Network Security Threat Situation Recognition Based on Attack and Defense Game Model

Binbin Liu¹,*

¹Chengdu Jinsoft Data Processing Co., Ltd.chengdu sichuang 610000, China

*Corresponding author e-mail: liubinbin@cdjdpc.org

Abstract. At present, network security is a problem that needs to be solved urgently in the current network era. In order to reduce the loss caused by network security threats, and also use limited computer resources to select the best defense strategy, a set of network attack and defense game models are designed to identify the situation of network security threats. Aiming at the unstable problem of the security quantification process of traditional network node information, a network security threat situation identification based on the offensive and defensive game model is proposed. First, build an offensive and defensive game model, design the corresponding situation identification strategy, and calculate the overall utility and expected output of both offensive and defensive parties while clarifying the changes in the authority of both sides during the offensive and defensive process. This paper takes the offensive and defensive game model as the theoretical basis of the research, uses the algorithm as the auxiliary research, and integrates its important content to analyze and research the optimization of the algorithm to improve the network security threat situation identification. This paper uses the classic offensive and defensive game model as the research object to identify the threat situation of network security. In the process of selecting the offensive and defensive game model, it is necessary to have a better grasp of the relevant algorithms. This article introduces the offensive and defensive game model into the network security threat situation identification, and on this basis, it deeply discusses the applicability and effectiveness of the offensive and defensive game model in the complex network security threat situation identification, and provides better for the establishment of future network security systems. Reference. The experimental results show that this study is effective and feasible in the offensive and defensive game model in the network security threat situation identification. It should be noted that in the defense process, the probability of success and the degree of damage of the attack path must be grasped to ensure that the optimal offensive and defensive decision-making meets the actual needs of network security.
Keywords: Offensive and Defensive Game, Game Model, Network Security Threat, Situation Recognition

1. Introduction

With the continuous enhancement of computer functions, the hidden dangers of network security and information security have been exposed continuously, so the research in the field of information security has received more and more attention. At present, the application research of offensive and defensive game theory has become a hot spot in various fields, and the theoretical evolution model of the game provides an important theoretical basis for the research in the field of network security [1]. The application of offensive and defensive game theory in network security issues mainly focuses on preliminary analysis and research to ensure the security of information networks. From the perspective of network attack and defense, the offensive and defensive game model is constructed, and the vulnerabilities in the network defense process are clearly identified through situation identification [2]. Therefore, the security analysis method of the offensive and defensive game model is given, and the game theory in the model is well introduced [3]. Through the improvement of network security threat situation identification, the human factor in the offensive and defensive behavior game can be better avoided, and those unknown attack methods can be prevented in time. According to the research, the model can accurately judge the effectiveness of security defense [4].

The offensive and defensive game model involves the construction of mathematical models for research to resolve the collaboration and conflicts between decision makers. The offensive and defensive game model contains four cores: person, strategy, payment and information. Throughout the process, the staff must use the available information to make strategic decisions, and then make appropriate profit adjustments after the selection. As people recognize the convenience of network technology, the threat of network security to people is also growing, and network security is gradually becoming a key factor in network security applications [5]. On this basis, appropriate protection systems have been continuously developed to determine the status of network security threats, thereby reducing the risks and losses caused by network security to a certain extent [6]. In the offensive and defensive game model confrontation, the attacker will use all possible attack methods for security confrontation, in order to maximize the use of limited resources to achieve the effect of the attack. In fact, the nature of offensive and defensive networks is a game between offensive and defensive parties. Therefore, to select the optimal security defense strategy, game theory must be used for analysis and verification [7].

Traditional network security protection measures basically rely on certain anti-virus software, viruses, Trojan horse intrusion detection, and firewall technologies. They usually target the intrusive target and respond to the attack target after detecting it. Relatively passive, the above-mentioned technologies have poor processing capabilities for new and difficult viruses and Trojan horses in some networks, and they usually bring serious economic losses to related production areas [8]. Therefore, in order to ensure the safe and stable operation of the network system, through the establishment of an offensive and defensive game model, an active real-time protection model is used to enhance the active processing and predictive capabilities of suspicious targets. The network security test is a tool to determine whether the computer network is secure [9]. The methods currently applied to the optimal offensive and defensive decision-making of network security are mainly based on the state offensive
and defensive diagrams. By combining the security vulnerabilities to evaluate the system security situation, and combining with the utility matrix, the optimal offensive and defensive decision is obtained. The use of optimal offensive and defensive decision-making methods can make up for the current firewall and anti-virus software passive defense defects, and better ensure network security. And this research is based on the offensive and defensive game model to identify the situation of network security threats, so as to make development breakthroughs in network security protection [10].

2. Algorithm establishment

When constructing a network attack and defense game model, it is necessary to optimize the algorithm design so that the algorithm can understand the information of network attacks and host defense, and ensure that the system can effectively resist attacks. At the same time, when developing algorithm models for cyber attack games, it is necessary to better understand the costs and benefits, create a complete offensive and defensive model, and better understand the attack and defense factors. As the formula shows:

$$\text{PR}(i) = 1 - m + m \sum_{j \neq i} (\text{PR}(j) | R_j)$$

$$\text{PR}(i) = \frac{\pi(i)}{a_i}$$

Among them, the parameter m is the damping coefficient, its value is in the range of 0 to 1, usually set to 0.85.

$$\sum_{i \in G} P(x|c(z),o)P(c(z)|o) = \sum_{i \in G} H^*(x-z)l(z)W_o(z-x')$$

$$\sum_{i \in G} H^*(x-z)l(z)W_o(z-x') = H^*(x)\otimes l(x)W_o(x-x')$$

After detecting the vulnerabilities of each node, it is necessary to better understand the attack path, calculate the possibility and risk of a successful attack, so that network security has a high degree of reliability and relevance. The attack path is shown in Table 1.

| Tool   | Server1 | Server2 | Server3 | Server4 |
|--------|---------|---------|---------|---------|
| Nessus | 2005-0768 | 2005-1415 | 2003-0500 | 2002-0694 |
| ISS    | 2005-0768 | 2004-2366 | 2003-0500 | 2002-0694 |
| SARA   | 2005-0768 | 2005-1415 | 2004-0010 | 2002-0694 |

For the attacker, the defender must provide targeted attack solutions to ensure the security of the system. The best host attack strategy is applied to vulnerabilities and gain user rights. When implementing protection, it is necessary to update the protection nodes to ensure that the best offensive and defensive solutions can meet the actual security requirements of the network.
3. Modeling method

By using offensive and defensive game models, the best defense strategy can be created and the cost-benefit ratio can be doubled. When using the offensive and defensive game model to analyze network security issues, the loss of network security is beneficial to the attacker. When creating an offensive and defensive game model, the correct algorithm must be selected. Applied to the equilibrium point, the local stability analysis method of the Jacobian matrix is used to analyze the stability of the evolutionary equilibrium point. The matrix of the offensive and defensive game dynamics system consists of the following equations:

\[ J = pq(1-p)(1-q) \alpha^2 \]  

(5)

Improve the efficiency of analyzing the stability of the strategy. When classifying and analyzing the situation, the defenders adopting strong or weak defense strategies and the attackers adopting strong or weak attack strategies are simulated respectively. There are two types of equilibrium solutions for the evolution of the offensive and defensive game system:

\[ \det J = (1-2p)(1-2q)(-aq+T-S) \times [ap+Q-Z] \]  

(6)

\[ \text{tr} J = (1-2p)(-aq+T-S) + (1-2q) \times [ap+Q-Z] \]  

(7)

Assuming that the equilibrium point in the game is \( k \), because even with different combinations of strategies, the benefits generated may be exactly the same. The maximum benefit that the attacker can obtain in this attack behavior can be obtained by assuming the offensive and defensive game model. Regardless of the attack method, the probability is \( \frac{1}{k} \). Therefore, for each node \( N \) appearing in the Internet, the risk value is calculated as:

\[ L_i = G_{i}^{-1} \text{EXPAND}(G_{i}) \]  

(8)

Because the attacks are aimed at a certain server, not the overall organizational structure, the server may have a denial of service response, where the EXPAND function is defined as:

\[ G_{i,j}^{(i,j)} = \text{EXPAND}(G_{i,j}) \]  

(9)

Taking into account the different situations of each node, according to the relative importance value specified above, the network organization structure is calculated: the risk value is:

\[ G_{i,j}^{(i,j)} = 4 \sum_{\sum_{i=1}^{2}} G_{i,j}^{(i,j)}(\frac{2i+j}{2}, \frac{2j+n}{2}) \]  

(10)

According to the calculation results, the simulation experiment proves the effectiveness of the method in this paper. It can conduct different analysis from the risk value of each node in the Internet, and conduct key real-time monitoring of key parts of the network, which can comprehensively find risk changes and take corresponding measures. Ways to circumvent.

4. Evaluation results and research

4.1. Network vulnerability evaluation and analysis
As shown in the data in Figure 2, node vulnerability detection was performed on "OWL", "DMS", "ISS" and "SARA" in the network vulnerability evaluation and analysis. It can be seen that to study network information security, we must first understand the advantages and disadvantages of network security testing to correct the deficiencies in network security testing. Network vulnerabilities are related to weak links in the network system. Attackers use weak link attacks to increase the possibility of damage. In order to increase the security of network information, it is necessary to analyze the vulnerability of the network. In the evaluation of the system, on the one hand, recursive mathematical algorithms are used to express the attacking system, and on the other hand, the defects in the defense system are analyzed and the attack authority is changed. Research makes it more likely that attackers violate the attack method and then actively follow it. Used for network security. The actual quantitative data shows that in the real network environment, most of the data is intuitively visible, but in practical applications, it is easier to use quantitative processing. Because the processing of network information security vulnerabilities is based on knowledge, the knowledge description in quantitative processing is more intuitive and efficient, and the quantitative database can be updated easily. It is also widely used to solve practical problems. Since the intuitive expression of network information is very similar to quantitative expression, and quantitative evaluation can be expressed as a derivative relationship that is not easily decomposed into separate lines, it is recommended to use the offensive and defensive game model as a demonstration mechanism to analyze the security of network information, and its quantitative treatment is Effective solutions to problems.

4.2. Application of Game Theory
As shown in Figure 2, in the process of using the game model to analyze the optimal offensive and defensive decision-making of network security, we must pay attention to grasping the network reachability and vulnerabilities, and generate a state offense and defense map. In this process, we must pay attention to grasping the probability of success and the damage of the attack path, so as to ensure that the focus of the defense process can be grasped, so that the optimal offensive and defensive decision can meet actual needs. The mechanism of the offensive and defensive game model is to comprehensively consider the predicted behavior and actual behavior of the individual in the research target, so as to study the optimization strategy of prediction and actual behavior. The offensive and defensive game model is applied to specific network evaluation and real-time protection, and its mechanism of action is mainly manifested in four aspects. First, through game theory, the defender can find malicious nodes and normal nodes in the computer system, so as to comprehensively analyze the vulnerable links and possible security threats in the system, and prepare for possible threats in advance. Based on random game theory, it can not only analyze the Nash equilibrium of both offense and defense, but also effectively analyze the offense and defense strategies of both parties. Finally, applying the theory of offensive and defensive game model to the computer real-time active defense system can analyze the attacker's attack intention and establish the system's offensive and defensive game model, thereby ensuring the effectiveness of network information security evaluation and system protection.

5. Conclusion

The research and analysis of offensive and defensive game models are based on the experience of offense and defense in typical network scenarios. Therefore, it is shown that the offensive and defensive network offensive and defensive game model and the selection algorithm of offensive and defensive network strategies can describe the quantitative relationship between the offensive and defensive processes of the two parties. This paper proposes an offensive and defensive game model based on the network security threat situation identification information risk assessment method based on the offensive and defensive game model. By repeating the offensive and defensive game on the incomplete information in the system by the offensive and defensive parties, the attack and defense behaviors are established. The dual offensive and defensive game model improves the defense effect of the network system and predicts the risks that may appear on the Internet. The offensive and
defensive game model avoids excessive and complex computational complexity and computational cost, and the effectiveness of the risk assessment method is tested through experimental simulation, thereby avoiding unnecessary losses. It is used to conduct cyber attacks and defenses based on the best practices of offensive and defensive game models, combining vulnerabilities and network availability information to create an attack and defense status, and then a map of the attack status, finding the defense path and formulating the ideal of offensive and defense strategies Choose to establish an offensive and defensive game model to reduce risks by identifying the threat situation of network security.

References

[1] Albahar M A, Olawumi O, Haataja K, et al. Novel Hybrid Encryption Algorithm Based on Aes, RSA, and Twofish for Bluetooth Encryption[J]. Journal of Information Security, 2018, 09(2):168-176.

[2] Murugan C A, Karthigaikumar P, Priya S S. FPGA implementation of hardware architecture with AES encryptor using sub-pipelined S-box techniques for compact applications[J]. Automatika, 2020, 61(4):682-693.

[3] Agarwal A, Raj P, Katiyar S. Secured Audio Encryption using AES Algorithm[J]. International Journal of Computer Applications, 2019, 178(22):29-33.

[4] Friedhelm, Meyer, auf, et al. Paul Curzon, Peter W. McOwan: Computational Thinking; Die Welt des algorithmischen Denkens – in Spielen, Zaubertricks und R?tseln[J]. Mathematische Semesterberichte, 2019, 66(2):259–260.

[5] Kumar S S, Sherfin A. A cryptographic encryption technique byte – Spiral rotation encryption algorithm[J]. Journal of Discrete Mathematical Sciences and Cryptography, 2019, 22(6):1-6.

[6] Beenu V P. Mathematical formulation of des algorithm[J]. International Journal of Pure and Applied Mathematics, 2018, 118(10):363-376.

[7] Uka K K, Oguoma S I, Chuma-Uba U P. Analysis of Blockchain Architecture in File Sharing Management for Tertiary Institution[J]. Intelligent Information Management, 2020, 12(3):88-104.

[8] Zhu X G, Shen Y. MapReduce optimisation information query method for file management system[J]. International Journal of Reasoning-based Intelligent Systems, 2018, 10(2):117-121.

[9] Khelif N, Ghorbel A, Aydi W, et al. Generation of Chaotic Signal for Scrambling Matrix Content[J]. International Arab Journal of Information Technology, 2020, 17(4):548-553.

[10] Yang L, Yang B, Xiang C. Quantum public-key encryption schemes based on conjugate coding[J]. Quantum Information Processing, 2020, 19(11):1-16.