Transactions on Computer Science and Intelligent Systems Research
ISSN: 2960-1800, eISSN: 2960-2238 | Volume 9
AIDML 2025

Research on Network Security Attack Defense Mechanism and Its Development Trend

Xiulin Yang *

Department of Computer Science and Software Science, Hebei University of Technology, Tian Jin, China

* Corresponding Author Email: Y1039155192@outlook.com

Abstract. In the digital era, network security has become a core issue concerning the global informatization process. This article first explores the current research progress in the field of network security from two dimensions: network attack and network defense. It systematically analyzes the classic methods of each. Then, this article delves into the application prospects of blockchain technology and reinforcement learning methods in network security. Blockchain technology, with its decentralized and immutable characteristics, provides a new solution path for enhancing network security. Reinforcement learning, through its adaptive mechanism and intelligent decision-making ability, demonstrates great potential in dynamic attack defense and intrusion detection. Finally, based on the aforementioned content, this article looks forward to the future development direction of this field. This article aims to provide systematic theoretical analysis and discussion for academic research and practical application in the field of network security, reveal the limitations of existing technologies and the application potential of frontier technologies, and provide new theoretical bases and technical directions for the construction of future network security defense systems.

Keywords: Network Security; Attack; Defense.

1. Introduction

Computer network security mainly refers to the security of network information, that is, taking corresponding security prevention and control measures and technologies to ensure the security and reliability of the network environment used by users [1]. With the development of science and technology, especially in the aspect of network usage, the demand for computer network security is increasing day by day. It is widely applied in the economy, military, politics, culture and other aspects, and has slightly changed the way people live and work, becoming an indispensable part of people's life and work.

However, with the increase in network penetration rate and people's dependence on the network, network security has also exposed a series of problems. Network attacks, data leakage, malicious software and other problems constantly test the reliability of network security. These problems not only threaten personal privacy and enterprise assets, but also may trigger public safety and national security risks. Therefore, the research and exploration of network security is not only a passive defense against network threats, but also a key path to actively build a trusted network environment and improve the social digital governance ability. Identifying the core problems faced by network security, sorting out the existing defense technologies and research results, has become an important task in the field of network security research.

Against this background, this article will conduct a review of network security from three perspectives: attack technology, defense technology and future development direction. Analyzing the current status and characteristics of attack and defense technologies, and discussing their development trends, provides a comprehensive perspective for network security practitioners and researchers, helping them better understand the dynamic changes in the field of network security and formulate more effective protection strategies to enhance the security protection ability of the network.

2. Network Attack

Network security attack refers to the unauthorized access to networks, computer systems or digital devices, and the intentional theft, exposure, tampering, disabling or destruction of data, applications or other assets. According to traditional classification, network attacks can be divided into two types: passive attacks and active attacks. Passive attacks refer to attackers obtaining information by monitoring network traffic without directly damaging the network system. The main methods include traffic analysis, eavesdropping and cracking encrypted data streams, etc. Their main feature is that they do not change the original data information but obtain the data information without the user's knowledge or permission. Active attacks refer to attacks that damage the network system. The main methods include tampering with information, forging information, or causing the terminal to deny service. Their main characteristic is that this type of attack will cause some data streams to be tampered with and false data streams to be generated.

Network attack methods are constantly emerging. Commonly used network intrusion behaviors include password intrusion, IP spoofing and DNS spoofing.

Password intrusion refers to the behavior where network hackers obtain the password of the computer user system and directly login to the computer user's computer system to carry out subsequent network attacks. However, this method is used after obtaining a legitimate account, and the password of the legitimate user is cracked.

IP spoofing refers to the attacker forging the source IP address of the IP data packet to impersonate other systems or the identity of the sender, thereby deceiving the target system. This attack method exploits the vulnerability in the TCP/IP protocol and has a high execution difficulty, but it can cause serious network security threats.

DNS spoofing refers to a type of deception where the attacker impersonates a domain name server. However, it does not actually change the website of the other party, but uses the method of impersonating the domain name server to impersonate and make users believe that their website has been changed.

3. Network Defense

Network security defense refers to various policies, processes, and technologies adopted to prevent, detect, and monitor unauthorized access, abuse, modification, or denial of computer networks and their resources. Traditionally, network defense can be classified into two categories: passive defense and active defense. Currently, most defense methods are passive defense, which are security measures taken after a computer is attacked. The main methods include firewall technology and intrusion detection system technology. Passive defense usually refers to organizing attackers to a certain extent but cannot completely prevent attacks or protect data. Active defense refers to proactive defense with prior planning, which prevents attackers from launching attacks on targets through certain mechanisms [2]. The active defense strategy mainly consists of three parts: intrusion prevention, network security intrusion detection, and network security intrusion response [3]. It provides timely warnings before a computer is invaded and builds a defense system in real time. By quickly capturing changes in network traffic and analyzing programs, suspicious behaviors are prohibited to ensure the security of the computer system.

Network defense is an indispensable part of computers. Common network defense methods include firewall technology, data encryption technology, and intrusion detection technology. Firewall technology refers to a network barrier set up by computer technology to block external adverse factors, preventing others from stealing computer user information and blocking unauthorized access, providing reliable data management and security guarantees for users. Data encryption technology refers to transforming information (plain text) into meaningless ciphertext through encryption keys or encryption functions. When the recipient receives it, it can be restored to the original information through decryption keys. Intrusion detection technology refers to collecting information from various

computer and network systems and analyzing it to detect intrusion characteristics. It can well make up for the shortcomings of firewall technology and is usually regarded as the second line of defense after the firewall.

4. Application

Network attack methods are continuously evolving, increasing in complexity and diversity on a daily basis. Simultaneously, network security defense technologies are also being constantly updated and iterated to enhance the reliability of network security more effectively. From early rudimentary protective measures to today's sophisticated and multi-dimensional detection systems, network security technologies have consistently focused on risk and attack detection, prevention, and response. To better address emerging challenges, network security must incorporate new technologies to overcome the limitations of traditional defense mechanisms and improve defense capabilities to align with future development trends.

4.1. Research on Network Security Based on Blockchain

In the domain of network security, blockchain technology offers a broad range of application scenarios. Blockchain is a decentralized distributed ledger characterized by blockchain storage, immutability, and security and trustworthiness. It is a technology that ensures security, transparency, and immutability.

With the advancement of technology, traditional consensus mechanisms have increasingly exposed limitations in performance and scalability. Consequently, researching novel consensus protocols and hybrid mechanisms has become a critical direction for enhancing the security and scalability of blockchain. Venkatesan et al. explored new consensus protocols and hybrid consensus algorithms incorporating machine learning technology. By integrating traditional consensus mechanisms with machine learning techniques, they dynamically adjusted parameters during the consensus process using machine learning algorithms (e.g., Particle Swarm Optimization (PSO)) to optimize node selection and transaction verification processes. This approach proposed an effective method to enhance the security and scalability of blockchain-based network security. Compared to traditional Proof-of-Work (PoW) and Proof-of-Stake (PoS) mechanisms, this method demonstrates superior throughput, handles a higher volume of transactions, reduces transaction confirmation time, and significantly enhances security [5].

Bao proposed a heterogeneous identity trust exchange framework based on consortium blockchain, investigating the application of dynamic data security storage modeling and ownership state transfer functions. Through an analysis of blockchain technology's characteristics, it was determined that blockchain provides significant advantages in ensuring network security, particularly in preventing data tampering and protecting data integrity. The blockchain-based network security protection mechanism system he proposed achieved efficient data encryption and distributed storage through dynamic data security storage modeling, thereby effectively enhancing network security. Additionally, the ownership state transfer function he designed offered a reliable solution for data ownership management and state tracking [6].

Yang Huan proposed a blockchain-based system that integrates the Cam Shift active defense algorithm and other intelligent algorithms to enhance network data security. Upon detecting potential dangerous behaviors, the system can automatically activate pre-defined defense functions to mitigate network security threats. Test results indicate that this system can accurately identify signals exhibiting dangerous behaviors within a short timeframe and implement corresponding defense measures [7].

4.2. Research on Network Security Based on Reinforcement Learning

Reinforcement learning (RL) game technology has recently gained prominence in the field of network security. RL is a machine learning paradigm rooted in the Markov Decision Process (MDP)

framework, enabling agents to learn optimal strategies through trial-and-error interactions with their environment.

Alam et al. introduced a Federated Deep Reinforcement Learning (FRL) framework integrated with blockchain technology. This framework performs local deep reinforcement learning at the IoT device layer to generate local model parameters. Subsequently, the blockchain layer records device interactions and the history of model parameter updates. The federated learning layer aggregates these local parameters to construct a global model. Additionally, the smart contract layer automates the verification of model parameter legitimacy and incentivizes data-contributing devices. Experimental findings demonstrate that this approach significantly mitigates the risk of data privacy leakage, enhances data security, reduces data transmission volume, improves computational efficiency, and markedly boosts overall system performance [8].

Wang Gang et al. examined the defense mechanism of the Actor-Critic algorithm, which integrates policy gradients and value functions. This algorithm operates via two primary components: Actor and Critic, functioning within a simulated environment. Experimental results indicate that while a 10% false alarm rate requires further optimization, the algorithm effectively strengthens network security defenses [9].

Su employed a deep reinforcement learning methodology to compute the network interference efficiency factor, design a differentiated time series prediction structure, and establish a normalized deep reinforcement learning prediction model. This approach facilitates the evolutionary prediction of security scenarios under deep reinforcement learning. By leveraging a hybrid optimization strategy, it successfully predicts network security situations, offering significant potential for the future development of network security [10].

5. Current Limitations and Future Prospects

As new technologies continue to evolve, they bring both unprecedented opportunities and challenges to the field of network security. In recent years, the application of big data has expanded significantly, leading to an increase in the number of users. This growth also exposes vulnerabilities within network security systems, making them susceptible to attacks. For instance, attackers leveraging reinforcement learning technology can efficiently gather large volumes of network data, conduct rapid analyses, and effectively identify vulnerabilities and weaknesses in target system programs. Such capabilities enable attackers to devise precise strategies for launching sophisticated assaults. Conversely, defenders utilizing big data analysis technology can now perform real-time monitoring and analysis of massive amounts of network data with relative ease. Furthermore, they are able to promptly detect abnormal behaviors, extract attack characteristics, respond swiftly, and formulate effective defense strategies. Despite the convenience provided by big data analysis, it also intensifies offensive and defensive interactions. These interactions, however, play a crucial role in driving the development and improvement of network security technologies.

In the increasingly perilous network environment, there is a pressing need to transition from passive defense mechanisms to proactive defense strategies that incorporate predictive capabilities. Traditional passive defense measures, while partially effective in mitigating losses caused by network attacks and preventing such incidents, often result in information leakage or tampering. With the advent of new technologies, passive defense mechanisms are gradually becoming insufficient to meet the demands of modern network security. Active defense, on the other hand, emerges as a more viable alternative. It enables the proactive identification of potential threats and vulnerabilities, allowing for preemptive deployment of defense measures. This approach not only reduces the success rate of attacks but also minimizes associated losses. Consequently, network security professionals must enhance their predictive and adaptive skills, ensuring they can not only swiftly identify defense methods to counteract network attacks but also anticipate and mitigate potential risks and threats in advance.

6. Conclusion

A deeper understanding of the dynamic changes occurring within the network security domain is essential for formulating more effective protection strategies and enhancing overall network security capabilities.

Network security has become a global focal point. This article systematically analyzes the types and methods of network attacks, highlighting the severe challenges faced by network security. It further elaborates on the current state and advancements of network defense technologies, particularly emphasizing the emerging technologies based on blockchain and reinforcement learning within the network security field. These technologies demonstrate significant potential in strengthening defense capabilities. However, network security remains a complex and dynamic field where attack methods continuously evolve, necessitating ongoing innovation in defense technologies. In the future, the advancement of network security will increasingly depend on interdisciplinary integration, including collaborative applications of artificial intelligence, blockchain, and the Internet of Things. Additionally, improvements in policies, regulations, and technical standards will provide critical support for network security. Global cooperation and exchanges are called for to collectively address network security challenges and construct a safer, more reliable network environment.

References

[1] Liu L. Discussion and Practice of Computer Network Information and Network Security Protection Strategy. 2020 5th International Conference on Mechanical, Control and Computer Engineering (ICMCCE), Harbin, China, 2020, pp. 1810 – 1813.

[2] Yang R., Yang X. Establishment of Network Security System Based on Active Defence Technology. Neijiang Science and Technology, 2008, 29 (5): 138 – 138.

[3] Wu K., Zhang T., Chen F. Research on Active Controllable Defense Model Based on Zero-PDR Model. 2010 Third International Symposium on Intelligent Information Technology and Security Informatics, New York: IEEE, 2010, pp. 572 – 575.

[4] Du J. Y. Research and Countermeasures on Network Security Issues. Electronic Components and Information Technology, 2022, 6 (11): 209 – 213.SHI Biao, LI Yu Xia, YU Xhua, YAN Wang. Short-term load forecasting based on modified particle swarm optimizer and fuzzy neural network model. Systems Engineering-Theory and Practice, 2010, 30 (1): 158 - 160.

[5] Venkatesan K., Rahayu S. B. Blockchain Security Enhancement: An Approach Towards Hybrid Consensus Algorithms and Machine Learning Techniques. Sci Rep, 14, 1149 (2024).

[6] Bao Z. Research on Network Security Protection Mechanism System Based on Blockchain Technology. 2024 IEEE 7th International Conference on Information Systems and Computer Aided Education (ICISCAE), Dalian, China, 2024, pp. 1217 – 1221.

[7] Yang H. Construction of Network Data Security Active Defense System Based on Blockchain. Network Security Technology and Application, 2025, (03): 88 – 90.

[8] Alam T., Gupta R., Ullah A., et al. Blockchain-Enabled Federated Reinforcement Learning (B-FRL) Model for Privacy Preservation Service in IoT Systems. Wireless Personal Communications, 136, 2545 – 2571 (2024).

[9] Wang G., Peng Q., Duan H. J., et al. Design and Implementation of Computer Network Security Defense System Based on Artificial Intelligence Technology. Heilongjiang Science, 2024, 15 (18): 70 – 73.

[10] Su J. Intelligent Network Security Situation Prediction Method Based on Deep Reinforcement Learning. 2021 IEEE International Conference on Industrial Application of Artificial Intelligence (IAAI), Harbin, China, 2021, pp. 343 – 348.