Research on Computer Network Security Problems and Protective Measures under the Background of Big Data

Guoyu Luo1,*

1School of Computer Science, Hubei University of Technology, Wuhan, 430068, China
*Corresponding Author’s E-mail: 877189650@qq.com

Abstract: In the information age, human beings have entered the era of big data due to the large-scale data generated every day. Computer networks in people's lives are very common. In the construction of social infrastructure and economic development, networks and information systems are essential core elements. When a network attack fails due to a malicious attack, it will bring about more serious security accidents, which will make the public interest and the national economy safe. Studying and strengthening the detection of cyberattacks to provide basic security for network infrastructure is the core link to ensure the controllability of core technical equipment and the construction of a national network security system. Therefore, this paper first analyzes big data, network security models and intrusion detection frameworks, and analyzes the key issues facing computer network security under the current circumstances. Protective measures are used to reduce the various security problems caused thereby, to prevent computer users from suffering major losses.

1. Introduction

Until now, many industries have used big data for data analysis to provide data support for various decisions; Big data in the computer network has been widely used, which has broken the traditional models of various industries and formed a brand-new socio-economic development model [1]. In the context of big data, computer network technology has gradually become a major component of society, economy, and life; Data is quickly spread and shared in the computer network, which provides great convenience to people's lives. However, there is a problem in the network, that is, the openness is very high, so a lot of information with viruses is also randomly interspersed in the network, which brings a great hidden danger to the computer network security [2].

At this stage, computer network security is not only facing threats from traditional network security issues such as network viruses, hacker attacks, and network system vulnerabilities. A series of new threats generated by big data and cloud computing are also constantly evolving. This makes computer network security technology the importance continues to increase. In order to ensure that the computer network can operate safely and stably for a long time, the research content will carry out specific analysis around the computer network security, and put forward specific measures for security prevention and control [3].

2. Overview of network big data and analysis of intrusion detection framework

2.1. Overview of network big data
The rapid growth of data poses severe challenges to various industries and also brings valuable opportunities. Network big data refers to big data generated by the interfusion of “people, machines, and objects” in cyberspace and available on the Internet. Network big data, no matter in scale or complexity, has challenged the processing of existing computers [4]. International Data Corporation (International Data Corporation, IDC) has released a related research report, the report pointed out that the total amount of online big data in 2011 has reached 1.8ZB, and in 2020 is expected to reach 35ZB. The company also pointed out that big data needs to meet four characteristics: volume, diversity, velocity, and value [5]. In addition, IBM also believes that big data must have veracity.

The research on network big data is of great significance. At present, the related research mainly focuses on three aspects, namely the cleaning, storage and analysis of network big data. Network big data is often used in the fields of relationship monitoring, pattern and keyword search, data engineering, etc. In the foreseeable future, this technology will revolutionize various industries, making it easier for people to obtain valuable information for more efficient processing and application of data [6].

2.2. Network security model

With the continuous deepening of the informatization process and rapidly developing network technology, the connotation of the field of network security is becoming more and more abundant, and gradually deepened into a multi-layered three-dimensional network architecture security [7].

The main characteristics of computer network security are availability, integrity, confidentiality, controllability, and reliability.

From the perspective of security protection, the concept of computer network security includes three parts: network platform operation security, physical security and security management. Physical security is the foundation, and network platform operation security and security management are guaranteed. Together, they constitute a relatively complete network system security protection system. The conceptual model of network security is shown in Figure 1.

![Network security model](image)

2.3. Intrusion detection framework

The intrusion studied in this paper refers to network intrusion, which refers to various behaviors that may damage the network. Network intrusion is an abstract concept. Network intrusion will cause certain damage to network resources. These damages are mainly reflected in three aspects: one is to destroy the integrity of network resources, another is to destroy the availability of network resources, and the third is to destroy the network the confidentiality of resources and these sabotages may cause network security problems [8]. From the perspective of network intrusion, network intrusion can be divided into disguise attacks, denial of service attacks, security level upgrade attacks, and attempted intrusion attacks. Figure 2 shows the described system.
Detection is used to discover the network intrusion behavior that may or has already appeared in the network, and thus respond to the intrusion behavior. In terms of network defense methods, intrusion detection is an active defense technology. By analyzing and detecting communications, hosts, logs, etc. in the network, network data and behavior are analyzed to discover intrusion behaviors and respond to intrusion behaviors to avoid Network resources are destroyed, effectively preventing network attacks. Intrusion detection not only targets behaviors from outside the network, but also detects network behaviors inside the network [9]. A basic principle of intrusion detection is to assume that the network intrusion behavior is different from the normal network behavior in the network system, so intrusion detection can be performed by analyzing the system, network logs, and audit records.

The intrusion detection system needs to provide the following functions: First, the intrusion detection system can help the system administrator to understand various hardware and software changes of the network system, operating procedures, communication changes, etc. The intrusion detection system should also develop a network for the system administrator Security strategy provides data support; Secondly, the network intrusion detection system monitors and manages the network through a simple and easy-to-use management method. The network administrator can implement various configurations of network security through the intrusion detection system to enhance the security of the network system. The third intrusion detection system should have a quick response level. When an intrusion is detected, it can record the malicious behavior in the system log in a timely manner and respond positively to the malicious behavior, such as removing the corresponding network connection and issuing an alarm to the administrator.

Network intrusion detection works by analyzing the information transmitted on the network line between the hosts. It usually uses a network card working in "Promiscuous Mode" to monitor and analyze the data flow through the network in real time. Its analysis module usually uses techniques such as pattern matching and statistical analysis to identify attack behaviors. Its structure is shown in Figure 3.

![Figure 2. Typical intrusion detection system](image-url)
3. Analysis of existing problems in network security

Many fields have resorted to big data processing technology in practical applications, making enterprise decisions more reasonable and scientific, and playing the role of data information, but at the same time also expose computer networks to many security threats. Although many computer platforms and users have realized the importance of network security issues and made corresponding preventive measures, security issues are still emerging. Solving computer network security issues is not only a general trend, but also imminent and imperative.

3.1. There is an illegal invasion

The network is open, so many criminals took the opportunity to invade the network. Due to the extremely large scale of data information, the value density of data information has been reduced to a certain extent. If traditional computer network security technology is also used, it is difficult to detect hacker intrusions and the huge data scale increases in order to hide the concealment of hacking behavior. If a hacking occurs, it will usually lead to information leakage.

In addition, viruses have become more powerful with the further development of Internet technology. For computer networks, viruses are one of the main security threats. The computer has the characteristics of reproducibility, so the spread of viruses and the speed of spreading are greatly accelerated. If the virus attacks the computer, even if the computer is in normal operation, the virus will still attack other links of the computer, which in turn leads to paralysis of the entire computer system.

3.2. The relevant policy system is not perfect

From a national perspective, how to use big data, lack of legal requirements, is also an important factor leading to information security. With the development of national constructions, some policy encouragement and financial support have also been introduced for Internet technology. According to survey data, developed countries have much higher investment in information security than China, which shows that China needs to further strengthen its awareness of information security. Related domestic laws lag behind the development of technologies, leading to more legal “blind spots”. Therefore, the follow-up speed of China's information security related policies and regulations urgently needs to be improved.

From the enterprise level, a sound management mechanism can ensure the safe operation of the network. Some users, especially enterprise users are lacking a sound network security prevention and control system during the process of using the network, which increases the hidden dangers of network security. From the perspective of industry characteristics, some computer network information security
supervision systems do not match user industry. From the perspective of the management team, the lack of professional network management talents and the lack of professionalism in the team have led to the failure of the supervisory system to fully realize its effectiveness, resulting in many security risks not being discovered and the network security factor continuously decreasing.

3.3. Weak awareness of network security

After the emergence of network security problems, the actual effect of patching and maintenance is not good. Only when the source is properly maintained and security is set up consciously at the beginning of data generation can network security be better maintained. However, at present, network security administrators and ordinary users lack security awareness. Many websites have simple login password settings, and many users use the same password for different software logins. Some users don't even set security passwords at all, which can easily cause hidden security risks.

4. Protection measures to improve network security

4.1. Prevent illegal intrusion through computer network monitoring technology

For network companies, government and other relevant departments, they should continuously improve computer network monitoring technology and manage the network in an all-round way through this intelligent technology of network monitoring. For computer networks, some areas cannot be fully covered by human monitoring, at this time, you can use the accurate monitoring features of intelligent technology. Virus intrusion database construction, monitoring model construction and abnormal monitoring technologies are all network monitoring technologies. Monitoring technology can be used throughout the development, operation, and application of system programs to prevent illegal intrusion as much as possible.

In addition, re-encode the information before data transmission, so that the interceptor cannot get the real content of the information. Data encryption technology is a basic security technology in computer networks, which provides guarantee for the safe transmission of data. At present, asymmetric key encryption is the most widely used encryption method, and its security is higher than that of symmetric encryption. It uses a pair of interrelated keys, one of which is public and the other is private. At present, the relatively safe asymmetric encryption algorithms mainly include RSA, DSA, PKCS and PGP. The schematic diagram of asymmetric encryption is shown in Figure 4.

![Figure 4. Schematic diagram of asymmetric encryption](image)

4.2. Improvement of network information security management system

The technology of the Internet is used by more and more people. At the same time, there will also be many computer-type talents who have made personal development in the context of this big data. It’s just that not all people have a deep understanding of the law. This is contrary to the legal norms. This kind of people cannot correctly apply the technology they learned, but turned to join the hacker cause. China's network information security has caused relatively large constraints and impacts.
In order to fundamentally combat and suppress the illegal interference of hackers on the Internet, we must start with the safety management system and take strict measures as soon as possible. In addition, for those hackers who have proven to have illegally invaded other people's computer networks and websites, they need to set up an illegal intrusion barrier to generate resistance, and they can also return the other party's IP address in time to avoid the computer as much as possible. The important documents and personal information content in the stolen content have been stolen.

4.3. Strengthen computer network security awareness
With the help of some network example analysis, users are encouraged to do security defense of computer networks and make them aware of the harmfulness of illegal intrusions and the importance of network security precautions. Allow users to use a combination of higher security levels when setting user names and security passwords. For example, characters, letters, and numbers can be mixed to increase the difficulty of cracking. Do not use the same password for different websites. At the same time, it is necessary to do a regular password change to improve its security. On the other hand, in order to allow each user to have their own access rights, their network routers should be limited to their own access rights as much as possible. Some software and websites that contain personal privacy information, users should not apply public WIFI to log in.

5. Conclusion
In summary, in the context of big data, because of the high degree of freedom in computer networks, there will be various security issues in the network. This article first briefly analyzes the main network security problems, and finally proposes corresponding solutions to these common problems to protect it, so that the computer network technology can better serve people. It is of great practical significance to carry out computer network information security protection work. People must fully realize the importance of security issue and make corresponding preventive technology, and formulate targeted solutions based on actual conditions. Computer network security provides comprehensive guarantees to create a secure network environment.

Reference
[1] Yang, J.W. (2019) A brief analysis of computer network security precautions in the era of big data. Science and Technology Communication, no.2, pp.108-109.
[2] Long, Z.H. (2019) Computer network information security and protection strategy in the era of big data. Management Informationization in China, no.3, pp.161-162.
[3] Deng, Q.F. (2019) Computer network information security technology and its development trend. Electronic Technology and Software Engineering, no.24, pp.194-195.
[4] Liu, W. (2018) Research on Optimizing Network Security Strategy Based on Big Data. Software, vol.39, no.9, pp.205-208.
[5] Zhao, L. (2019) Research on computer network security protection strategy under the background of big data. Journal of Heihe University, vol.10, no.1, pp.217-218.
[6] Wang, Q., Pan, C. (2017) Analysis of Network Complete Vulnerabilities and Preventive Measures in the Era of Big Data. Network Security Technology and Application, no.2, pp.77 + 79.
[7] Bao, L.J. (2019) Application of Big Data-based Network Security Situation Awareness Platform in Private Network Field. Information Security Research, vol.5, no.2, pp.168-175.
[8] Wang, B. (2019) Network security fuzzy risk assessment based on computer network technology. Foreign Electronic Measurement Technology, vol.38, no.5, pp.11-16.
[9] Liu, Q., Cai, Z.P., Yin, J.P., et al. (2017) Research on the framework and methods of network security detection. Computer Engineering and Science, vol.39, no.12, pp.2224-2229.