Grey Evaluation Model and Algorithms of Computer Network Attack

Bin Chen

Tourism and Culture College of Yunnan University, Yunnan, China 674100

Keywords: Computer network attack; Grey theory; Evaluation model; Algorithm

Abstract. With the rapid development of computer technology, the research of evaluation of computer network attack has become a hot topic in recent years. This is a very complex problem, which requires that it can attack the intended target accurately. The two main points are the effectiveness of online assessment attacks and the rational and scientific development of attack strategies. In this paper, the grey evaluation model and algorithm of computer network attack are analyzed, and the online evaluation model and algorithm are put forward according to the effect and characteristics of computer network attack. The determination of evaluation index is also analyzed, and a relatively complete evaluation index system of congratulations is established, and the thought of computer network attack is obtained.

Nowadays, in the computer age, computers have developed at a high speed, which also makes network attacks change from small-scale to large-scale, more cooperative and multi-level. Network attack is a more complex problem, and its complexity is mainly manifested in two aspects. On one hand, it is uncertain; on the other hand, it is diversity. Nowadays, network attacks are carried out in complex environments, and the main thing is to evaluate their effectiveness and qualitatively. Effective evaluation results can test the effectiveness of network attacks, and ensure the security of network attacks. In most network attack and defense systems, it is difficult to control the target effectively, which leads to incomplete evaluation information and imperfect evaluation indicators. This requires a powerful tool to deal with such problems, and gray theory is the best one. Gray theory can solve the problems of incomplete information and incomplete data, and its requirements are not strict, and it does not distribute according to any data. It is a simple calculation tool, and it is a very good tool for estimating the effect of computer network. Therefore, the grey evaluation model and algorithm of computer network attack are analyzed and discussed in this paper.

1. Analysis of the Current Situation of Computer Network Attack

At present, it is precisely because of the rapid development of computer networks that computer networks play a very important role in people's lives and work. The society is gradually developing towards informationization. People's demand for computers is getting higher and higher. Whether in educational institutions or industrial production, the application of computers is more and more extensive, which has a positive effect on the development of information science and technology. At present, the computer network has established a relatively secure protection system due to the need for computer security. In recent years, computer attacks have occurred, so that more and more people are paying more and more attention to the security of computer information. The current competition for computer information is mainly due to the looting of network information and the transformation of offense and defense. It has become the most important two points in computer security. In the past, the competition of computer networks mainly stayed at the concept. Nowadays, it has gradually developed into a realistic competition. With the development of information technology and its importance, computer network information technology will become one of the most important contents in the war. Due to the large risk of computer network attacks, it is necessary to have a sound security system and advanced concepts to make a correct assessment of the computer network attack.

DOI: 10.25236/ciais.2019.041

2. Analysis of the Level Assessment of the Security Level of Computer Network Systems and that of Evaluation Index

2.1 Assessment of the Security Level of Computer Network Systems

The main characteristics of the computer are divided into reliability, usefulness and confidentiality. It is due to its complex characteristics that it must be consistent with the characteristics of the computer when evaluating it, and make an overall assessment of the aggression of the computer information network. First of all, the system security of computer networks must be evaluated, in which the target layer is the most important, and the security level is also the highest. In addition, the criteria layer and the indicator layer should be estimated [1]. The computer system needs to summarize the overall security, which is basically completed by the target layer; the main requirements of the computer system are completed by the criterion layer; the evaluation of the data of the computer system is completed by the indicator layer. Under normal circumstances, safety assessment and corresponding computer security guidelines are used to analyze the security of computer systems. Further analysis of computer security guidelines is required, and the computer index should be refined to improve the security of computer network system to the greatest extent. When evaluating computer network attacks, in addition to the overall evaluation of the computer network system, the evaluation of individual scores is added to make the evaluation more realistic and achieve the true evaluation purpose. The overall evaluation score of the computer network will be related to the operation of the computer network. When the computer network is attacked, the overall evaluation score will decrease and the computer network safety factor will decrease.

2.2 Analysis of Evaluation Index System of Computer Network Attack

The diversity and complexity of computer network attacks lead to the effect of computer network attacks is also complex. We must evaluate the effect of computer network attacks from many aspects and at many levels. This requires a perfect evaluation index system of computer network attacks to enable it to reflect the effect of computer network attack effectively. When evaluating the effect of computer network attack, the principle is that the effect of network attack is reflected by the evaluation index of network attack, and the target host is calculated quantitatively. Among them, the selection of evaluation index of computer network attack is the most important. The selected index should reflect the attack effect very well. Moreover, it should not only be sensitive to some computer network parameters, but also reflect what kind of attack means, what kind of attack mechanism is generated, and the difference in attributes between various attack networks.

3. The Method of Determining Index Weight

There are many kinds of computer network attacks, and they are evaluated differently. When evaluating computer network attacks, it is very important to determine what kind of evaluation indicators correspond to each type of attacks to distribute the weight of evaluation indicators more reasonably and scientifically [2-3]. The method of rough set theory can be used to determine the index weight, which is a very useful theoretical method. It can mainly distribute the index weight for imperfect information and uncertain data expression. By using this method, we can measure the importance of attributes of network attacks very well. It is an objective process, unlike expert scoring, and we adopt analytic hierarchy process, which is easy to cause subjective errors and can quantitatively evaluate the effect of network attacks.

4. Grey Evaluation Model and Algorithms

In this paper, the grey evaluation model and algorithm for computer network attack are studied. It is usually based on the whitening weight function of grey number to divide the evaluation index of network attack into several categories, and then the network attack is corresponded with the grey class. Rough set attributes are used to determine the importance of weights of several kinds of factors, so that they can correctly reflect [4]. It is required to reflect the differences of various factors in the clustering process. This method is mainly based on the examples in the universe. It is objective and has little to do with people's subjective experience and knowledge. The grey fixed weight model of computer network attack effect is mainly evaluated by computer network attack effect, including evaluation index 1, evaluation index 2 and evaluation index n. The weight of index is mainly based on the importance of rough set. The evaluation index and whitening function are used to calculate the clustering coefficients, and the clustering vectors are constructed, so that the grey classes can be judged, and finally the results are tested.

4.1 Determination of the Weight of Evaluation Index of Network Attack

In the research of this paper, the weight coefficient of each index of computer network mainly adopts the objective weighting method. The main reason for not adopting the subjective weighting method is that it can avoid the mistakes caused by human subjective factors [5]. At the same time, in order to better reduce the error caused by human factors, the computer network indicators are measured by the importance of the attributes of the rough set. This metric does not depend on human experience, and is usually based on the domain of the sample. In the determination of specific indicator weight, the weight of each indicator is obtained according to the formula $\omega = \{\omega_{1,} \omega_{2,} \ldots, \omega_m\}$.

4.2 Complexity Analysis of Gray Algorithm

There are two main parts in the complexity of grey algorithm, including calculating index weight and calculating grey class [6]. In this study, for the actual evaluation, when the index weights are obtained, the sample training is first carried out, and then obtained from the training. The calculation time of the gray class determines the processing speed of the algorithm, and the obtained real-time processing speed is relatively correct. The algorithm of computer clustering coefficient is more complicated. In general, the stage of gray class is determined by the maximum value of each group number, which is called the half-folding algorithm. The time complexity of the algorithm is represented by o, and the attack effect is evaluated. The indicator is represented by m, the object of evaluation is represented by s, and the number of gray classes is represented by n.

4.3 Determination of Evaluation Gray

The determination of the gray class is mainly determined according to two parts. One is the attack method of the computer network, and the other is the attack mechanism of the computer network. It is mainly to determine the number of grades and grays. In this study, there are n evaluation grays, which are represented by the whitening function f_k, and the formula k (k = 1, 2, n) is adopted.

5. Summary

In a word, in the current attack and defense of computer network, because of the uncontrollability of computer network attack, the evaluation index data of computer network is incomplete, so it is difficult to evaluate and calculate, and it is very meaningful to study the grey theory. The determination of weight can make reasonable and scientific evaluation according to the importance of rough set attributes. In order to better solve the problem of attack effect in attack types, it is necessary to study the grey evaluation model and evaluation algorithm of computer network to make the attack effect more accurate.

References

[1] Wang Huimei, Jiang Liang, Xian Ming, et al. *Grey Evaluation Model and Algorithm for Computer Network Attack* [J]. Journal of Communications, 2009, 30 (S2): 17-22.

[2] Wang Xinan, Zhou Man, Wan Xin. *Quantitative Evaluation Method of Computer Network Attack Based on Network Entropy* [J]. Science and Technology Information, 2013 (5): 18-18.

[3] Wang Xian, Liu Sunjun, Tang Yiqian, et al. *A Quantitative Method for Risk Assessment of Cyber Attack Based on Grey Analytic Hierarchy Process* [J]. Journal of Chengdu University (Natural Science Edition), 2012, 31 (1): 57-60.

[4] Wang Ningning. *Research on Vulnerability Analysis and Evaluation Technology of Computer*

Network Topology [D]. Beijing Jiaotong University, 2011.

[5] Li Chengyu, Qi Yudong. *DDoS Attack Situation Assessment Based on Grey Fuzzy Hierarchical Model* [J]. Ship Electronic Engineering, 2018, v.38; No.289 (07): 26-30.

[6] Qi Wen. *Application of HHT Algorithm Improved by Grey Prediction Model in Fault Diagnosis* [D].