Grey Synthetic Clustering Method for DoS Attack Effectiveness Evaluation

Zimei Peng, Wentao Zhao, and Jun Long

National University of Defense Technology, Changsha, Hunan 410073, China
pengzimei@126.com

Abstract. Effectiveness evaluation of DoS attack is a complex problem, in which the information is incomplete and vague. The grey theory, which deals with the "less data uncertainty" matter, is a powerful tool to solve the problem. We propose a grey synthetic clustering method for DoS attack effectiveness evaluation in this paper. Firstly, we calculate grey clustering coefficient with general grey clustering method. Secondly, if there is no significant difference about grey clustering coefficient, we calculate the synthetic clustering coefficient. Finally, clustering objects can be clustered accurately with the synthetic clustering coefficient. The experimental results show that the approach is feasible and correct.

Keywords: DoS attack effectiveness, grey synthetic clustering, effectiveness evaluation.

1 Introduction

Denial of Service attack (DoS) is a widespread means of attack on the network. This attack is easy to carry out and difficult to prevent, which poses a great threat to the normal operation of Internet network system. The aim of DoS attack is to affect the normal service of attacked target system or make the functions of system be lost partially or completely. Such attack usually aims at some weakness of TCP/IP protocol or holes in computer systems. Using improper connection method, it will make the attacked target system be flooded with a lot of useless information in a short time so as to consume network bandwidth or system resources. The result is that the attacked target system is overwhelmed and could not provide normal services to legitimate users[1]. The evaluation of DoS attack effectiveness is one of the important parts of integrated assessment and safety evaluation for network attack, and it is an important and urgent task of the computer attack and defense research. There are a variety of methods for DoS attack effectiveness evaluation, such as index-based analysis[2], BP (Back-Propagation) neural network based analysis[3], and network performance based analysis[4].

Grey theory is raised for the uncertain problem lack of experience and data, in other words, the "less data uncertainty" issues[5]. The evaluation of DoS attack effectiveness is a complex problem, in which the information is incomplete and uncertain. The grey theory, which deals with the "less data uncertainty" matter, is a powerful

V. Torra et al. (Eds.): MDAI 2011, LNAI 6820, pp. 139–149, 2011.

tool to solve the problem. Evaluation methods such as the variable weight clustering method pioneered by Professor Deng Julong, fixed weight grey clustering evaluation analysis and grey clustering evaluation based on triangle whitening weight function proposed by Professor Liu Sifeng, have been widely used in part of the project areas, such as knowledge management capability evaluation[6], military information network evaluation[7]. Wang Huimei has proposed the application of grey theory in network attack effectiveness evaluation, as well as the grey fixed weight clustering effectiveness evaluation model and evaluation algorithms of computer network attack effectiveness[8]. However, the method of grey clustering evaluation proposed in paper [8] determines which grey class the clustering object belongs to with the method that compares the size of the grey clustering coefficient vector, but in practice, it is common that there is no significant difference about grey clustering coefficient. In such case, the evaluation objects can't be determined accurately with this method. After study on grey theory, we have found that grey synthetic clustering method can solve the problem. Therefore, this paper proposes a grey synthetic clustering method for DoS attack effectiveness evaluation.

The structure of this paper is as follows: Section 1 is the introduction. Section 2 describes the index system of DoS attack effectiveness evaluation. Section 3 gives the details of the grey synthetic clustering method for DoS attack effectiveness evaluation. Section 4 presents an experiment and analysis of the result. Finally, Section 5 gives the conclusion.

2 Index System of Effectiveness Evaluation of DoS Attack

The DoS attack effectiveness evaluation mainly focuses on the impact of attack on the attacked target system[9]. The purpose of DoS attack is mainly to destroy the availability and reliability of attacked target, consume up its resources, and thus make the target unable to provide normal service to legitimate users. Therefore, we can choose the following evaluation indexes.

Network bandwidth utilization rate. When DoS attack occurs, the attacker intends to make a lot of useless information to occupy the limited network resources, which results in block of network bandwidth and realization of the attacker's intent, so the network bandwidth utilization rate will change significantly.

Server's CPU and memory usage. In other words, it is the server's CPU utilization and memory utilization before and after attack. When DoS attack occurs, the attacked target will receive a large number of packets requesting for service, which will consume a large amount of CPU and memory, so the usage of CPU and memory will change greatly.

Service response delay. It is the time that the attacked target requires from receiving service request signal to providing the service. It is an important index of DoS attack effectiveness evaluation. The difference of service response delay before and after attack can reflect DoS attack effectiveness directly.

Packet loss rate. After DoS attack, the service ability of attacked target will be reduced, and it will not be able to provide normal network service to the legitimate users. At the same time, the network bandwidth will be occupied by a large number of attack packets that created by attackers deliberately, resulting in serious packet loss.

Recovery time. After DoS attack, the attacked target needs some time to recover in order to provide normal service to legitimate users. The length of recovery time can reflect the strength of DoS attack effect.

Attack mechanism. It means the way that an attack influences the attacked target. DoS attack mechanism can be divided into three types: resource consuming, service crashing and system crashing. Resource consuming means that the attacker tries to consume the legitimate resources of target, such as network bandwidth, memory, disk space, CPU, and so on. Service crashing means that the attacker makes the service of target crashed or suspended by using some weakness of service. System crashing means that the attacker makes the system crashed by using some defects of the system. It can be concluded that the attack effectiveness of these three types of attack mechanism increases step by step. In other words, system crashing attack is the most devastating, which can make the target system unaccessible; service crashing attack only makes a particular service of target unaccessible; resource consuming only consumes resources of target in order to make the target system respond more slowly, and the attacker must send packets to target system continuously to keep the attacking going on, since the system will become normal if the attacker stops sending packets.

3 Grey Synthetic Clustering Evaluation Model

This paper presents the grey synthetic clustering algorithm of DoS attack effectiveness evaluation. Based on the effectiveness evaluation index of DoS attack and in accordance of the whitening weight function of grey number, it summarizes the attack effectiveness that need to be evaluated according to grey classes, in order to determine the grey class that the effectiveness of each attack belongs to.

Definition 1[10, 11]. Assume there are n clustering objects, m clustering indexes, s grey classes, the quantitative evaluation value of clustering object i on clustering index j is $d_{ij}(i=1,2,...,n; j=1,2,...,m)$, then, $f_j^k(*)(j=1,2,...,m; k=1,2,...,s)$ is called the whitening weight function of clustering index j on grey class k. If the clustering weight of clustering index j on grey class k is independent of k, that $w_j(j=1,2,...,m)$ is the clustering weight of cluster index j, and $\sum_{j=1}^{m} w_j = 1$, then call

$$\sigma_i^k = \sum_{j=1}^{m} f_j^k(d_{ij}) w_j \tag{1}$$

the clustering coefficient of clustering object i on grey class k. Call

$$\sigma = \begin{pmatrix} \sigma_1^1 & \sigma_1^2 & \cdots & \sigma_1^s \\ \sigma_2^1 & \sigma_2^2 & \cdots & \sigma_2^s \\ \vdots & \vdots & \ddots & \vdots \\ \sigma_n^1 & \sigma_n^2 & \cdots & \sigma_n^s \end{pmatrix} \tag{2}$$

the fixed weight clustering coefficient matrix.

Definition 2[10, 11]. Set

$$\delta_i^k = \frac{\sigma_i^k}{\sum_{k=1}^{s} \sigma_i^k}, \tag{3}$$

call δ_i^k the normalized clustering coefficient of clustering object i on grey class k.

Call $\delta_i = (\delta_i^1, \delta_i^2, ..., \delta_i^s)(i = 1, 2, ..., n)$ the normalized clustering coefficient vector of clustering object i. Call

$$\prod = (\delta_i^k) = \begin{pmatrix} \delta_1^1 & \delta_1^2 & \cdots & \delta_1^s \\ \delta_2^1 & \delta_2^2 & \cdots & \delta_2^s \\ \vdots & \vdots & \ddots & \vdots \\ \delta_n^1 & \delta_n^2 & \cdots & \delta_n^s \end{pmatrix} \tag{4}$$

the normalized clustering coefficient matrix.

Definition 3[12]. Assume there are n clustering objects, s grey classes, let $\eta = (1, 2, ..., s-1, s)^T$, then call

$$\omega_i = \delta_i \cdot \eta = \sum_{k=1}^{s} k \cdot \delta_i^k (i = 1, 2, ..., n) \tag{5}$$

synthetic clustering coefficient of clustering object i. Where call $\eta = (1, 2, ..., s-1, s)^T$ synthetic clustering coefficient weight vector. It can be proved that $1 \le \omega_i \le s, i = 1, 2, ..., n$.

Definition 4[12, 13]. When there is no significant difference about grey clustering coefficient of clustering object i, if synthetic clustering coefficient of object i $\omega_i \in [1 + (k-1)(s-1)/s, 1 + k(s-1)/s]$, we call that object i belongs to grey class k.

The grey synthetic clustering evaluation algorithm of DoS attack effectiveness is as follows.

Step 1: Determine the evaluation index system. According to the index system of DoS attack effectiveness evaluation as discussed in section 2, we can identify the grey synthetic clustering evaluation index set $I = \{I_1, I_2, ..., I_m\}$.

Step 2: Determine the weight of each index. There are many means to determine the index weight, such as AHP (Analytic Hierarchy Process) method and Rough Set method. Through Rough Set method, the weight of each index can be identified: $W = \{w_1, w_2, ..., w_m\}$. The method is described in detail as follows.

We use the knowledge representation system $S = (U, A)$ in rough set theory to represent the attack samples, where U is a finite nonempty set of objects, called domain of discourse; A is a finite nonempty set of indexes including the condition indexes set I and the decision indexes set J, and $I \bigcup J = A$, $I \bigcap J = \Phi$.

The dependence degree of the decision indexes set J on the condition indexes set I is defined as:

$$\gamma_I(J) = card(pos_I(J)) / card(U) \ . \tag{6}$$

The dependence degree of the decision indexes set J on the condition indexes set $I-\{a\}$ ($a \in I$) is defined as:

$$\gamma_{I-\{a\}}(J) = card(pos_{I-\{a\}}(J)) / card(U) \tag{7}$$

where $card(\bullet)$ is the radix of set, $pos_I(J)$ is the I positive domain of J, that is,

$$pos_I(J) = \bigcup_{X \in U/J} \underline{IX} \ . \tag{8}$$

The I positive domain of J is the object set which can be precisely partitioned to the equivalence class of J according to the information of U / I.

The importance degree of condition index a is defined as:

$$\sigma_J(a) = 1 - \frac{\gamma_{I-\{a\}}(J)}{\gamma_I(J)} \ . \tag{9}$$

We can calculate the importance degree of each condition index according to the method described above. Let

$$w_i = \sigma_J(i) \Big/ \sum_{a \in I} \sigma_J(a) \ , \tag{10}$$

and we can get the weight vector of evaluation indexes as $W = \{w_1, w_2, ..., w_m\}$.

Using the definition of attribute importance in rough set theory, it needn't any prior information beyond the research data set in data processing to get the weight of each index, so the subjectivity brought by experts in subjective weighting methods such as AHP method can be effectively overcame, and the weights obtained can be more objective.

Step 3: Determine the sample matrix. Assuming the value of attack i on index j is $d_{ij} (i = 1, 2, ..., n; j = 1, 2, ..., m)$, then construct the sample matrix D according to the data sample of DoS attacks as follows:

$$D = \begin{pmatrix} d_{11} & d_{12} & \cdots & d_{1m} \\ d_{21} & d_{22} & \cdots & d_{2m} \\ \vdots & \vdots & \ddots & \vdots \\ d_{n1} & d_{n2} & \cdots & d_{nm} \end{pmatrix} . \tag{11}$$

Step 4: Determine the evaluation grey class and the whitening functions. Determine the grade of grey types and grey number in accordance with the evaluation requirement. Assuming there are s grey classes, we can give the whitening function of index j on grey class k $f_j^k(*)(j = 1, 2, ..., m; k = 1, 2, ..., s)$.

(1)Upper bound level, grey number $\otimes \in [0, \infty]$, the corresponding whitening function is as follows:

$$f_j^k(d_{ij}) = \begin{cases} \dfrac{d_{ij}}{c_j^k}, d_{ij} \in [0, c_j^k] \\ 1, d_{ij} \in (c_j^k, \infty) \\ 0, d_{ij} \notin [0, \infty) \end{cases} . \tag{12}$$

(2) Middle level, grey number $\otimes \in [0, c_j^k, 2c_j^k]$, the corresponding whitening function is:

$$f_j^k(d_{ij}) = \begin{cases} \dfrac{d_{ij}}{c_j^k}, d_{ij} \in [0, c_j^k] \\ \dfrac{d_{ij} - 2c_j^k}{-c_j^k}, d_{ij} \in (c_j^k, 2c_j^k] \\ 0, d_{ij} \notin [0, 2c_j^k] \end{cases} . \tag{13}$$

(3) Low bound level, grey number $\otimes \in [0, c_j^k, 2c_j^k]$, the corresponding whitening function is:

$$f_j^k(d_{ij}) = \begin{cases} 1, d_{ij} \in [0, c_j^k] \\ \dfrac{d_{ij} - 2c_j^k}{-c_j^k}, d_{ij} \in (c_j^k, 2c_j^k] \\ 0, d_{ij} \notin [0, 2c_j^k] \end{cases} . \tag{14}$$

Step 5: Calculate clustering coefficient. According to the whitening function $f_j^k(*)(j = 1, 2, ..., m; k = 1, 2, ..., s)$, the index weight $w_j(j = 1, 2, ..., m)$ and the sample value of attack i on index j $d_{ij}(i = 1, 2, ..., n; j = 1, 2, ..., m)$, we can calculate the clustering coefficient of attack i on grey class k σ_i^k using Eq. (1).

Step 6: Calculate the normalized clustering coefficient. Calculate the normalized clustering coefficient of attack i on grey class k δ_i^k using Eq. (3).

Step 7: Construct the normalized clustering coefficient vector. Construct the normalized clustering coefficient vector of attack i as follows: $\delta_i = (\delta_i^1, \delta_i^2 ... \delta_i^s); (i = 1, 2, ..., n)$.

Step 8: Calculate the synthetic clustering coefficient. According to the normalized clustering coefficient vector δ_i and weight vector of clustering coefficient $\eta = (1, 2, ..., s-1, s)^T$, we can calculate the synthetic clustering coefficient of attack i ω_i using Eq. (5).

Step 9: Determine the grey class, and give out the evaluation results. The range of synthetic clustering coefficient is divided into s disjoint intervals of equal length, which is $\left[1,1+\frac{s-1}{s}\right],\left[1+\frac{s-1}{s},1+\frac{2(s-1)}{s}\right],...,\left[s-\frac{s-1}{s},s\right]$. When synthetic clustering coefficient $\omega_i \in [1+(k-1)(s-1)/s,1+k(s-1)/s]$, we can determine that the attack i belongs to grey class k.

4 Example and Verification

DoS attack effectiveness evaluation is conducted using the grey synthetic clustering evaluation model and algorithm of DoS attack effectiveness in order to validate the availability of the algorithm. There is no open data source found in the area of DoS attack effectiveness evaluation. Even if there is, the evaluation indexes could not be exactly as same as ours. Therefore, we need to generate the data source by ourselves. The method is to set some corresponding attack scenarios and generate sample data of various DoS attack effectiveness evaluation indexes. Table 1 are the experimental data of dozens of DoS attacks generated using simulated DoS attack scenarios, where: a1, said the network bandwidth utilization, a2, said the change in CPU utilization, a3, said the change in memory utilization, a4, said the response delay, a5, said packet loss rate, a6, said the recovery time, a7 that the mechanism of attack, the sample space is {wr, srvc, sysc}, where wr that resources consuming, srvc said the service crashing, sysc that system crashing. Results of the evaluation is represented with K = {1,2,3,4} 4 grey types, where k=1 means "very good", k=2 means "good", k=3 means "general" and k=4 said "poor". We can use the rough set method described in paper [8] to determine the index weight, and we get the weights of DoS attack effectiveness evaluation index:

$$w = \{0.122, 0.213, 0.162, 0.113, 0.089, 0.136, 0.165\} . \quad (15)$$

Table 1. Data of DoS attacks experiment

attack	a1	a2	a3	a4	a5	a6	a7
1	81%	92%	78%	9.5s	34%	2.5m	srvc
2	30%	10%	61%	1.1s	14%	7.5m	wr
3	30%	28%	40%	4.5s	16%	0.9m	wr
4	94%	71%	81%	6.5s	35%	9m	sysc
5	22%	20%	10%	0.1s	1%	0.15m	wr
6	68%	94%	79%	3.2s	40%	2.7m	sysc
7	58%	74%	71%	1.8s	10%	3.25m	srvc
8	20%	13%	10%	7.0s	20%	5.35m	wr
9	48%	80%	40%	3.1s	11%	4.25m	wr
10	20%	20%	17%	4.4s	11%	7m	wr

According to the data of Table 1, we can get the sample matrix after quantifying a7:

$$D=\begin{vmatrix} 0.81 & 0.92 & 0.78 & 9.5 & 0.34 & 2.5 & 2 \\ 0.30 & 0.10 & 0.61 & 1.1 & 0.14 & 7.5 & 1 \\ 0.30 & 0.28 & 0.40 & 4.5 & 0.16 & 0.9 & 1 \\ 0.94 & 0.71 & 0.81 & 6.5 & 0.35 & 9 & 3 \\ 0.22 & 0.20 & 0.10 & 0.1 & 0.01 & 0.15 & 1 \\ 0.68 & 0.94 & 0.79 & 3.2 & 0.4 & 2.7 & 3 \\ 0.58 & 0.74 & 0.71 & 1.8 & 0.1 & 3.25 & 2 \\ 0.20 & 0.13 & 0.10 & 7.0 & 0.2 & 5.35 & 1 \\ 0.48 & 0.80 & 0.40 & 3.1 & 0.11 & 4.25 & 1 \\ 0.20 & 0.20 & 0.17 & 4.4 & 0.11 & 7 & 1 \end{vmatrix}. \tag{16}$$

According to the steps of grey synthetic clustering evaluation algorithm, we firstly give out the whitening weight functions of each index on each grey class according to sample set, and then summarize the attack effectiveness that need to be evaluated according to whitening weight functions, and at last determine the grey class that effectiveness of each attack belongs to. According to the training sample set, whitening weight function is given in Table 2.

Table 2. Whitening weight function of each index on each grey class

Grey class 1	Grey class 2	Grey class 3	Grey class 4
$f_1^1(c_1^1,\infty)=f_1^1(0.8,\infty)$	$f_1^2(-,c_1^2,+)=f_1^2(-,0.6,+)$	$f_1^3(-,c_1^3,+)=f_1^3(-,0.4,+)$	$f_1^4(0,c_1^4)=f_1^4(0,0.2)$
$f_2^1(c_2^1,\infty)=f_2^1(0.9,\infty)$	$f_2^2(-,c_2^2,+)=f_2^2(-,0.7,+)$	$f_2^3(-,c_2^3,+)=f_2^3(-,0.5,+)$	$f_2^4(0,c_2^4)=f_2^4(0,0.3)$
$f_3^1(c_3^1,\infty)=f_3^1(0.8,\infty)$	$f_3^2(-,c_3^2,+)=f_3^2(-,0.65,+)$	$f_3^3(-,c_3^3,+)=f_3^3(-,0.4,+)$	$f_3^4(0,c_3^4)=f_3^4(0,0.1)$
$f_4^1(c_4^1,\infty)=f_4^1(8,\infty)$	$f_4^2(-,c_4^2,+)=f_4^2(-,6,+)$	$f_4^3(-,c_4^3,+)=f_4^3(-,1,+)$	$f_4^4(0,c_4^4)=f_4^4(0,0.1)$
$f_5^1(c_5^1,\infty)=f_5^1(0.4,\infty)$	$f_5^2(-,c_5^2,+)=f_5^2(-,0.2,+)$	$f_5^3(-,c_5^3,+)=f_5^3(-,0.1,+)$	$f_5^4(0,c_5^4)=f_5^4(0,0.01)$
$f_6^1(c_6^1,\infty)=f_6^1(8,\infty)$	$f_6^2(-,c_6^2,+)=f_6^2(-,6,+)$	$f_6^3(-,c_6^3,+)=f_6^3(-,2,+)$	$f_6^4(0,c_6^4)=f_6^4(0,0.25)$
$f_7^1(c_7^1,\infty)=f_7^1(3,\infty)$	$f_7^2(-,c_7^2,+)=f_7^2(-,2,+)$	$f_7^3(-,c_7^3,+)=f_7^3(-,2,+)$	$f_7^4(0,c_7^4)=f_7^4(0,1)$

The mathematical expressions of four whitening functions of index 1 are

$$f_1^1(d_{ij})=\begin{cases} \dfrac{1}{0.8}d_{ij}, & d_{ij}\in[0,0.8] \\ 1, & d_{ij}\in[0.8,\infty] \\ 0, & other \end{cases}, \tag{17}$$

$$f_1^2(d_{ij})=\begin{cases} \dfrac{1}{0.6}d_{ij}, & d_{ij}\in[0,0.6] \\ -\dfrac{1}{0.6}d_{ij}+2, & d_{ij}\in[0.6,1.2] \\ 0, & other \end{cases}, \tag{18}$$

$$f_1^3(d_{ij}) = \begin{cases} \frac{1}{0.4} d_{ij}, & d_{ij} \in [0, 0.4] \\ -\frac{1}{0.4} d_{ij} + 2, & d_{ij} \in [0.4, 0.8] \\ 0, & other \end{cases}, \tag{19}$$

$$f_1^4(d_{ij}) = \begin{cases} 1, & d_{ij} \in [0, 0.2] \\ -\frac{1}{0.2} d_{ij} + 2, & d_{ij} \in [0.2, 0.4] \\ 0, & other \end{cases}. \tag{20}$$

Similarly, we can get the mathematical expression of whitening functions of index 2, 3, 4, 5, 6, 7.

According to the evaluation index weights and the formula in step-five of grey synthetic clustering evaluation algorithm, we can get the fixed weight clustering coefficient matrix:

$$\sigma = (\sigma_i^k) = \begin{vmatrix} 0.83 & 0.65 & 0.31 & 0 \\ 0.42 & 0.51 & 0.45 & 0.44 \\ 0.36 & 0.50 & 0.55 & 0.44 \\ 0.92 & 0.66 & 0.21 & 0 \\ 0.16 & 0.22 & 0.31 & 0.99 \\ 0.82 & 0.58 & 0.24 & 0 \\ 0.62 & 0.78 & 0.54 & 0 \\ 0.37 & 0.49 & 0.24 & 0.66 \\ 0.54 & 0.67 & 0.51 & 0.16 \\ 0.37 & 0.47 & 0.38 & 0.55 \end{vmatrix}. \tag{21}$$

With further calculation, we can get the normalized clustering coefficient matrix:

$$\prod = (\delta_i^k) = \begin{vmatrix} 0.47 & 0.36 & 0.17 & 0 \\ 0.23 & 0.28 & 0.25 & 0.24 \\ 0.19 & 0.27 & 0.30 & 0.24 \\ 0.51 & 0.37 & 0.12 & 0 \\ 0.10 & 0.13 & 0.18 & 0.59 \\ 0.50 & 0.35 & 0.15 & 0 \\ 0.32 & 0.40 & 0.28 & 0 \\ 0.21 & 0.28 & 0.14 & 0.37 \\ 0.29 & 0.35 & 0.27 & 0.09 \\ 0.21 & 0.27 & 0.21 & 0.31 \end{vmatrix}. \tag{22}$$

And the synthetic clustering coefficients of the ten attacks are: $\omega_1 = 1.7074$, $\omega_2 = 2.4968$, $\omega_3 = 2.5745$, $\omega_4 = 1.5996$, $\omega_5 = 3.2624$, $\omega_6 = 1.6425$, $\omega_7 = 1.9597$, $\omega_8 = 2.6759$, $\omega_9 = 2.1589$, $\omega_{10} = 2.6223$.

By analyzing in accordance with step-nine in the grey synthetic clustering evaluation algorithm, we can obtain the evaluation of attack effect:

$\omega_1, \omega_4, \omega_6 \in [1,1+3/4]$

shows that the effect of attack 1, 4 and 6 is "very good";

$\omega_2, \omega_7, \omega_9 \in [1+3/4,1+6/4]$

shows that the effect of attack 2, 7 and 9 is "good";

$\omega_3, \omega_8, \omega_{10} \in [1+6/4,1+9/4]$

shows that the effect of attack 3, 8 and 10 against "general";

$\omega_5 \in [1+9/4,4]$

shows that the effect of attack 5 is "poor".

Using the general fixed weight clustering evaluation algorithm proposed by paper [8], analyzing the fixed weight clustering coefficient matrix, we get the results as following: the effect of attack 1,4,6 is "very good"; attack 2,7,9 is "good"; attack 3 is "general"; attack 5,8,10 is "poor. "

By analyzing and comparing the results of the general fixed weight clustering evaluation algorithm and the synthetic clustering evaluation algorithm, we can conclude that there are some differences between results of the two methods, but it is in accordance with the conclusion in paper [12], that is, when the significant difference of clustering coefficient of clustering objects satisfies $\theta \geq 1-2/s$, the evaluation results of the two methods is of the same.

This evaluation method, which uses the definition of attribute importance in rough set theory, determines the weight of each index according to the samples of discourse domain. Compared with other evaluation methods such as AHP-based method and index-based analysis method, it needs no experts' marking and thus decreases subjective influence and increases the objectivity of the evaluation results. Different with the traditional evaluation methods such as fuzzy comprehensive evaluation method and regression analysis method, this evaluation method not only needs very little information and does not require the sample subject to any distribution, but also greatly simplifies the complex horizontal comparison of indexes which makes calculating simple and convenient. With this method we can not only evaluate the effectiveness of a single attack, but also do some sorting work on effectiveness of different attacks of the same attack type. By analyzing the experimental results, we can conclude that the evaluation results accord with reality.

5 Conclusion

DoS attacks are widespread network attacks, they are diverse in means and very destructive. How to evaluate the effectiveness of DoS attack is an important and urgent task of the computer attack and defense research. This paper presents a grey synthetic clustering method for DoS attack effectiveness evaluation. It solves the problem that the evaluation model of network attack effectiveness, which is based on general grey

clustering, can not accurately evaluate the object when there is no significant difference between the clustering coefficients. Finally, we compare the results of the two methods through an experiment, and it is proved that the grey synthetic clustering evaluation model is correct and feasible.

References

1. Qi, J., Zhou, X.: Simulation and evaluating efficiency of DoS attacks. Journal of Information Engineering University 8(3), 360–363 (2007) (in Chinese)
2. Wang, Y., Xian, M., Wang, G., Xiao, S.: Study on effectiveness evaluation of computer network attacks. Computer Engineering and Design 26(11), 2868–2870 (2005) (in Chinese)
3. Cheng, W., Lu, Y., Xia, Y., Yang, G.: Research on the vulnerability evaluation of computer network. Journal of Anhui University Natural Science Edition 31(4), 29–32 (2007) (in Chinese)
4. Zhang, W., Zhao, R., Zhang, Z., Shan, Z.: Simulation and effect evaluation of DoS attacks. Computer Engineering and Design 30(3), 544–546 (2009) (in Chinese)
5. Deng, J.: Elements on Grey Theory. Huazhong University of Science and Technology Press, Wuhan (2002) (in Chinese)
6. Zheng, W., Hu, Y.: Grey evaluation method of knowledge management capability. In: Second International Workshop on Knowledge Discovery and Data Ming, pp. 256–260. IEEE Computer Society Press, Washington (2009)
7. Tang, H., Zhang, J., Su, K.: On evaluation model of military information network based on multilevel grey evaluation method. In: Proceedings of the 27th Chinese Control Conference, pp. 113–116. IEEE Press, New York (2008)
8. Wang, H., Jiang, L., Xian, M., Wang, G.: Grey evaluation model and algorithm of network attack effectiveness. Journal on Communications 30(11A), 17–22 (2009) (in Chinese)
9. Zhang, L., Cao, Y., Wang, Q.: A DoS attack effect evaluation method based on multisource data fusion. In: 2010 International Conference on Communications and Mobile Computing, pp. 91–96. IEEE Computer Society Press, Washington (2010)
10. Liu, S., Guo, T., Dang, Y.: Grey System Theory and Application. The Science Press, Beijing (1999) (in Chinese)
11. Liu, S., Lin, Y.: An Introduction to Grey Systems: Foundations, Methodology and Applications. IIGSS Academic Publisher, Slippry Rock (1998)
12. Dang, Y., Liu, S., Liu, B., Zhai, Z.: Research on the grey synthetic clustering method in clustering coefficient of no significant difference. Chinese Journal of Management Science 13(4), 69–73 (2005) (in Chinese)
13. Dang, Y., Liu, S., Liu, B., Tang, X.: Study on Grey Synthetic Clusters Appraisals Model. In: 2004 IEEE International Conference on Systems, Man and Cybernetics, pp. 2398–2402. IEEE Press, New York (2004)