Research on Real-Time Monitoring Method of Communication Network Blocking Based on Cloud Computing

Wei-yan Li[1], Kui Gao[1], Yu Li[1], and Pei-ying Wang[2](✉)

[1] College of Information Science and Engineering, Shandong Agricultural University, Taian 271000, China
liweiyan254@sina.com
[2] Tianhe College of Guangdong Polytechnical Normal University, Guangzhou 510540, China
wangpeiying258@sina.com

Abstract. Aiming at the problems that the traditional method has long response time to communication network congestion monitoring and the detection effect is not ideal, a real-time monitoring method based on cloud computing for communication network blocking is proposed. Firstly, the communication network monitoring point is established, and the communication data collection process is completed by the radio-frequency receiver. On this basis, the real-time traffic calculation of the collected data is performed to determine the existence of abnormal blocking status in the communication network link, and the precise positioning of the blocking point is obtained. The information thus generates an alarm message to obtain a monitoring result. The real-time and accuracy of the monitoring method are analyzed experimentally. It is found that the monitoring method can control the delay time within 0.2 s and the monitoring error rate is low. It can be seen that the monitoring algorithm has high performance.

Keywords: Cloud computing · Telecommunication · Network congestion · Real-time monitoring

1 Introduction

In the process of communication network construction, there are often various interferences that affect the performance of the network; if the interference problem is not cleared, the network optimization work in the network construction is difficult to carry out. Among these interference problems, blocking interference is a systematic, whole network and serious interference problem. If it is not solved, network construction will not be possible. Blocking interference is that when the strong interference signal and useful signal are added to the receiver at the same time, the nonlinear components of the receiver link will be saturated, resulting in nonlinear distortion and blocking the receiver, which is beyond the working range of the amplifier and mixer, making the receiver unable to demodulate normally, interfering with the work of the receiver, resulting in the failure to report the bottom noise level of the communication network normally. When the signal is too strong, the useful signal will also produce amplitude

S. Liu and L. Xia (Eds.): ADHIP 2020, LNICST 347, pp. 88–97, 2021.
https://doi.org/10.1007/978-3-030-67871-5_9

compression, and will block when it is serious. The main reason for blocking is the nonlinearity of the device, especially the multi-step products of intermodulation and intermodulation. At the same time, the dynamic range limitation of the receiver will also cause blocking interference. Blocking will cause the receiver to fail to work properly, and long-term blocking may also cause permanent performance degradation of the receiver.

So, how to confirm that blocking interference does occur? There are the following steps to confirm:

(1) Frequency shift. According to the principle of blocking interference, for the RF terminal whose filter type is if filter, the strong interference signal can be excluded from RF reception by frequency shift (changing the center frequency point of RF reception), so that the signal strength falling into RF reception is less than -40 dbm. If the RTWP of communication network is reduced, it can be determined that the interference network is blocked.
(2) Att (VGA) attenuation. For the single-mode station suspected to be jammed, if the degree of interference is not very serious, ATT or VGA attenuation can be used to determine whether the communication network is jammed by the interference signal suppression ability. If in the process of att (VGA) attenuation, the RTWP of the communication network has a sudden change, it means that the cell is blocked.
(3) Add wave trap. The notch filter (narrow-band filter, also known as band stop filter) can be customized to attenuate the strong interference signal to a reasonable degree according to the actual situation on site, so that the total received signal in the RF reception is lower than the threshold value of blocking interference, so as to judge whether the disturbed signal network is blocked.
(4) Turn off the interference source. This method is the simplest way to judge. If the network RTWP returns to normal after the suspected interference source (the interference signal does not fall into the wireless network receiving), it can prove that the communication network is blocked. It can be seen from the above content that for the severity of blocking interference, corresponding solutions can be adopted: according to the frequency shift, att (VGA) attenuation, the installation of notch filter, and direct processing of interference source in order. According to the solution of network congestion, this paper introduces cloud computing technology to realize the real-time monitoring of communication network congestion.

In general, cloud computing refers to a business computing model. It distributes computing tasks across resource pools of large numbers of computers, enabling applications to acquire computing power, storage space, and information services as needed. In short, it provides on-demand, scalable, and affordable computing services over the network. Anyone can share and retrieve resources in the world of network communication. The network uses physical links to connect isolated workstations or hosts to form a data link for resource sharing and communication purposes [1–3]. Network communication connects various isolated devices through the network, and realizes communication between people, people and computers, computers and computers through information exchange. However, with the complication of information in the communication network and the large-scale data volume, some network problems occur in the communication network, such as communication network congestion [4]. Communication network congestion is a state of continuous overloaded network. The network transmission performance is degraded due to the limited resources of the storage and forwarding nodes.

As far as the architecture of the Internet is concerned, the occurrence of congestion is an inherent attribute. However, if the blocking condition has a certain persistence, when the cache space is exhausted, the router only discards the packet to ensure that the network avoids the lockup condition. Generally speaking, there are many reasons for the communication network blocking, including the insufficient bandwidth or overload of the server where the target website is located, the network cable problem, the existence of a loop in the network, and the like, and eventually the network speed is slow. In the big environment of cloud computing, in order to maintain the normal communication of the network and avoid the negative impact of congestion on the network, some countermeasures need to be taken to maintain the normal operation order of the communication network.

2 Design of Real-Time Monitoring Method for Communication Network Blocking

2.1 Set Communication Network Monitoring Point

First, a network monitoring device needs to be set up at a certain node in the network to obtain performance parameter data of all links related to this node. Therefore, in order to obtain performance data of all links, it can generally be implemented by setting network monitoring devices on some switching nodes. Therefore, it is necessary to consider which nodes are set up with network monitoring devices, and it is possible to obtain performance data of all links and enable monitoring. The minimum number of devices. Multiple network monitoring devices can be divided into multiple network monitoring areas. One network monitoring device can logically belong to multiple network monitoring areas, that is, multiple network performance monitoring services for multiple users, thereby reducing the number of devices and reducing construction costs [5, 6]. This requires reasonable setting of network monitoring points and rational division and management of network monitoring areas. In order to fully realize the monitoring function of the monitoring point, the structure of the communication network monitoring point is divided into a local area network part, a server system, various workstations, a terminal server, a protocol converter and a remote network device. The structure of the monitoring point is shown in Fig. 1.

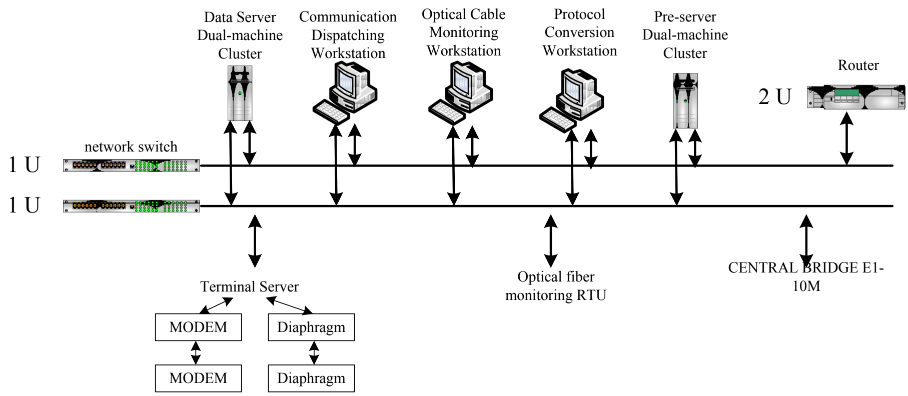

Fig. 1. Schematic diagram of the monitoring point structure

The dual Ethernet LAN device adopts the networking mode of 100M dual Ethernet to ensure the reliability of the system. The monitoring point is configured with dual network switches. Each server and workstation are equipped with dual network interfaces to ensure the failure of any network switch. The following does not affect the function of the system. Set the two network segments, the internal network segment and the external network segment through the bridge function of the network switch to ensure that the data of the internal and external network segments do not interfere with each other. The function of connecting to the remote LAN is realized through the router. The dual-master server cluster adopts the server working mode of the dual-master server cluster, establishes the link between the two servers, and makes the two servers into a cluster working mode. The two servers are hot backups to each other, and the system guarantees that it encounters on any one server. The system function is not affected after the fault.

Add high-performance input and output peripherals such as laser printers to share with online users. The data of each substation is sent to the central station through the bridge. Each bridge is configured with a dual network port to realize the connection with the dual network port [7–9]. At the same time, the dual WAN port is provided to realize the dual E1 channel of the main and standby, and the automatic switching of the dual channel is ensured. In addition, a protocol conversion processor is required to input data from various communication monitoring subsystems of different protocols.

2.2 RF Receiver Collects Communication Network Data

Data collection and storage are the basis for performance monitoring, enabling the acquisition and storage of raw information. With the RF receiver principle, the RF link has an adjustable digital attenuator and VGA to ensure sufficient dynamics to meet the in-band blocking specification. However, if the blocking signal is far from the operating frequency, it may fall within the proximity of the ADC or other Nyquist sampling bandwidth and be sampled by the ADC [10]. If the interference frequency is sampled and falls into the useful signal, causing the in-band signal to alias, the RF and digital filters do not have any suppression of the signal. In this case, an intermediate frequency filter is needed to prevent the unwanted signals from being digitally sampled. The structure of the performance monitoring data table is shown in Fig. 2.

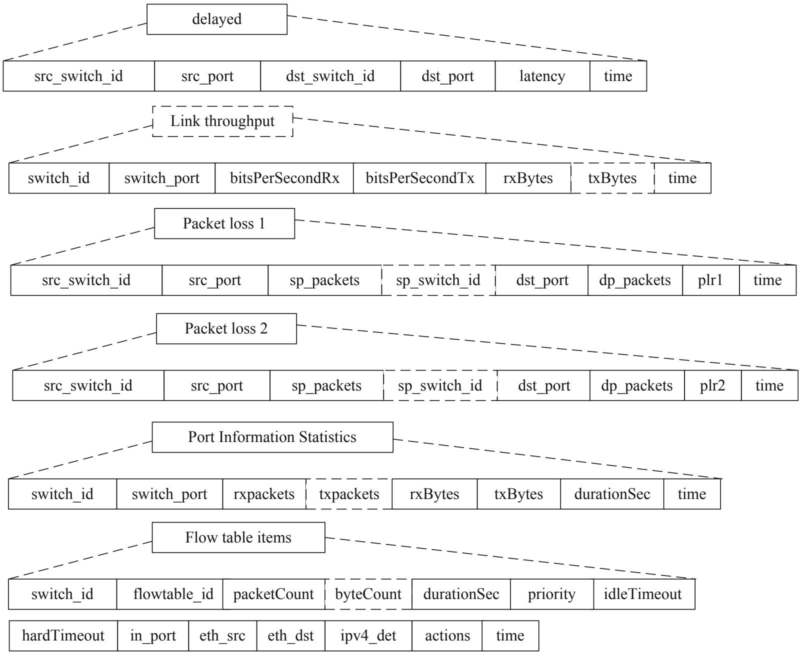

Fig. 2. Communication data acquisition chain diagram

The establishment of the above table and the connection to the database in the controller are implemented by the JDBC interface. Combined with the speed, low cost and open source of the MySQL database, using JDBC as the interface of MySQL has become a common usage. JDBC is a standard API for the Java language to interact with databases. Java applications can access the database directly through this standard interface. JDBC also supports the ability to access different types of databases in a uniform manner. Create a real-time performance data collection thread and store the collected data. The data acquisition and storage implementation relationship module is mainly divided into three implementation packages: the database connection package CLOS.sql, the main function is to realize the connection and management functions of the database; JavaBean package colSto.bean mainly defines the data structure of various performance data tables. The business operation package cloSto.op mainly completes the data receiving and storage functions. When the performance monitoring module obtains the performance parameters, it calls the corresponding class in the business operation package. Data storage operations to enable distributed storage of real-time collected data.

2.3 Communication Network Real-Time Flow Calculation

The data traffic collected in the communication network is calculated in real time, and the real-time computing structure is compared with the maximum storage space and the maximum load of the bandwidth capacity, and it is verified whether the data traffic can smoothly reach the specified storage space through the bandwidth for data storage [11–14]. The calculation formula for the real-time flow calculation of the communication network is as follows:

$$Q = \min\left\{ \sum_{k \in I_l} \frac{F_l}{\sum_{k \in I_l} P_{lk} y_{lk} - F_l} + G \sum_{\substack{l \in L \\ k \in I_l}} (S_{lk} y_{lk} + d_i m_{lk}) + V \sum_{\substack{l \in L \\ k \in I_l}} (C_{lk} \mathrm{F_l} y_{lk}) \right\} \tag{1}$$

In formula 1, F_l represents the local data traffic on the communication network link; Q is the total data traffic; I_l represents the candidate link model indicator set of the first link; P_{lk} represents the model index of the first link selected as Link capacity at k; S_{lk} represents the candidate route set of the node of the first link; C_{lk} represents the line variable coefficient when the model index of the first link is selected as k; d_i is the length of the first link; m_{lk} represents the communication link I Packet arrival rate; G is a fixed weighting factor; L is a set of all links in the communication network; the constraints in Eq. 1 include:

$$\sum_{k \in S_p} \mathrm{x}_p = 1(\forall p \in \Pi) \tag{2}$$

$$\sum_{k \in I_l} \mathrm{y}_{lk} = 1(\forall l \in L) \tag{3}$$

Where Π represents the set of all communication node pairs in the network; x_p is the optimization variable and takes a value of 1 when the route is selected as the communication route with other related node pairs, otherwise 0. Where y_{lk} represents the optimization variable. When the model index of the first link is selected as k, the value is 1; otherwise, it is 0; according to the formula, the real-time communication traffic of a certain link can be obtained, and the maximum limit and bandwidth of the storage space can be obtained. The maximum limit of capacity is compared to determine the flow of the flow under normal conditions.

2.4 Abnormal Blocking Recognition and Feature Analysis

In addition to the communication data traffic in the communication network exceeding the maximum bandwidth of the communication network can cause network congestion, data anomalies are also another cause of network congestion. Therefore, it is also very important for the identification of communication network anomalies and system inspections. In the real-time monitoring of communication network blocking, in order to realize real-time monitoring of abnormal data nodes, nodes need to be automatically patrolled. The node monitoring program reads the IP address of the device from the database, and sends a PING command periodically and cyclically. Record the returned result to the working state of the node device. If the returned result times out, the node device is not working properly. Once the network traffic is abnormal, the IP address and port distribution will change. If the network configuration error occurs, the original IP address and the destination IP address will increase, causing the host's packets to increase sharply. According to this feature, the network traffic matrix method is used to analyze the dispersion of traffic distribution characteristics. Suppose the traffic characteristic is A, the total number of samples is B, the number of samples selected is C, and the number of occurrences of a particular traffic characteristic i is n_i. Therefore, the traffic characteristic sample can be selected as:

$$F(x) = -\sum_{i=1}^{C} \left(\frac{n_i}{B}\right) \log_2 \left(\frac{n_i}{B}\right) \tag{4}$$

If all the selected samples have the same result, then $F(x) = 0$; if all the selected samples have a large degree of dispersion, then $F(x) = \log_2 C$ can describe the abnormal behavior of different flow characteristics, and then perform packet capture processing.

When the traffic monitoring system captures the transmitted Ethernet frame, it needs to parse the data packet first, and then extract the related data, and store the extraction result in the database, which is convenient for real-time analysis of network abnormal traffic. In order to ensure the accuracy of packet capture, the packet capture function interacts with the hardware in real time. In order to ensure the accuracy of the system capture, you need to read the configuration file first; then establish a connection with the database, register the ODBC data source, use the OpenDataBase() function in the Python script file to connect to the database; configure the capture driver to create various types. Timers and threads, real-time monitoring of abnormal traffic using timers; Finally, create a real-time monitoring server, and call the Bind() function to obtain the IP address of the monitoring server from the configuration file, thereby completing the packet capture behavior. The abnormal traffic data packet can be captured in real time, and the real-time monitoring display function can be added, so that the user can view the packet capture result in real time, and then locate the abnormal node.

3 Experiment Analysis

In order to verify the feasibility of the research on the real-time monitoring method of communication network blocking, experiments were conducted. The 50 sets of data in a certain period of time are selected as experimental objects, and the experimental data of the normal state is obtained according to the historical records of previous years, and standardized processing is performed. First of all, set up the experimental environment. Because of the limitations of the lab equipment, it is necessary to use the Mininet to establish a communication network topology in the virtual machine and connect to the remote controller to realize the construction of the communication network environment, and then establish a connection with the remote database for data access. The real-time monitoring error and communication delay time of the communication network are taken as experimental targets. The traditional monitoring method is compared with the real-time traffic monitoring of the communication network. The result is used as the basis for judging the feasibility of the method. The reasons for the communication delay include monitoring the substation measurement and processing delay, data transmission delay, information propagation delay, delay generated by the digital transmission equipment, and delay of the pre-processing of the primary station and the data uploading server. Through the experiment, the traditional monitoring method and the designed real-time monitoring method are compared, and the comparison results are shown in Fig. 3.

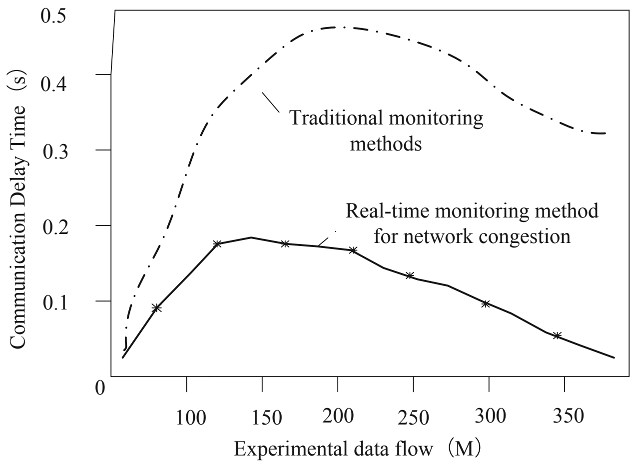

Fig. 3. Communication delay time comparison results

The delay time of the communication network blocking method for real-time monitoring directly reflects the real-time performance of the method. It can be seen from the comparison of the experimental results in the figure that the communication delay time of the traditional monitoring method will be extended with the increase of the data amount. Although there is a clear trend of shortening the delay when the quantity reaches 280M, the delay time is always higher than 0.3 s. In contrast, the communication network blocking real-time monitoring method uses the real-time data acquisition and calculation method, so the experimental results show an ideal delay result, the delay time is always controlled within 0.2 s, and when the data flow After more than 250M, it shows a clear downward trend, which fully reflects the real-time nature of the monitoring method. In addition, the accuracy of the monitoring method monitoring results is also very important. The results of the alarm information obtained by the real-time monitoring method designed by the experiment can be accurately located to the position where the blockage occurs and the blocking value is calculated, which is convenient for timely blocking accidents. Processing, it can be seen that the method has low monitoring error and high accuracy.

In order to further verify the monitoring accuracy of this method, the traditional method and this method are used to verify the monitoring accuracy. The results are shown in Table 1.

Table 1. Monitoring accuracy of communication network data

Monitoring the time/min	Monitoring accuracy of communication network data/%	
	The traditional method	The method of this paper
10	67	89
20	69	96
30	71	93
40	70	92
50	65	95
Mean value	68.4	93

According to Table 1, the accuracy of data monitoring is different in the monitoring time. When the monitoring time is 10 min, the accuracy rate of communication network data monitoring of traditional method is 67%, and that of this method is 89%. When the monitoring time is 50 min, the accuracy rate of communication network data monitoring of traditional method is 65%, and that of this method is 95%. The average accuracy rate of traditional method is 68.4%, while that of this method is 68.4%. The accuracy of communication network data monitoring based on this method is obviously higher.

4 Conclusion

In summary, in the cloud computing environment, in order to ensure the stability of the computer communication network operation, it is necessary to ensure that the network traffic is always in a normal state. Through the real-time monitoring method of a communication network, the real-time running status of the entire communication network is grasped, and the blocking problem of the network is detected in time to facilitate the daily management and maintenance of the network staff. In the design process of the monitoring method, it is found that although the method has high monitoring accuracy, the long-term stable operation of the method has yet to be studied, and a high-performance monitoring method is developed in the future to support real-time monitoring of the communication network.

References

1. Zhao, A.: Research on simulation of blind signal real-time separation in network communication. Comput. Simul. **26**(2), 31–35 (2018)
2. Anonymous: Real-time generation simulation of candidate communication network information in emergency. Comput. Simul. **34**(12), 165–168 (2017)
3. Wang, D., Tian, A.: Real-time monitoring simulation of safety signals in high-speed railway network. Comput. Simul. **38**(4), 25–28 (2018)
4. Lu, N., Lu, K.: Cooperative scheduling method for control and communication in real-time Ethernet system. Comput. Eng. Appl. **53**(7), 15–20 (2017)
5. Liu, H.: Research on control method of blocking jamming in HF communication system. Digit. Technol. Appl. **37**(1), 29–30 (2019)
6. Jiao, Y., Tian, F., Shi, S., Liu, J., Liu, H.: Multipath routing based congestion control strategy for LEO satellite networks. Electron. Des. Eng. **26**(18), 119–123+128 (2018)
7. Liu, S., Lu, M., Li, H., et al.: Prediction of gene expression patterns with generalized linear regression model. Front. Genet. **10**, 120 (2019)
8. Lv, J.: Design and implementation of equalization controller in network communication system. J. Henan Inst. Sci. Technol. (Nat. Sci. Ed.) **47**(2), 60–64 (2019)
9. Huang, Q., et al.: Coordinating SNOP control and AC-line switching for congestion management of hybrid urban grid. Adv. Technol. Electr. Eng. Energy **38**(2), 55–62 (2019)
10. Liu, P., Cai, Y., Lu, G.: Space environment data transfer system based on BBR congestion control algorithm. Chin. J. Space Sci. **39**(1), 117–123 (2019)
11. Hu, L., Yang, J., He, Y., et al.: Urban traffic congestion radiation model and damage caused to service capacity of road network. China J. Highw. Transport **32**(3), 149–158 (2019)
12. Shuai, L., Gelan, Y.: Advanced Hybrid Information Processing, pp. 1–594. Springer, New York (2019)https://doi.org/10.1007/978-3-030-19086-6
13. Zhang, J.: Analysis of TCP packet dropping behaviors in data center. Intell. Comput. Appl. **8**(6), 172–173+176 (2018)
14. Liu, G., Liu, S., Khan, M., et al.: Object tracking in vary lighting conditions for fog based intelligent surveillance of public spaces. IEEE Access **6**, 29283–29296 (2018)