ISSN: 2688-8645

Research on Software Development Amd Design of Computer Network Automatic Detection and Control System

Yue Xu

Salesforce Service Cloud, Redmond, 98052, USA

yxu.joyce@gmail.com

Abstract

In response to the practical needs of automatic monitoring and control systems in the field of computer networks at present, this study constructs a new system development strategy with modular thinking as the core. After in-depth exploration of system requirements, this study points out the problems existing in traditional systems and proposes innovative design concepts for key modules such as information collection, anomaly detection, and control feedback. On this basis, this study applied distributed system architecture and cutting-edge algorithm technology, significantly improving the monitoring efficiency and response speed of the system. The research conclusion shows that the system has made significant progress in multiple dimensions such as performance, scalability, and security, and is expected to provide solid technical support for future network management.

Keywords

Automatic Detection; Control System; Software Development; Computer Network; System Architecture.

1. Introduction

With the continuous expansion of the scale of the computer Internet and the increasing complexity of its structure, the probability of network anomalies is also rising gradually. In this context, the use of automation technology for real-time monitoring and management of network conditions has become particularly critical, and it has become an urgent research problem that needs to be solved. The current method of relying on manual network intervention is no longer suitable for the high efficiency and security requirements of network management. Therefore, building an automatic detection and control system with intelligent features is of great significance for enhancing network stability and reducing operation and maintenance costs. This study elaborates on the construction plan of an innovative computer network automatic detection and control system, including system requirement analysis, architecture building, and specific implementation at the software level.

2. System Requirements Analysis

2.1. System Functional Requirements

The system should implement real-time data capture function, track the running status, data traffic, and machine log records of each node in the network in real time, in order to lay a solid data foundation for subsequent analysis and control work. In addition, the system needs to be equipped with an anomaly detection mechanism, which can quickly detect abnormal conditions in the network through in-depth analysis of real-time captured data, such as sudden changes in data traffic, node damage, network latency, and can issue alerts in real time. The system should also have the ability to automatically develop and implement intelligent management strategies

ISSN: 2688-8645

based on detected anomalies, such as adjusting data flow, changing network routes, or restarting nodes, to ensure the continuous and stable operation of the network. The specific classification and explanation of system functional requirements are detailed in Table 1.

Table 1. Specific Classification and Explanation of System Functional Requirements

functional module	Function Description	Demand Priority
Real time data collection	Dynamically monitor network status and collect basic data	high
anomaly detection	Identify and warn of abnormal situations in the network	high
Intelligent control strategy execution	Automatically generate and execute corresponding control strategies to ensure stable network operation	in
Logging and Reporting	Record the detection and control process, generate reports to assist in network optimization	in

2.2. Non Functional Requirements

In the process of building a computer network automation monitoring and control system, in addition to focusing on basic functional requirements, it is also necessary to consider numerous non functional requirements, which are crucial for ensuring the efficiency, stability, and ease of maintenance of the system in actual operation. The system should meet high performance standards, effectively handle large amounts of network information processing, and have rapid response capabilities to meet the needs of real-time monitoring and emergency regulation. The reliability and robustness of the system are equally indispensable, and it needs to work consistently and stably under changing and complex network conditions to prevent communication failures caused by system anomalies. Security is also one of the core elements, and the system needs to ensure the security of information during transmission and processing, and resist the risks of external invasion and information leakage. At the same time, the system should also have good scalability and easy maintenance features to support possible future functional upgrades and daily maintenance work. The specific list of non functional requirements is detailed in Table 2.

Table 2. Non functional Requirements

Non functional requirements	describe	Demand Priority
performance requirement	Process large-scale data and respond quickly, supporting real-time monitoring and control	high
Reliability and stability	Ensure long-term stable operation of the system and avoid interruptions caused by malfunctions	high
Security	Ensure the security of data transmission and processing, prevent attacks and data leaks	high
Scalability and maintainability	The system is easy to expand and maintain, making it convenient for feature updates and system upgrades	in

3. Overall System Architecture Design

3.1. Requirement Analysis

The main purpose of designing a computer network automatic monitoring and management system is to improve the automation and intelligence of network management, with the aim of maintaining the smoothness and stability of the network under changing and complex network conditions. The primary task is that the system must have real-time monitoring capabilities, which can collect detailed and accurate operational data of various nodes within the network,

ISSN: 2688-8645

such as data traffic, transmission delay, packet loss rate, and device operating status. By relying on real-time data collection and transmission mechanisms, network administrators can stay informed of the network's operational status at any time, enabling them to promptly identify and address potential issues.

With the continuous expansion of the scale of the Internet and the increasing complexity of its structure, the method of relying on manual network monitoring has become insufficient to meet modern needs. It is crucial to build a system that relies on setting thresholds and advanced intelligent algorithms for this purpose. This system can deeply mine historical data, conduct comparative analysis, and quickly identify hidden abnormal conditions within the network, such as sudden changes in data traffic, hardware failures, or security risks. Once an anomaly is detected, the system will promptly convey warning information to the administrator through various channels such as SMS, email, or app push, ensuring that the problem is resolved quickly. In the event of abnormal network conditions, the system should not only have the ability to detect problems, but also automatically perform network configuration adjustments and optimization operations according to established strategies or intelligent decision-making mechanisms, such as reallocating bandwidth, changing routing paths, or restarting related devices, with the aim of restoring smooth network operation as soon as possible and reducing reliance on manual intervention.

The system must have powerful data storage and processing capabilities, be able to archive past monitoring information, and conduct in-depth mining and analysis of these archived contents. Relying on massive data analysis and the application of intelligent algorithms, the system can continuously improve its monitoring and control solutions, thereby enhancing its adaptability and intelligence in dealing with changing network conditions.

3.2. Technical Selection

When developing an automatic monitoring and management system for computer networks, the chosen technical route directly affects the system's operational efficiency and future expansion potential. In terms of client development, a fusion solution of HTML5, JavaScript, and WebSocket technology was chosen. HTML5 technology ensures that the system interface can run seamlessly on different platforms, JavaScript technology is responsible for implementing dynamic page effects and data display, and WebSocket technology is responsible for achieving real-time two-way information exchange between the client and server. This technology fusion solution effectively ensures real-time feedback of network conditions on the monitoring interface, meeting the high standard requirements of real-time monitoring.

In the backend of the system architecture, Python or Java was adopted as the dominant programming tool. These two programming languages are known for their stability and outstanding performance, with Python particularly outstanding in data mining and automation processes, while Java demonstrates extraordinary strength in handling concurrent tasks in large-scale enterprise applications. By leveraging the strengths of these languages, the system is able to efficiently perform monitoring and automated control tasks of network conditions. In addition, the backend will also use protocols such as SNMP and NetFlow to monitor and collect real-time data from network devices and data streams, ensuring accurate data as a basis for subsequent automatic detection and control work.

For data storage, the system combines the traditional relational database MySQL with the modern non relational database MongoDB. MySQL is mainly responsible for the storage of orderly data, including but not limited to machine configuration and Internet settings. MongoDB focuses on processing massive real-time monitoring records and data without fixed format. This storage solution strikes a good balance between flexible data manipulation and retrieval efficiency, enabling the system to maintain high-performance operation even under high data loads. In addition, the system also integrates the Hadoop/Spark big data processing

ISSN: 2688-8645

platform to deeply explore the value of data and improve monitoring and management strategies through machine learning technology, further enhancing the system's intelligent response capability.

3.3. System Architecture Design

When constructing the architecture of the computer network automatic monitoring and management system, a hierarchical structural design concept was adopted, aiming to enhance the modularity, scalability, and ease of maintenance of the system. The system mainly consists of three key levels: user interface layer, business processing layer, and data storage layer. These three levels remain independent of each other and rely on standardized interfaces to achieve close coordination, thereby ensuring the efficiency of network management and control.

The user interface layer serves as the interactive interface between the system and users, utilizing HTML5 and JavaScript technologies to achieve real-time interface interaction. With the help of WebSocket technology, this layer can synchronously obtain data refreshes sent by the backend, allowing users to monitor real-time network conditions, review historical information, and receive warning messages for network anomalies on a visual interface. In addition, this layer is not only responsible for presenting information, but also allows users to manually perform network configuration and management tasks through an interactive interface.

The business logic layer bears the responsibility of automatic monitoring, warning, and management. This level relies on Python or Java languages to build a framework for business logic, while utilizing communication protocols such as SNMP and NetFlow to collect the working status and data traffic of network devices. It also has built-in automatic monitoring units, warning systems, and intelligent control components, which can make timely decisions based on fluctuations in network conditions, such as adjusting network settings, optimizing route selection, and other operations. The system also specially plans a strategy management unit, which can automatically implement response actions based on pre-set strategies.

4. Software Development and Implementation

4.1. Data Collection and Processing Module

In the network automation monitoring and regulation system, the information collection and analysis unit constitutes the foundation of the system. Its main function is to collect core data from network facilities and data streams, and conduct preliminary analysis and processing of this information in order to provide strong data support for subsequent automatic monitoring, alarm issuance, and management operations. This unit integrates numerous network communication protocols, such as Simple Network Management Protocol and NetFlow, to obtain critical intelligence such as the working status and data traffic of network devices.

Taking network traffic monitoring as an example, the system must track the transmission volume of critical routers in real-time. With the help of NetFlow technology, the system can periodically obtain traffic information from various network ports within the router, and its data collection process can be represented as:

$$F(t) = \sum_{i=1}^{n} P_i(t)$$

Among them, $F(t)$ represent the total traffic at time, $P_i(t)$ represent the traffic of the th i th t and th network interfaces at time. n It is the number of interfaces in network devices. By using this algorithm, the system can instantly summarize and analyze the transmission data of all interfaces, which is extremely beneficial for subsequent observation and analysis work. The collected transmission data often contains detailed information of numerous basic data packets. In order to optimize the system's performance and improve data processing speed, the data

ISSN: 2688-8645

processing unit must perform preliminary processing on this information, which involves multiple steps such as data sorting, merging, and filtering. In the data organization stage, the system will eliminate useless data packets and duplicate records; The data merging process will integrate the transmission data from different time periods according to the set time interval (such as every five minutes), which can reduce the burden of data storage. The data filtering stage is to select specific types of network transmission (such as HTTP, DNS transmission), in order to achieve more in-depth and detailed monitoring and analysis.

4.2. Abnormal Detection and Analysis Module

The key component of the network automatic monitoring and management system is the anomaly monitoring and analysis unit, whose main function is to track the real-time operation status of the network, detect unusual activities, and conduct in-depth analysis of these anomalies, aiming to achieve real-time warning and make management decisions. This unit conducts comprehensive analysis of captured real-time information, while referring to past records and preset detection standards, to autonomously identify abnormal behaviors within the network, such as abnormal fluctuations in data traffic, unstable links, or hardware device errors.

In a normal operating enterprise network environment, the data transmission volume usually remains at a relatively stable level, showing a certain fluctuation pattern. However, during a specific period of time, the monitoring system captured a surge in traffic, which far exceeded the usual fluctuation range. After in-depth analysis of traffic data by the anomaly detection module, it was revealed that this surge in traffic was sudden and far exceeded the network's past traffic records. Based on this, the system quickly makes a judgment of abnormal traffic and speculates that this abnormality may be caused by network attacks, such as DDoS attacks, or improper device settings.

When unusual network activity is detected, the system will conduct in-depth analysis of the starting point, ending point, and nature of the data flow, aiming to identify the exact root cause of the problem. The system may observe an abnormal concentration of data traffic generated by an external IP address, and the pattern of these requests is consistent, thus marking it as a possible indication of an attack. The abnormal event analysis unit will conduct a detailed exploration of these abnormal situations to determine their nature and scope of impact. For example, the system can distinguish whether traffic anomalies are caused by external attacks or problems with the network devices themselves by analyzing the patterns of traffic anomalies. During this process, the anomaly monitoring and analysis unit will closely cooperate with the automatic control system to implement a series of emergency strategies, such as restricting abnormal data streams, switching to backup network channels, or restarting faulty devices, in order to maintain network continuity and stability.

4.3. Control Strategy and Response Module

In the network automatic monitoring and regulation system, the core link is the control strategy and response unit, which is responsible for automatically implementing appropriate handling actions when abnormal situations are detected, ensuring the smooth operation of the network system. This unit relies on a pre-set set of control strategies and integrates real-time monitoring information to quickly respond, automatically adjust network parameters, allocate resources reasonably, and perform necessary other tasks, aiming to alleviate or eliminate the impact caused by abnormal conditions. The essence lies in reducing human intervention and improving the efficiency of network management through automated means.

In the network environment of enterprises, once the monitoring system detects an unusual surge in data traffic during a certain period of time, it may be due to malicious behavior or configuration errors. In response to such anomalies, the system's control and response unit will

ISSN: 2688-8645

automatically activate pre-set management strategies based on the captured anomaly information. The system will conduct in-depth analysis of the source IP and its behavior patterns of abnormal traffic to determine whether it has attack properties. During this process, the system will automatically create detailed reaction records, including the details and effectiveness of each operation. These records can be used by network administrators to review the exception handling process, in order to make subsequent improvements to control strategies.

4.4. System Integration and Testing

The process of verifying the functionality and operational stability of computer network automatic detection and control systems is where the importance of system integration and testing lies. In this process, the various components of the system, such as the information collection unit, anomaly detection unit, and control strategy unit, must be efficiently integrated to ensure their collaborative operation in practical scenarios and achieve seamless integration. The fundamental purpose of system integration is to verify whether the interaction between various units is smooth, whether the transmission of information is accurate and error free, and to evaluate whether the performance indicators of the entire system meet the established design standards.

In the system integration process, the primary task is to integrate the data collection component with the anomaly warning component, ensuring that the data collection component can accurately and instantly capture the operating status of network devices, and transmit this information to the anomaly warning component. In the comprehensive testing phase, the system is deployed to a real enterprise network environment, and components are collected to extract traffic information from numerous network devices using SNMP protocol. The purpose of comprehensive testing is to verify whether this information can be accurately input into the anomaly warning component for processing.

At this stage, the system continuously monitors network traffic. Once a sharp increase in traffic is detected during a certain period, exceeding the established limit, the abnormal warning component will evaluate whether to activate the abnormal response mechanism based on the following formula:

$$F(t) > F_{threshold}$$

Among them, $F(t)$ It's in time t The actual network traffic detected at all times, $F_{threshoid}$ it is the normal traffic threshold set in the system $F(t)$ When the traffic exceeds $F_{threshoid}$ When, After this series of tests, the system's ability to cooperate in data collection, anomaly recognition, and control instruction execution has been verified.

5. Conclusion

In this study, a modular concept-based computer network automation monitoring and management platform was developed. This platform integrates multiple functional units such as data collection, anomaly detection, and automatic control, greatly enhancing the intelligence and automation level of the system. After a series of integrations and tests, the platform is now capable of real-time monitoring and rapid response under changing network conditions, greatly reducing the necessity of manual operations. The research results show that the platform demonstrates excellent capabilities in improving network performance, enhancing system stability, and ensuring network security, and has good flexibility, scalability, and environmental adaptability.

ISSN: 2688-8645

References

[1] Xu, Feixiang, Jiayin Lu, and Yejin Lin. "Multi person collaborative training and evaluation system for ship engine room based on network cloud." Computer Applications and Software 40.10 (2023): 10-16.

[2] Chen, Yanhong, and Bin Guo. "Research on the Development, Utilization, and Management Mechanism of Network Teaching Resources for Computer Programming Courses." Theoretical Research and Practice of Innovation and Entrepreneurship 2023.10 (2023): 127-129.

[3] Cheng, Peng, Zhenyong Zhang, and Xin Che. "Review of Industrial Control System Safety Hotspots in 2023." Technology News 42.1 (2024): 314-328.

[4] Cao, Songhao. "Development and Design of Computer Automatic Detection and Control System Software." Information Industry Report 2023.8 (2023): 0106-0108.

[5] Chen, Xiujuan. "Exploration of Automated Development Technology for Computer Application Software." Network Security Technology and Applications 2023.4 (2023): 68-69.

[6] Cheng, Yuanyao, Xinyi Wang, and Yi Chen. "Design and Implementation of ATS Cache System Based on Redis." Computer Applications and Software 40.7 (2023): 111-115.