Research on Service Controlling Algorithm of Electric Power Communication Network based on QoS Traffic Recognition and Routing Optimization

Ningzhe Xing
School of Electronic and Information Engineering, Beijing Jiaotong University, Beijing, China
Information & Communication Branch, State Grid Jibei Electric Power Company Limited, Beijing, China
Email: xingningzhe@163.com

Yutong Ji
Information & Communication Branch, State Grid Jibei Electric Power Company Limited, Beijing, China
Email: yutong.ji@live.cn

Abstract—With rapid progress in power communication networking, the present power communication network has become an integrated transmission network that supports various services (e.g., control data, service data, voices, and images). Compared with traditional network services, real-time services in the present power communication network have stricter requirements on delays, delay jitters, and packet losses. QoS techniques can guarantee the network service qualities overall, provide different QoS for different power communication network services, and improve network resource utilization, as well as satisfying the requirements of key services (e.g., relay protection and power dispatching). After analyzing the problems and challenges facing the QoS routing of the present power communication network, a QoS routing module is proposed under the service classification system. The most prominent feature of the proposed model is its ability to match different network services with suitable QoS. Our model consists of the service recognition and classification module, the routing module, and the client service analysis module. In the system tests, the proposed method for classifying power communication network services is used to implement the routing model under the service classification system. At the client end, the service types of the data are statistically analyzed, and service type maps are plotted. The statistical analysis shows that the proposed model has excellent QoS performance.

Index Terms—QoS; Electric Power Communication Network; Service Identification

I. INTRODUCTION

With the deepening of the reform of electricity market and the improvement of the informationization degree of electric power industry, the amount and type of electric power service increase rapidly and the demand for communication indicators tends to be diversified, in order to ensure the quality of service (QoS), it no longer takes "reachable" and "the shortest path" as the measurable indicators of route selection, but wishes to consider the specific communication needs of electric power service, the dynamic characteristics of network and other requirements.[1]

Currently, the electric power system is being transferred from the pure voice service provided for the production scheduling and government affairs command of electric power communication network position in traditional view to be non-voice and data business service provided for the whole process of electric power market, power production and varied business to form an integrated electric power communication private network by combining with all kinds of safe, real-time and high-speed flexible services.

The services of electric power communication could be divided into key operation service and business management service those two categories. Key operation business refers to remote signal, data acquisition, monitoring control system, energy management system, relay protection signal, dispatching telephone, etc; business management service includes administrative telephone, conference television, video conferencing, information data management, etc. There are different requirements for different electric power communication services. Key operation service doesn't have large volume of information, but it has high requirement of real-time, accuracy and reliability for communication; business management service is characterized by various services, frequent changes and large communication flows. [2]

Distributed control systems, called DCS for short, refers to the automatic control system controlling multiple control loops in production process respectively, meanwhile it is capable for centralized data getting, centralized management and centralized control. DCS has the functions of data acquisition, direct digital control, human-computer interaction and monitoring and management, etc. Developed on the basis of computer
supervisory control system, direct digital control system and multilevel computer control system, DCS is a relatively complete control and management system in production process. In DCS, the control function is distributed as far as possible and the management function is relatively centralized. Such kind of decentralized control method could improve the reliability of control and is incapable to make the whole system out of control because of computer failures. When failures happen to the management level, the level of process control still has individual control ability, and the overall situation won’t be affected when failures happen to individual control loop. Compared with multilevel computer control system, DCS is more flexible on structure, more reasonable on layout and lower on cost.

QoS, quality of service, a kind of security mechanism of network, is a kind of technology to solve network delay and congestion and other problems. In normal condition, if network is only used in specific application system without time limit, it doesn’t need QoS, such as Web application, E-mail setting, etc. But it is very necessary for key application and multimedia application. When the network is overloaded and congested, QoS could ensure important service won’t be delayed or abandoned, meanwhile ensure the network to run efficiently.

In recent years, some scholars have done a lot of research work. In [3], a hierarchical structure was proposed, in which the QoS model supports the selection of combined services, including the QoS model of the basic service that can guarantee basic QoS, the associated QoS model for basic services that reflects the properties of the combined services, and the QoS model for comprehensively evaluating the quality of the combined services. Based on this, a QoS-driven algorithm for selecting combined services was proposed. In [4], the computation service scheduling problem of the trusted QoS was examined, the weaknesses of the traditional dispatching algorithms were analyzed, and a trust-based algorithm for scheduling grid services was proposed. This algorithm can guarantee QoS while satisfying the requirements of the trusted QoS. Comprehensive analysis and simulations were performed to evaluate the algorithm. In [5], a Web Services Discovery Model that supports QoS constraints (WSDM- Q) was proposed. The model defines a group of classification tModels to describe QoS and credibility of the web services, introduces the concept of QoS quantification, uses the QoS negotiation and feedback mechanisms, and supports the publication of services carrying QoS descriptive information and the QoS constraints-based service discovery. The negotiation mechanism allows service providers to exercise admission control over service requests according to running states. Additionally, the feedback mechanism allows the service registration center to dynamically evaluate and adjust the credibility of the provided QoS. In [6], a mathematical model was established involving network structure, link quality, intra-node and inter-node competition, and data performance analysis. The basic theories on the application of the wireless sensor network in the high-performance communication of the smart distribution network were investigated. This provided several insights into methods of improving wireless sensor network performance, and is theoretically and practically beneficial to the high-performance communication of the smart distribution network.

Currently, the QoS of electric power communication mainly realizes the centralized QoS indicators, namely guarantees each communication service with the whole QoS of transport network. As there are varied services in electric power communication network, especially the services are much different from each other, such as relay protection and some other important services which requires extremely strict QoS. But for ordinary services transferred on communication network, the requirement for QoS should be very low. In such a condition, if only one kind of QoS is used to provide communication service with guarantee, not only the QoS of each communication service can’t be guaranteed, but also the services with low requirement for QoS service are provided with high QoS, resulting in enormous waste. Meanwhile, the QoS security of the system can’t be guaranteed, because once the current QoS system being out of service, there’s no QoS for all services. In order to make electric power communication network run efficiently and reliably, it must study on the QoS control method in electric power communication network.

Based on the existing methods for controlling QoS services of the power communication network, an algorithm for controlling power communication network services based on QoS service recognition and routing optimization is proposed. The control process of the proposed control algorithm majorly involves the QoS service recognition module and the QoS routing optimization module. The QoS service recognition module includes preprocessing, port matching-based coarse-granularity recognition, traffic feature analysis, moderate-granularity recognition based on traffic feature and port matching, and DPI-based fine-granularity recognition. The received traffic is first processed at the control nodes, and then labeled at the service recognition module. Each power communication network service has a corresponding DSCP value. Generally, the services with high values of ri have higher requirements on path parameters, and are thus provided with more priority services. After service recognition, the QoS service control will perform routing optimization. After entering the routing stage, instead of choosing addresses based on destinations only, the destination addresses and the DSCP values will be combined for path selection. This method also reflects the features of QoS service control.

II. CLASSIFICATION OF ELECTRIC POWER COMMUNICATION SERVICE

A. Classification Criterion of Electric Power Communication Service

Aiming at the physical structure and traffic needs of electric power communication network, reasonable route should be selected to meet the QoS need of traffic, meanwhile improve the service quality of electric power
communication network and balance the network load. In electric power communication network, time delay, bandwidth and packet loss rate are three important parameters, for which different electric power traffics have different requirements. According to the different requirements for communication indicator, the current traffics of electric power system are classified into five categories, specifically including:

1) high reliable broadband real-time traffic;
2) high reliable narrowband real-time traffic
3) reliable broadband real-time traffic
4) reliable narrowband real-time traffic
5) low reliable narrowband non-real-time traffic

The key operation traffic of safety category 1 is the core traffic of power generation, it plays an important role in the reliable operation of electric power system. As a necessary link of electric power system, the key operation traffic of safety category 2 is mainly responsible for all kinds of dispatching and intelligent management; the key operation traffic of safety category 3 is responsible for transformer substation video monitoring and distribution automation performance monitoring. Typical key operation traffics of safety category 1 includes stability control, circuit relay protection, etc. Key operation traffics of safety category 2 mainly includes dispatching telephone, dispatching automation data network, expert meeting dispatching system traffic, intelligent communication management system, etc. Key operation traffics of safety category 3 mainly includes condition monitoring of power transmission and distribution, transformer substation video monitoring, distribution automation performance monitoring, position monitoring system of thunder and lightning, etc.

The broad category of business management traffic could be classified into safety category 4 and safety category 5 from the real-time angle, in which the business of safety category 4 is the company management business, assisting in stability and reliability of Marketing traffics of electric power system; the safety category 5 is the enterprise information and management traffic, taking charge of the ERP traffic of power enterprises. Typical traffics of safety category 4 includes Electric power market trading operation, Electricity information acquisition, power quality management system, marketing business management system, hotline and breakdown rescue management system, customer contact system, customer relation management system, etc; the typical traffics of safety category 5 include data center, electric power system ERP, video conference system, administrative telephone traffic, etc.

**B. Importance and DSCP Value Distribution of Electric Power Communication Network Traffic**

The traffic importance indicator $r_i$ is used to represent the (risk degree of some traffic caused to the safe and reliable operation of electric power communication network), which refers to the impact degree of the safe and stable operation of electric power communication network when interruptions and imperfections happens. $r_i$ is in direct proportion to the network risk impact. Considering the functions of electric power system traffics are diversified with different requirements for transmission channel, when $r_i$ value is being extracted, the transmission characteristic requirement of traffic channel and the security requirement of different traffics are combined with to evaluate the influence of traffic to the operation risk of electric power communication network. The $r_i$ values of typical electric power communication network traffics are shown in Table 1.

According to the characteristics of DSCP label value in IP data package, there are totally 6 places of distributive DSCP, from 0 to 63, the corresponding binary coding is from 000000 to 111111. The first place is considered as the brand category of traffic, 0 as key operation traffic, 0 as business management traffic; the second and the third places are used to distinguish the subcategories of each broad category, the first three places are combined to distinguish each different subcategory, 111 refers to safety category 1, 110 refers to safety category 2, 101 refers to safety category 3, 011 refers to safety category 4, 010 refers to safety category 5. The last three places are used to indentify different $r_i$ traffics. According to 8 quantization levels, 0~0.124 is 000, 0.125~0.249 is 001, 0.250~0.374 is 010, 0.375~0.499 is 011, 0.5~0.624 is 100, 0.625~0.749 is 101, 0.75~0.874 is 110 and 0.875~0.999 is 111.

<table>
<thead>
<tr>
<th>Traffic name</th>
<th>Traffic ID</th>
<th>Traffic importance</th>
<th>DSCP value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Circuit relay protection</td>
<td>T11</td>
<td>0.97</td>
<td>111111</td>
</tr>
<tr>
<td>Stability control</td>
<td>T12</td>
<td>0.94</td>
<td>111111</td>
</tr>
<tr>
<td>Dispatcher telephone</td>
<td>T21</td>
<td>0.86</td>
<td>110110</td>
</tr>
<tr>
<td>Dispatching automation networks</td>
<td>T22</td>
<td>0.6</td>
<td>110110</td>
</tr>
<tr>
<td>Expert meeting dispatching system traffic</td>
<td>T23</td>
<td>0.08</td>
<td>110000</td>
</tr>
<tr>
<td>Intelligent communication management system</td>
<td>T24</td>
<td>0.06</td>
<td>110000</td>
</tr>
<tr>
<td>Power transmission condition monitoring</td>
<td>T31</td>
<td>0.3</td>
<td>101010</td>
</tr>
<tr>
<td>Transformer substation video monitoring</td>
<td>T32</td>
<td>0.29</td>
<td>101010</td>
</tr>
<tr>
<td>Distribution automation performance monitoring</td>
<td>T33</td>
<td>0.2</td>
<td>101001</td>
</tr>
<tr>
<td>Lightning location monitoring system</td>
<td>T34</td>
<td>0.12</td>
<td>101000</td>
</tr>
<tr>
<td>Electric power market trading operation</td>
<td>T41</td>
<td>0.6</td>
<td>011100</td>
</tr>
<tr>
<td>Electricity information acquisition</td>
<td>T42</td>
<td>0.21</td>
<td>011001</td>
</tr>
<tr>
<td>Electric power quality management system</td>
<td>T43</td>
<td>0.11</td>
<td>011000</td>
</tr>
<tr>
<td>Marketing management system</td>
<td>T44</td>
<td>0.1</td>
<td>011000</td>
</tr>
<tr>
<td>Hotline and breakdown rescue management system</td>
<td>T45</td>
<td>0.06</td>
<td>011000</td>
</tr>
<tr>
<td>Customer contact system</td>
<td>T46</td>
<td>0.06</td>
<td>011000</td>
</tr>
<tr>
<td>Customer relationship management system</td>
<td>T47</td>
<td>0.06</td>
<td>011000</td>
</tr>
<tr>
<td>Data center</td>
<td>T51</td>
<td>0.56</td>
<td>010100</td>
</tr>
<tr>
<td>Electric power system ERP</td>
<td>T52</td>
<td>0.5</td>
<td>010100</td>
</tr>
<tr>
<td>Video-conference system</td>
<td>T53</td>
<td>0.06</td>
<td>010000</td>
</tr>
<tr>
<td>Administrative telephone traffic</td>
<td>T54</td>
<td>0.06</td>
<td>010000</td>
</tr>
</tbody>
</table>
According to the characteristics and requirement of power generation and management, detailed DSCP values could be distributed to all kinds of traffic in electric power communication network based on the importance of traffic and the effectiveness of route, as it shown in table 1.

III. QoS TRAFFIC CONTROL PROCESS OF ELECTRIC POWER COMMUNICATION NETWORK

The process of conducting QoS traffic control in electric power communication network includes the identification QoS traffic module and QoS routing optimization module.

The QoS traffic identification module includes pretreatment, coarse-grained identification based on port matching, analysis of flow characteristics, medium-grained identification based on flow characteristics and port matching and fine-grained identification based on DPI. The received business is pretreated firstly at the control node. In the pretreatment process it mainly grasps the original business data packet and divides business flow according to quintuple which refers to source address, destination address, source port, destination port, transport protocol and the termination of business flow that is determined by timeouts and obvious end mark of business flow. The pretreated business flow will be processed with port matching and the main purpose of port matching method is to segregate the business flow, including regular business and P2P application with fixed port, which is known and registered in the administration of Internet number distribution. As some P2P applications are disguised to be well-known ports in order to pass through NAT and avoid the limitation of firewall. Disguised ports are identified according to the list of known disguised ports in port matching method and the flow of those ports are not disposed temporarily. Load characteristics of protocol and application and the protocol port in use are modifiable. However, it is very difficult to modify the characteristics of protocol and business flow, not only the known power communication network traffic but also the unknown or encrypted similar electric power communication network traffic could be identified according to the behavior characteristics of flow and the statistical characteristic of flow. Flow characteristic analysis method is suitable for the coarse-grained classification of traffic and is capable to rapidly classify the flow of electric power communication network into several security classes. Indentifying modules by flow characteristic method, it could distinguish the electric power system P2P traffic of disguised ports from internet traffics, eliminate the disguise of P2P stream, and then adopt port mapping to identify regular traffics. For those only demanding for coarse-grained identification to P2P and other traffics, the result could be directly output to implement the flow caching and control of traffics and the QoS routing. But for the occasional demanding for sophisticated category of all traffics, the traffics could be sent to DPI module for further distinguishing of each application and reach accurate sophisticated classification. Through composite network flow classification, we could realize real-time, accurate, fast and flexible QoS traffic identification of electric power communication network.

Some new traffics of electric power communication network (such as P2P application) adopts disguise or dynamic port and the method of encrypted application layer to avoid the identification and classification of flow, which makes the method that only uses port mapping or net load analysis be limited. Adopted with the traffic classification method based on flow statistical property and established on the basis of flow characteristic and flow behavior analysis, this invention could solve the problem. Considering the load characteristic of protocols and the protocol port in use are modifiable, whereas the characteristic of protocol and traffic flow are very difficult to be modified. Not only the known network traffics but also the unknown traffics of electric power communication network are identifiable according to the statistical characteristic of flow.

Main identification methods based on flow characteristics include identifying specific P2P traffic by using (TCP, UDP) pair; judging whether it is P2P application by means of data package statistical information, such as the distribution diagram of length, quantity, etc; distinguishing traffic through the behavior pattern of host group; identifying some P2P traffic through (IP, port) pairs; and fine identifying unknown traffic and encrypted traffic based on unsupervised machine learning flow classification and identification method.

Considering that TCP and UDP protocols are simultaneously used by 70% of P2P protocols, the identification of (TCP, UDP) pair usually adopts with UDP for ordinary flow control, request and its response adopts TCP for actual data transmission. Regular applications using two protocols simultaneously mainly include P2P and several special applications, such as DNS, NETBIOS, IRC, game and streaming media. These special applications are specific ports which could be identified. Therefore, only if two protocols are used simultaneously and (IP, port) pair is not in the static port mapping table, it could be considered as P2P flow and the matching of bit string characteristic method and others could be adopted to identify specific P2P applications.

This condition is considered in the identification method based on the distribution diagram of the length, quantity and other statistical information of data packet. Using the information in communication network is much different from the system information. Additionally, the control and routing package of P2P is much different from other traffics, such as DDoS attack package, and the control or routing information of regular traffics on the length of data package, the source and destination address distribution of data package, the arrival rate of data package, the quantity of data package and other aspects. The atlas of each traffic could be formed by measurement, analysis and curve fitting, even the clear identifiable distribution diagram of flow characteristics could be formed through the statistical flow characteristics of
The traffic identification method based on host group behavior pattern classifies traffic according to packet correlation and other rules, and forms host group to distinguish traditional C/S application and P2P application by analyzing the patterns of the diameter of host group and the association diagram of the number of stream with source port.

(IP, port) pair is used to conduct specific P2P traffic identification method and record the IP connection to some (IP, port), the port numer, the size of datagram and the transmission flow, based which traffic identification is conducted. Since pure distributed or hybrid P2P network allows user not be allocated with random port number and port numbers of the hosts that conducting peer-to-peer communication are always different from each other, so the number of host IP is a little different from port number. If the number of connected IP address is approximately equal to the number of port, namely different numbers of IP are corresponding to different numbers of port, it is regarded as P2P flow. To the contrary, it would not be treated as P2P flow if the number of connected IP differs by more than ten from the number of port.

The flow analysis and identification method based on unsupervised machine learning achieves the classification of electric power communication network traffic with the help of a machine learning method through collecting stream statistical characteristic parameters including average packet length, packet arrival interval and others of the first several packets in traffic flow. This method could realize good classification accuracy and speed up identification unknown traffic and encrypted traffic.

Selecting suitable strategies and the corresponding characteristics from flow statistics database to indentify and classify flow could screen out P2P flow, regular traffic and irregular traffic. Since the regular traffic may be disguised by P2P and other traffics, it could be identified and classified with its fixed port when the traffic disguising flow is separated. The identification method based on stream characteristics could realize the identification and classification of known/unknown kind of traffic and realize the classification of traffic only according to the head information of transport layer in case it is unavailable to obtain application layer data. When fine-grained classification is required, it could be realized by other identification methods, such as deep packet inspection.

Deep packet inspection (DPI) could find specific applications, such as P2P traffic, through inspecting the application layer protocol of data package. DPI uses the net load characteristic information stored in the network load character string characteristic database and those network load characteristic matching with data package could be considered as the data package of such application. However, there are limitations for DPI that it has hysteresis quality to the inspection of emerging network applications and cannot inspect encrypted P2P application and its algorithm performance is affected by the complexity of net load characteristic. In view of the limitations of DPI, this invention is adopted with compound flow classification and identification method, also flow characteristic analysis method could be used to make unknown application and encrypted application map to the relevant application categories. It can be treated as complementation of DPI. When electric power network traffics has sophisticated category, DPI accurate recognition and classification method could be adopted together to automatically sort out unknown traffics, as well draw and indentify the corresponding character string, in order to supplement DPI database, realize the closed-loop DPI fine identification and classification and reduce the hysteresis quality of DPI identification, as it shown in figure 1. For encrypted flow, it is adopted with the representing method with different characteristics, paying attention to the flow characteristic at signaling establishment stage and the net load characteristic after being encrypted, and could be solved by the compound method that combing the flow characteristics method in traffic identification module with DPI.

According to the QoS traffic classification module design of electric power communication network, the broad category of traffic is classified by flow characteristics identification module before DPI classification, the know port traffic is identified by port matching module, unclassified traffic flows and traffic categories are dramatically reduced, and DPI classification only need to be done in this category, it only need to check the subsets respectively in DPI characteristic database, in order to reduce the workload of DPI. Additionally, stream is taken as the unit for processing, generally the network load characteristics could be matched by taking the first several packets or first n bytes of the stream. Thus the complexity of DPI calculation is reduced and the real-time application could be realized in high-speed routing. Currently it is required by the application environment of electric power communication network that test system should support the processing speed of line speed and big rule sets with fewer expenses. Therefore corresponding model matching method is needed. The accurate hit of dedicated chip TCAM is used to search the hardware method of fast parallel processing that speed has nothing to do with the size of meter and the method using multinuclear CPU for processing. Starting from the scale of cost speed mode, the complexity of realization and other key points, DPI matching scheme is combined with software matching algorithm and hardware support.

![Figure 1. Sketch map of closed-loop DPI identification](image-url)
After traffic identification module is being tabbed, each category of electric power communication network traffic corresponds to a DSCP value. Generally speaking, traffics with higher $r_i$ require more path resource. Therefore they should be provided with more priority services. The relationship between DSCP value and $r_i$ value is that the traffics with bigger numbers on the last three places of DSCP value would have bigger $r_i$ value, but it may be not like this on the contrary, two traffics with approximate $r_i$ values may have the same numbers on the last three fields of their DSCP values, for details please refer to figure 2. For the business with the same numbers on the last three fields of DSCP value, please refer to the first three fields of DSCP value, bigger values indicate higher security category and should be given higher priority.

Traffic of safety category 1, safety category 2 and safety category 3 with the traffic importance $r_i$ value of above 0.5 belong to high real-time traffics, should be given higher priority of bandwidth and transmission in routing distribution, traffics of safety category 4 and safety category 5 with the $r_i$ value of below 0.1 belongs to as-far-as-possible non-real-time traffics to the best of capability, should be given lower transmission priority in routing distribution, beyond those, other traffics belong to general real-time traffics could be done with QoS resource distribution according to the DSCP value.

After traffic identification, QoS traffic control will conduct QoS route optimization control, as it shown in figure 2. The specific method is that it is no longer the address selection solely according to destination address when entering the route selecting stage, but the path selection combining destination address and DSCP value those two parameters. This method also represents the characteristics of QoS traffic control. For example, for a number of traffic to the same destination address, where the DSCP value of a certain traffic flow is 0x110110, it indicates that this traffic is a high real-time traffic flow and it has high requirement for delay and bandwidth, so the path with low latency feature is distributed for retransmission; but for some other point-to-point, namely P2P traffics, with large consumption of bandwidth reaching the same destination address, the as-far-as-possible path could be selected for retransmission. The performance of those low latency or as-far-as-possible paths could be statically set in advance.

Traffic of safety category 1, safety category 2 and safety category 3 with the traffic importance $r_i$ value of above 0.5 belong to high real-time traffics, should be given higher priority of bandwidth and transmission in route distribution, traffics of safety category 4 and safety category 5 with the $r_i$ value of below 0.1 belongs to as-far-as-possible non-real-time traffics to the best of capability, should be given lower transmission priority in route distribution, beyond those, other traffics belong to general real-time traffics could be done with QoS resource distribution according the DSCP value.

In order to succeed in providing different traffics with different retransmission paths, it need to maintain the multiple available paths to the same destination address in routing list and could be realized by setting the path parameters of each selectable path. In the process of searching, destination address is considered as the primary index and the DSCP value is considered as the secondary index in order to find the corresponding next-hop path of retransmission for different traffics to the same destination address. Thus it could achieve the route distribution according to different requirement of electric power traffic based on the routing selection of destination, thereby our method improves the traffic transmission quality of electric power communication network and finally achieves the optimization control of QoS route.

![Figure 2. The QoS traffic control system of electric communication network](image)

![Figure 3. The QoS traffic control system of electric communication network](image)

IV. TEST OF THE QoS TRAFFIC CONTROL SYSTEM OF ELECTRIC COMMUNICATION NETWORK

The traditional routing list takes destination address as the index, such kind of routing list is insufficient to support the route based on traffic classification, namely
based on the type of data traffic to decide the route. In order to realize the route model in the traffic classification system designed in this paper, we need to design a kind of new routing list which is a kind of secondary index routing list containing DSCP values. The list includes the definition of list structure, data structure and operating function design.

![Figure 4. The real-time monitoring result of the data volumes of various traffics of router A](image1)

The traditional routing list takes destination address as the main index and there are three parts of contents in the list entry: destination address, subnet mask and next hop; while for the traffic classification system in this paper, the tradition routing list can’t meet the requirement of business, so we design the secondary index routing list based on DSCP values. Figure 3 shows that the primary index of routing list is a set of destination address, in which every element of destination address points to a secondary routing list with DSCP values as the index. When a data package arrives at a Router, the Router will firstly search the primary index for the list entry according to the destination address, if that is successful, it will search the list for that whether there’s a corresponding list entry according to DCSP value and finally determine the next-hop address: if the list entry exits, it will transmit the data package directly; if not, it will implement the corresponding routing algorithm and add the generated list entry into the routing list to make it convenient for the later use.

![Figure 5. The real-time monitoring result of the data volumes of various traffics of router B](image2)

The secondary index routing list is especially suitable for the condition that many network applications have the same source address and destination address. In such a condition, there may be multiple feasible paths between the source address and the destination address, which are different in QoS performance. With the help of the routing list containing DSCP values, we can distribute different paths to traffics with different QoS demands. For example, we distribute a path with high performance and good QoS guarantees to traffics with high demand of delay and sensitivity of delay variation; while distribute a path providing as-far-as-possible traffics to simple text transfer traffics. This kind of secondary index routing list can monitor and control the current status of the whole network, improve the utilization ratio of network resource, reduce congestions and provide higher-level QoS guarantees compared with traditional routing list.

Adopting the routing strategy based on traffic classification proposed in this paper, a simulation experiment based on practical condition is conducted in the electric power communication system in northern Hebei Province, in the process of which we simulate various network traffic flows: real-time video conference, relay protection, automatic dispatch, general network traffics, and some non real-time data traffics. In the following figure of traffic classification are shown the
data types transferred on each path, in which Type 1 refers to the real-time traffic of electric system; Type 2 refers to the video conference traffic; Type 3 refers to the automatic dispatch traffic; Type 4 refers to the non real-time data traffic, such as Email, FTP and other traffic flows; Others refers to network traffics in common use, such as web browser, etc. Figure 4 and Figure 5 respectively shows the real-time data flow of various traffics monitored by two Routers in the system, for traffics with high priority, optimized paths are selected for data forwarding to ensure the quality of traffic of the network; for the data of non real-time traffics, such as mail traffic, FTP transmission, etc, which has low real-time demand for the network, general paths with comparatively long delay are selected to save the bandwidth resource of the whole network and reasonable optimize the configuration of network resources.

V. CONCLUSION

In conclusion, this paper proposes the QoS route model in the traffic classification system, elaborately states the important technical components needed to realize this model, and verifies the feasibility and superiority of the scheme in the way of simulation experiment. Additionally, no matter the research result or the design thought and idea going through the stating process of this paper are both equipped with universality and extendibility, which could be applied in more complex systems which need to consider more QoS parameters and involve more classes of traffics.

ACKNOWLEDGEMENT

This paper is funded by Science and technology project of State Grid Corporation of China (8EE000M14001).

REFERENCES