RETRACTED: Optimizing Strategies for Analyzing Computer Network Security Technology Based on Big Data Era

J. Phys.: Conf. Ser. **1648** (2020) 022219 https://doi.org/10.1088/1742-6596/1648/2/022219

Retraction

Retraction: Optimizing Strategies for Analyzing Computer Network Security Technology Based on Big Data Era (*J. Phys.: Conf. Ser.* **1648** 022096)

Published 16 September 2022

This article has been retracted by IOP Publishing following an allegation that raises concerns this article may have been created, manipulated, and/or sold by a commercial entity. In addition, IOP Publishing has seen no evidence that reliable peer review was conducted on this article, despite the clear standards expected of and communicated to conference organisers.

The authors of the article have been given opportunity to present evidence that they were the original and genuine creators of the work, however at the time of publication of this notice, IOP Publishing has not received any response. IOP Publishing has analysed the article and agrees there are enough indicators to cause serious doubts over the legitimacy of the work and agree this article should be retracted. The authors are encouraged to contact IOP Publishing Limited if they have any comments on this retraction.

Retraction published: 16 September 2022

Optimizing Strategies for Analyzing Computer Network Security Technology Based on Big Data Era

Huiyun Chen[1,*]

[1]Yunnan Technology and Business Universtiy, China, 651700

*Corresponding author e-mail: 65948142@qq.com

Abstract. With the rapid development of information technology, the era of big data has officially arrived. The era of big data expands the functions of the Internet, which improves the speed of data transmission. The increase in speed means that more information can be exchanged at the same time. The enhancement of information exchange function will make information technology more diverse in life. However, the development of big data also brings opportunities for illegal elements. Many illegal elements steal and modify data information by means of computer. Therefore, computer network security technology has been paid more and more attention. This paper first analyses the application of network security. Then, this paper analyses the optimization strategy of network security technology.

Keywords: Big Data, Network Security Technology, Optimizing Strategy

1. Introduction

With the rise and development of cloud computing and other technologies, the processing of massive data has gradually been solved. At the same time, the ability of data acquisition has been greatly improved. However, changes in the scope of computer network security make the original network protection system no longer applicable. If we want to reduce the threat of network attack to information security, we need to optimize and upgrade the application of computer network security technology, which will ensure the security and stability of data and information interaction. In the problem of computer network security, the attack means of computer virus has brought great threat to the security of network data. According to the published data, network attacks will cause great economic losses to enterprises and even society. In the era of big data, hackers use more covert attack methods. Therefore, the construction of security system and the prevention of network attacks are facing greater challenges[1]. No matter how the system is perfected, there will inevitably be some loopholes. The management of computer network can not only affect the operation effect of the whole network, but also affect the probability of security problems.

2. Application of network security

2.1. Application of intrusion detection technology

Intrusion detection is the detection of intrusion behavior. By collecting and analyzing network behavior, security log, audit data, and information of several key points, intrusion detection system can check whether the network violates security policy or is attacked. Intrusion detection is a proactive security protection technology, which provides real-time protection against internal attacks, external attacks and misoperation. Before the network system is endangered, intrusion detection will intercept and respond to intrusion. Intrusion detection technology can make resources in computer network system more comprehensive, secure, confidential and available[2]. After collecting, screening, processing and analyzing network data, intrusion detection technology can form detection reports and feedback them to users in time, which will enable users to quickly find their own network security problems. By using intrusion detection technology to real-time monitor the operation of computer networks, we can protect computer networks from attacks, which will improve network performance.

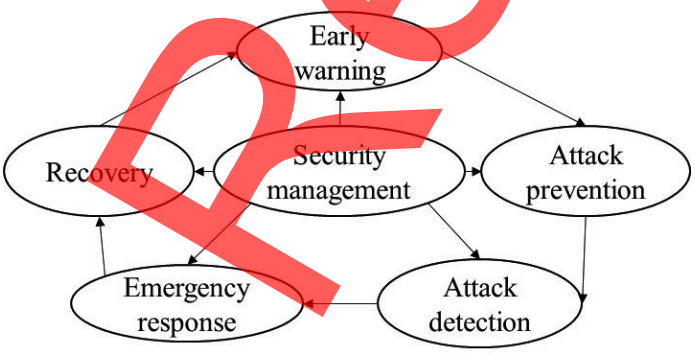
2.2. Application of intelligent firewall technology

Firewall is a protective barrier composed of software and hardware devices, which is constructed on the interface between internal network and external network, private network and public network. The firewall can protect the intranet from the intrusion of illegal users. All network communications and data packets flowing in and out of the computer must pass through the firewall. Intelligent firewall technology can intercept harmful information in network and computer successfully, which will prevent harmful information from entering computer system[3]. Through firewall interception technology, we can ensure the safe operation of computers. The security efficiency of intelligent firewall technology is higher than that of traditional firewall. It can solve the problem of denial of service. By resolving and processing data, computers can reduce the computational complexity of large data, which will increase the probability of discovering and dealing with network malpractices.

3. Design of network security system

3.1. Safety protection system

Information security prevention should be considered as a whole, which covers all levels of information system. Therefore, we should take comprehensive precautions against network, system, application and data. The model of information security system shows that security is a dynamic process. The technical means before, during and after the event should be complete[4]. Safety management should run through the whole process of safety precautions. As shown in Figure 1.



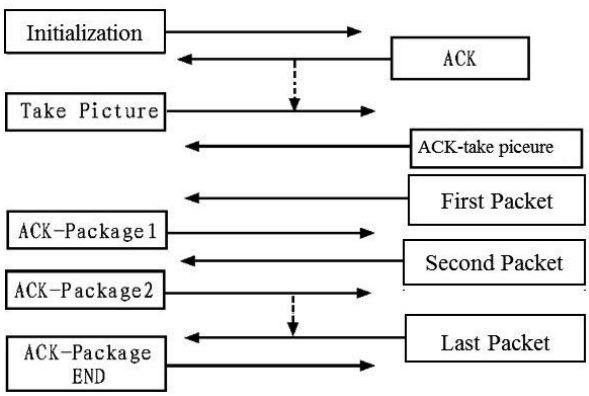


Figure 1. Network and information security defense system model

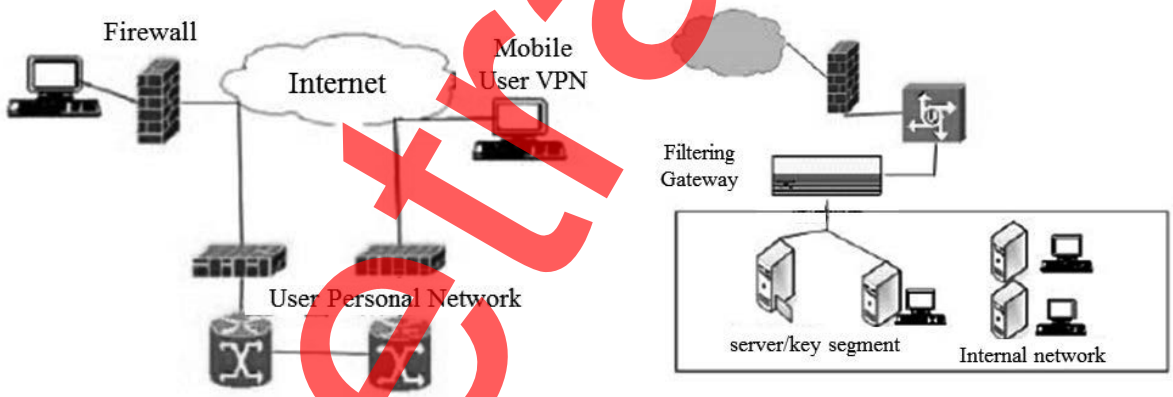
Figure 2. The design of security early warning module

3.2. Security early warning module

The main functions of security early warning system are behavior, vulnerability and attack. Figure 2 is the design of security early warning module. There are a lot of heterogeneous application software in large data computer network, which can communicate with each other by using different structures, development environments and languages in the process of integration. It is more prone to multiple vulnerabilities, which will increase the probability of security attacks. Vulnerability warning can achieve patch probability in a short time, which will resist external threats[5]. According to the abnormality of network traffic, network attack behavior can be predicted through a variety of algorithm behavior early warning, which will improve the early warning ability and system security.

3.3. Security protection

At present, the computer network security defense system mostly has the following security protection, such as firewall, VPN, antivirus software and so on. These software are single or integrated deployment, which will effectively improve the integrity of large data application center. In the continuous promotion and popularization of modern big data application centers, security defense measures also use digital signature defense technology, which will avoid denial behavior in data communications. By combining multiple defense technologies, we will avoid network data being infected and attacked. Figure 3 shows the design of the security protection module.



(a) Firewall and VPN Protection (b) Server and key segment protection

Figure 3. The design of the security protection module

3.4. Safety monitoring

By using intrusion detection, network traffic packet and other technologies, modern computer networks achieve timely access to network traffic[6]. Through hardware or software association rules technology, we can achieve in-depth mining. By reporting the mining results of the underlying layer, the network security response can achieve maintenance clearance. Figure 4 shows the design of the security detection module.

3.5. System Recovery

In modern computer network operation, most users do not receive formal training. So in the process of operation, the computer network will be threatened by security. If the computer server is threatened, the system recovery technology can restore the system to normal state, which will reduce the system loss. Figure 5 is the design of the system recovery module.

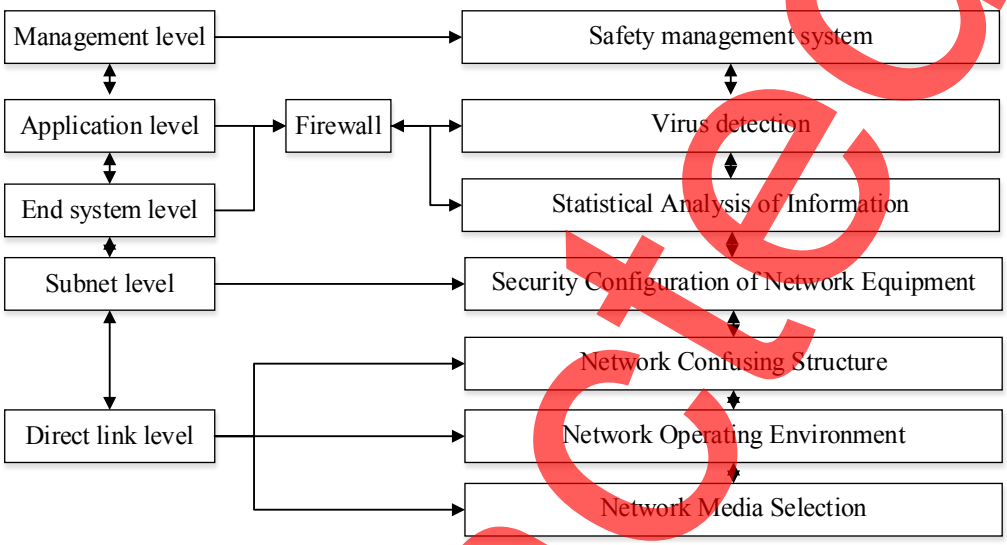


Figure 4. The design of the security detection module

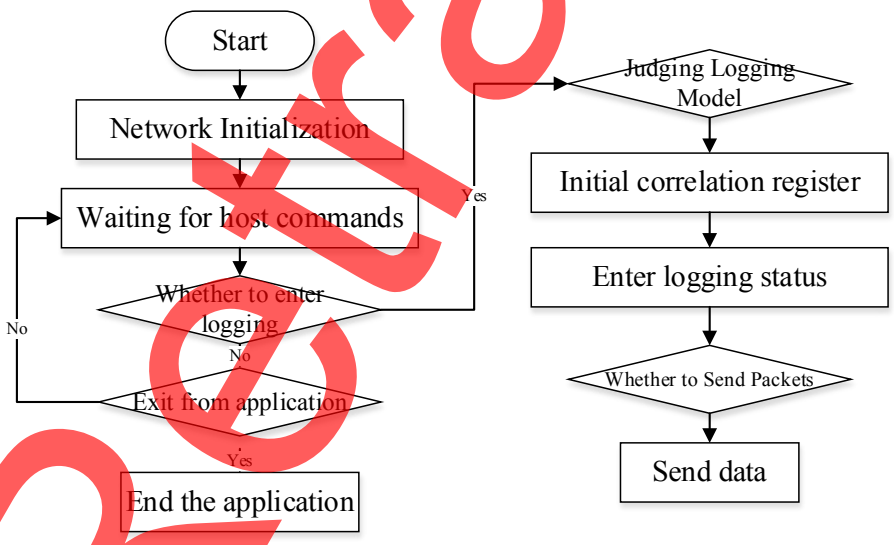


Figure 5. The design of the system recovery module

4. Conclusion

Computer network security management is very important in the era of big data. With more and more computer network security problems, system management must improve the network security management system. By strengthening the application of security protection technology, we can regard security management as the key point of computer network construction, which will improve the security of computer information network system.

References

[1] Wang Zhong. Research on Computer Network Information Security in Big Data Era [J]. Information and Computer: Theoretical Edition, 2017, 15 (15): 54-55.

[2] Tian Shuyi. Brief discussion on computer network security precautions in the era of big data [J]. Information and computer (theoretical edition), 2015 (12).

[3] Fu Mingli. Analysis of Computer Network Security and Preventive Measures in the Big Data Era [J]. Digital Users, 2017, 23 (2): 105-106.

[4] Male. Analyzing the optimization strategy of computer network security technology based on the era of big data [J]. China New Communications, 2017, 9 (15): 78-79.

[5] Wang Li. Discussion on Computer Network Security Technology in the Big Data Era[J]. Electronic Commerce, 2018, 000(009):47-48.

[6] Zhao Lihua. Computer network security and preventive measures in the era of big data[J]. Network Security Technology and Application, 2019(6):49-50.