Network Traffic Monitoring and Real-time Risk Warning Based on Static Baseline Algorithm

ZhaoliWu[1,2,3,*], Junwei Liu[4]

[1]School of Information and Electronics Engineering, Jiangsu Vocational Institute of Architectural Technology, Xuzhou,Jiangsu, China, 221000

[2]JiangSu Collaborative Innovation Center for Building Energy Saving and Construction Technology, Xuzhou,Jiangsu, China, 221000

[3]School of Computer Science and Technology, China University of Mining and Technology, Xuzhou,Jiangsu, China, 221000

[4]School of Internet of Things Technology, Wuxi Vocational College of Science and Technology, Wuxi, Jiangsu, China,214028

Article Info
Volume 83
Page Number: 5783 - 5789
Publication Issue:
July - August 2020

Article History
Article Received: *25 April 2020*
Revised: *29 May 2020*
Accepted: *20 June 2020*
Publication: *28 August 2020*

Abstract

In the development of modern society, network technology has been widely and comprehensively applied and it occupies an important position that cannot be ignored in the material life of the masses. In the context of the development of the times, the level of society has been further improved and computer technology and information networks have been widely used. The complexity of the network environment brings difficulties to the measurement of network traffic, but the measurement of network traffic is beneficial to the network environment In the big data environment, the traditional network traffic anomaly detection method is no longer applicable. What follows is the use of cloud computing technology to detect abnormal network traffic in the big data environment. This article analyzes the cloud computing platform and introduces The operating principle of the cloud computing platform is introduced and a new detection method is proposed. The current lives of the masses are increasingly inseparable from network technology and mobile terminal equipment. It can be said that the emergence of computer and network technology has provided the people with a strong convenience advantage. In terms of security, network monitoring and security is also a major issue that has been explored and studied in recent years. To this end, this article will conduct a detailed study on the design and implementation of the network monitoring system, hoping to provide more significant advantages for the development of this work.

Keywords: *Network Traffic, Monitoring, Real-time Analysis;*

1. Introduction

The network supervision security system is generally divided into "front-end network information security monitoring" and "back-end data collection", which is the main structure of the system. The network information security monitoring at the front desk mainly refers to the equipment connected to the network, which can effectively monitor and manage the existing network information resources. The background data collection is mainly to ensure the operation of the network monitoring security management system and is also the core of the entire system, with a certain degree of security and independence. The smooth operation of background data collection is critical to the entire network security system. After ensuring the safe operation of the two parts of the foreground and the background, the information resources will be connected to the connection port of the device and all the clients of the computer network after being transmitted to the computer and a new network attribute is established at the end of each client. Finally, add the corresponding network resource security manager. In the module management of the network resource server, the server is an important part of the network monitoring and management system. Therefore, a separate security management module is required for the management of the server. The server module of the Windows system will use relatively safe system data packets for collection and Management, data collection and data management for computer network resources and memory occupancy. In the process of computer access to the network, personal IP must be bound to the computer terminal address. Some of the computer terminals are computers with special requirements on the access port. These computers need to use the method of reading the connected terminal devices to maintain the system security and deal with the corresponding modules. The security system will automatically record the personal IP and the computer terminal address at the same time. Therefore, the two addresses cannot overlap during the process of accessing the terminal device. If other devices premeditatedly access the operating system, the network security device will issue an alarm and The sound of warning is an indispensable part of the current network supervision security system.

2. Static baseline algorithm

2.1 Sampling circuit estimates expansion warning threshold

Calculate the circuit expansion early warning threshold through circuit sampling and shorten the acquisition period, select circuits at each network level by sampling and shorten the acquisition period in a short period of time. Compare and calculate the circuit expansion early warning threshold based on the operator's 5-minute acquisition period. This threshold is applied to all circuits at the corresponding network level. In practical applications, it was found that the effect did not meet expectations. First, the difference in network topology and regional user bandwidth rates resulted in large fluctuations in the threshold; second, due to differences in user Internet habits, the same circuit was in different time periods. The peak flow ratio of the circuit based on different flow collection periods is not static. The estimated threshold can be used to roughly estimate whether the circuit is congested. However, there are situations where the flow has not reached the warning threshold but the circuit is already congested and the circuit has not been congested after reaching the warning threshold. The network traffic collection and circuit expansion early warning models used by operators have improved, but the accuracy is still difficult to meet the demand[1]. The network system is in the figure below.

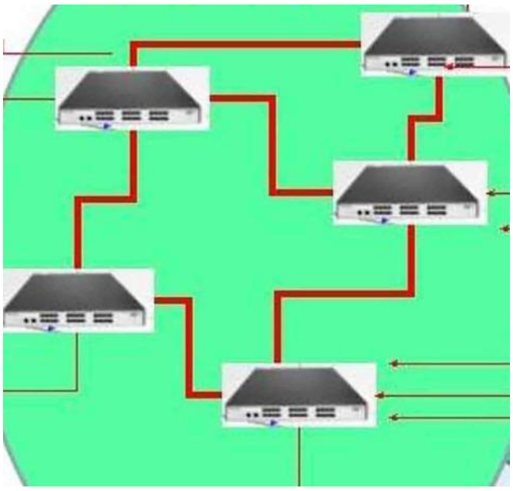

Figure1. Network system.

2.2 Shorten the entire network traffic collection cycle

Subsequently, the feasibility of shortening the network traffic collection period of operators from 5 minutes to 2 s was further discussed. Shortening the collection period can effectively improve the accuracy of network traffic collection, but high-frequency collection actions will occupy network bandwidth and equipment performance resources. , The number of circuits of

Published by: The Mattingley Publishing Co., Inc.

provincial-level operators exceeds hundreds of thousands and the number of single device ports can reach hundreds. If the current 5-minute collection period is shortened to 2 s, it is expected to increase the accuracy of network traffic collection by 50%, but The performance and resource usage of the collection server and equipment needs to be increased by 150 times. On the one hand, a large number of server computing and storage resources need to be expanded. On the other hand, high-frequency collection actions may cause high CPU utilization of network equipment and cause business operation risks. The solution to shorten the network traffic collection cycle is difficult to promote and use in the entire network of operators[2]. The network connect system is in the figure below.

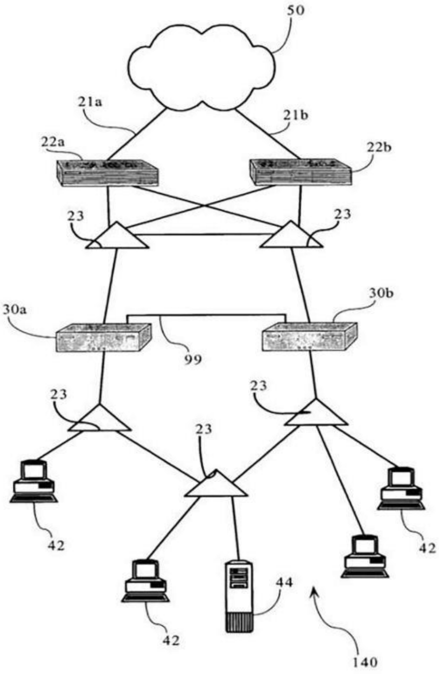

Figure2. Network connect system.

2.3 Traditional acquisition plus triggered second-level acquisition

Based on the above attempts and analysis, a new model of operator network traffic collection and circuit expansion early warning with traditional collection plus triggered second-level collection is finally proposed. That is, shorten the collection period and calibrate the operator's circuit expansion warning threshold. When the circuit flow reaches the expansion warning threshold, Trigger second-level acquisition to accurately determine whether the circuit needs expansion. The specific work implementation is: on the basis of the operator's original daily network traffic collection based on a 5-minute period, periodically start the collection of a 2 s period and calibrate the circuit expansion warning threshold based on the 5-minute period. In the daily network traffic collection process, When the circuit flow is close to the expansion warning threshold, a 2 s cycle flow collection is triggered for 3 minutes and the circuit flow of the 2 s collection cycle is calculated. If the circuit flow exceeds 95%, the circuit expansion warning is immediately given[3]. The network management system is in the figure below.

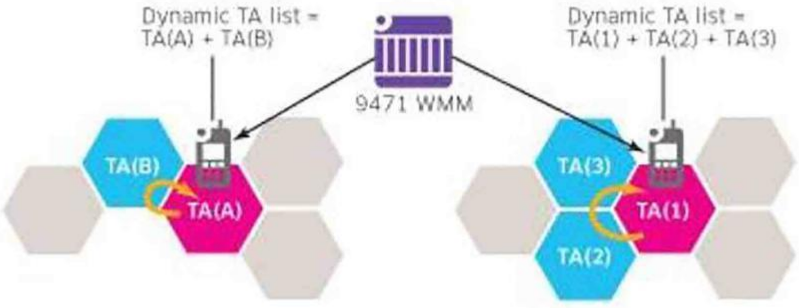

Figure3. Network management system.

3. Network traffic monitoring

The detection of network traffic is actually to standardize the network environment, optimize network configuration and improve user efficiency. At present, the measurement methods for network traffic are mainly divided into two categories, one is the active measurement method and the other is the passive measurement method. The difference between the two is that the active measurement method will increase the network traffic burden and cause unnecessary network congestion:

3.1 Active measurement technology

Active measurement is actually adding network traffic between two designated endpoints to test the performance of the two endpoints. Therefore, during the measurement process, new traffic will be generated between the two endpoints. The active measurement method has drawbacks, because increasing the traffic between the two ends will increase the network load. The additional network traffic may cause network congestion, cause additional problems and may cause inconvenience to users[4]. The network adapter system is in the figure below.

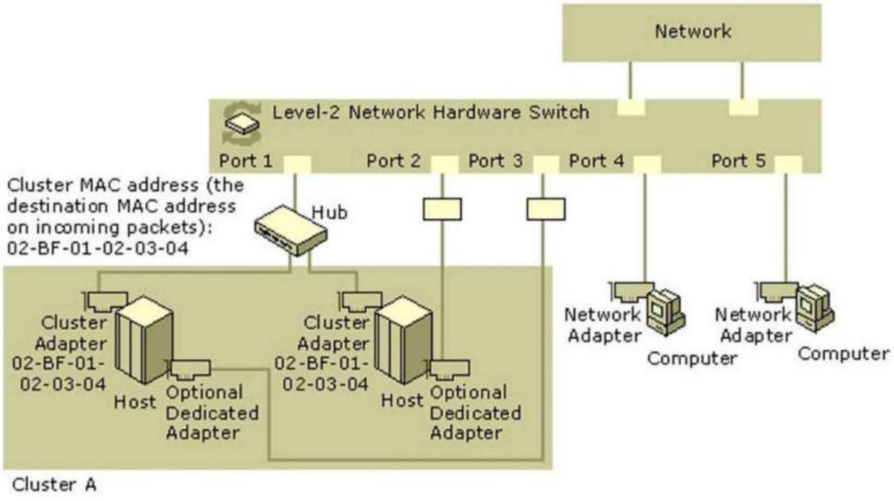
Network
Level-2 Network Hardware Switch
Port 1
Port 2
Port 3
Port 4
Port 5
Cluster MAC address (the destination MAC address on incoming packets): 02-BF-01-02-03-04
Hub
Cluster Adapter 02-BF-01-02-03-04
Host
Optional Dedicated Adapter
Cluster Adapter 02-BF-01-02-03-04
Host
Optional Dedicated Adapter
Network Adapter
Computer
Network Adapter
Computer
Cluster A

Figure4. Network adapter system.

3.2 Passive measurement technology

The passive measurement method is not to add traffic between two designated endpoints, but to detect traffic at a special location, such as using a router or switch to collect data. The advantage of passive measurement is that it does not generate additional traffic and does not increase the burden on the network. Therefore, the development of passive measurement technology is also increasing and it is more and more widely used in real life. The data obtained by passive measurement is grouped information of different sizes, which can be used for various traffic analysis. The development of passive measurement technology is conducive to the development of the Internet[5]. The network system is in the figure below.

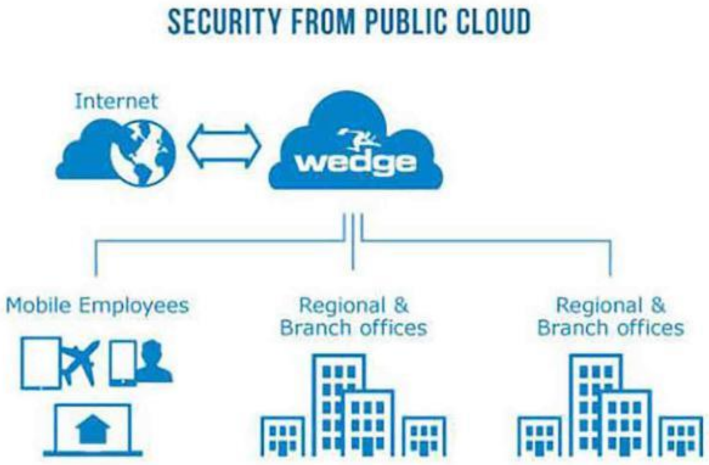
SECURITY FROM PUBLIC CLOUD
Internet
wedge
Mobile Employees
Regional & Branch offices
Regional & Branch offices

Figure5. Network system.

4. Real-time risk monitoring and analysis

4.1. Hardware design

The main content of the hardware design of the network traffic monitoring system based on the background of big data application is the wireless digital monitoring meter, the model is MD-S280G-P2. The wireless digital monitoring meter is a digital monitoring meter with wireless digital output powered by a power supply. It can be equipped with GPRS or LORa-iot wireless communication mode. The built-in high-precision pressure sensor in the wireless digital monitoring meter can accurately monitor the network traffic in real time and has the characteristics of high accuracy and long-term stability. At the same time, the wireless digital monitoring meter is equipped with a large-size LCD liquid crystal display, built-in MCU and the overall design of low power consumption. The wireless digital monitoring meter adopts 406 stainless steel housing and connectors and has passed the safety and explosion-proof certification. And the function is practical, real-time monitoring of the current network traffic, the upload rate only needs 1 minute to 24 hours to be adjustable. In addition, the wireless digital monitoring meter can preset alarm points based on the remaining network traffic and once the alarm pressure is triggered, the alarm network traffic will be sent in time. Therefore, the wireless digital monitoring meter is particularly suitable for the field of network traffic monitoring that requires unattended and remote monitoring and can realize accurate distributed synchronous monitoring of network traffic[6]. The network mode system is in the figure below.

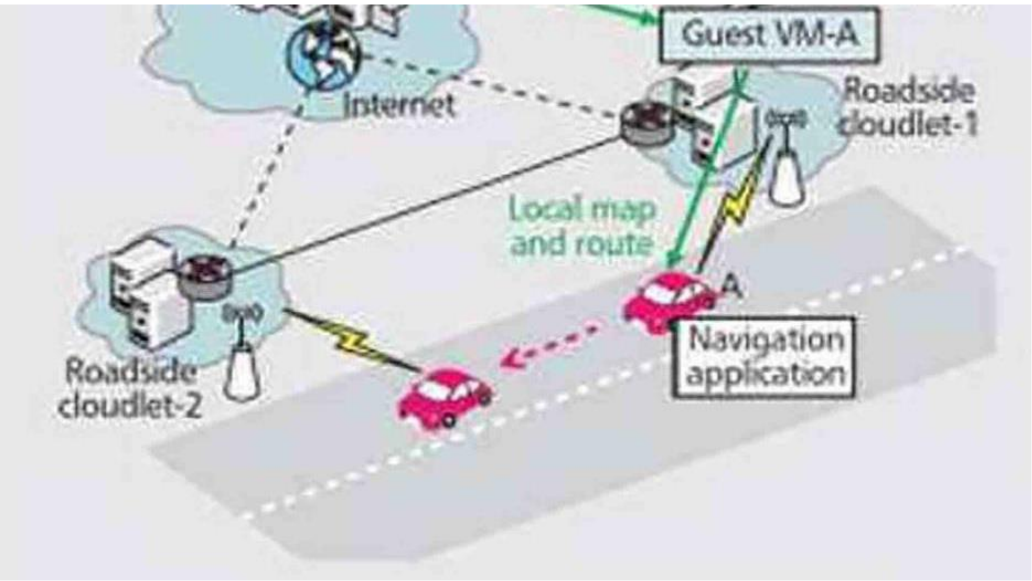

Figure6. Network mode system.

4.2 Software design

In the software design of the network traffic monitoring system based on the big data application background, the monitoring terminal is used to preprocess the network traffic and the database is designed to realize the real-time monitoring of the network traffic. In the process of network traffic data monitoring, the monitoring terminal is used to preprocess the network traffic and network traffic monitoring can be completed without configuration. In the context of the application of big data, first set the network traffic monitoring field, after entering the URL, the software can automatically identify the network traffic on the page and generate network traffic monitoring results. After completing the addition of the network traffic monitoring task, you can start to use the database to start the network traffic real-time monitoring task. Before starting, some settings of the database are required to improve the stability and success rate of monitoring network traffic. Click the "Settings" button, you can set the operation settings and anti-blocking settings in the pop-up operation settings page. Here, check "Skip continue to confirm data", set "3" second request waiting time and check "Don't load webpage pictures" , The anti-shielding setting is in accordance with the system default setting and then click Save to complete the database setting. In the software design of the network traffic monitoring system based on the big data application background, a mature database is needed to change and manage the monitored network traffic. All the data preprocessed by the monitoring terminal is directly updated to the database. When a second search is performed, the real-time situation of network traffic can be directly monitored through historical data.

5. Conclusion

In the information age, computer networks are closely related to each of us. At the same time, certain network traffic monitoring and risk warning problems have emerged. The current public network traffic monitoring and risk warning issues have received close attention. This article first puts forward some network traffic monitoring and risk early warning problems in the current society, then analyzes the structure of the network monitoring security management system and finally makes further improvements and enhancements to the design and implementation of the entire network monitoring security management system. Including the improvement of the network system security level protection system, the implementation of an effective monitoring and management system, regular audits of network traffic monitoring and risk early warning and the setting of relevant security inspection posts. According to the design guidelines of the network supervision security management system, the current network supervision system is comprehensively improved to prevent information viruses from spreading and copying in the network system and to maximize the network traffic monitoring and risk warning in the information age

Acknowledgments

Jiang Su Collaborative Innovation Center for Building Energy Saving and Construction Technology:《XT-Research and application of public building energy consumption monitoring system based on big data》,ProjectNo:SJXTY1603, Project Leader: Wu Zhaoli.

References

1. Arista Networks Inc.; Patent Issued for Accelerated Network Traffic Sampling For A Non-Accelerated Line Card (USPTO 10,756,989) [J]. Computer Weekly News, 2020.
2. Go-Idea Ltd.; Researchers Submit Patent Application, "Method For Deterring Malicious Network Traffic", for Approval (USPTO 20200267124) [J]. Information Technology Newsweekly, 2020.
3. Engineering; Findings in Engineering Reported from Yanshan University (A Two-layer Deep Learning Method for Android Malware Detection Using Network Traffic) [J]. Computer Technology Journal, 2020.
4. Juniper Networks Inc.; Patent Application Titled "Network Traffic Switching For Virtual Machines" Published Online (USPTO 20200252437) [J]. Computer Weekly News, 2020.
5. Lixia Huang, Karlo Abnoosian. A new approach for service migration in cloud-based e-commerce using an optimization algorithm [J]. International Journal of Communication Systems, 2020, 33(14).
6. Engineering; New Engineering Findings from New Jersey Institute of Technology Described (Gan Tunnel: Network Traffic Steganography By Using Gans To Counter Internet Traffic Classifiers) [J]. Journal of Engineering, 2020.