iteration, until the acquisition value of the objective function J_m.

(4) Using the correlation matrix of the cluster centers to obtain individual group membership matrix and calculate to obtain the corresponding value of the objective function J_m. The average value of the objective function for this operation: $\bar{J}_m = \frac{1}{n}\sum_{k=1}^{n} J_m(k)$. Where if met $t = 0$, then $t = t + 1$, need to return to step (3); if the t value meets $t \geq G_{\max}$ or will meet the conditions $\left|\bar{J}_m = (t) - \bar{J}_m(t-1)\right| < \varepsilon$, then go to the next step to continue operations.

(5) Compare to get the best individual through operation, and evaluation of clustering. As $C_k = C_{k+1}$ can be seen $C_k = C_{k+1}$, the need to return to step (3) to re-operation, on the contrary, select the best individual, decodes and outputs the corresponding optimal number of clusters C_{opt} and the optimal cluster centers V_{opt}. According to function evaluation system to obtain optimal number of clusters, and the output training data set optimal clustering results.

(6) By the width of the cluster threshold value calculation, completing the detection of anti-attack performance in large network.

Analysis of experimental results

In order to verify the effectiveness of the proposed optimization method for detecting anti-attack capability in large network, it is necessary to conduct a test. In the experiment, MATLAB is used to simulate anti-attack performance testing in large-scale network. Experimental environment can be described by following table.

Table 1 Experimental environment data

Name	Type
CPU	P4 3.0
RAM	4G
Operation System	Windows XP
Programming Language	JAVA

Experiments are carried on for different types of network attacks. Types of network attacks can be described by following table.

Table 2 Types of network attacks data

Types of network attacks	Numbers
DOS	345
U2R	362
R2L	673
Probe	316

In response to these types of network attacks, using the traditional algorithms and large-scale network algorithm to detect the anti-attack performance, respectively, test results can be described by following table.

Table 3 Comparison of different methods of detection results

Measure standard	Traditional algorithm	Large-scale network algorithm
The average false positives rate (%)	11	7
The average detection rate (%)	82	90
The average missing rate (%)	7	3

According to the experiments, using the proposed algorithm for large networks anti-attack performance detection, detection accuracy is very high, demonstrating the superiority of the proposed algorithm.

To organize the data in the table above, will be able to get below:

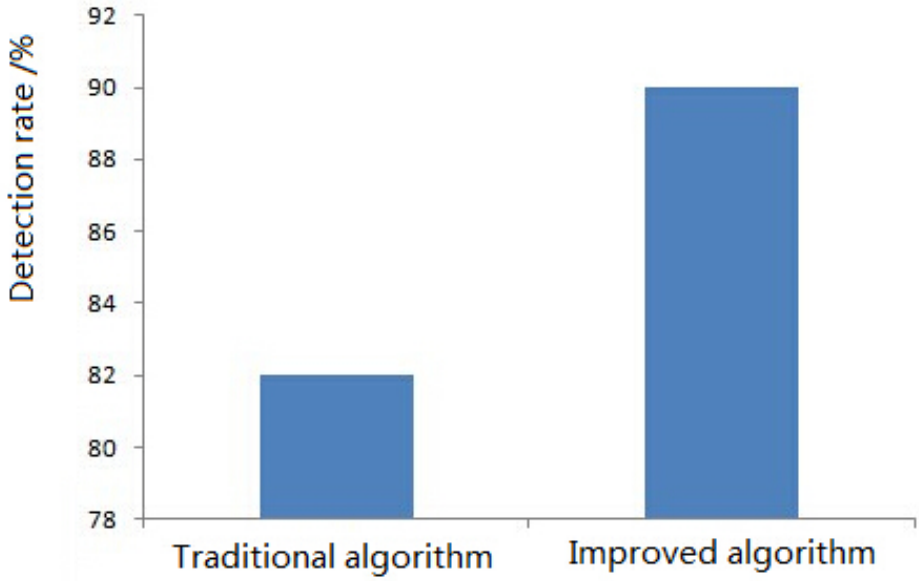

Figure 1 different algorithms contrast detection rate

According to the above can be told, the algorithm presented in this paper with a large network attack resistance detection, detection rate is much higher than traditional algorithms.

Conclusions

This paper presents an anti-attack performance detection method based on fuzzy C-means clustering algorithm. Collected relevant data of sample characteristics to extract and analysis, using fuzzy C-means clustering method for classification of data for further calculations, to gain the behavior patterns of attack data to complete anti-attack performance testing in large network. Experimental results show that using the proposed algorithm for anti-attack performance testing in large network can greatly improve the accuracy of detection, so as to effectively maintain a large network security, and to provide users with good network environment.

References

[1] Perrig A, Stankovic J, Wagner D. Security in wireless sensor networks [J]. CACM, June 2004, 47: 53–57.

[2] Anjum F, Subhadrabandhu D, Sarkar S, et al. On Optimal Placement of Intrusion Detection Modules in Sensor Networks[C]. 1st International Conference on Broadband Networks. Washington: IEEE Press, 2004: 433–439.

[3] Zhuge Jianwei, Han Xinhui, Zhou Yonglin.Research of botnet［J］.Journal of Software, 2008,19(3):702－715.

[4] Zhang Renbin, Li Gang.computer virus and anti-virus technology［M］.Beijing: Tsinghua university press, 2006: 215－219.

[5] Su Purui, Feng Dengguo. Abnormal detection model based on progress behavior [J]. Acta Electronica Sinica, 2006, 34(10): 1809-1811.

[6] Zhang Ran, Qian Depei, Zhang Wenjie, et al. Review on intrusion detection technology [J]. Min-Micro computer system, 2003, 24(7):1113-1118