www.cad-journal.net
Computer-Aided Design AND APPLICATIONS

Network Attack Simulation and Defense System Optimization based on Big Data

Yimeng Xu[1], Haiyang Wang[2], Baogang Chang[3] and Biao Lu[4]

[1,2,3,4] China Mobile Group Shandong Co., Ltd, Jinan, Shandong 250001, China,
[1]xuyimeng@sd.chinamobile.com, [2]wanghaiyang@sd.chinamobile.com,
[3]changbaogang@sd.chinamobile.com, [4]lubiao@sd.chinamobile.com

Corresponding author: Yimeng Xu, xuyimeng@sd.chinamobile.com

Abstract. With the continuous development of network environments and information technology, new network models such as the Internet of Things, smart cities, network satellites, and the Internet have gradually matured. These heterogeneous networks are connected to each other, which together support large-scale information exchange and bring great convenience to life and work. Compared with traditional networks, complex network structures have more vulnerabilities. The information exchange and security guarantee of users in the network have been threatened to a certain extent, and the open network environment has enriched more attack means. In view of the above situation, this paper uses big data-driven and computer-aided technology to study the optimization of network attack simulation and defense systems. Focusing on multi-device intrusion detection, we analyze the attack behavior and generate the corresponding network security defense mechanism. Firstly, computer-aided technology is used to generate the attack path under the graph simulation, and the comprehensive and rapid detection of the attack path is completed from the aspects of mining the matching and evaluation of multiple attack paths. In view of the diversity of heterogeneous network node types, the multi-constraint exploration method is used to find potential attacks. In addition, the computer-aided function is used to describe the attack simulation scenario and abstractly analyze the correlation behaviour of network attack elements. Finally, driven by big data, it accurately presents the development trend of network security, warns of network risks in a timely manner, and completes network active defense according to the prompts of computer-aided networks. A data-driven network capture model is constructed, and a security defense system based on data access is established. The experimental results show that the computer-aided technology driven by big data can analyze the mode of a network attack, analyze the simulation path of a network attack, and provide help for the subsequent defense system and security optimization.

Keywords: Big Data-Driven; Computer Aided; Cyber Attacks; Attack Simulation; Network Defense
DOI: https://doi.org/10.14733/cadaps.2025.S9.181-194

© 2025 U-turn Press LLC, http://www.cad-journal.net

1 INTRODUCTION

In today's network environment, network attacks have a serious impact on people's lives. Attackers use vulnerabilities to invade users' networks or nodes and ultimately achieve the purpose of network control or information theft [1]. In order to detect and intercept network attacks in time, it is very important to defend and protect the network environment. After the cause statistics of network attack simulation events, it is found that 95% of the attack events occur in companies that have deployed security defense systems [2]. 99% of the attacks were caused by years of vulnerability or by a known attack method. Other cyber attacks are caused by misdeployment of the company's network security equipment [3]. This shows that although we have deployed security defense systems in our networks, network security protection cannot play its role without the right upgrade protection or configuration. Conventional network security protection means it is difficult to detect key nodes after passive response, so they cannot know the attack means and complete targeted defense and elimination [4]. How to detect the attack mode and capture the attack path has become a major issue of network security defense [5]. Cyber attack simulation is a way to test network environments and systems by simulating attack behaviour, based on simulated events to determine vulnerabilities and attack paths that attackers may exploit. Therefore, network attack simulation can detect the effectiveness of network protection measures and help enterprises and organizations find potential network problems, which is a brand-new defense system [6].

In the infiltration process of network attacks, the data information involved is relatively diverse [7]. It is difficult for many researchers to describe or accumulate the attack process, and it is also difficult to use symbolic representations to replace the attack simulation method. Therefore, in the field of network attack simulation and defense, the construction of automated defense systems driven by big data and computer-aided has become a hot technology. Computer-aided detection and analysis of network attack path simulation can penetrate data information, eliminate manual intervention in attacks, and automate attack simulation [8]. At the same time, computer-aided can also propose the descriptive growth of network attack elements to achieve unified management in the face of diverse attack situations. The adoption of big data drive can also solve the problem of initiative and passivity in network security protection [9]. The passive defense mechanism is changed from a data-driven approach to an active defense to give early warning of the occurrence of network attack events. Finally, security protection at the physical level, aiming at the complexity of computer networks, builds an efficient and specific protection system [10]. From the physical level, ensure the stable operation of computer equipment. The selection of the external environment and various influencing factors should also be combined with the reliable data provided by the computer-aided network [11]. In the computer system, after the user's access rights are confirmed and guaranteed, each type of access control must complete digital encryption. It not only defines the scope of the user's rights but also limits it according to the three-dimensional computer system so as to avoid the loss of hardware and software caused by external influences. To sum up, big data-driven and computer-aided technologies play an important role in network attack simulation and defense system optimization.

Computer-aided network attack simulation is a method of evaluating and optimizing network security defense systems by simulating real or potential attack scenarios. The introduction of big data technology enables simulation processes to handle massive amounts of network traffic data, simulating attack scenarios that are closer to the real world, thereby improving the accuracy and effectiveness of simulations [12]. Big data technology can collect and integrate network security data from multiple sources, including network traffic, logs, user behaviour, etc. By deeply mining and analyzing these data, the behavior patterns and trends of attackers can be revealed, providing strong support for future defense strategies. This real-time capability is crucial for mitigating the harm of DDoS attacks. By using machine learning models such as Random Forest (RF) and Multi-Layer Perceptron (MLP) combined with big data frameworks such as Apache Spark, real-time detection of DDoS attacks can be achieved [13]. For example, when a DDoS attack is detected, the system can automatically increase bandwidth resources, adjust routing policies, or start backup servers to

© 2025 U-turn Press LLC, http://www.cad-journal.net

ensure the normal operation of critical services. This simulation can help security teams gain a deeper understanding of attackers' strategies and tactics in order to discover and fix potential security vulnerabilities before a real attack occurs. The distributed computing capability of big data enables models to process and analyze massive amounts of data in a very short amount of time, thereby quickly identifying attack behavior and triggering corresponding defense mechanisms. Driven by big data, network security defense systems can dynamically adjust resource allocation and defense strategies based on real-time network conditions and attack threats. In addition, prediction models based on big data can also provide early warning of potential DDoS attacks, buying valuable time for defense work.

2 DEVELOPMENT STATUS OF BIG DATA-DRIVEN AND COMPUTER-AIDED NETWORK ATTACK SIMULATION

As the main driving force of information networks, big data has shown deep integration in the industry in the face of the popularization of computer networks. It can not only improve the efficiency of data processing but also expand the information storage capacity to meet the multi-directional operational needs of users. When users complete their functional requirements in the network, they also bear the risk of information leakage, which can easily cause information loss to individuals and businesses. Therefore, ensuring user privacy and security in the big data environment and creating a healthy and green network environment is very important. The characteristic of computer networks is openness, and in the process of providing data transmission for people, the information diversity structure will face security risks. Papanikolaou et al. [14] Invasions caused by computer viruses, hackers, and malicious software. Especially for large enterprises and organizations, a series of information about their operations is stored in computer networks. Once the internal network is exposed to security risks, it is inevitable that losses related to the economy will be incurred. In the era of big data, data-driven high-capacity transmission has increased operational pressure at the network level. This efficient and intelligent operating environment has caused serious harm to network vulnerabilities and triggered problems such as network vulnerabilities. Meanwhile, Ponmalar and Dhanakoti [15] use data-driven information analysis and extraction to study the current status of network attack models.

The attack model of the network includes infiltration, which uses multiple steps, such as information collection and vulnerability attacks, to complete attack decisions. Penetration attacks complete full coverage attack operations in network environments and can also launch unified attacks on heterogeneous network environments. In order to better address this issue, Rathore et al. [16] constructed a digital network attack path detection system using computer-aided modelling to understand better and analyze the practical problems of network security and used model calculations and simulations to guide decision-making. In addition, the chain attack penetration model is also a major vulnerability in the network. It infiltrates every step of network decision-making with relatively fixed attack methods through stages such as attacking and implementing monitoring assistants. Sadeghi et al. [17] used computer-aided techniques to simulate penetration models, enabling testers to understand the simulated attack process better and apply targeted supplements at each stage to reduce losses. Finally, from a definition perspective, we can analyze the role of computer-aided models. We can consider this as a process of collecting, analyzing, and inferring computer technology-related data to achieve specific goals. In addition, network applications can be completed in a highly logical and qualified environment. The characteristic of computer-aided technology is that it requires users and computers to work together, using its auxiliary role to complete logical reasoning and compensate for the lack of mathematical and logical abilities of staff. Therefore, in order to conduct information analysis at the network level, it is necessary to select qualified data during the data collection process to facilitate future statistics and calculations. In summary, we have found that big data-driven and computer-aided technologies have good effects on network information processing, data security analysis, and other aspects. Therefore, we will also apply them to network attack simulation and defense system optimization, striving to improve the quality of network security.

© 2025 U-turn Press LLC, http://www.cad-journal.net

Network defense is a multidimensional and comprehensive process that relies on advanced tools and technologies, such as intrusion detection systems (IDS), threat intelligence analysis, and intrusion defense strategies, which collectively weave a tight security protection network. These models can not only effectively learn and automatically discover abnormal behavior patterns from massive IoT data but also transform these findings into human-understandable language through XAI technology, providing security analysts with intuitive and accurate threat intelligence. However, relying solely on the high-precision output of the model is far from enough. We also need to understand the logic and foundation behind these predictions, which is exactly the value XAI can provide. Meanwhile, the integration of XAI technology makes this process more transparent and interpretable, which can help us gain a deeper understanding of the decision-making process of deep learning models in detecting network attacks and enhance our trust in the model's predictive results. In interdisciplinary research on XAI and IoT network security, Vaccari et al. [18] witnessed the widespread application of various artificial intelligence models (including machine learning and deep learning) in anomaly detection applications. Deep learning models are highly favoured in anomaly-based intrusion detection systems due to their powerful pattern recognition capabilities. In the Internet of Things environment, the influx of big data provides unprecedented opportunities for network attack simulation and optimization of defense systems. Through big data-driven computer-aided network attack simulation, researchers can construct attack scenarios that are close to the real world, comprehensively evaluate the effectiveness of defense systems, and discover potential areas for improvement. The integration of big data technology has injected new vitality into DDoS defense. How to efficiently process and analyze big data, as well as identify and respond to DDoS attacks in real time, is the key issue we are currently facing. In terms of defense mechanisms, the combination of artificial intelligence and statistical technology has opened up new avenues for DDoS attack defense. This simulation is not limited to static defense testing but can also dynamically adjust attack parameters, simulate various strategies that attackers may adopt, and provide valuable data support for the continuous optimization of defense systems. Through big data-driven computer-aided network attack simulation, Zhong et al. [19] simulated highly complex DDoS attack scenarios that are close to the real world in order to more comprehensively evaluate the effectiveness of existing defense systems and identify potential weak links. This combination not only improves the accuracy of the defense system but also enhances its adaptability and scalability. At the same time, statistical techniques help us extract valuable features from massive amounts of data, providing a scientific basis for developing defense strategies. By utilizing the rich resources of big data, artificial intelligence algorithms can learn and identify complex DDoS attack patterns, even if these patterns are novel or unknown. However, there are still many challenges to overcome in order to truly achieve efficient and intelligent DDoS defense. Secondly, different types of DDoS attacks have different characteristics and behavioural patterns. How to design a universal and effective defense mechanism to adapt to diverse attack scenarios is also an urgent problem to be solved.

3 RESEARCH ON OPTIMIZATION OF NETWORK ATTACK SIMULATION AND DEFENSE SYSTEMS BASED ON BIG DATA-DRIVEN AND COMPUTER-AIDED

3.1 Research on Computer-Aided Network Attack Path Detection and Simulation Generation

In the digital age, the popularization of computers and the application of networks have brought a significant impact on people's lives and work, accompanied by the continuous upgrading of network attacks and network intrusion. From simple malware to sophisticated cybercrimes, cyberattacks have become a global challenge. In the face of this threat, building a multi-level defense system, protecting network security, and providing effective solutions are the main ways to protect the interests of individuals and enterprises. Although the rapid development of computer networks has brought unprecedented convenience to human society, the challenge of network security has become the biggest threat. The constantly evolving and varied network attacks have warned and affected the harmony of the network environment. First, we analyze different types of network attacks, among which distributed denial attacks are the most common means of attack, using traffic patterns to

© 2025 U-turn Press LLC, http://www.cad-journal.net

overload the target server and cause server loss. The second is the malicious spread of software, which is embedded in the user device by various means, not only taking information but also destroying the system structure. At present, with the increasing demand for attack path detection, a large number of attack detection methods are proposed and applied. We use computer-aided technology to analyze the attack path and generate the attack simulation under the special structure of the graph model so as to provide reliable help for the subsequent defense system. Because of the special form of the graph model, it is necessary to match and predict the attack path according to the corresponding relationship of the graph information nodes so that computer-aided technology can play a good role in it. Computer-aided technology itself has many functions, such as graph information processing, data storage, parameter adjustment, and so on. After receiving the relevant information, the work of filtering and classifying the data can be completed. The attack path detection method based on the graph model can form many forms, such as a directed acyclic graph and attack tree, and it can match the related attack path according to the node relationship in the graph. We demonstrate the graph isomorphism algorithm and bounded simulation algorithm by using computer-aided models, as shown in Figure 1.

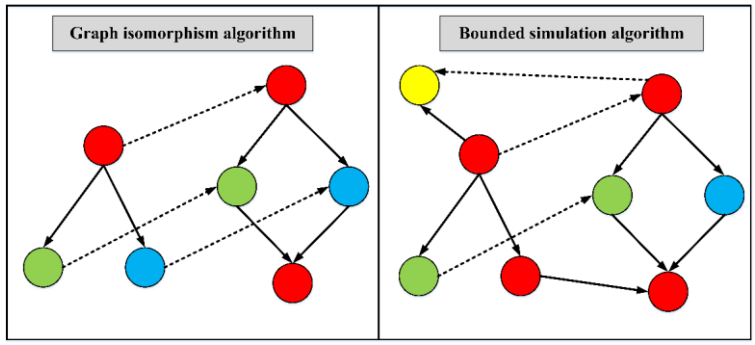

Figure 1: Structure of graph isomorphism algorithm and bounded simulation algorithm.

As can be seen from Figure 1, these two methods both play a role in preferentially processing data in computer security and attack path detection, which not only improves the matching efficiency of attack paths but also completes functional calculation for data graph compression and reduces repeated generation of fruitless matches. Because of the diversity of attack modes in a network environment, we need to use a vulnerability scoring system to evaluate the degree of threat to network vulnerability when simulating attack paths. The impact, attack channels, and complexity of network vulnerabilities are analyzed from multiple dimensions, as shown in Table 1.

Basic factors	*Essential factor*	*Evaluation criterion*	*0.7/1.0*
	Attack route	Local/Remote	1.0/1.2
	Attack complexity	High/Medium/Low	1.2/1.3
	authentication	Not affected	0.8/1.5
	confidentiality	Not affected	0.9/2.1
	integrity	Not affected	0/1/3
time factor	Availability	Not proven	0.1/2.0
	Repair measures	Official patch	0.5/1.2
	Confirmation level	Not proven	0.1/0.2/0.3
environmental factor	Hazard impact	Official patch	0/1
	target distribution	Official patch	0.5/1.4

Table 1: Assessment data of network vulnerability threat level.

© 2025 U-turn Press LLC, http://www.cad-journal.net

As can be seen from Table 1, the function is divided into basic factors, time factors, and environmental factors, and the key factors are divided into attack paths, complexity, confidentiality, integrity, availability, and other ways, and corresponding scores are generated according to different evaluation criteria. The basic score is used to represent the intrinsic characteristics of network vulnerability, which consists of two sets of indicators: one is exploitability, and the other is impact. Exploitability reflects the technical means of exploiting network vulnerability, such as attack vectors and attack complexity. The basic score for required permissions is calculated using the following formula:

$$r(B) = Roundup[1.08 \times w] \tag{1}$$

Through the time index, the dynamic score of network vulnerability is measured, and the network utilization is calculated by the patch solution method:

$$r(T) = Roundup[w \times E \times r(x)] \tag{2}$$

Since the units of measurement of various indicators are not uniform, it is necessary to conduct standardized processing before comprehensively evaluating the risk of attack means and converting the absolute value of indicators into relative data. The conversion formula is as follows:

$$y = \frac{x - \min(x)}{\max(x_j) - \min(x_j)} \tag{3}$$

$$y_i = \frac{\min(x) - u_i}{\max(x_j) + \min(x_j)^2} \tag{4}$$

After standard processing of the data, the weight of each sample in multiple indicators is calculated:

$$p = \frac{x_{ij}}{\sum_{j}^{m} x_{ij}}, 0 \le p \le 1 \tag{5}$$

$$e = -k\sum_{i=1}^{n} p_{ij} \ln(p_{ij}), k\frac{1}{\ln(n)} > 0 \tag{6}$$

After obtaining the proportion of samples, the risk ranking of network attacks can be judged. After ranking the risk of cyber-attacks, we determined that attack penetration is an instruction-based simulation. After the attack path is mastered, the attack path can be simulated with the help of computer assistance to help improve network security. From the form in the language table, the entity, relation, and attribute in the attack scenario are formally described. We built a computer-aided model to describe the complete attack path penetration process by means of graphical simulation, as shown in Figure 2.

As can be seen from Figure 2, first of all, network port scanning in the information search module is the interface for subsequent vulnerability scanning verification. In the attack implementation module, vulnerability characteristics are used to provide a reference for subsequent control residency implanted by the backdoor. Finally, in horizontal penetration, the acquisition of user credentials is the key node of the attack path. The final result of network attack simulation is to eliminate user log information to achieve the purpose of data deletion and replication. In addition, without spending much money to complete network security defense, we extract different device types in the real network and use computer-aided tools to simulate and generate a large-scale network environment. We show the topology of the network environment. Mark the possible harmful objects of network attacks, as shown in Figure 3.

Figure 3 shows that the network topology is a simple network model, with the Internet on the left and the interior on the right. The network firewall can separate the internal and external areas of the network. There are various types of hosts in the network, and the hosts can communicate with each other as well as transmit data to the server. Every host and server is a prime target. The internal network on the right of the firewall is less vulnerable to network attacks because of the firewall's defense function.

© 2025 U-turn Press LLC, http://www.cad-journal.net

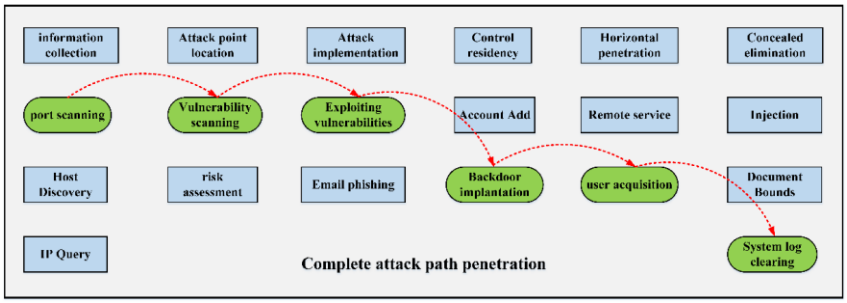

Figure 2: Complete attack path penetration process.

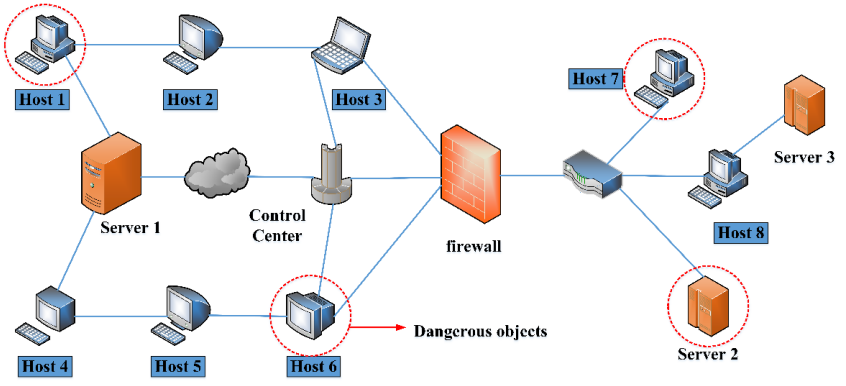

Figure 3: Network topology.

Through the simulation of computer-aided technology, we can not only generate the complete attack path but also build the related network topology environment, which provides the basis for the subsequent defense system optimization.

3.2 Research on Optimization of Computer-Aided Network Active Defense Security Based on Big Data

The management of computer network security is mainly a three-dimensional prevention and control design for the whole computer drive system and the external network environment. To solve all kinds of security problems in network operations from the source, users need to have a correct understanding of network security operations when driving the network system and understand the harm brought by network attacks. We study network active defense driven by big data and get intrusion records and network vulnerabilities by analyzing terminal security data, run log data, security log data, and other information. Add it to big data-driven analysis, predict user behavior, optimize network protocol, and other normal network model construction under the premise of normal network information operation. Active defense is a kind of technology with a deep resistance to network attacks. It can monitor the network environment and is a countermeasure to intercept external illegal intrusion. We use big data to drive the construction of an active defense system; the principle is shown in Figure 4.

As can be seen from Figure 4, intrusion tracking, attack reweighting, and automatic counterattack programs are added to network response technology. The active defense principle also includes detection and prediction and reduces network risks through identity authentication, virus, gateway, and vulnerability scanning. In addition, it is necessary to combine the network weakness database, analyze the vulnerability information of the host and the network, and establish the corresponding rules and network models to protect network security. In order to better cover the

© 2025 U-turn Press LLC, http://www.cad-journal.net

network scope, we use data-driven impact analysis on different network attack forms, as shown in Figure 5.

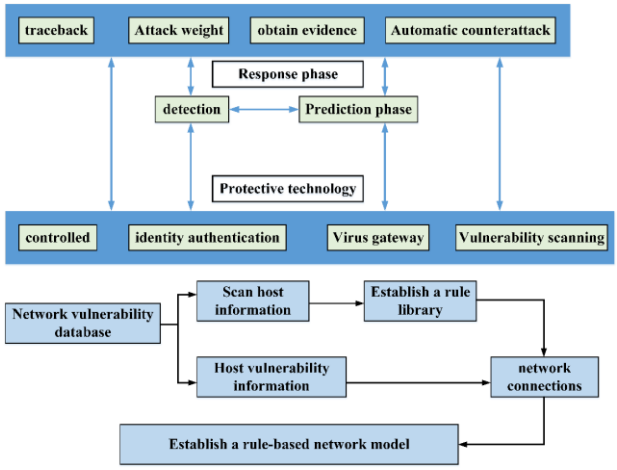

Figure 4: Building an active defense system structure driven by big data.

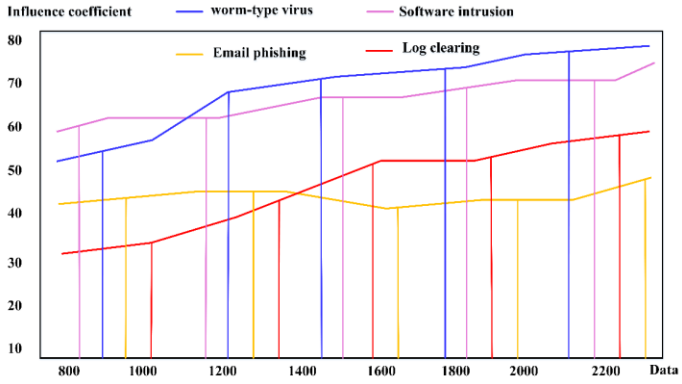

Figure 5: Analysis of the impact of different forms of network attacks.

As can be seen from Figure 5, four representative network attack forms, namely software intrusion, email phishing, log deletion, and worm virus, are extracted as detection objects. Among them, worm viruses and software intrusion have a great influence. It not only endangers network security but also affects the security of users' personal information. In establishing the active defense system, we add the response module according to the mechanism of traditional defense technology and take detection and prediction as the core technology to build a security network evaluation model. In the mathematical model, it is assumed that there are network attackers in the data set, the spatial scope of malicious behaviors, and the probability of malicious attacks. The calculation formula is as follows:

$$w = t^{i} + t(x)[k, uv_{2}] \tag{7}$$

$$s_{0} = (s, w\frac{2}{\ln}, u(\min(x)) \tag{8}$$

The formula w indicates the probability of malicious attacks. Active defense behaviours powered by big data can add a designated target to the defender. At the same time, according to the types of devices and network topology, multiple attack levels are divided to determine the state of network

© 2025 U-turn Press LLC, http://www.cad-journal.net

security. Different states represent different phases of network defense. According to both the defense and attack sides, the visual mathematical model is constructed as follows:

$$q = w + \sum_{t=1}^{k} p_{ij}(Q_i \mid q, S_2, S) \tag{9}$$

$$Q = \ k, 2, 3, \ldots, \max_{\ 0} \tag{10}$$

In the formula q represents the defender's gain. Assuming that the network attack is established, we can use the formula to calculate the network state at this time:

$$Z = \sum_{i=1}^{k} p(Q_i \mid q, S_x, U)_i \tag{11}$$

In the process of building the model, it is easy to be affected by external attacks, which leads to indirect security evaluation interference in the network, which seriously affects the evaluation result. Therefore, we introduce dynamic entropy to combat interference problems and improve the accuracy of calculation results:

$$q^1 = w + k^w p \,/\, (Q \mid S_{ij}) \tag{12}$$

$$q^2 = S + k^w p \,/\, (Q \mid \max_{ij}) \frac{1}{\ln} \tag{13}$$

Finally, the possible defense behaviours in the database are collected and integrated into the following data set using the formula:

$$E = \sum_{j=1}^{m} EA_{ij} \tag{14}$$

$$E_{DI} = \sum_{j=1}^{m} ED_{ij} + q^1 \tag{15}$$

The above formula can represent both the network defense phase and the active defense phase. According to the number of attacked devices and attack mode, the current network security level and state must be judged. The active defense network security driven by big data is essentially oriented to large-scale complex network environments. Therefore, we use mathematical methods to sense and calculate the network dynamics, which can obtain the changes in network security. At the same time, we can judge whether the active network defense system is effective by combining the computer-aided attack simulation path.

4 ANALYSIS OF RESEARCH RESULTS OF NETWORK ATTACK SIMULATION AND DEFENSE SYSTEM OPTIMIZATION BASED ON BIG DATA-DRIVEN AND COMPUTER-AIDED

4.1 Analysis of Research Results Based on Computer-Aided Network Attack Path Detection and Simulation Generation

In a society where the Internet is deeply developed, the means and motivations of cyberattacks are increasingly sophisticated, ranging from economic to political to pure cyber malevolence. We should not only deeply analyze the thinking and strategy of the attackers but also develop effective defense measures according to the attack mode. There are various motives for cyber-attacks, which, in addition to affecting individuals, revealing personal privacy, identity information, and other content, may also lead to the loss of personal property. More egregious cyberattacks will affect social institutions, disrupt public services, and affect national security. In our research, we mainly use computer-aided technology to simulate network attacks so as to detect the attack path, analyze its function, and put forward the threat strategy disposal plan. In attack path analysis, a graph model is used to expand the computer-aided performance. The network attack is shown in graph data. To

© 2025 U-turn Press LLC, http://www.cad-journal.net

verify the performance of the network attack path detection algorithm generated by computer-aided technology. We compared the accuracy rate of network attack path detection before and after using computer assistance, as shown in Figure 6.

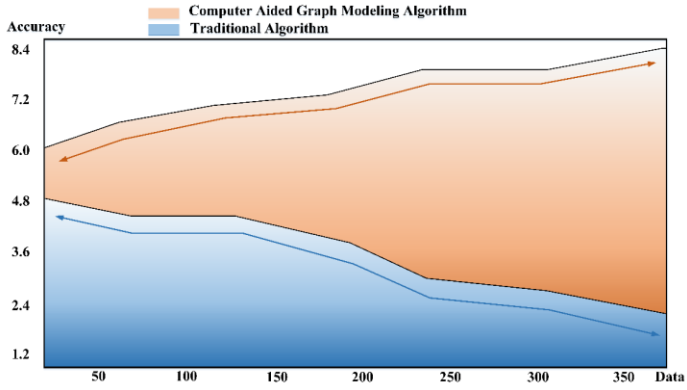

Figure 6: Comparison of accuracy of network attack path detection before and after computer assistance.

As can be seen from FIG. 6, before the computer-aided graph model is formed, the traditional algorithm can only detect the network attack path through trace analysis, which is less accurate. After analyzing the network attack path with a computer-aided graph model, the detection accuracy can be improved under the interference of a large amount of data. Next, we also use cyber-attack simulation to improve the targeted defense of the network environment. Before this, computer-aided modelling technology was used to construct the specific attack scenario, and the elements in the attack scenario are represented in formal language. The entity of the generated attack simulation scenario is shown in Figure 7.

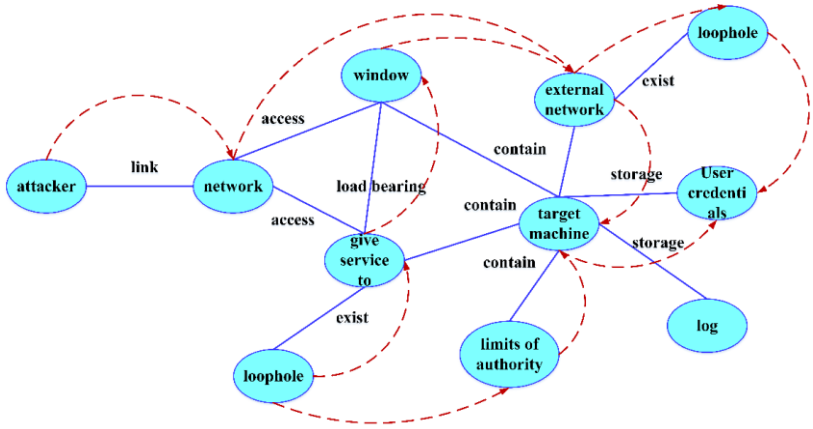

Figure 7: Attack simulation scene entity diagram.

Figure 7 shows that in the entity diagram of the attack simulation scenario, there are attackers, network ports, vulnerabilities, target machines, permissions, logs, users, and external networks. A complete description of the brief process of network attack. According to the formalization of the attack scenario, we can define the form of the network attack, and provide targeted solutions to establish the active defense network.

© 2025 U-turn Press LLC, http://www.cad-journal.net

4.2 Analysis of Research Results on Security Optimization of Computer-Aided Network Active Defense Based on Big Data

The optimization of active defense systems driven by big data essentially balances the gap between a cyber attack and defense. Network attack Network defense is the establishment of network behaviour in a specific scenario to complete the self-judgment and identification of network system security. When the effect of defense behaviour is greater than that of attack behaviour, the network system is in a secure state; when the effect of defense behaviour is less than that of attack behaviour, the network system is in a dangerous state. Due to the individual differences in network attacks, multiple dialogue boxes will be formed. Therefore, we need to analyze the attack scenario of each attack intention and make clear the ultimate goal of the attack behaviour, so as to establish the corresponding defense network. To verify the performance of the active defense system driven by big data. In the same network attack environment, we compared the response times of the active defense system before and after big data-driven optimization, as shown in Figure 8.

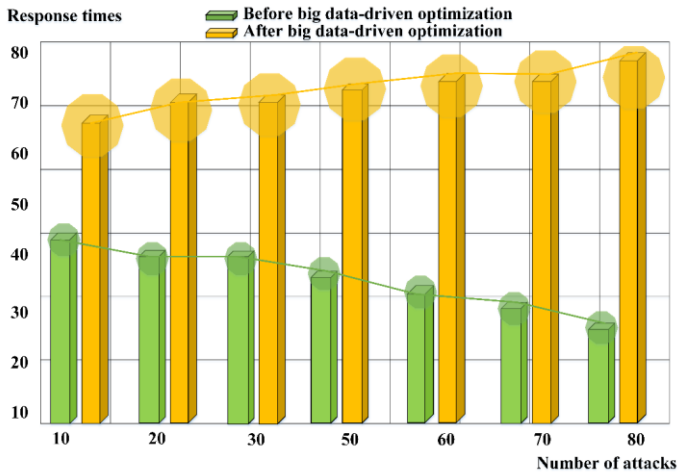

Figure 8: Changes in response times of active defense systems before and after big data-driven optimization.

As can be seen from Figure 8, before adopting big data-driven optimization, the response times of the network defense system were low, and some network attacks entered the Intranet through network vulnerabilities. After adopting big data-driven optimization, the response times of the network defense system are significantly increased. Relatively speaking, the impact of cyber attacks is low. We regard the network security problem as a game state between the defender and the attacker, and each stage should correspond to a network security form. By solving the problem, we can deal with the mixed strategy in the security state. The actual situation of network security is obtained, and corresponding patches and countermeasures are provided. In order to further verify the impact of computer-aided network attack simulation driven by big data on network defense system optimization, we compare the network security state before and after optimization through a security assessment.

As can be seen from Figure 9, before big data-driven and computer-aided optimization, the network security coefficient was low, and it could be threatened by network threats from inside and outside the Internet at any time. After optimization with this technology, the network security factor is significantly increased. The index information of the active defense network is also above the standard security factor. It can be seen that the way to protect the network is not only to use the firewall but also to improve the network security state according to the attack path detection and simulation training.

© 2025 U-turn Press LLC, http://www.cad-journal.net

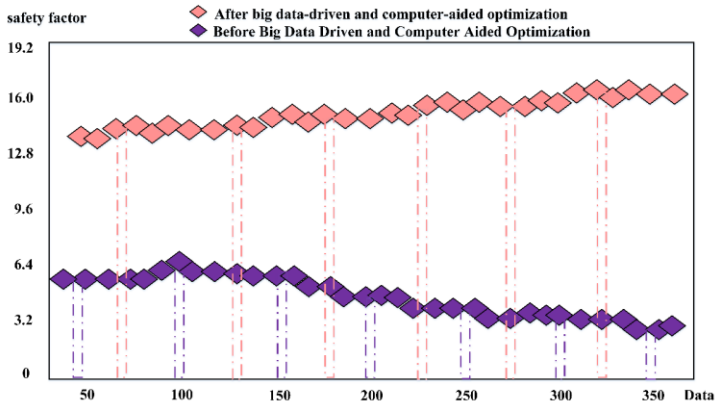

Figure 9: Network security status before and after optimization.

5 CONCLUSIONS

As the development of the network becomes more and more mature, various communication and electronic technologies continue to be studied and applied, and the frequent use of the network level is vulnerable to malicious attacks and intrusion, resulting in data leakage, information damage, equipment damage, and so on. Traditional network attack detection and defense can only judge the attack means through the firewall and network damage state, which makes it difficult to meet the needs of network security protection. In this paper, the simulation path of a network attack is analyzed under computer-aided technology driven by big data, and the active defense system is established to optimize network security. Firstly, the characteristics of network attacks are analyzed, and the security threats faced by the network are expounded. From two aspects of attack path and threat assessment, the path mining method of computer-aided graph simulation is introduced, and computer-aided technology is applied to the simulation generation of the attack path to improve the performance of the simulation detection algorithm. From the point of view of attack, the possibility of attack path is quantified in many aspects to improve the reliability of detection results. Finally, with the help of big data drive, the network active defense technology is introduced to build a network security system, and the network security problem is transformed into a multi-stage dynamic problem. Build an active defense network based on big data and on the premise of network resilience. Combined with computer-aided network attack simulation training, it provides more accurate security repair for network vulnerabilities. Based on massive data analysis, the network defense system is constantly evolving to evaluate the level and status of the network. The results show that computer-aided network attack simulation driven by big data can provide reliable help for training network security defense systems. The internal structure of the optimized defense system is relatively stable and can resist most network attacks.

Yimeng Xu, https://orcid.org/0009-0001-7345-1967
Haiyang Wang, https://orcid.org/0009-0004-6099-1923
Baogang Chang, https://orcid.org/0009-0006-9173-8909
Biao Lu, https://orcid.org/0009-0004-6654-7815

REFERENCES

[1] Ahsan, F.; Dana, N.-H.; Sarker, S.-K.; Li, L.; Muyeen, S.-M.; Ali, M.-F.; Das, P.: Data-driven next-generation smart grid towards sustainable energy evolution: techniques and technology

© 2025 U-turn Press LLC, http://www.cad-journal.net

review, Protection and Control of Modern Power Systems, 8(3), 2023, 1-42. https://doi.org/10.1186/s41601-023-00319-5
[2] Alcaraz, C.; Lopez, J.: Digital twin: A comprehensive survey of security threats, IEEE Communications Surveys & Tutorials, 24(3), 2022, 1475-1503. https://doi.org/10.1109/COMST.2022.3171465
[3] Awan, M.-J.; Farooq, U.; Babar, H.-M.-A.; Yasin, A.; Nobanee, H.; Hussain, M.; Zain, A.-M.: Real-time DDoS attack detection system using big data approach, Sustainability, 13(19), 2021, 10743. https://doi.org/10.3390/su131910743
[4] Bi, K.; Lin, D.; Liao, Y.; Wu, C.-H.; Parandoush, P.: Additive manufacturing embraces big data, Progress in Additive Manufacturing, 6(1), 2021, 181-197. https://doi.org/10.1007/s40964-021-00172-8
[5] Chaalan, T.; Pang, S.; Kamruzzaman, J.; Gondal, I.; Zhang, X.: The path to defense: a roadmap to characterising data poisoning attacks on victim models, ACM Computing Surveys, 56(7), 2024, 1-39. https://doi.org/10.1145/3627536
[6] Hu, W.; Chang, C.-H.; Sengupta, A.; Bhunia, S.; Kastner, R.; Li, H.: An overview of hardware security and trust: Threats, countermeasures, and design tools, IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems, 40(6), 2020, 1010-1038. https://doi.org/10.1109/TCAD.2020.3047976
[7] Iqbal, R.; Doctor, F.; More, B.; Mahmud, S.; Yousuf, U.: Big data analytics and computational intelligence for cyber-physical systems: Recent trends and state of the art applications, Future Generation Computer Systems, 105(1), 2020, 766-778. https://doi.org/10.1016/j.future.2017.10.021
[8] Khalaf, B.-A.; Mostafa, S.-A.; Mustapha, A.; Mohammed, M.-A.; Abduallah, W.-M.: Comprehensive review of artificial intelligence and statistical approaches in distributed denial of service attack and defense methods, IEEE Access, 7(1), 2019, 51691-51713. https://doi.org/10.1109/ACCESS.2019.2908998
[9] Krishna, S.: Advancing cyber resilience for autonomous systems with novel AI-based intrusion prevention model, International Journal of Data Informatics and Intelligent Computing, 3(3), 2024, 1-7. https://doi.org/10.59461/ijdiic.v3i3.121
[10] Krishnamurthy, P.; Surabhi, V.-R.; Pearce, H.; Karri, R.; Khorrami, F.: Multi-Modal Side Channel Data Driven Golden-Free Detection of Software and Firmware Trojans, IEEE Transactions on Dependable and Secure Computing, 20(6), 2022, 4664-4677. https://doi.org/10.1109/TDSC.2022.3231632
[11] Mahmood, R.-K.; Mahameed, A.-I.; Lateef, N.-Q.; Jasim, H.-M.; Radhi, A.-D.; Ahmed, S.-R.; Tupe, W.-P.: Optimizing network security with machine learning and multi-factor authentication for enhanced intrusion detection, Journal of Robotics and Control (JRC), 5(5), 2024, 1502-1524. https://doi.org/10.18196/jrc.v5i5.22508
[12] Moustafa, N.; Koroniotis, N.; Keshk, M.; Zomaya, A.-Y.; Tari, Z.: Explainable intrusion detection for cyber defenses in the internet of things: Opportunities and solutions, IEEE Communications Surveys & Tutorials, 25(3), 2023, 1775-1807. https://doi.org/10.1109/COMST.2023.3280465
[13] Panchigar, D.; Kar, K.; Shukla, S.; Mathew, R.-M.; Chadha, U.; Selvaraj, S.-K.: Machine learning-based CFD simulations: a review, models, open threats, and future tactics, Neural Computing and Applications, 34(24), 2022, 21677-21700. https://doi.org/10.1007/s00521-022-07838-6
[14] Papanikolaou, A.; Alevizopoulos, A.; Ilioudis, C.; Demertzis, K.; Rantos, K.: An autoML network traffic analyzer for cyber threat detection, International Journal of Information Security, 22(5), 2023, 1511-1530. https://doi.org/10.1007/s10207-023-00703-0
[15] Ponmalar, A.; Dhanakoti, V.: An intrusion detection approach using ensemble support vector machine-based chaos game optimization algorithm in big data platform, Applied Soft Computing, 116(1), 2022, 108295. https://doi.org/10.1016/j.asoc.2021.108295
[16] Rathore, M.-M.; Shah, S.-A.; Shukla, D.; Bentafat, E.; Bakiras, S.: The role of ai, machine learning, and big data in digital twinning: A systematic literature review, challenges, and

© 2025 U-turn Press LLC, http://www.cad-journal.net

opportunities, IEEE Access, 9(1), 2021, 32030-32052. https://doi.org/10.1109/ACCESS.2021.3060863
[17] Sadeghi, K.; Banerjee, A.; Gupta, S.-K.-S.: A system-driven taxonomy of attacks and defenses in adversarial machine learning, IEEE Transactions on Emerging Topics in Computational Intelligence, 4(4), 2020, 450-467. https://doi.org/10.1109/TETCI.2020.2968933
[18] Vaccari, I.; Carlevaro, A.; Narteni, S.; Cambiaso, E.; Mongelli, M.: Explainable and reliable against adversarial machine learning in data analytics, IEEE Access, 10(1), 2022, 83949-83970. https://doi.org/10.1109/ACCESS.2022.3197299
[19] Zhong, W.; Yu, N.; Ai, C.: Applying big data based deep learning system to intrusion detection, Big Data Mining and Analytics, 3(3), 2020, 181-195. https://doi.org/10.26599/BDMA.2020.9020003

© 2025 U-turn Press LLC, http://www.cad-journal.net