Proceedings of the 5th International Conference on Signal Processing and Machine Learning
DOI: 10.54254/2755-2721/120/2025.18746

Research on Network Security Threat Detection and Defense Strategies

Yuchen Huang[1,a,*]

[1]*College of Artificial Intelligence, Wuchang University of Technology, Wuhan, China*
a. yuchen.0831@outlook.com
**corresponding author*

Abstract: With the popularization of the Internet and the rapid development of information technology, network security issues have become increasingly prominent in the context of research. People are facing new network security threats brought about by the development of information technology. Network attacks are becoming increasingly complex, leading to frequent incidents of data breaches. This has also made cybersecurity an important area of competition between countries. The significance of network security lies in protecting personal information security, safeguarding the interests of enterprises, ensuring national security, promoting economic development, and enhancing social trust. Text work is aimed at focusing on a specific issue or technical problem in the field of network security, such as new attack detection and defense mechanisms, network security products and technology evaluation, etc. By studying network security threat detection and defense strategies, researchers can deepen their understanding of network threats and learn how to use existing technologies to detect various threats. By understanding the types of attacks, researchers can then develop effective defense measures.

Keywords: Threat detection, Defense strategy, Network security.

1. Introduction

With the rapid development of information technology, the internet has penetrated into every aspect of people's lives and become an indispensable part of modern society. However, with the continuous expansion of cyberspace, cybersecurity threats are becoming increasingly prominent, posing serious challenges to individual, corporate, and even national security. In this situation, the research on network security threat detection and defense strategies is particularly urgent and important.

Firstly, the severe situation of cybersecurity threats cannot be ignored. The methods of cyber attacks are constantly evolving, and the targets of attacks are becoming increasingly diverse. Hackers use Advanced Persistent Threat (APT) attacks, Distributed Denial of Service attack (DDoS) attacks, ransomware, and other means to attack individuals, businesses, and government agencies, steal sensitive information, damage critical infrastructure, and even cause social unrest. These threats not only pose a threat to information security, but may also have serious impacts on social stability and economic development.

Secondly, the research on network security threat detection and defense strategies is of great significance for addressing network security challenges. Effective threat detection technology can help people detect and respond to potential security risks in a timely manner, reducing losses. At the

DOI: 10.54254/2755-2721/120/2025.18746

same time, research on defense strategies can provide theoretical guidance and practical basis for network security protection, and improve the level of network security protection.

In today's rapidly developing technology, many people have raised many questions about network security, and many people have done a lot of work on these issues. Literature 1 constructs a new neural network by understanding various threats to network security and the technologies currently available for detecting network threats [1]. Reference 2 aims to understand the existing technologies used for detecting network security. Strengthen and improve its detection technology to better resist external threats [2]. Literature 3 further identifies the attack methods and types of network threats by improving network security detection techniques [3]. Researchers will conduct a series of research on network security issues, starting with network security detection technology. Network threat detection technology is an important component of the field of network security, aimed at identifying and defending against potential malicious activities. This article will summarize the network threat detection technology, including its basic principles, main methods, challenges, and future development trends. Then, network security defense strategies were introduced, which are not just ordinary steps, but measures that need to be synchronized with network threat detection technology.

2. Threat detection technology

Network threat detection technology is an important component of the field of network security, aimed at identifying and defending against potential malicious activities. The following is a summary of network threat detection technology, covering its basic principles, main methods, challenges, and future development trends.

The evaluation and optimization of network security threat detection technology and defense strategies are key links in ensuring network security. The purpose of evaluation and optimization is to ensure the effectiveness and adaptability of security measures. Here are some key points:

Firstly, the assessment should be based on the actual threat environment. By simulating real attack scenarios, test the accuracy and response speed of the detection system, as well as the robustness of defense strategies. The evaluation should include indicators such as detection rate, false positive rate, false negative rate, and response time.

Secondly, the optimization of defense strategies needs to consider the following dimensions:

1. Multidimensional analysis: Combining multiple detection techniques such as anomaly detection, intrusion detection, behavior analysis, etc., to form a multi-level security protection system.

2. Adaptive capability: With changes in attack methods, defense strategies should be able to automatically adjust to adapt to new threat patterns.

3. Resource optimization: Reasonably allocate security resources to ensure maximum security effectiveness within a limited budget.

4. Personnel training: Enhance the professional skills of the security team to ensure quick response and handling of security incidents.

During the optimization process, the following methods should be adopted:

-Continuous monitoring: Real time monitoring of system status, timely detection of abnormal behavior and potential threats.

-Feedback mechanism: Establish a feedback mechanism for security incidents, learn from actual events, and continuously improve detection and defense strategies.

-Automated testing: Regularly conduct automated security testing to verify the effectiveness of defense measures.

People can only prevent all unnecessary factors by continuously improving and innovating network threat detection technologies from various aspects. During personnel training, a new neural network is constructed based on common network intrusion detection deep learning techniques [1]. The threat detection technology in network security has the advantages of detailed and real-time

DOI: 10.54254/2755-2721/120/2025.18746

response, which can help people identify and solve specific system behavior problems, and respond immediately when attacked, effectively preventing or mitigating the impact of attacks [2]. People not only need to be able to achieve technological breakthroughs, but also need to be able to pinpoint the location of network threat attacks and determine the type of attack that poses the threat [3]. Currently, most technologies are based on known static protection policies. Threats are dynamic through cybersecurity, so they need to be detected beforehand so that protection policies can be updated in a timely manner, which means dynamic, proactive defense. Establish thresholds through immune selection, and realize intelligent detection of network security through knowledge maps. Improve the architecture of the intelligent detection system. It makes cyber security threat detection dynamic and intelligent, which greatly improves the performance of cyber security threat detection and analysis [4]. In the IoT environment, cybersecurity has also become a challenging issue, and the presence of cyber threats needs to be addressed. Leveraging machine learning (ML) and artificial intelligence (AI) tools to develop automated tools for cyber threat detection and classification is critical to achieving security in IoT environments. Security issues associated with IoT devices need to be effectively minimized [5]. Finally, people need to conduct an assessment of the threats to the network. Assessment is a systematic process that can identify, analyze, and quantify potential network risks, so that organizations can take corresponding preventive and mitigation measures [6]. Cybersecurity has become a long-term concern for everyone.

Through regular evaluation and optimization, the network security threat detection technology and defense strategy can maintain its progressiveness and effectiveness, and provide a solid network security guarantee for the organization. In short, network threat detection technology is a dynamically developing field that requires constant adaptation to new threats and environments. With the advancement of technology, future network threat detection will become more accurate, efficient, and automated.

3. Network Security Defense Strategy

The defense strategy of the network is a key measure to ensure network security and system stability. The following is a detailed overview of network defense strategies, including common defense methods, techniques, and best practices.

Common defense strategies

1. Firewall:

-A firewall is the first line of defense in a network, which can monitor and control data traffic entering and leaving the network.

2. Intrusion Detection and Prevention Systems (IDS/IPS):

-IDS is used to detect suspicious activities, while IPS can actively prevent these activities.

3. According to encryption:

-Encrypt data using SSL/TLS and other technologies to ensure the security of data transmission.

4. Access control:

-Implement strict user authentication and authorization to restrict unauthorized access.

5. Security updates and patch management:

-Regularly update systems and applications, and patch known security vulnerabilities.

6. Security configuration:

-Configure the security of network devices and systems, and disable unnecessary ports and services.

7. Backup and Disaster Recovery:

-Regularly backup important data and develop disaster recovery plans.

-Adopting the principle of 'never trust, always verify', strengthen access control and data protection.

DOI: 10.54254/2755-2721/120/2025.18746

In the management of network security in reality, the selection of network security defense strategies is a common problem, but existing methods for selecting defense strategies are difficult to balance the cognitive limitations of network administrators and the network topology structure. Establish an optimization model for selecting network security defense strategies based on prospect theory. This model further develops and improves the security game method, providing a new approach for solving the optimization problem of network security defense strategies from the perspective of bounded rationality, and expanding the application field of security games [7]. Many places require defense, and the power system is one of them. To ensure the normal operation of the power system and address the security issues faced in the energy optimization scheduling process of the power monitoring system, a defense strategy against malicious network attacks under a directed network topology is proposed. Researchers have designed an optimization scheduling algorithm based on elastic consistency to ensure the reliable operation of the system under non covert attacks. Then, for covert network attacks, a watermark signal labeling mechanism is introduced to prevent the impact of covert attacks on the convergence of optimization scheduling algorithms [8]. With the continuous advancement of technology, online education has become increasingly popular. Various universities in China have made certain achievements in skills practice, curriculum design, publicity and popularization, and educational reserves, and diversified teaching methods can further attract students to actively integrate into cybersecurity education. The importance of network ideological security defense for college students can be seen, and it is necessary to solve and optimize the existing problems in network ideological security defense for college students. Corresponding optimization measures should be proposed based on the actual situation, aiming to effectively strengthen college students' awareness of network security [9]. Researchers also need to continuously test the completeness of our defense strategies through drills, organizing network exercises between the red and blue teams, with a focus on offense and defense. Practical exercises require clear attack scenarios and corresponding defense strategies. However, systematic guidelines on network attack scenarios or defense strategies still need to be improved [10].

Network defense is a constantly evolving field, and organizations need to constantly adapt to new threats and technologies to protect the integrity of their networks and data. By implementing comprehensive defense strategies and best practices, organizations can better prepare for and respond to cybersecurity challenges.

4. Challenges and Prospects

With the rapid development of information technology, network security has become an indispensable part of today's society. However, the field of cybersecurity faces many challenges and also indicates future development trends.

The Challenge of Cybersecurity

1. Diversified attack methods:

-The increasingly diverse methods of network attacks, including phishing, ransomware, DDoS attacks, APT attacks, etc., make network security protection more difficult.

2. Data leakage:

-With the development of technologies such as big data and cloud computing, data breaches have occurred frequently, causing huge losses to individuals and businesses.

3. IoT device security:

-The number of IoT devices has surged, but due to their weak security protection capabilities, they are prone to becoming an entry point for hacker attacks.

4. Artificial Intelligence and Network Security:

-The development of artificial intelligence technology has made network security attacks more covert and complex, while also bringing new challenges to network security protection.

DOI: 10.54254/2755-2721/120/2025.18746

5. Imperfect laws and regulations:

-The incomplete laws and regulations on cybersecurity in various countries have increased the difficulty of cybersecurity governance.

6. Weak safety awareness:

-Some users and employees have weak security awareness, making them easy targets for hacker attacks.

Prospects for Cybersecurity

1. Technological innovation:

-With the continuous development of new technologies such as artificial intelligence, blockchain, and quantum computing, new solutions will be brought to the field of network security.

2. Safety awareness enhancement:

-By strengthening network security education, enhancing the security awareness of users and employees, and reducing network security incidents caused by human factors.

3. Improvement of laws and regulations:

-Governments of various countries should strengthen the formulation and implementation of laws and regulations on cybersecurity, and improve the level of cybersecurity governance.

4. Zero trust architecture:

-The zero trust architecture emphasizes "never trust, always verify", which helps improve network security protection capabilities.

5. Cross industry cooperation:

-Network security involves multiple industries, and cross industry cooperation helps to jointly address network security challenges.

6. Network security industry ecosystem:

-Cultivate a network security industry ecosystem, promote technological innovation and industrial upgrading.

7. Global cybersecurity governance:

-Strengthen global cybersecurity governance and jointly address transnational cybersecurity threats.

The challenges and prospects of network security coexist. In the face of network security threats, people should actively respond, strengthen technological innovation, enhance security awareness, improve laws and regulations, and jointly build a secure and stable network environment. In the future, the field of cybersecurity will continue to maintain a high level of attention to cope with the constantly changing cybersecurity situation.

5. Conclusion

The main focus of this article is to detect signals from various threats through detection techniques, and to prevent the damage caused by network attacks through various defense measures.

Network security is an important component of today's digital age, and it is crucial for the security of individuals, businesses, and countries. With the advancement of technology and the popularization of the internet, network security threats are constantly evolving, becoming more complex and diverse. Therefore, people need to take comprehensive measures to protect the security of networks and data.

Firstly, people need to strengthen technical defense measures, including the use of firewalls, encryption technology, access control, etc., to prevent malicious attacks and illegal access. At the same time, people also need to raise employees' awareness of network security, through training and education, so that they can identify and prevent threats such as phishing and social engineering.

Secondly, people need to establish effective network security management and supervision mechanisms, including developing and implementing network security policies, conducting regular security audits and evaluations, and promptly fixing vulnerabilities. At the same time, people also

DOI: 10.54254/2755-2721/120/2025.18746

need to establish emergency response plans so that they can quickly respond and handle security incidents.

Finally, people need to strengthen international cooperation and the development of laws and regulations to address cross-border cybercrime and cyber attacks. At the same time, people also need to pay attention to the social ethics and legal issues of network security, and protect the privacy and rights of users.

Overall, cybersecurity is an area that requires comprehensive, dynamic, and sustained attention. Only through the comprehensive application of various means such as technology, management, and law can the security of networks and data be effectively protected.

References

[1] *Dong, Y., Li, C., Yang, Y. K. (2024). Information Path Risk Scoring System Based on Vulnerability Information and Attack Graph. Automation Technology and Applications, 43 (10): 122-125+130. DOI: 10.20033/j. 1003-7241. 10-0122-05.*

[2] *Ding, X. Y. (2024). Analysis of Intrusion Detection and Defense Technologies in Network Security. Electronic Technology, 53 (06): 368-369*

[3] *Zhou, T. (2024). Research on Network Intrusion Detection Method Based on Deep Learning. Yunnan University of Finance and Economics, DOI: 10.27455/d.c nki.gycmc.2024.000543*

[4] *Tao, Y., Yuan, T., Wei, H., et al. (2020). An Intelligent Learning Method and System for Cybersecurity Threat Detection. Journal of Physics: Conference Series, 2020, 1575(1): 012128.*

[5] *Alrowais, F., Althahabi, S., Alotaibi, S. S., et al. (2023). Automated Machine Learning Enabled Cybersecurity Threat Detection in Internet of Things Environment. COMPUTER SYSTEMS SCIENCE AND ENGINEERING, 2023, 45(1): 687-700.*

[6] *Niu, X. B., Fang, Q., Shao, X. (2022). Network Security Emergency Response Based on Threat Assessment. Network Security Technology and Applications, (11): 3-4.*

[7] *Yu, G. F., Li, D. F. (2014). Optimization Method of Network Security Defense Strategy Based on Prospect Theory. Chinese Management Science, 1-12. https://doi.org/10.16381/j.cnki.issn1003-207x.2023.1778.*

[8] *Du, Q. W., Xu, H. Q., Zheng, X., et al. (2024). Design of defense strategy for power monitoring system against malicious network attacks. Control Engineering, 31 (01): 185-192. DOI: 10.14107/j.cnki.kzgc.20210939.*

[9] *Zou, Y. H. (2023). Analysis of college students' network ideology security defense strategy in the mobile Internet era. China New Communications, 25 (19): 120-122. Journal. The Journal of Supercomputing. Volume 80, Issue 15. PP 21642-21675*

[10] *Kim, D., Jeon, S., Kim, K., et al. (2024). Guide to developing case-based attack scenarios and establishing defense strategies for cybersecurity exercise in ICS environment. The Journal of Supercomputing, 80(15): 21642-21675.*