Application of Digital Twin Technology in Campus Network Security

Gang Li[1,*], Kun Sha[2], Hai Fu[1], Yaowen Sun[1]
[1]Naval Submarine Academy, Qingdao, Shandong, China
[2]Naval Medical University, Shanghai, China
**Corresponding Author.*

Abstract: With the popularization of computer networks, information resources have been shared to the greatest extent possible, and the construction of campus networks in colleges and universities has been paid more and more attention to, and campus networks are an important component of computer networks, which are developing very rapidly. The construction of campus network can provide convenient network services to teachers and students as well as administrators on campus, but at the same time, it is also subject to many network security threats, resulting in serious consequences such as student information leakage. This paper analyzes the application of digital twin technology in campus network security management, especially in the security risk assessment and attack detection and response module, the digital twin model shows powerful data processing and intelligent analysis capabilities, not only real-time analysis of network traffic, user behavior and device status, but also timely detection and response to network security events. The digital twin technology builds a safer, smarter and more dynamic campus network environment for teachers and students.

Keywords: Campus Networks; Network Security; Digital Twins, Risk Assessment; Attack Detection

1. Introduction

The modern means of informationization based on the Internet is also becoming more and more widespread, and the campus network can realize resource sharing and improve work efficiency. With the rapid expansion of university network scale, the growth of the number of users and the improvement of network openness, the security challenges faced by the campus network are also becoming more and more prominent [1]. The network infrastructure is the nerve center of the campus network operation and a possible target for focused attacks. An attack on the campus network can be extremely destructive, leading to problems such as campus paralysis and disruption of campus services. Campus network plays an important role in today's higher education, it is not only an important support for teaching and research, but also connects many systems related to the operation of the school, but the campus network security is often not paid enough attention by universities. In the high-speed development of campus network today, many domestic universities have been building faster and more convenient campus network, but at the same time, the leakage of confidentiality, sabotage of network system security and other behaviors have been a serious threat to the self-interest of network users [2]. The development of the network is a dynamic process of change, with the release and application of major application software, operating systems, etc., a variety of vulnerabilities, viruses and other programs that jeopardize network security have also appeared one after another, and the campus network as an important information platform for the learning and communication of all teachers and students of the university, its security must be given high priority [3].

The security challenges facing campus networks and how to build a solid, secure network system that is safe from viruses, hackers, and other malicious behaviors has become an urgent issue for institutions of higher learning. Based on this background, digital twin technology provides a new solution. Digital twin technology can provide a new perspective for security management of campus networks through real-time data

modeling and analysis. In other words, after launching a network attack in reality, the effect of the attack can be displayed in real time on the digital twin platform. This not only allows network administrators to more intuitively and accurately understand the specifics of network attacks, but also provides a vivid practical experience for information security teaching. This network strategy cannot directly affect the entire campus network, but it can be counteracted by operating the twin platform to experimentally build the network environment [4].

With the help of campus digital twin architecture, this paper empowers digital twins in the security management of smart campus network, and promotes the application of digital twin technology and campus smart network security deduction, which has certain reference significance.

2. Analysis of Campus Network Security Status Quo

In today's information society, campus networks have become an important part of higher education. As the dependence of teaching, research and management activities on campus networks strengthens, the security of campus networks is particularly important. As a platform for providing diversified information services, campus networks need to ensure their openness as well as strengthen confidentiality [5]. And campus network is a local area network (LAN) where a large number of users exist in a small area, bringing together a lot of network devices and computer users within the school. Campus networks are concerned with the ease of stabilization, construction and use of internal networks [6].

Foreign research on the management and development of computer networks is more rigorous and efficient, the campus network can basically meet the daily communication and exchange of teachers and students, the network environment is relatively stable, but also formed a stable and good management level. The hotspot of research in the United States is the construction of campus network, which focuses on setting up access rights and not being able to access other interfaces at will, and the management requirements for the construction of campus network are also quite strict to ensure that the campus network operates efficiently and effectively, and at the same time, protects the personal information security of teachers and students in the school [7]. Network security problems are mainly focused on three areas: security of software, security of hardware, and security of information. In the application of university campus network, the security of information is the most important, many invasive events or attacks will be a threat to the data and information, so we must ensure the security of the data and information, so that it is not damaged and can be used intact [8].

With the continuous progress of China's science and technology, all sectors of society are paying more attention to the campus network construction project of colleges and universities. At the same time, the cooperation and exchange relationship between the major universities is also more and more common, and the promotion of information exchange and communication between the major universities is another important content of the campus network construction and management [9]. From the point of view of the national information network construction and management of schools, the campus network construction management and optimization in colleges and universities make the exchange and communication between universities more convenient and fast [10]. In all-out efforts to improve the efficiency of the use of the user, it is very easy to ignore the user's privacy and security issues, which indicates that in the construction of campus network rapid development at the same time, but also pay more attention to the use of scientific, rigorous, standardized management provisions to make the whole system complete and safe [11].

Although the current university campus network management aspects of the basic standardization, but also from time to time campus network security accidents, comprehensive major research and practical application found that the current research on network security management is more only relevant theory, without taking into account the actual situation, although there are major software applications to deal with antivirus, firewalls and other issues, but there is no unified and standardized management tools, once the occurrence of security incidents, will bring very serious impact [12].

3. Overview of Digital Twin Technology

3.1 Definition of Digital Twin Technology

The concept of digital twins was first introduced by Michael Grieves, a professor at the University of Michigan, in his course on Total Product Lifecycle Management in 2003, where it was referred to as a "virtual digital representation of a physical product" [13]. However, due to cognitive and technological limitations, the concept did not receive much attention at that time. In 2011, NASA, together with the U.S. Air Force Research Laboratory, clearly defined the concept of "digital twin", which can be briefly summarized as shown in Figure 1.

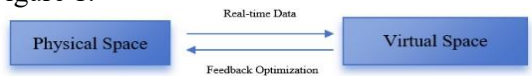

Figure 1. Conceptual Graph of Digital Twin

Digital twin technology is to digitally create a virtual model of a physical entity and simulate the behavior of the physical entity in the real environment with the help of data, and add or extend new capabilities for the physical entity through virtual-real interaction feedback, data fusion analysis, and iterative optimization of decision-making. Digital twin technology builds high-fidelity digital twin virtual models by utilizing a collection of science and technology such as the Internet of Things, cloud computing, artificial intelligence, etc., connecting the physical world and the information world to provide more real-time, efficient, and intelligent services [14].

Digital twin firstly needs to create a digital twin model of the application object. Tao et al. [15] proposed a five-dimensional model of digital twin based on the three-dimensional model of digital twin with the addition of two dimensions of twin data and services, and explored the initial concept of applying digital twin technology to 14 fields, which is widely recognized in digital twin research in China. Nie et al. [16] defined digital twin as a fine-grained digital description of physical entities with the ability to interact with reality, and simulation experiments using the digital twin model can truly reflect the characteristics, behavior, and performance of products.

Digital twin technology has the following characteristics:

1. Virtual-real mapping: The concept of digital twin is to map, connect and interact physical objects in the real world through digital representation in digital space to achieve two-way correspondence.
2. Synchronized real-time: Through the instantaneous acquisition of diverse data such as sensors, the twin is able to display changes in the state of physical items in an all-encompassing, precise and dynamic manner, covering aspects such as shape, utility, premises and malfunction.
3. Coexisting rendition: In the ultimate condition, the digital twin should encompass the entire process from design, manufacturing, operation to end-of-life, and progress and update with the object's lifecycle.
4. Closed-loop optimization: The end goal to create twin twins is to analyze the operating rules, research patterns and development trends of the physical world and use parsing and mimicry to accomplish corrective instructions or strategies for the physical reality individual, so as to achieve the closed-loop improvement function of the unit decision.

3.2 Principles of Digital Twin Technology

1. Data Acquisition

Various types of data from physical entities (e.g., machines, devices, systems, etc.) are collected in real time by means of sensors, devices, Internet of Things (IoT) technology, and so on. And the collected data is transmitted to the central platform via network for storage and processing. Data transmission usually requires high-bandwidth, low-latency technology support to ensure the real-time and integrity of the data.

2. Modeling and simulation

A virtual digital twin model is created based on the collected physical data as well as the design and behavioral characteristics of the physical entities. These models not only include the appearance of physical objects, but also need to cover their internal working mechanisms, performance characteristics, etc. On the digital twin model, computer simulation is used to simulate the behavior and performance of physical entities in different environments.

3. Real-time monitoring and feedback

Digital twins are able to recognize anomalies or performance degradation in a timely manner by monitoring the status of physical objects in real time. And it can make timely adjustments based on the data to provide targeted solutions.

4. Analysis and optimization

Using technologies such as data analytics,

artificial intelligence (AI), and machine learning, we process large amounts of data obtained from physical entities and virtual models, and optimize the performance and efficiency of physical objects by simulating their performance under different operating conditions.

5. Closed-loop control

Based on the analysis results, the digital twin technology can provide real-time control commands for the physical objects to adjust the operating conditions or repair faults. This closed-loop control mechanism ensures continuous optimization and stable operation of physical objects in different scenarios.

4. Application of Digital Twin Technology in Campus Network Security

In order to meet the needs of domain-wide data as well as scenario integrated governance, this paper designs a campus network security management platform based on digital twin, which provides a configurable, manageable, and second-developable service system for campus network security. The specific content is shown in the following Figure 2. The architecture diagram needs to show the core components of the platform, including data collection, network monitoring, attack detection, risk assessment, and management and response modules.

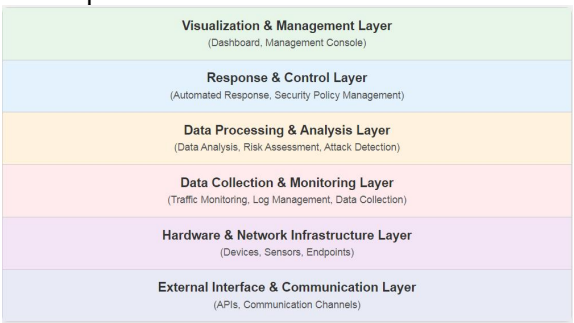

Figure 2. Digital Twin's Campus Network Security Management System

4.1 Security Risk Assessment

The data processing and analysis layer is the core layer of the campus network security management platform, which is responsible for in-depth analysis and risk assessment of the massive network data collected. This layer provides real-time network security situational awareness through the collaborative work of multiple modules and relies on digital twin technology to help managers make smarter decisions. This layer consists of the following four modules: data analysis module, risk assessment module, attack detection module and digital twin model. Digital twin technology builds a virtual mirror of the network environment by synchronizing with the real-time data of the campus network. The mirror can accurately reflect the data flow, node connections, device status and other information in the network to help managers understand the network's operational status in real time. Through the data collection module, the system is able to continuously monitor network traffic, host status, and user behavior to ensure that risks can be detected in a timely manner before potential threats appear. The details are shown in the following Figure 3.

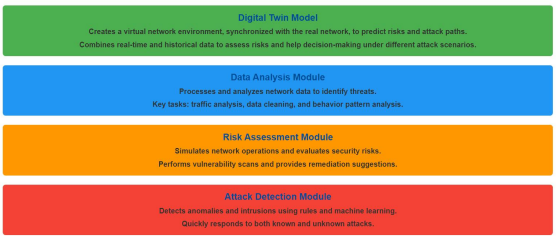

Figure 3. Campus Network Security Risk Data Assessment

The Data Analysis Module is the basic part of the Data Processing and Analysis Layer, and its main task is to process, analyze and store the data collected from the campus network in order to further identify potential threats. The core functions of this module include: network traffic analysis, data processing and cleaning, and behavioral pattern analysis. Based on the real-time collected data, the digital twin model is able to intelligently analyze various risk factors in the network. Using machine learning and big data analysis techniques, the system can identify abnormal traffic patterns, malware behavior, configuration errors, or potential security vulnerabilities. By simulating different attack scenarios, it evaluates the impact of various types of threats on the campus network and provides targeted risk assessment reports for managers.

The Risk Assessment module is able to simulate the operational status of the campus network in real time and perform security assessment automatically. Its core task is to identify potential risks in the network, assess vulnerabilities and configuration errors, and provide security recommendations for managers. The main functions include: virtual

network simulation supported by digital twin technology, vulnerability scanning and configuration checking, and risk assessment report generation. During the risk assessment process, the system is also able to automatically perform vulnerability scanning to detect security weaknesses in the network, such as open ports, un-updated patches or insecure configurations. The scanning results can be directly fed back into the digital twin model, and the system will provide corresponding remediation recommendations to help administrators fix vulnerabilities in a timely manner and further strengthen network security protection measures.

The attack detection module identifies abnormal behavior or intrusion through real-time monitoring and analysis of network behavior. The module combines machine learning models and rule-based detection algorithms to enable rapid response to known and unknown attacks. Its core functions include: rule-based attack detection, and machine learning-based anomaly detection. During the risk assessment process, the system is also able to automatically perform vulnerability scans to detect security weaknesses in the network, such as open ports, un-updated patches or insecure configurations. The scanning results can be fed directly into the digital twin model, and the system will provide appropriate remediation recommendations to help administrators fix vulnerabilities in a timely manner and further strengthen network security protection measures.

The digital twin model is the core technology of the data processing and analysis layer, which simulates and predicts potential network risks and attack paths by constructing a virtual campus network environment that runs in sync with the real network. This model not only reflects the network status in real time, but also enables in-depth analysis of network traffic and behavioral patterns to identify abnormal activities and their possible threats. By combining real-time data with historical data, the digital twin model is able to generate accurate risk assessments, helping administrators make effective decisions under different attack scenarios. In addition, the model's learning capability enables it to be continuously optimized to react quickly to new threat types, providing the ultimate security protection for campus networks.

4.2 Attack Detection and Response

Attack detection and response play a crucial role in the digital twin's campus network security management system. Digital twin technology enables network administrators to monitor network status in real time, identify potential security threats, and respond quickly to attacks by creating a virtual copy of the physical campus network.

With digital twin technology, the process of data collection and integration can be realized through real-time monitoring and the construction of virtual models. First, the system collects various types of data in the campus network in real time through sensors, network traffic monitoring and user behavior analysis. These data are then integrated into the digital twin model to ensure that the virtual environment accurately reflects the state of the real network. Through the integration of different data sources, the system is able to deeply analyze the network operation and identify potential risks. At the same time, the process of data collection and integration can form a dynamic monitoring environment. Digital twin technology Through machine learning algorithms, the system is able to identify traffic or user activities that do not match historical behavioral patterns, and then mark them as abnormal. As new data comes in, the model is continuously updated and adjusted so that it can adapt to changes in the network environment in real time. This method of combining historical and real-time data makes anomaly detection more accurate, enables timely identification of potential threats, and improves network security response capabilities.

By simulating the campus network environment, digital twin technology is able to effectively identify different types of attacks and quickly implement response mechanisms. First, the model monitors network traffic and behavior in real time, analyzes the data using machine learning algorithms, identifies anomalous patterns and compares them with known attack characteristics. In this way, the system is able to quickly determine the type of attack, such as a DDoS attack, phishing or malware intrusion. Once an attack is recognized, the digital twin model automatically triggers appropriate response

mechanisms, such as isolating affected devices, adjusting network configurations, or issuing alerts, to ensure the timeliness and effectiveness of network security protection.

After an attack is detected, the campus network should adopt a multi-level response strategy, including automated response and manual intervention. First the automated system quickly isolates affected devices to prevent the attack from spreading and instantly blocks suspicious IP addresses or traffic to protect the overall security of the network. Secondly, based on the type of attack detected, firewall rules are automatically updated to strengthen the defense. In turn, alerts are generated and sent to notify network administrators of detailed information about the attack. After the automated response, the network security team should perform an in-depth analysis of the incident to identify the source of the attack and the scope of its impact. Depending on the findings, the team may need to manually adjust the network configuration to prevent similar attacks.

The future of digital twin technology in campus cybersecurity will increasingly leverage AI and big data to improve attack detection and response. By leveraging big data analysis, the system can extract deeper patterns and trends from massive amounts of network traffic and historical data to improve the accuracy of identifying abnormal behavior. At the same time, AI algorithms are able to continuously learn and adapt to new types of attack techniques, enhancing automated response capabilities. In the future, the digital twin model will integrate more advanced deep learning technologies to achieve real-time prediction and defense, and help administrators take preventive measures before an attack occurs through intelligent decision support to build a more secure and dynamic campus network environment.

5. Conclusion

This paper discusses the application of digital twin technology in campus network security management, the core of this technology lies in its ability to combine real-time data with historical data to more accurately identify abnormal behavior and potential threats. Especially in the security risk assessment and attack detection and response modules, the digital twin model shows powerful data processing and intelligent analysis capabilities. Through the collaborative work of multiple modules, the system is able to analyze network traffic, user behavior, and device status in real time, and detect and respond to network security events in a timely manner. Digital twin technology will continue to play an important role in campus network security management. With the development of artificial intelligence and big data technology, digital twin models will be able to analyze and predict network risks more intelligently, thus providing more accurate security protection. Future research can focus on the following aspects: first, strengthening the ability to learn complex attack patterns and improving the real-time response speed of the system; second, further integrating deep learning and adaptive algorithms in order to improve the accuracy of the identification of abnormal behaviors; and third, exploring cross-platform data sharing and collaborative mechanisms to enhance the security protection capability between different network environments.

References

[1] Wu Jianli, Yang Hua, Zhang Liang. Research and application implementation of cross-campus campus network IPv6 security based on HCL simulation. Journal of Hangzhou Normal University (Natural Science Edition), 2019, 22(3): 319-328.

[2] Miller P.Inoue. Acollaborative Intrusion Detection System. Fuzzy Information Proeessing Societ, IEEE, 2003.519-524.

[3] Luo Xi. Research and application of Campus Network security system

[4] Tang Wenchun, Xu Qin, Lv Yunshan, Liu Ling. Application of digital twin technology in campus network security. Integrated Circuit Applications. 2024, 41(7), 360-361.

[5] Hu Yuanjun. Research and application of campus network security risk assessment method. SCIENCE & TECHNOLOGY INFORMATION. 2024, 12, 19-21

[6] Cai Xinchun. Research and implementation of campus network security prevention technology. Hefei: Hefei University of Technology, 2014. 06

[7] Xie Zhijian, Xie Dongqing, Zhou Zhouyi. VPN virtual private network architecture based on IP packet encryption. Computer Engineering, 2012, (3): 45-46.

[8] Qian Minye. Research on campus network security control strategy. Hebei University of Technology, 2017.

[9] Rosene, Rekhtery. BGP/MPLS VPNs. IETF RFC 2547. 2012, 3.

[10] Stalling W. Cryptography and Network Security: Principles and Practice. (Second Edition) Prentice-hall Inc, 2013, 212-216.

[11] By Bruce Schneier. Translated by Wu Shizhong et al. Applied Cryptography. Beijing: China Machine Press, 2000, 115-119.

[12] Zou Changchun, Gong Weibo, Donald Towsley. Code red worm propagation modeling and analysis. ACM Conference on Computer and Communications Security, 2002: 321-322.

[13] Grieves M. Grieves M. Digital twin: manufacturing excellence through virtual factory replication. White paper, 2014, 1(2014): 1-7.

[14] Tao Fei, Liu Weiran, Liu Jianhua, et al. Exploration of digital twin and its application. Computer Integrated Manufacturing Systems, 2018, 24(1): 1-18.

[15] Tao Fei, Liu Weiran, Zhang Meng et al. Digital twin five-dimensional model and ten fields of application. Computer Integrated Manufacturing System, 2019, 25(01): 1-18.

[16] Nie Ronmei, Zhou Xiaoya, Xiao Jin et al. Digital twin technology review analysis and development prospects. Total Aerospace Technology, 2002, 6(01): 1-6.

