Proceedings of the 2023 International Conference on Machine Learning and Automation
DOI: 10.54254/2755-2721/38/20230530

Design and implementation of computer network security detection and control system

Xi Chen

[1]School of Information and Design, Guangxi Vocational and Technical College of Industry and Commerce, Nanning 530007, Guangxi, China

451809509@qq.com

Abstract. With the widespread application of computer network technology, computer network security defense capability has become a focus of attention in various industries. The extensive use of computer information systems in various sectors has significantly improved work efficiency but has also introduced security risks and management issues. The deployment of network security detection and control systems allows for effective security monitoring and management of computer operations and real-time network information. This paper presents a computer network security detection and control system based on human-computer interaction, which enables users to handle daily key business processes. The work principles and overall architecture of the network security detection and control system are analyzed and demonstrated. It offers functions such as filtering options, address rules, network security detection, network unreachability, overall traffic analysis, subnet definition, fault diagnosis, and security analysis. Testing and analysis indicate that the system's design achieves the intended goals. In the application of network security features, it can effectively combine various forces to enhance the quality and efficiency of network security, making it widely applicable in various industry units.

Keywords: Network Security, Detection, Attacks.

1. Introduction

With the rapid development of network technology, computer information processing has found extensive applications in various industries' daily operations. The network-enabled work mode has led to a significant increase in work efficiency but has also brought about security management issues. In the realm of network security, the deployment of computer network security detection and control systems plays a crucial role. Existing network security detection systems often focus on external network environments while overlooking internal information security issues. The use of user software and the uncontrollability of network terminal configurations are important factors leading to network security problems.

To effectively combine various forces in the application of network security features and improve industry work efficiency, a computer network security detection and control system has been developed for the benefit of a wide range of users. The system aims to assist users in managing their daily key tasks. It includes functions such as filtering options, address rules, network security detection, network unreachability, overall traffic analysis, subnet definition, fault diagnosis, and security analysis. It aims

DOI: 10.54254/2755-2721/38/20230530

to enhance work efficiency and reduce operational costs for users. Real-time monitoring of controlled computer network access and system information is achieved through the input of basic data.

2. Technical Selection

2.1. Visual Studio Development Tool

Visual Studio is a powerful development tool for developers, offering a comprehensive integrated development environment (IDE) for writing, editing, debugging, and generating code [1]. Additionally, Visual Studio includes compilers, code completion tools, source code management, extensions, and many other features to enhance various stages of the software development process.

2.2. Introduction to MySQL Database

MySQL is a robust SQL database management system and an open-source data management system. Its powerful features, flexibility, rich application programming interfaces (APIs), and well-structured system have made it popular among users, particularly when combined with Apache and PHP/PERL for building database-driven dynamic websites [2]. MySQL is a true multi-user, multi-threaded SQL database server, designed to provide large-scale database capabilities on relatively inexpensive hardware platforms. SQL is a standardized language that makes storing, updating, and retrieving information easier. MySQL's main goals are speed, robustness, and ease of use, making it suitable for a wide range of applications [3].

3. System Design

In practice, network viruses and malicious software often attack internal networks in the form of instructions and operations specified by external networks, resulting in incorrect instructions and operations being received by internal networks [4]. To efficiently defend against external network attacks, a detection and control system for network security, which can effectively integrate various forces to enhance network security, has been constructed. This "Computer Network Security Detection and Control System" is installed in users' computers in the form of software and includes functions such as filtering options, address rules, network security detection, network unreachability, overall traffic analysis, subnet definition, fault diagnosis, and security analysis. The system contains characteristic data from the network threat and vulnerability database and can automatically analyze network packets to generate a characteristic set for building network command traffic. The data detection module can be combined with the data collection and analysis module, running on various devices such as network terminals, application servers, and network boundaries, significantly improving resistance to network attacks [5]. Due to limitations in application scale and high real-time requirements, this control system adopts a client/server (C/S) architecture. The control system consists of three parts: a system database, a detection server control program, and a security detection controlled terminal program. The system database stores detection schemes and detection information, the detection server control program issues management control requests, and the security detection controlled terminal program reads and executes detection schemes in response to requests. The deployment process is illustrated in Figure 1.

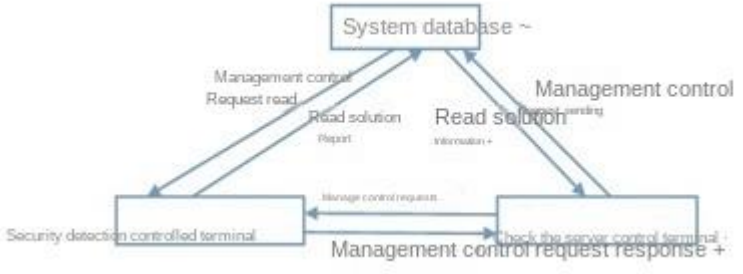

Figure 1. Detection Control System Deployment Configuration.

DOI: 10.54254/2755-2721/38/20230530

3.1. Implementation of Module Functions

After user login, they enter the system's homepage, which serves as the core of the entire system and displays detailed information. Depending on the user's needs, they can click on configuration preview buttons within the system, which automatically redirect to the corresponding configuration preview interface, where they can view the displayed configuration information. By clicking on the corresponding buttons, users can perform related function settings. The homepage includes a real-time analysis option that, when clicked, takes users to the real-time analysis interface, displaying real-time analysis information. Within this interface, there is an analysis settings option, which, when clicked, directs users to the analysis settings interface where analysis settings information is displayed. In the analysis settings interface, there is a filtering option, which, when clicked, leads to the filtering interface displaying filtering information, including address rules, port rules, protocol rules, and more (see Figure 2).

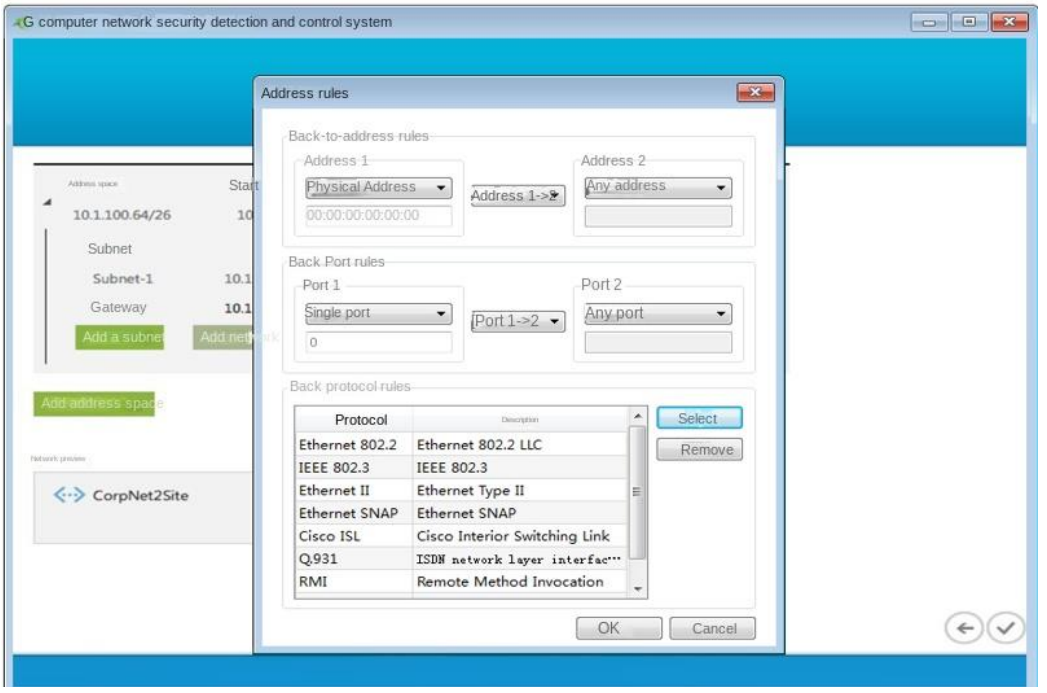

Figure 2. Computer Network Security Detection and Control System Homepage.

The real-time analysis module includes a traffic analysis option, displaying traffic analysis information, including start analysis time, data items, traffic information, reference values, analysis duration, and more. The network security detection interface displays network security detection information, including top protocol options, top host options, top broadcast packet-sending hosts, top multicast packet-sending hosts, and top packet send/receive ratio hosts. In the analysis interface, there is a security analysis option that, when clicked, takes users to the security analysis interface, which displays security analysis information, including network unreachability options, network congestion options, IP address conflict options, route loop options, DNS issues, and more. Clicking on different options leads to different interfaces. The homepage includes a scheduled analysis option that, when clicked, directs users to the scheduled analysis interface, which displays task name information, creation information, execution cycle information, start time information, end time information, and start analysis options (see Figure 3).

DOI: 10.54254/2755-2721/38/20230530

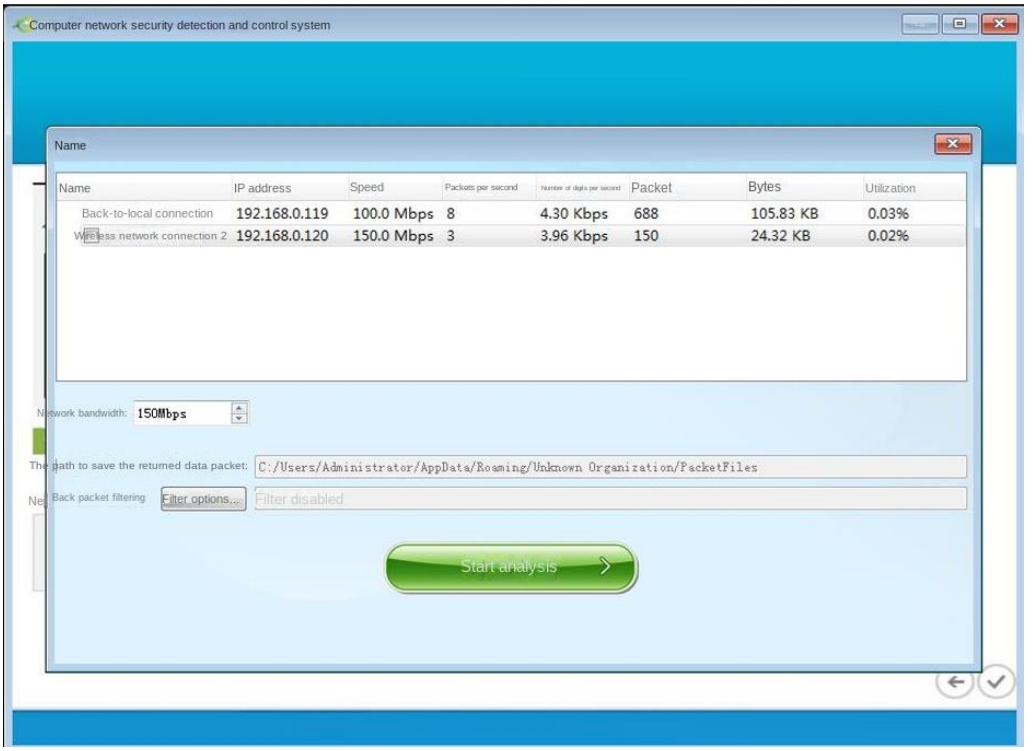

Figure 3. Network Detection Analysis Management.

Users can access the network settings functionality within the system based on their specific requirements. Upon clicking the network settings button, the system will automatically navigate to the corresponding network settings interface. Depending on their actual needs, users can click the relevant buttons to configure various functions. Within the homepage interface, there is an option labeled "Reference Values." Clicking on this option will lead users to the reference values interface, which displays information related to various reference values. This includes overall traffic analysis, IP traffic analysis, TCP data stream analysis, packet analysis, and more. The packet information section includes details about broadcast packets. In the reference values interface, there is a specific section for IP traffic analysis, which further encompasses information about broadcast traffic. In the system settings interface, there is an option for segment configuration. Clicking on the segment configuration option will take users to the segment configuration interface, where they can find information such as segment names, address location details, segment rules, and support for three different formats of IPv4 segments. Additionally, within the system settings interface, there is an option for event configuration. Clicking on the event configuration option will lead users to the event configuration interface, which displays information related to various event settings. This includes details about fault diagnosis and security analysis, among others. Within the event settings interface, there is a section specifically dedicated to fault diagnosis information, which covers details such as event names, time types, severity levels, and more. As illustrated in Figure 4:

DOI: 10.54254/2755-2721/38/20230530

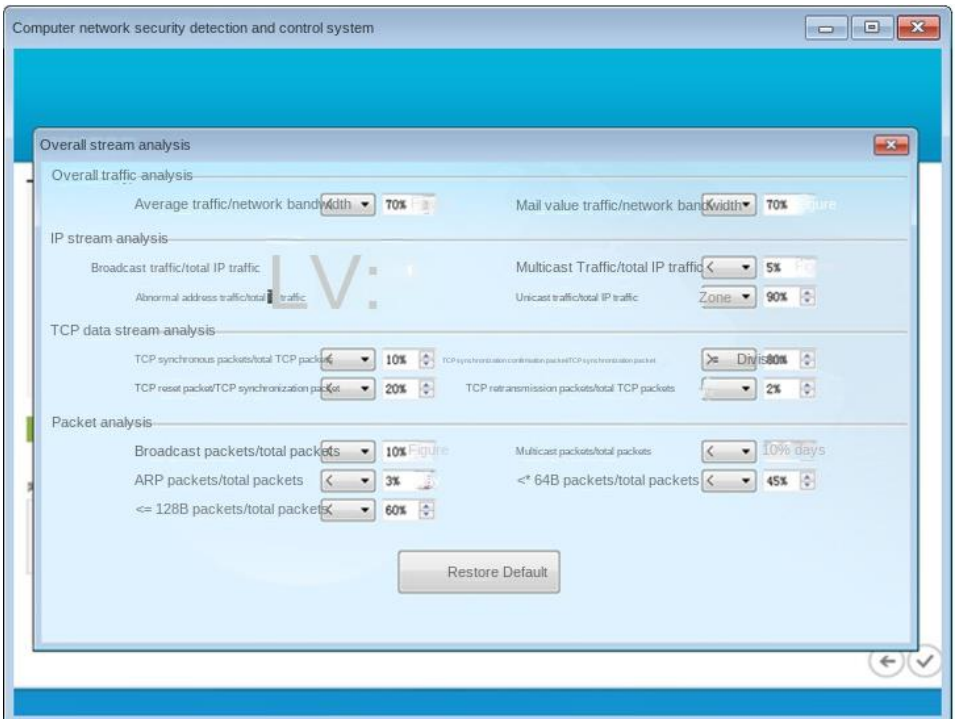

Figure 4. System Parameter Configuration Diagram.

3. System Testing

In order to analyze the practical effectiveness of the computer network security detection and control system, experiments were conducted to validate pre-collected data [6]. Normal traffic data and abnormal traffic data were imported into the system for comprehensive testing. By comparing the feature data of the test samples, the results showed an accuracy of over 99.99% in data structure modeling. From the experimental data, it is evident that the system exhibits a high level of accuracy in abnormal detection. Similarly, in terms of accuracy in detecting network attacks, favorable results were obtained. Random network attack testing was conducted by running the random network attack detection module [7] without known sample data. The results demonstrated an accuracy of over 95% in detecting random network attacks, indicating the system's effectiveness in handling such attacks. Comprehensive testing was performed on the system's functionality and performance [8]. The key performance metrics are summarized in Table 1:

Table 1. System Response Time and Resource Utilization.

Test Content	Expected Result	Average Response Time	Remarks
30 Controlled Hosts	≤1s	0.48s	
60 Controlled Hosts	≤1s	0.78s	All security policies on
80 Controlled Hosts	≤1s	0.93s	

Test Content	CPU Usage	Memory Usage	Remarks
Real-time Monitoring	2%	40M	CPU Frequency 2.0G
Software Object Management	4%	40M	Memory 4GB
Hardware Object Management	2%	40M	
Network Object Management	4%	40M	
File Object Management	5%	40M	
Full Security Policy	9%	40M	

DOI: 10.54254/2755-2721/38/20230530

The test results indicate that the system can meet the performance requirements within an environment of a maximum of 80 controlled host machines, and the memory usage remains unaffected by the loading of policies. Due to the loading of system functions for network object management and file object management, the CPU utilization rate is higher compared to real-time monitoring and hardware object management. Furthermore, the security detection scope for controlled host machines is broader, allowing for content audit detection. These test results affirm that the current system implementation is capable of fulfilling application requirements.

4. Conclusion

The research and design of the computer network security control system involved an in-depth analysis of the system's working principles and key technologies. The system was implemented using the C++ language. It effectively combines various forces in the application of network security features [9], thereby enhancing efficiency. The system enables remote real-time retrieval and control of the computer network file system and its operational status, achieving the intended design goals. Through human-computer interaction, it provides users with a better user experience. By incorporating features such as filtering options, address rules, network security detection, network unreachability, overall traffic analysis, subnet definition, fault diagnosis, and security analysis [10], the system demonstrates good stability in the application of network security, significantly improving the quality and efficiency of network security.

References

[1] Yang Jiahai, Ren Xiankun, Wang Peiyu, Network Management Principles and Implementation Techniques, Tsinghua University Press, 2020.
[2] Zhao Jiye. Layered Detection Technology of Network Space Mimetic Security Based on Machine Learning Algorithms[J]. Electronic Design Engineering, 2021, 29(19): 121-125.
[3] Lin Xingchen. Strengthening the Security Protection of Key Information Infrastructure through Network Security Detection and Evaluation[J]. China Information Security, 2021(9): 38-39.
[4] Yang Zongyue. Data Extraction and Analysis in Intelligent Network Security Attack Detection[J]. Computer Measurement and Control, 2021, 29(5): 174-178.
[5] Lei Dong. Application of Machine Learning in Network Security[J]. Network Security Technology and Applications, 2021(6): 40-42.
[6] Liu Sanman, Jia Wangjing. Network Security Detection and Protection Based on Neural Network Algorithms[J]. Shanxi Electronics, 2020(6): 48-51.
[7] Feng Renjun, Wu Ji, Wang Zhenyu. Network Security Detection Based on Asymmetric Decomposition Convolution[J]. Software Engineering, 2020, 23(10): 8-11.
[8] Zhai Diqing, Lv Qi, Yang Huairen, et al. Research on Network Anomaly Detection and Security Threat Level Prediction Based on Machine Learning[J]. Computer Knowledge and Technology, 2021, 17(34): 10-12.
[9] Li Lang. Research on Comprehensive Solutions for Computer Network Security in Small and Medium-sized Enterprises under New Situations [D]. Gansu University of Science and Technology, 2019.
[10] Nie Yuanming, Qiu Ping. Network Information Security Technology, Science Press, 2021.

Acknowledgments

This research was supported by:

(1) The 2023 Guangxi Vocational Education Teaching Reform Research Project "Research on Core Competence Cultivation Strategies for Vocational College Students in the Perspective of Industry-Education Integration" (Project Number: GXGZJG2023B032).

(2) The 2022 Guangxi University Young Teachers' Scientific Research Basic Ability Enhancement Project "Research on Network Visualization Course Selection Platform under the Background of Big Data" (Project Number: 2022KY1374).

DOI: 10.54254/2755-2721/38/20230530

(3) The 2023 Guangxi Vocational and Technical College-Level Project “Research on Core Competence Cultivation Strategies for Vocational College Students in the Perspective of Industry-Education Integration” (Project Number: XY2023ZD03).

Author Bio

Chen Xi (1983—), female, native of Zhangshu, Jiangxi, holds a master’s degree, and is a lecturer. Her research interests include computer technology, network security, and vocational education.