Research of Detection Method of Server Network Storm Attack

Lang Liao

Shenzhen Institute of Information Technology, ShenZhen GuangDong 518172, China

22900699@qq.com

Keywords: intrusion detection; density clustering; feature selection

Abstract. In the detection process of server network storm attack, the traditional method takes the signal detection algorithm, because the attack number is large, the detection error is big. According to the problem, an improved server network storm attack detection method is proposed based on improved density clustering algorithm, the server network storm attack detection problem is transformed into a multi class classification problem, wrapper features selection model is taken, IDBC network connection record distance calculation method is combined, based on DBSCAN clustering results, the data clustering and attack detection is obtained. Simulation results show that, the improved density clustering algorithm is applied in detection of server network storm attack, it can reduce the detection error, the performance of the detection system is improved.

Introduction

The Internet has the property such as open, free of charge and undefended, the number and extent of network attacks are rising, and the network attack detection is an important means to protect the security of computer system. In China, research and development of the attack detection system is just on the start stage, network attack detection is kind of active defense technology, it has become a research hotspot in network security[1-3].

How to set up a server network storm attack detection method is a focus in the field of network security detection, it has high efficiency, in present research, network storm attack detection is important, and it has good application value in practice. The detection method of the previous network attack has the large number of attacks, it will produce the problem of big error detection [4,5].

Aimed at these problems, an improved server network storm attack detection method is proposed based on improved density clustering algorithm, the server network storm attack detection problem is transformed into a multi class classification problem, wrapper features selection model is taken, IDBC network connection record distance calculation method is combined, based on DBSCAN clustering results, the data clustering and attack detection is obtained. Simulation results show that, the improved density clustering algorithm is applied in detection of server network storm attack, it can reduce the detection error, the performance of the detection system is improved.

Principle of improved server network storm attack detection method based on density clustering algorithm

Attack detection system is an attempting detection, for a system or network attacks, the warning system is designed, therefore, the server storm attack detection method based on improved density clustering can be regarded as a multi class classification problems in pattern recognition. The server storm attack detection method based on improved density clustering has the very big relations with the number of samples and the sample dimension, it is related with the classifier selection based on the detecting effect. The sever storm attack detection method is proposed based on improved density clustering algorithm, there are two main research contents:

(1) Feature extraction and selection; (2) Classifier construction

The original server network attack characteristics contain a large amount of redundant information, the detection result has of "counterproductive" noise characteristics, if not screening

and used directly, it not only greatly weakens the classifier performance, but also increases the "dimension disaster", it reduces the detection speed. At the same time, there is no linear relationship between network attack detection and feature the algorithm, when the number of features exceeds a certain limit, it will lead to decrease the performance of detection algorithm.

A.Network attack feature selection model

In order to improve the accuracy of detection server network storm attack, aiming at solving the problem of selecting feature detection of server network storm attack, the detection problem transforms into a problem of combinatorial optimization, wrapper features selection model is taken, the specific steps are expressed in the following details:

Given sample set $\{ (x_1, y_1), (x_2, y_2), ...(x_i, y_i), ...(x_n, y_n) \}$, nonlinear mapping function is $\varphi(x)$, the original input space data are mapped into the high dimensional feature space, and the optimal classification hyper plane structure is mapped in high dimensional feature space:

$$f(x) = w \cdot \varphi(x) + b = 0 \quad (1)$$

In the formula, w is the weight vector, b is the threshold.

In order to minimize the structural risk, the optimal classification plane should satisfy the following constraint conditions:

$$yi \cdot (w \cdot \varphi(x_i) + b) \geq 1 \quad (2)$$

The non negative slack variable ξ_i is introduced, the learning method is improved, the generalization ability of classification svm can be improved. The optimization problem can be described as formula (1) :

$$\min \frac{1}{2} w \cdot w + c \sum_{i=1}^{n} \xi_i$$
$$s.t. y_i (w \cdot x_i + b) \geq 1 - \xi_i, \xi_i \geq 0, i = 1, 2, ..., n \quad (3)$$

In the formula, c is the error penalty factor. By introducing Lagrange multiplier, the optimization problem as above is transformed into a dual form:

$$\min \frac{1}{2} \sum_{i,j=1}^{n} \alpha_i \alpha_j y_i y_j (\varphi(x_i) \cdot \varphi(x_j)) + \sum_{i=1}^{n} \alpha_i \quad (4)$$

At the same time, it meets:

$$\sum_{i,j=1}^{n} \alpha_i y_i = 0, c \geq \alpha_i \geq 0 \quad (5)$$

In the formula, $\alpha_i \geq 0$, the corresponding bit is called as support vector.

For the nonlinear classification problem, by introducing the kernel function $k(x_i, x_j)$, the svm classification model:

$$f(x) = sign\left(\sum_{i,j=1}^{n} \alpha_i y_i k(x_i, y_j) + b \right) \quad (6)$$

To sum up, the server network attack detection problem is transformed into a multi class classification problem, the wrapper feature selection model is taken into consideration, the improved density clustering provides an effective basis for the server network storm attack detection.

B.Realization of server network storm attack detection

The DBSCAN algorithm is very suitable for cluster server network storm attack detection process, the wrapper feature selection model of integration is taken, the IDBC network connection record distance is calculated. According to the local density clustering, if you use the DBSCAN algorithm to detect the single server network storm attack treatment, it is easy to generate many small clusters after clustering, and contains the normal number records, the number is more than

70% part of clustering clusters, leading to high error, at the same time, these small clusters is closer to normal records. In order to solve this problem, the wrapper feature selection model of integration is proposed, IDBC network connection record distance is calculated. Based on the local density clustering, based on the local density clustering, the detection algorithm is realized, the specific steps are shown as follows:

Read the training set DB, in the DB, n objects are proceed as follows:

$$D\text{int} = \sqrt{\left(x - x_n\right)^2 + \left(x_{n2} - x_n\right)^2 + \left(x_p + x_{p2}\right)} \quad (7)$$

Computing distance between object i to all objects:

$$Dsir = \sqrt{2 \times \sum_{i=b}^{n} \left(\frac{\delta_i}{n_j}\right)} \quad (8)$$

If $1 \prec card\left(N\varepsilon(i)\right) \prec Minpts$, i is the core object,then $i++, type[i] = 0$;

The new clusters are generated as:

$$\delta = \begin{cases} 0 & x_{if} = xf_f \\ 1 & x_{if} \neq x_f \end{cases} \quad (9)$$

In the detection, for a connection record, first carries on the pretreatment of attribute values, and then search the clustering results, to determine whether the server network storm attack is true.

$$\bar{\varepsilon} = \frac{1}{n} \sum_{K=1}^{D} x_{fm} \quad (10)$$

If $D_{IJ} \leq \varepsilon$, T is taken with the same class label with i, if $D_{IJ} \geq \varepsilon$, T class label is $class = -1$.

According to the $class$, judge if the test records are in order, so as to realize the detection of the server network storm attack.

Simulation results

In order to prove the validity of the server network storm attack detection method based on improved density clustering algorithm proposed in this paper, we need for an experiment, the improved density clustering algorithm and traditional density clustering algorithm are taken in the experiment for comparison, the correct detection rate (Dr), the false alarm rate (Fr) are taken as the evaluation standard, performance comparison of two algorithms is obtained. The test platform is $MicrosoftWindowsXP\,\text{Pr}ofessional$, the OS is $AMD2600+1.60GHz,512M$ memory, $MatLab7.1$, test data is $KDDCUP99$.

The test is carried out for 3 times, each time of test, randomly selected 2399 and 1999 data in the $KDDCUP99$ as the sample, and the training set $Train$ and test set $Test$ are formed, the test results are shown in Table 1.

Table 1 Correct detection rate (Dr), false alarm rate (Fr)

	Test data set 1		Test data set 2		Test data set 3	
	Dr	Fr	Dr	Fr	Dr	Fr
Standards						
Traditional algorithm	95.7%	25.5%	93%	25%	98%	25%
New method	90.8%	4%	91%	5%	96%	3%

From the test results, it can be seen, although this algorithm in the correct detection rate is lower than traditional algorithm, but the false alarm rate dropped sharply, from about 25% to about 3% in average, the reason is that, for the traditional clustering algorithm, the number of clusters is too large, most clusters collected together, and another part is clustered in small classes. Some of these

small classes contain a record, more than the normal number of 70% in total. Because of the characteristics are small, the cluster will be seen as aggressive behavior, therefore, clustering in normal record has too much, it will inevitably influence the attack detection and false alarm rate. In order to overcome these limitations, this paper algorithm merger these small class, it contains a large number of normal data, from the test results, the correct detection rate of this algorithm and the traditional algorithm is decreased slightly, the false alarm rate is reduced, the performance is improved obviously. So this algorithm maintain good correct detection rate, it has a satisfactory effect in effectively reduce the false alarm rate.

Conclusions

In this paper, an improved server network storm attack detection method is proposed based on improved density clustering algorithm, the server network storm attack detection problem is transformed into a multi class classification problem, wrapper features selection model is taken, IDBC network connection record distance calculation method is combined, based on DBSCAN clustering results, the data clustering and attack detection is obtained. Simulation results show that, the improved density clustering algorithm is applied in detection of server network storm attack, it can reduce the detection error, the performance of the detection system is improved, it has good application value in the network security defense.

References

[1] LUO Liang, WU Wen-Jun, ZHANG Fei. Energy Modeling Based on Cloud Data Cente r[J]. Journal of Software, 2014,25(7):1371-1387.

[2] Liu Xiangdong. Data Clustering Algorithm and Software Design Based on Disturbance Searching of Logistic Series[J]. Bulletin of Science and Technology, 2014,30(2): 161-163.

[3] Zhang Yi, Zhou bingying, Hu Guangbo. Hardware System Design of Underwater Motor Pump Faults Diagnose Detector[J].Computer & Digital Engineering, 2012, 40(11): 162-166.

[4] ZHANG Yi, SHENG Huiping, HU Guangbo. Study on Compressor Fault Diagnosis Bas ed on Space Reconstruction and K-L Transform[J].Compressor Technology, 2011, 4: 19-21.

[5] SHAN Dong-hong, ZHAO Wei-ting. Research on Intrusion Detection System Neural Net works and Principal Component Analysis[J]. Computer Simulation. 2011; 28(6): 153-156.