Attack characteristic detection for large scale network based on collaborative planning

Liu Bingzhan, Jia Lianqin

Shandong Institute Of Commerce And Technology, 250103

Keywords: collaborative planning; network attack; characteristic detection;

Abstract. In the process of research on the characteristic detection method for large scale network attacks, due to the use of the current algorithm for large-scale network attack detection, it is unable to describe the attack characteristics of network attacks or detect in low accuracy. Therefore, an attack detection method for large scale network based on cooperative planning is proposed. The method is based on collaborative planning to design the detection characteristic of large scale network attacks, which is transformed into a space search problem. The difference between the parameters of the flow vector and the normal vector of the normal network spatial data is extracted as characteristics, combining Gauss mixture model with the expectation maximization algorithm, to design Lorenz chaotic asynchronous tracking detection algorithm for modeling and detection of network data stream. The experimental simulation shows that the detection method of large scale network attack detection method has high accuracy and high efficiency.

1 Introduction

In computer and information age, with the continuous progress and improvement of digital and network technology, there is no doubt that the network plays an important role in all aspects of production and life of the people [1.2.3]。High speed and mass of network information is filled with people's lives in every space and corner, which become a part of human life [4.5.6]. However, the network is relatively open platform in the face of the continuous covert and sharp attack by hackers, the security threat of large-scale network system is also growing [7.8]. Characteristic detection method for large-scale network attack is an effective way to solve this problem, which attracts the attention of many experts and scholars. As the characteristics of large network attacks detection method have profound significance for development, it has become the focus course for professional exports and received extensive attention. Therefore there are a lot of good methods proposed [9.10].

Currently, characteristic detection technology for network attack is based on ant colony algorithm, particle algorithm and the fuzzy algorithm for large-scale network. Among them, the commonly characteristic detection method is technology based on the fuzzy algorithm for large scale network attack. However the current algorithms with characteristic detection for network attack could not describe attack characteristics in detail, which lead to low accuracy.

In view of the above defect, a method for large scale network attack detection based on cooperative planning is proposed. The method is represented for network attack with characteristic feature, which is transformed into a search problem in the space.

To extract difference of parameter vector characteristic of network spatial data flow between to test network and normal network, with Gaussian mixture model and expectation maximization algorithm combined, Lorenz chaotic asynchronous detecting and tracking algorithm is designed to model and test the network data flow. The experimental simulation shows that the detection method for large scale network has high accuracy and efficiency.

2 Principles of attack characteristics for large scale network

In process of large-scale network attack detection, meaningful network attack characteristics are extracted from the original network flow, while feature description of each aggressive behavior is

attained as detection rules. By comparing test network behavior and characteristic rules, network behavior is identified as aggressive behavior if behavior between test network and characteristic are the same. Detailed procedures are as follows.

Employing the similarity principle to calculate the Euclidean distance of the samples X, Y, difference between the two samples is:

$$De = \sqrt{\sum_{L=1}^{N} \left(x_l - y_l \right)^2} \quad (1)$$

It is said that the larger the distance is, the smaller similarity of two samples are. If the similarity exceeds a certain threshold, it is judged as the network attack behavior.

In summary, the detection principle for large-scale network attack is described, and the characteristics of large scale network attack are obtained.

3 optimization principle of attack characteristics

According to defects that description of the attack characteristics for network attacks is undetailed or in low accuracy, an attack detection method for large scale network based on cooperative planning is proposed.

3.1 description of characteristic detection

In the optimization process of attack detection for large scale network, collaborative planning is designed for network attack detection, which will transform the characteristic detection issue into a space search one.

Consider $V = \{V_i, i = 1, 2, \ldots, N_V\}$ as sample set of network attack detection based on collaborative planning. $S = \{S_i, i = 1, 2, \ldots, N_S\}$ and $T = \{T_i, i = 1, 2, \ldots, N_t\}$ respectively means different test target set corresponding to sample sets of attack detection based on collaborative planning.

With $F = \{F_i, i = 1, 2, \ldots, N_f\}$ as density function of collaborative planning，planning space is constructed as trajectories of network attack detection at Row R Column C in network environment. Detection trajectories are represented as corresponding target point $\{p_k = (x_k, y_k, z_k), k = 1, 2, \ldots, N\}$.

Considering time collaborative, collaborative coefficient λ is employed to measure the constraint matched degree of the time coordinated and trajectories of network attack.

$$\lambda = \frac{T_{\max} - T_{\min}}{T} \quad (2)$$

Time constraint requires that λ is no more than 1, the more λ close to 0, the better the performance of the time is. With collaborative coefficient and constraints, evaluation is formula as

$$\min F = (1 + \lambda) \times \sum_{i=1}^{N} F(R_i) \quad (3)$$

$$\left\| p_i(t) - p_j(t) \right\| \geq d_s i \quad (4)$$

Where F presents comprehensive cost of detection track, N means collaborative track numbers. Two inequality represents the time and space constraints. The objective of collaborative track planning is: F is as small as possible once in satisfaction of collaborative time and space.Characteristic detection is transformed into a space search problem, which lays the foundation for the optimization of large scale network attacks.

3.2 Implementation of attack optimization detection

Assuming that the network data flow vector given by the monitoring can be expressed as：

$$U = \{U_1, U_2, \ldots, U_N\} \quad (5)$$

where U_i means random variable of d dimension, with random variables U_i independently. Provided U is accordance with mix distribution of K Gaussian density function, its probability function is

$$P(u/\Theta)=\sum_{K-1}^{K}\alpha_K G(U/u_k,\sum_k) \quad (6)$$

$$\Theta=\left[\alpha,u,\sum\right] \quad (7)$$

Where $G(U/u_k,\sum_k)$ means Gaussian density function, $P(u/\Theta)$ presents weighted sum of Gauss density functions, Θ is a set of three parameters $\alpha,u,\sum$ of network attack optimization, $\alpha,u,\sum$ are

$$\alpha=[\alpha_1,\alpha_2,\alpha_3] \quad (8)$$

$$u=[u_1,u_2,u_3] \quad (9)$$

$$\sum=\left[\sum_1\sum_1\cdots\sum_K\right] \quad (10)$$

The set of parameters in the model is defined as the Gauss mixture model for the optimization of network attacks.

Set $Z=(U,V)$ as sets of monitoring data U and V. However, Z is parameter vector of normal network data stream, U is parameter vector of test network data stream. Joint probability density function is defined as $P(U,V/\Theta)$.

Set Θ as the parameters set, when V means continuous variable, the formula is

$$P(U,V/\Theta)L(\Theta|U)=\log p(U/\Theta) \quad (11)$$

The maximum of the log likelihood function $L_C(\Theta|Z)$ of the missing data is achieved by maximum complete data of log likelihood function $L_C(\Theta|Z)$:

$$L_C(\Theta|Z)=\log(U,V/\Theta) \quad (12)$$

The nonlinear part $f(X)$ of the Lorenz chaotic system satisfies

$$\|f(X)-f(Y)\|\le N\|X-Y\| \quad (13)$$

Where, N is positive constant. As the chaotic system is bounded, the upper bound of the state variable set $\{|x|,|y|\}$ of chaotic system is

$$\|f(X)-f(Y)\|_2^2=\left[x_3^2+|x_3y_1|+16(x_1+y_1)^2\right] \quad (14)$$

Since the parametric value N of u is a positive constant, the K value can be taken as 1 and $N=\sqrt{66}$ when the chaotic system is normalized.

In summary, the principle of large scale network attack detection is effective.

4 Experiments and Simulation

In order to prove the proposed detection method based on collaborative planning for large-scale network attack, experiments are performed. Experiment simulation platform for characteristic detection is built in the Matlab environment. Experiments on attack detection for large scale network employ the improved algorithm and the traditional algorithm. There are 99 experiment sets to randomly collect data set. Comparing the two algorithms with accuracy, running time and error rate, effectiveness of such algorithms are shown in Table1.

Table1 characteristic detection result between algorithms

	Improved algorithm			Traditional algorithm		
Experiment times	Detection Accuracy (%)	running time(S)	Detection error（%）	Detection Accuracy (%)	running time(S)	Detection error（%）
15	96	3.3	0.01	83	4.14	0.3
25	95	3.6	0.01	86	4.32	0.4
35	94	3.6	0.01	86	4.55	0.5
45	95	3.7	0	84	4.61	0.3
55	96	3.7	0.01	84	4.76	0.5
65	98	3.7	0.01	87	4.76	0.3
75	98	3.8	0	85	4.76	0.3
85	97	3.9	0	87	4.76	0.4

It is seen in table 1 that the overall performance of the improved algorithm for large-scale network is better than the traditional algorithm with high precision and practicability.

5 Conclusions

Due to the employment of the current algorithm for large-scale network attack detection, it is difficult to describe the attack characteristics of network attacks or detect in low accuracy. Therefore, an attack detection method for large scale network based on cooperative planning is proposed. The method is based on collaborative planning to design the detection characteristic of large scale network attacks, which is transformed into a space search problem. The difference between the parameters of the flow vector and the normal vector of the normal network spatial data is extracted as characteristics, combining Gauss mixture model with the expectation maximization algorithm, to design Lorenz chaotic asynchronous tracking detection algorithm for modeling and detection of network data stream. The experimental simulation shows that the detection method of large scale network attack detection method has high accuracy and efficiency.

References

[1]Chen Hairui,Wang Huajun. Based on the Characteristics of the Sensor Network Attack Screening Node Attack Graph Construction [J]. Bulletin of Science and Technology, 2013, (12):163-165.

[2]Zhao Na. Many means converged network attacks Detection Technology [J]. Digital Technology and Application, 2014, (9):194-194.

[3]Peng Fei,Ceng Wenxue,Deng Haojiang. Unsupervised Detection of Shilling Attack for Recommender System Based on Feature Subset [J].Computer engineering, 2014, 40(5):109-114.

[4]Wu Minghui. Detection of Network Attack Signal Based on EMA and Lorenz [J]. Bulletin of Science and Technology, 2014, (2):203-205.

[5] Song Hongtao,Wang Xiaofeng,Wang Yongjun.Design and implementation of Distributed Denial service attack collaborative detection system based entropy .Mini-micro computer systems, 2015, 36(1):133-137.

[6] Yu Peng,Li Yan. Method for forecasting and DDoS attacks detecting of data center network based HEQPSO-SVM algorithm [J] .Mini-microcomputer systems, 2015, 36(1):143-149.

[7] Xia Qin,Wang Zhiwen,Lu Ke.A Method to Detect Network Attacks Using Entropy in the Intrusion Detection System[J]. Journal of Xi'an Jiaotong University, 2013, 47(2):14-19.

[8] Liu Meiling,Gao Huming.Geometrically Invariant Watermarking Using Harris-Laplace Feature Point Detector[J]. Science Technology and Engineering, 2014, 14(10):242-246.

[9]Rong Hong,Wang Huimei,Xian Ming. A Novel Method for Detecting Reduction of Quality (RoQ) Attack Based on Fast Independent Component Analysis [J]. Journal of Electronics & Information Technology, 2013:2307-2313.

[10]Zhang Hui. Optimizing Algorithm Simulation of Network Intrusion Detection of Autologous Set [J].Computer simulation, 2013, 30(8):297-300.