The Analysis Method of Secure Network Attack Graph based on Stochastic Game

Xiaoxiang Ji
Nanjing Normal University Taizhou College, Taizhou, 225300, China

Abstract: The traditional analysis method of secure network attack graph has low accuracy in practical application, and the analysis results cannot correspond with the actual threat situation of the secure network, which causes the maintenance of network environment security not timely and affects the operation of various services. Therefore, we carry out the design and research of analysis method of secure network attack graph based on stochastic game in this paper. Through the construction of network attack model based on stochastic game and the decomposition calculation of secure network attack graph, this paper has realized the threat analysis of the vulnerability of the network environment. Experiments show that the new method is more accurate than the traditional method, and the analysis result is the same as the actual attack situation of the attacker, which provides support for the follow-up network security maintenance.

Keywords: Stochastic game; Secure network; Attack graph; Analysis

1. Introduction

Network environment has a strong vulnerability, so it is often subject to the vulnerability threat of illegal attackers in the using process. It is an effective analysis method to analyze the secure network environment from the perspective of vulnerability utilization. Attack graph is a new analysis technique that has emerged in recent years. Due to its strong application advantages, it has been widely used in a short time, especially in the field of vulnerability utilization [1]. Attack graph analysis method, starting from the perspective of the attacker, through analyzing various configurations and vulnerability degree information in the network environment, finds out the essential relationship between vulnerability utilization, in order to find all possible attack paths and provide the basis for managers to take corresponding protective measures, thereby further reducing the probability of security risks. Therefore, the current attack graph is an important assessment basis for security risk assessment and performance analysis in various fields [2]. A stochastic game is a process in which many or one of the players conducting uncontrollable stochastic game. Therefore, according to this characteristic, the stochastic game is regarded as an integral game mode composed of various game stages. At the beginning of each game stage, the game is in a specific state. By introducing the concept of stochastic game into the security protection angle of network environment, the specific behavior of the network environment under attack can be fully simulated, so as to more accurately find out the path that is likely to cause network security risks through the corresponding analysis method. Therefore, based on the stochastic game, this paper carries out the design and research of analysis method of the whole network attack graph.

2. The Generation of Secure Network Attack Graph

A secure network attack is regarded as a network vulnerability attack, and the influencing factors in the attack process can be divided into four parts: the attacker's permission factor, the attacker's feasibility factor, the attacker's activeness factor and the network environment vulnerability existence factor. According to the general situation of secure network attacks, the secure network attack diagram is shown in Figure 1.

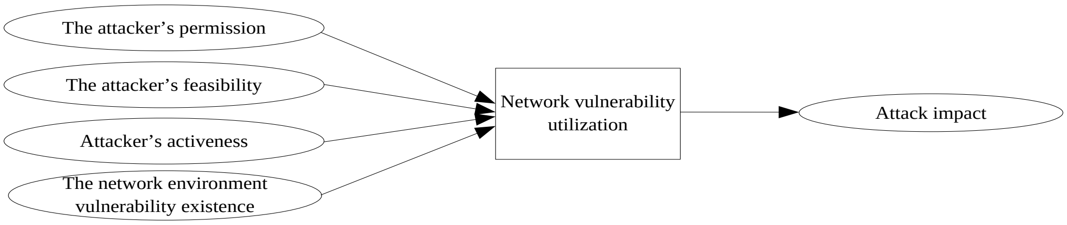
The attacker's permission
The attacker's feasibility
Attacker's activeness
The network environment vulnerability existence
Network vulnerability utilization
Attack impact

Figure 1. Secure network attack graph

In Figure 1, an attacker can successfully attack the network environment only if the above four elements are simultaneously met. Therefore, all factors are prerequisites for an attacker to attack. The first factor is that the attacker obtains the corresponding permissions through the source host connected to the network during the attack. The second factor refers to whether an illegal attacker can reach the corresponding target host when he makes a request to the network attack through the source host. The third factor refers to whether the relevant service content can still operate normally after the successful implementation of the illegal attacker's network attack. The fourth factor refers to whether there are other service contents when an illegal attacker uses the network vulnerability to attack [3]. In the actual attack process, the structure of successful implementation of network attack is mainly reflected in whether the attacker's ability has been improved. The secure network attack graph in Figure 1 is regarded as the CCSDS main network structure, in which the four factors and the impact of attack are equivalent to the libraries in the CCSDS main network structure. The attack graph can be used to indicate that the attacker's attack action itself is equivalent to the change in the CCSDS main network structure.

3. Design of Secure Network Attack Graph Analysis Method based on Stochastic Game

3.1. The construction of network attack model based on stochastic game

When the secure network is attacked, the network information is not completely limited, so the stochastic game theory can be introduced and regarded as the incomplete information supplier game. During the game, it is difficult to fully grasp the attackers' preference and attack environmental conditions. Moreover, stochastic games will be interfered by many influencing factors such as the attacks and protection strategies of both parties and the operating environment of network information. Therefore, there will still be a certain degree of randomness when considering secure network attacks as network vulnerability attacks [4]. Based on this, this paper uses the stochastic game theory to build a network attack model to simulate the attacker. The attack state of the attacker at different stages is set as a random process, and the multistage evolution process is combined with stochastic game to obtain the network attack model based on stochastic game as shown in Figure 2.

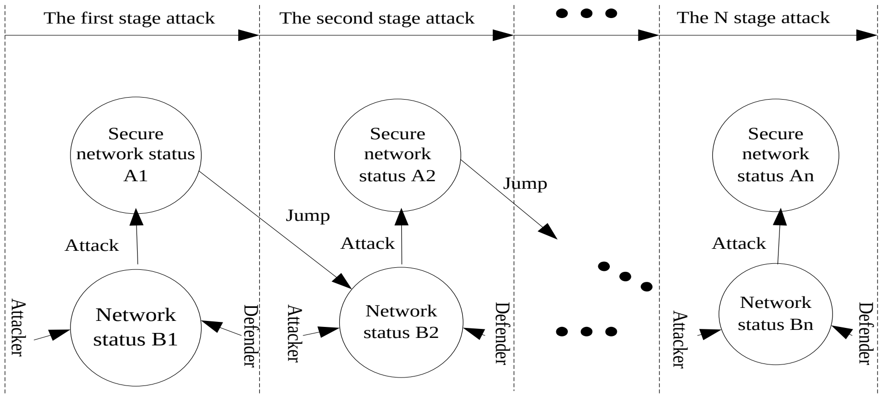

Figure 2. The network attack model based on stochastic game

In this paper, for the convenience of subsequent analysis, both the attacker and the defender in a secure network attack are regarded as ways to learn from others to improve their own capabilities, thus obtaining the maximum benefit. At the same time, the process is considered as a process of multiple states, which will change over time.

3.2. The decomposition calculation of secure network attack graph

Suppose that when an attacker attacks a secure network, the number of devices contained in the attacked network is expressed as n, and each identifiable host device n contains m vulnerable attack points. In this process, it is assumed that the host equipment can be interconnected with n-1 equipment at most. At this point, the total number of host equipment and the number of vulnerable attack points can be used to calculate the vulnerability. The formula is as follows.

$$\begin{cases} T=(n-1)\times m \\ T_{Total}=T\times n=(n-1)\times m\times n \end{cases} \quad (1)$$

In formula (1), T represents the number of vulnerabilities that each host device needs to handle; T_{Total} represents the number of vulnerabilities that need to be treated across the secure network environment. According to the above formula, the maximum number of connecting arcs of the attacker can be deduced as follows:

$$H_{\max}=n\times k\times(n-1)\times m\times n \quad (2)$$

In formula（2）, $H_{\max}$ represents the maximum number of connected arcs; k represents total number of operation permissions per host device; $n \times k$ represents the number of state phases, regardless of the size of the input data. By using the above formula, the complexity of the stochastic game can be fully satisfied as well as the deductive needs of both sides [5]. Suppose the attacker's attack path in the secure network is： $a_1 \to a_2 \to ... \to a_n$, belonging to a transition sequence in a given secure network attack graph, ai represents changes, namely, an attacking atom, the value range of I is $i \in [1, n]$. when a_i meets the following constraints, then the path connecting with ai is attacking route： Firstly, the a_i transition is in independent forms; secondly, the intersection of the set of output libraries of an transition and the set of key nodes cannot be empty; finally, in the transition sequence, the output library of the precursor transition is the input library of the subsequent transition [6]. The problem of cyclic attack path and super long attack path can be solved by using network attack graph decomposition calculation. In the actual secure network attack process, the attacker does not need to regain the attack ability and complete the attack against the new secure network environment, so the circular attack path is of little significance. According to the previous secure network attacks, there is no super long attack path in the actual attack environment. Therefore, under the premise of only executing the transformation of this network attack graph, the above algorithm can complete the attack path corresponding to each vulnerability utilization threat in the secure network at one time.

3.3. Analysis on the degree of vulnerability utilization threat of network environment

In this paper, combined with the evidence uncertainty reasoning method, the threat degree of the vulnerability of the network environment is analyzed. Since there are special uncertain inference rules in the analysis of the secure network attack graph, it is necessary to carry out specific analysis according to the special situation. Suppose the inference rule of uncertainty is F, then $F = \{b_1, b_2, b_3, ..., b_n\}$. Then suppose E is the hypothesis set that supports the establishment of F and CF is the credibility factor, then $CF = \{c_1, c_2, c_3, ..., c_n\}$, CF is mainly used to represent the credibility of F under the condition that E is true. When the network security vulnerability and evidence reasoning have a certain evaluation relationship, the threat of the vulnerability to the network can be given [7]. At this time, it can be analyzed from the attack level of the secure network, and the value range of attack graph to attack atom I can be used to map, comprehensively evaluating the success rate of the attacker to achieve the vulnerability target. The higher the final success rate is, the greater the threat degree of vulnerability utilization is; on the contrary, the lower the success rate is, the smaller the threat degree of vulnerability utilization is.

4. Contrast Experiment

In this paper, a typical global WAN application business secure network environment is taken as an example to compare the application advantages of secure network attack graph analysis method and the traditional analysis method based on the stochastic game. The secure network environment is deployed at the network trust boundary, three secure network areas are set up respectively, and the following security policies are established on each secure area: Firstly, external network users are only allowed to access part of the service content; Secondly, the host with different service content is forbidden to directly access other hosts. Finally, the administrative host in the intranet allows direct access to the space between the firewalls. It is assumed that there are Hx, Hy and Hz, three hosts. Among them, Hx is used as an attack tool in the external network segment to execute 5 attack operations in total. Hy and Hz, installed in space between firewalls and within an intranet segment, provide Bind 8.x, IE 7.0, OpenS SH D for a secure network. The analysis method in this paper is set as the experimental group, while the traditional analysis method is set as the control group. Two methods are used to analyze the five attack operations in the secure network environment and determine whether the normal operation of the network would be affected by the attack. According to the above experimental process, the comparison experiment is completed, and we sort out the experimental data and plot into the comparison table of experimental results as shown in Table 1.

Table 1. Comparison of experimental results

Hx number of attacks	The actual situation of the network is threatened	Analyze whether the experimental group is threatened or not	Analyze whether the control group is threatened or not
The First Time	Yes	Yes	Yes
The Second Time	Yes	Yes	No
The Third Time	No	No	No
The Fourth Time	No	No	Yes
The Fifth Time	Yes	Yes	No
The Correct Times	——	5 Times	2 Times

As can be seen from Table 1, the experiment is conducted 5 times in total, as for the experimental group, there are 5 correct times whether the network is threatened or not, while that of control group is only for 2 times. In addition, the analysis results of the experimental group are almost synchronous with the actual results when analyzing the secure network attack, while the control group does not detect the threat of the secure network during the second and fifth attacks on Hx. It causes the disclosure of a large number of important information and results in the failure of the normal operation of the host Hy and Hz services. Therefore, through comparative experiments, it is proved that the secure network attack graph analysis method based on stochastic game proposed in this paper can analyze the threat level of attackers more accurately than that of the traditional analysis method, when analyzing the behavior of attackers, thereby provide more powerful basis for the implementation of network protection strategies for managers.

5. Conclusions

Combining stochastic game theory, this paper proposes a new analysis method of secure network attack graph to analyze the threat degree of secure network vulnerability utilization. The effectiveness of this method in practical application is proved by experiments. Compared with the traditional analysis method, the analysis result of this method is more accurate. In the following research, we will consider the coexistence of the secure network attack graph and the sub-attack graph to carry out comprehensive analysis, thus further finding out more suitable methods for assigning credibility when the secure network is under attack.

References

[1] Chen Lin, Xu Aidong, Jiang Yixin, etc. Attack pattern recognition algorithm of power information network based on dynamic incremental cluster analysis. Southern Power System Technology. 2020, 14(08), 25-32.

[2] Wang Delong, Wang Chaofeng. Analysis of cascading failure and resistance of network in civil airports based on deliberate attacks. Journal of Transportation Engineering and Information. 2020, 18(03), 172-178.

[3] Luo Zhiyong, Yang Xu, Liu Jiahui, etc. Network intrusion intention analysis model based on bayesian attack graph. Journal on Communications. 2020, 41(09), 160-169.

[4] Dong Wei, Li Yonggang. Research on analysis of attacks on smart grid network based on complex network. Netinfo Security. 2020, 20(01), 52-60.

[5] Ma Chencheng, Du Xuehui, Cao Lifeng, etc. Burst-analysis website fingerprinting attack based on deep neural network. Journal of Computer Research and Development. 2020, 57(04), 746-766.

[6] Zhang Hua, Long Can. Prediction method of ultra-dense network attack based on thermal mode analysis and network adaptive hopping algorithm. Computer Applications and Software. 2020, 37(06), 288-296.

[7] He Junzhong. Analysis and prevention strategy of network hacker attack technology based on python. Journal of Shantou University (Natural Science Edition). 2020, 35(03), 72-80.