Modeling and simulation analysis of computer network defense

Juan Wang*

College of engineering and technology, Xi’an FanYi University, Xi’an, Shaanxi, China, 710105

*Corresponding author e-mail: 3168385183@qq.com

Abstract. With the continuous development of computer network, its network drawbacks are also increasingly prominent. There are more and more computer network attacks caused by computer network hackers and viruses, which have gradually attracted the attention and attention of government departments, military agencies and national security departments. In order to effectively improve the security of computer network, various computer network attack and defense technologies are constantly updated, and the network attack and defense simulation methods are proposed for the characteristics of network attack and defense technologies Analysis and experiment provide a platform for development. In this context, the computer network modeling and simulation method is born. Applying the modeling and simulation method to the network attack and defense security of the computer can effectively avoid the damage of the computer network. At the same time, this modeling and simulation method also has certain repeatability, flexibility, and does not consume a lot of time, which can effectively ensure the network security of the computer. This paper mainly analyzes this computer modeling and simulation method, in order to promote the computer network security.

Keywords: Computer, network security, modeling and simulation, analysis

1. Understanding of network attack
Through the information collection, sorting and analysis of the computer network system, the dangerous loopholes in the network system are easy to be damaged and intruded by the server or other network resources, resulting in the loss of data and information in the network system or the phenomenon of being monitored is called network attack [1].

1.1 steps of network attack
The main steps of network attack are as follows: ① network attackers usually hide their real IP address to avoid intruding into the target host discovery; ② network attackers prepare for network
attack by analyzing the target host's system when searching for the target; ③ network attackers usually break the target host's login account by cracking it and password, intrude into the target host; ④ when the network attacker obtains the control power of the target host, he can change some settings of the system or put some Trojan horse programs into the system, and then carry out remote control programs; ⑤ when the network attacker is carrying out network attacks, he usually steals the data information, network resources or paralyzes the host system Li et al.

1.2 types of network attacks
Generally, there are five common types of network attacks, that is, ① through password intrusion, that is, through cracking the account and login password of the target host, the network attacker implements the intrusion behavior; ② by putting a Trojan horse program into the target host for the intrusion behavior; ③ through email, the network attack behavior; ④ through hacker software, the target host implements the intrusion behavior ⑤ carry out network attack by using the security vulnerability of the target host network system.

2. Computer graphic analysis modeling and simulation method
In terms of the types of network attack modeling, attack graph and attack tree are commonly used modeling methods. The application of this model can attack the loopholes in the computer network, and form a specific network attack model, which effectively solves the loopholes in the computer network. Attack tree refers to the use of tree graphics to achieve network attacks, which is an effective way to achieve the effect of attacking network vulnerabilities. In the process of computer network attack, the target is taken as the sub node and then the attack direction is changed according to the characteristics of the network [2]. This attack tree model can effectively solve the risk and threat of the network. In the process of researching the attack tree model, we can analyze the vulnerability index of the network by using the computer as the node, and calculate the probability of successful attack. Number of tampered websites in Liaoning Province refer to figure 1.

![Figure 1](image.jpg)

**Figure 1.** Number of tampered websites in Liaoning Province

3 Characters of network virus in modeling
Common network defense software can provide users with visual display and monitoring information. Users can intuitively understand the operation of the network system through the network defense
software, and analyze whether the operation of the system is in a safe stage. The procedure behavior monitoring should be carried out simultaneously. Network defense technology is to monitor whether the computer network program is safe to run, but also has the ability of independent analysis. When the network is attacked, it can automatically prevent it from running, so as to play a role of network defense [3]. Multiple protection can be realized. When the computer network is running, dynamic simulation technology can effectively control the shortcomings of eigenvalue scanning technology in network attack, quickly and effectively detect the network system, so that the user system can run under the safe and efficient multiple protection. Work division of network technology refer to figure 2.

**Figure 2. Work division of network technology**

3.1 Research model of network infectious diseases

Worm is a common kind of computer network (as shown in Figure 2). The type and characteristics of this virus are similar to other infectious diseases. Therefore, the transmission model of network virus can be established according to the research model of network infectious diseases, and this model can be applied to the computer simulation model. The types of virus transmission are mainly represented by the types of Si, iwm and sis. In addition, there are many dual factor models. Such models can make the spread of network virus spread like the spread of epidemics. The network hosts are divided into susceptible hosts, infected hosts, removed hosts, etc., and mathematical analytic models are established by the number, time and infection coefficient of different types of hosts The simulation results can be calculated and plotted by the mathematical analysis software of MATLAB. The spread of this virus model is very scalable, and it can imitate tens of millions of node networks.

3.2 Model of data package

In order to reflect the network mop, protocol and traffic from the extensible network model, the details of the computer network environment have an impact on the spread of worms. Based on the propagation line of worm data packets, the simulation of worm data packets in the computer network can effectively reflect the network traffic, topology and other structures, thus causing the spread of worms To a certain extent, it can reflect the use of network defense strategy in time. However, the level of attention of this way is relatively low. However, in the process of establishing simulation modeling, it needs to consume a lot of computer resources. Generally, this way is difficult to be used in the simulation of some large-scale network worm modeling [4].

3.3 Hybrid model

The establishment of hybrid model mainly includes three kinds: worm spreading infection, scanning induced traffic model and routing information traffic change model. From a higher level, the worm
and transmission of computer network is a model of using network infectious diseases. The lower level takes the topology, node distribution, protocol and virus scanning into account, which leads to network traffic changes. The packet level modeling is used, and different simulation mechanisms are used for different levels of models. The infectious disease model is based on time running, while the packet model is based on event running. The two models are coordinated by a separate circular event timer.

4. Conclusions
With the continuous application of computer network, the continuous development of Internet business, the diversified development of computer science and technology and network technology, it is very important to improve the computer network defense measures and the security of network operation. At the same time, the development of network attack and defense simulation method has become a new direction of computer network research, which provides a theoretical basis for the research of virtual environment of network attack and defense, and promotes the development of network attack and defense technology.

Acknowledgement
Online course construction project of Xi’an FanYi University, project number: Z1420.

References
[1] Xiang Yangxia, Xiang Xiaoxuan. Application of virtual target based method in network attack and defense Experiment Teaching [J]. Computer engineering and design, 2009, 19 (06): 13-15.
[2] Hao Xuanwen. Research on anti destruction routing and network anti attack technology of spatial information network [J]. Xi'an University of Electronic Science and technology, 2013, 76 (23) 17-20.
[3] Liang Ying. Formal modeling and analysis of security situation of service-oriented mission critical network system [J]. Harbin University of engineering, 2009, 36 (02): 19-20.
[4] Jie Yang, Yudan Wang. An study of the type of interorganizational defamation risk based on Grounded Theory——an analysis from the Chinese scenario. International Journal of Frontiers in Sociology (2019), Vol. 1, Issue 1: 75-88.