A Flow Label Based QoS Scheme for End-to-End Mobile Services

Tao Zheng, Lan Wang, Daqing Gu
Orange Labs Beijing
France Telecom Group
Beijing, China
e-mail: {tao.zheng; lan.wang; daqing.gu}@orange.com

***Abstract* - As a network evolution goal, IPv6 is deployed in mobile network, including access network, core network and mobile carrier IP network. IPv6 introduction in mobile network will impact on Quality of Service (QoS) of mobile services. In this paper, a flow label based QoS scheme is proposed to improve QoS in mobile network. This scheme utilizes the flow label in IPv6 packet header to indentify the services and flows and make the mobile network and carrier IP network entities to perceive the existence of flows and control them. Particularly, the experiment results based this scheme indicate that it has the finest granularity of QoS and minimizes the affected flows with the help of flow label.**

Keywords-flow label; QoS; TFT; carrier IP network

I. Introduction

With the development of IP-based carrier network, Long Term Evolved (LTE) evolution and the rise of mobile Internet and multimedia services, QoS, especially Internet Protocol (IP) QoS is becoming more and more important in mobile networks.

The 3rd Generation Partnership Project (3GPP) TS 23.107 specification [1] defines the QoS architecture in Universal Mobile Telecommunications System (UMTS) as shown in Figure 1.

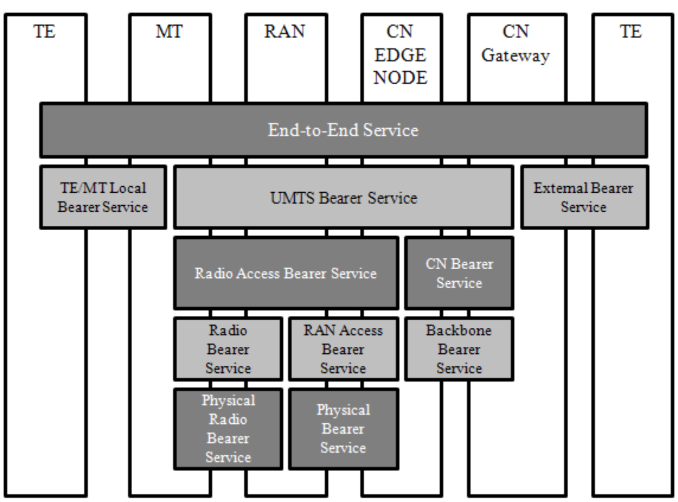

Figure 1. QoS architecture defined by 3GPP

The service on the higher layer consists of bearer services on the lower layer. Accordingly, the higher service's QoS is guaranteed by lower services' QoS. The End-to-End Service is finally mapped to Terminal Equipment/Mobile Terminal (TE/MT) Local Bearer Service, Physical Radio Bearer Service, Physical Bearer Service of Radio Access Network (RAN), Backbone Bearer Service, and External Bearer Service.

There are four different QoS classes defined by 3GPP: conversational class, streaming class, interactive class and background class. The main distinguishing factor between these QoS classes is how delay sensitive the traffic is: Conversational class is meant for traffic, which is very delay sensitive, while Background class is the most delay insensitive traffic class.

LTE utilizes a class-based QoS concept, which reduces complexity while still allowing enough differentiation of traffic handling and charging by operators. Bearers can be classified into two categories based on the nature of the QoS they provide: Minimum Guaranteed Bit Rate (GBR) bearers and Non-GBR bearers. The Figure 2 shows the QoS architecture in LTE [2].

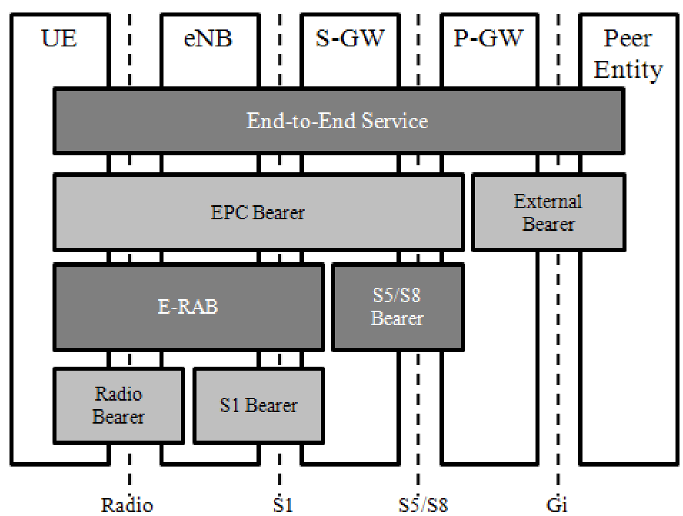

Figure 2. QoS architecture in LTE

The QoS architecture in LTE is similar to that in UMTS, as shown in Figure 1. The End-to-End Service is finally mapped to several bearers between mobile network entities.

In PS domain of UMTS and LTE, Traffic Flow Template (TFT) [3] mechanism is used to provide QoS guarantee. The TFTs contain packet filter information that allows the User

 ISBN: 978-1-61208-186-1

Equipment (UE) and Gateway GPRS Support Node/Public Data Network Gateway (GGSN/P-GW) to identify the packets belonging to a certain IP packet flow aggregate. This packet filter information is typically a 5-tuple that contains the source and destination IP addresses, source and destination ports as well as a protocol identifier (e.g., User Datagram Protocol (UDP) or Transmission Control Protocol (TCP)). Figure 3 describes the TFT architecture in LTE. The UE and the P-GW (for GPRS Tunneling Protocol (GTP)-based S5/S8) or Serving Gateway (S-GW) (for Proxy Mobile IP (PMIP)-based S5/S8) use packet filters to map IP traffic onto the different bearers. The TFTs are typically created when a new Evolved Packet System (EPS) bearer is established, and they are then modified during the lifetime of the EPS bearer.

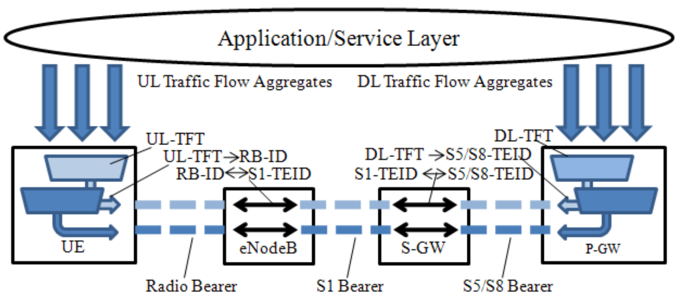

Figure 3. TFT reference network architecture

In the mobile IP carrier network, Differentiated Services (Diffsev) mechanisms or the Resource Reservation Protocol (RSVP) protocol can be used for QoS policy enforcement and resource reservation purposes at present. Multiple Protocol Label Switching Virtual Private Network/Traffic Engineering (MPLS VPN/TE) also can be used to provide QoS in IP carrier network. Such QoS policies and mechanisms design are usually engineered in advance.

From the above introduction, we can conclude that the current QoS mechanism used in mobile network is based on bearers (in access and core mobile networks) and Diffserv or RSVP techniques (in IP carrier network). With the deployment of LTE and the explosion of mobile Internet traffic, it's necessary to provide fine-grained control of traffic. Actually, each bearer includes some flows, such as http sessions from different websites, different applications in same Packet Data Protocol (PDP) context/Evolved Packet Core (EPC) bearer; there are more flows in same service class, e.g., active Voice over IP (VoIP) calls have the same QoS level in IP carrier network. So it's hard to perceive the existence of flows, and the controlled granularity can not be flows.

This paper is organized as follows. In Section 2, we introduce the current situation of IPv6 flow label. In Section 3, a flow label based QoS scheme is presented. In Section 4, an experiment based-on this scheme is implemented and experiment results are analyzed. Finally, Section 5 summarizes the conclusions.

II. IPv6 Flow Label and Applications

A sequence of packets sent from a particular source to a particular unicast, anycast, or multicast destination constitute a flow. In IPv4 network, the 5-tuple of the source and destination addresses, ports, and the transport protocol type is able to identify a flow.

IPv6 has introduced a field named flow label. The 20-bit flow label in the IPv6 header is used by a node to label packets of a flow. General rules for the flow label field have been documented in Request for Comments (RFC) 3697 [4]. But how to apply this field in real-world network is still an open issue since the research work on flow label is far from enough.

Some Internet Engineering Task Force (IETF) RFCs and drafts have been proposed to update flow label works.

In fact, some published proposals for use of the IPv6 flow label are incompatible with the original RFC 3697. Furthermore, very little practical use is made of the flow label, partly due to some uncertainties about the correct interpretation of the specification. In [5], the authors present some changes to the specification in order to clarify it, and to introduce some additional flexibility are discussed.

The draft "IPv6 flow label Specification" [6] is trying to update the RFC 3697. It specifies the IPv6 flow label field and the minimum requirements for IPv6 nodes labeling flows, IPv6 nodes forwarding labeled packets, and flow state establishment methods.

In [7], the author surveys various published proposals for using the flow label and shows that most of them are inconsistent with the standard. Methods to address this problem are briefly reviewed.

Various use cases have been proposed that infringe flow label rules. In [8], the authors describe how those restrictions apply when using the flow label for load balancing by equal cost multipath routing, and for link aggregation, particularly for IP-in-IPv6 tunneled traffic. In [9], the authors give an application that how the IPv6 flow label can be used in support of layer 3/4 load balancing for large server farms.

Flow identification is of vital importance for end-to-end QoS provision in mobile network. Many QoS management techniques can be achieved, e.g., Connection Admission Control (CAC), scheduling, etc, and some technologies have come out, e.g., MPLS, Scalable Core (SCORE), etc. with the ability to deal with per-flow and aggregated flow. At present, none of them is applied in mobile networks. In this paper, we proposed a QoS scheme utilized IPv6 flow label to provide a flow granularity QoS mechanism for end-to-end mobile services. Compared with other flow-based QoS techniques, our scheme is simpler and has minimal impacts on mobile networks.

III. Proposed Flow Label Based QoS Scheme

Previous QoS mechanisms in mobile network are based-on bearers, the packets contains in one same bearer share same QoS profile and be treated in the same way. According to the definition of a flow, there should be some flows in a same bearer. It's hard to handle each flow in such current QoS mechanisms. It's the same for the mobile IP carrier network.

We propose to employ IPv6 flow label to identify flows instead of bearers in mobile access, core and IP carrier networks.

A. Overview

In mobile network, the IP packets are transported in GTP Tunnel. Figure 4 shows the IP packet structure through GTP Tunnel.

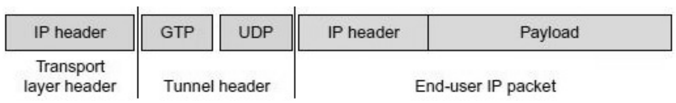

Figure 4. IP packet structure in GTP Tunnel

There are two IP headers, which correspond to the transport layer and the end-user IP packet respectively. That is, two IPv6 flow label fields can be handled by mobile network entities and IP carrier network entities respectively.

In our QoS scheme, the 20-bit IPv6 flow label is divided three parts from left to right: Access Point Name (APN) part, service part, and flow part. There parts are generated and stored by different entities. The flow label prefix definition can be adjusted by mobile operators according to their current situation.

The APN part (first several bits) of IPv6 flow label is defined and stored in Home Location Register/Home Subscriber Server (HLR/HSS) and each APN has one IPv6 flow label prefix. The lower APN part means higher QoS level.

The service part (middle several bits) of IPv6 flow label is provided by Application Function (AF), located in service platform, or GGSN/P-GW for the services without service platform, for example, Internet services. The lower service part means higher QoS level.

The flow part (rest bits) of IPv6 flow label is generated by terminal for different flows.

When the mobile terminal or mobile network launches a bearer, the APN part of flow label will be generated and sent from HLR/HSS to the terminal after the requested APN passes the authentication. When the terminal sends a service request to AF or GGSN/P-GW receives a service request to Internet, the service part of IPv6 flow label will be generated and sent to the terminal. At last, the terminal generated the flow part and forms the full flow label for each flow.

In mobile access and core network, Radio Network Controller (RNC), Service GPRS Supporting Node (SGSN)/S-GW and GGSN/P-GW entities process the packets according to the IPv6 flow label in the end-user packet header. The packets with lower IPv6 flow label prefix will have priority in processing. When the congestion happens, the packets with higher IPv6 flow label will be discarded at first and then the packets with same IPv6 flow label of discarded packets will be discarded. This mechanism guarantees that the service with high QoS level has priority and the impacted flows are minimal when congestion happens.

When the packets are sent the IP carrier network, the IPv6 flow label in end-user IP packet header will be copied to the transport layer header. The mobile IP carrier network will process the packets according to IPv6 flow label by the same way used in mobile network.

B. Entities Functions Related to Flow Label

- HLR/HSS: store the APN part of IPv6 flow label; and provide the APN part to the terminal after the requested APN passes the authentication.
- UE: generate the IPv6 flow label suffix for each flow; form the full IPv6 flow label with corresponding prefix provided by HLR; and be responsible for verifying the APN and service part of IPv6 flow label by TFT filters if necessary.
- AF: store the service part of IPv6 flow label; and provide the service part to the terminal after the service request is accepted by the service platform.
- RNC, SGSN/S-GW: process IPv6 flow label in end-user IP packet header; and copy flow label in end-user IP packet header to transport layer header and generate transport layer header.
- GGSN/P-GW: process IPv6 flow label in end-user IP packet header; copy flow label in end-user IP packet header to transport layer header and generate transport layer header; store the service part of IPv6 flow label for the services without service platform; provide the service part to the terminal when receiving a service request from terminal; and be responsible for verifying the APN and service part of IPv6 flow label by TFT filters if necessary.
- IP carrier router: process IPv6 flow label in transport layer header.

C. Process Flow of Flow Label Generation

The whole process flow related to IPv6 flow label generation is described in Figure 5, where only shows the UE-initiated services. First, UE initiates a bear establishment request to network entities. Then, according to the functions described in Section III B and the QoS profile of the service requested by UE, the network entities generate the corresponding parts of IPv6 flow label separately and provide them to the UE. Finally, the UE generates the flow part of flow label for each service flow and forms the full IPv6 flow label for communications.

D. Security Consideration

Because IPv6 flow label implies the QoS level, the security of flow label is vital important. The security problems come form two aspects: the flow label should be assigned according to the corresponding QoS level (e.g., QoS level of APN and service); and the flow label should be guaranteed not to be modified illegally during the transport.

 ISBN: 978-1-61208-186-1

In our proposed scheme, the APN part and service part of flow label are stored in HLR/HSS, GGSN/P-GW and AF. These entities belong to the mobile operators and can be trusted. Mobile terminals can get the APN and service parts of flow label and have the chance to modify them by itself, for example, give a small flow label to a service with lower QoS level. For avoiding the IPv6 flow label prefix to be modified illegally by mobile terminals, special TFT filters is added to UE and GGSN/P-GW. These filters are responsible for verifying whether the IPv6 flow label prefix is matched to the corresponding APN and service part, which had been provided to terminal. If the mismatch thing happens, the corresponding packet will be discarded and a wrong message will be sent to the terminal.

The consistency and integrity of flow label during the transport can be guaranteed by security mechanisms used in current mobile network and IP carrier network, such as VPN, firewalls, Access Control List (ACL), etc.

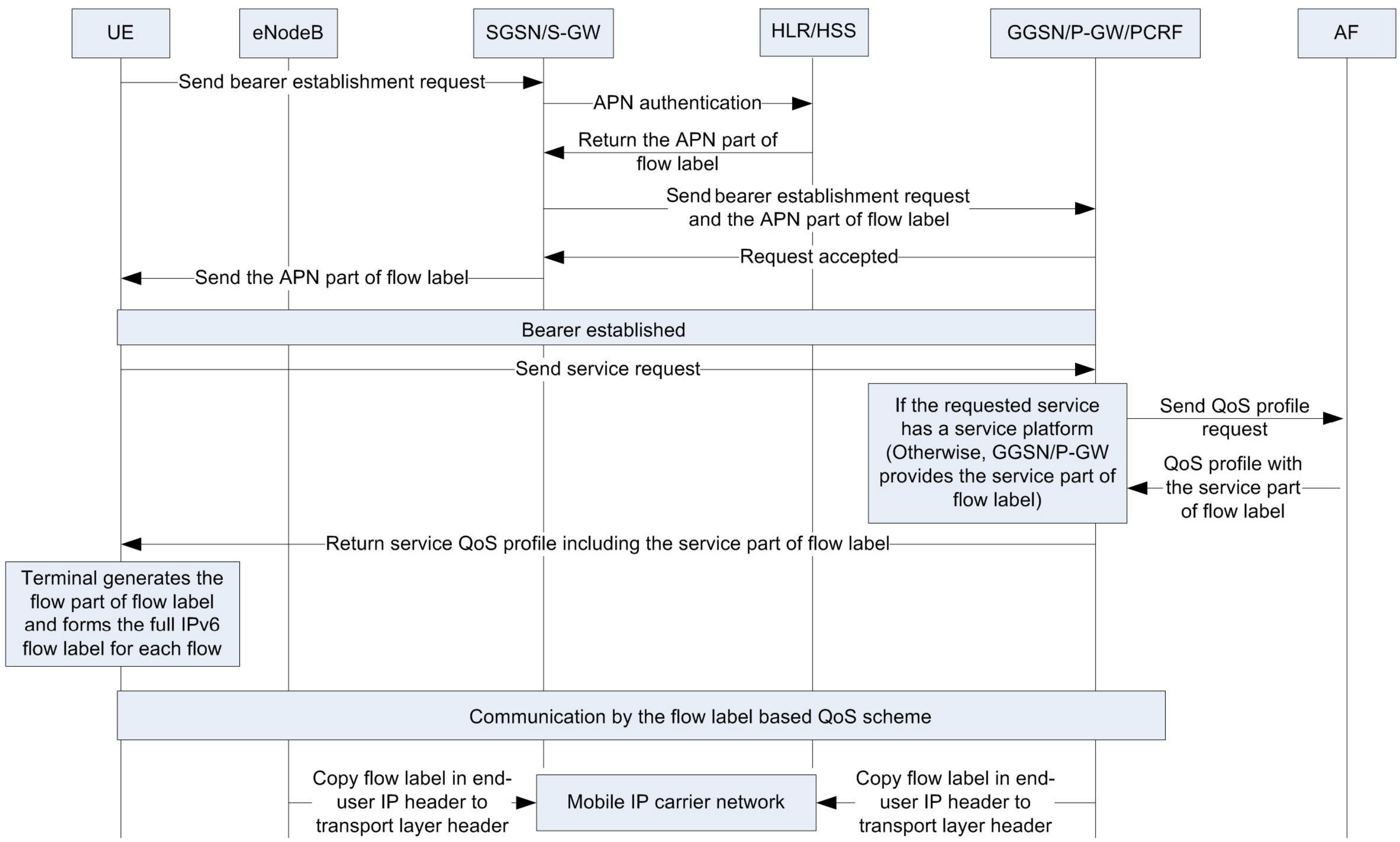

Figure 5. The process flow generating IPv6 flow label

IV. EXPERIMENT RESULT

In our experiment, the proposed flow label based scheme is evaluated by the simulation platform based-on OPNET software. According to the generation and QoS control methods described in section III, we programmed network entities functions on the simulation platform. The experiment we launched has two scenarios. One scenario tested different flows in a same PDP Context/EPC bearer transported in the mobile network, and another tested different flows with same QoS profile transported in the mobile IP carrier network.

The experiment platform includes mobile terminals, mobile network, mobile IP carrier network and external network. There are three mobile terminals and a simply mobile access and core network composed by NodeB, RNC, SGSN and GGSN. Four routers constitute the mobile IP carrier network. And the external network includes a switch, two File Transfer Protocol (FTP) servers and three VoIP clients (as the peer VoIP terminals). The topology of the experiment is described in Figure 6.

The services tested in this experiment platform are FTP downloading and VoIP, which have their own APN and QoS profiles. The QoS level of VoIP service is higher than that of FTP downloading. And three mobile terminals communicate with three peer VoIP clients respectively with same QoS level. For the FTP service, the QoS level of FTP server2 is higher than that of FTP server1.

The IPv6 flow label used in the experiment is defined as following. The first 2bits of IPv6 flow label belongs to APN part, and two of four combinations are assigned to APNs used in VoIP and FTP services. The next 2bits is allocated to service part, and VoIP service only occupies one combination and two

 ISBN: 978-1-61208-186-1

levels of FTP have two of combinations. The rest bits of flow label belong to the flows assigned by mobile terminals.

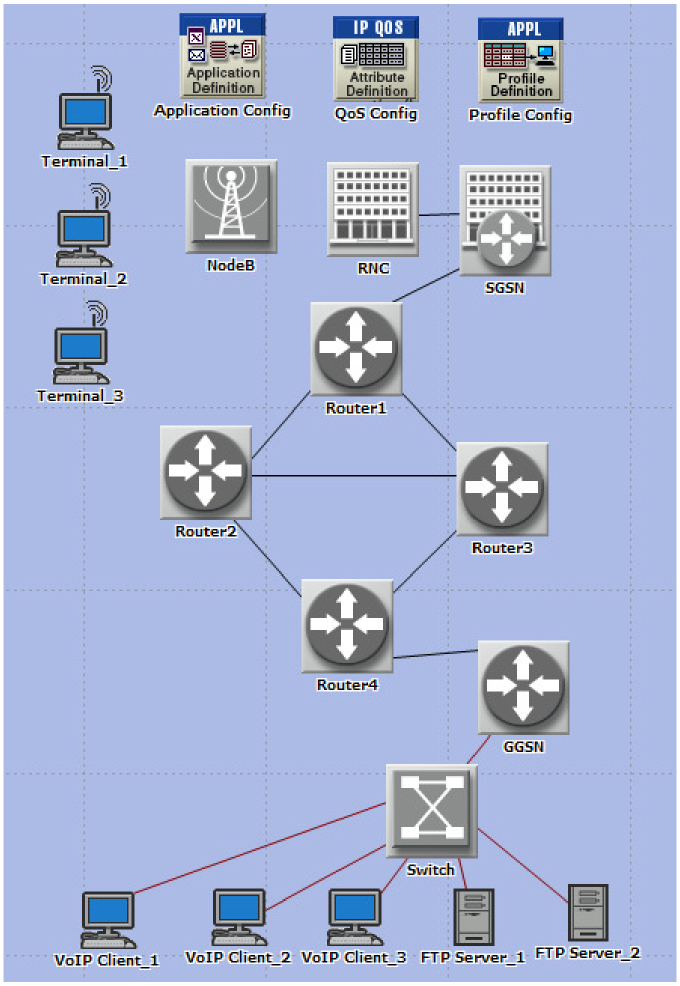

Figure 6. The network topology of the experiment

A. Experiment Results in Mobile Network Scenario

In this scenario, we tested different flows in same bearer. Mobile terminal1 established a bearer used for FTP downloading service. In this bearer, it communicated with two FTP servers respectively and the bandwidths were all 1.5Mbps. The packets of two flows arrived to all the interfaces randomly.

The bandwidth of all links was 10Mbps except for the link between SGSN and Router1, which was 4Mbps firstly and then reduced to 2Mbps for simulating network congestion.

We tested two cases: without and with the proposed flow label based QoS scheme. The test results are shown as following.

1) *Case1 without the proposed QoS scheme:* The Figure 7 shows the changes of two FTP flows after network congestion happened.

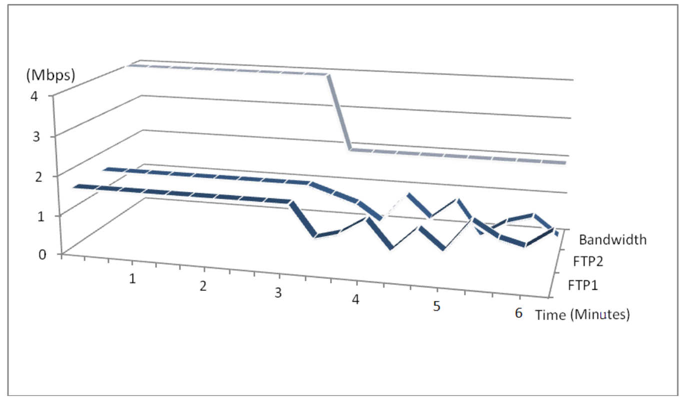

Figure 7. Test result in case1 of scenario1

We can conclude that the two FTP flows were all impacted due to the network congestion because that they were transported in a same bearer and the core network could not distinguish them and treated them with a same QoS policy.

2) *Case2 with the proposed QoS scheme:* The Figure 8 shows the change of two FTP downlodings after network congestion happened.

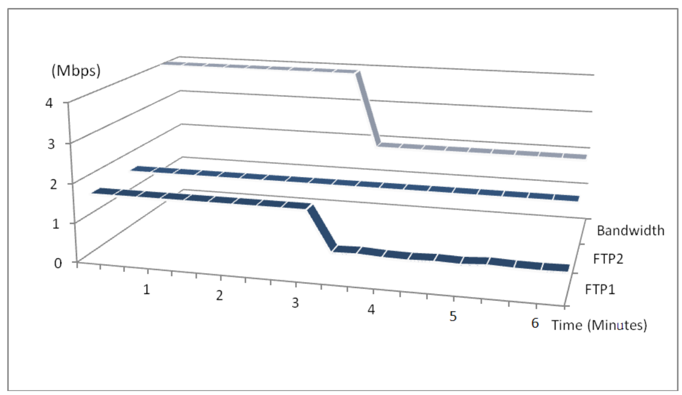

Figure 8. Test result in case2 of scenario1

In this case, we applied the flow label based QoS scheme. The core network entities could distinguish different flows by IPv6 flow label even they existed in same bearer and guaranteed the flow with high QoS priority. So when network congestion happened, the bandwidth of FTP2 was still in 1.5Mbps and that of FTP1 reduced to almost 0.5Mbps.

B. Experiment Results in Mobile IP Carrier Network Scenario

In this scenario, we tested different flows with same QoS profile transported in mobile IP carrier network. Three mobile terminals communicated with three peer VoIP clients respectively with a same QoS level. It supposed that the bandwidth of VoIP was all 1Mbps. The packets of three flows arrived to all the interfaces randomly.

The bandwidth of all links was 10Mbps except for the two links between Router1 and Router2, and between Router1 and Router3, which were all 2Mbps firstly and then the link

 ISBN: 978-1-61208-186-1

between Router1 and Router3 was down for simulating network congestion.

We tested two cases: without or with the proposed flow label based QoS scheme. The test results are shown as following.

1) Case1 without the proposed QoS scheme: The Figure 9 shows the changes of three VoIP flows after the link was down.

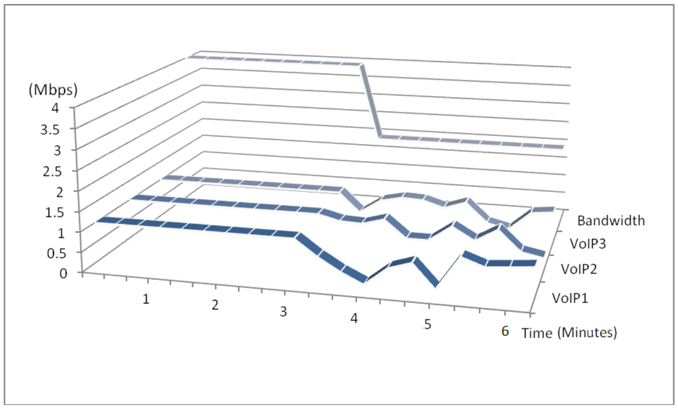

Figure 9. Test result in case1 of scenario2

For the test results, we can get that the three VoIP flows were all be impacted due to the network congestion because that they had same QoS level and the mobile IP carrier network could not distinguish them and treated them with a same QoS policy.

2) Case2 with the proposed QoS scheme: The Figure 10 shows the changes of three VoIP flows after the link was down.

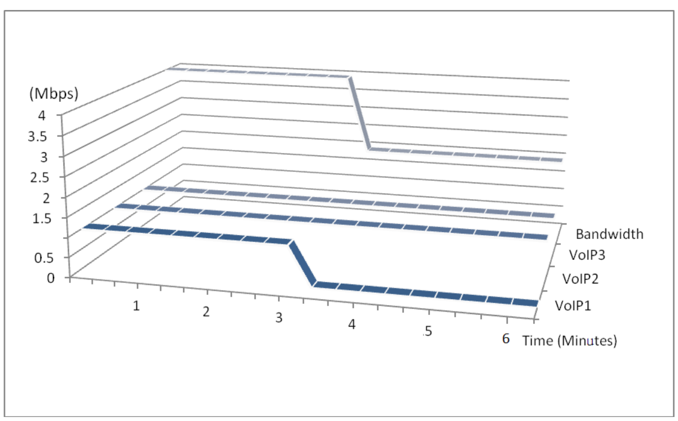

Figure 10. Test result in case2 of scenario2

In this case, we applied the flow label based QoS scheme in mobile IP carrier network. The carrier network entities could distinguish different flows by IPv6 flow label in transport layer header. When the link was down and the network congestion happened, routers could distinguish different VoIP flows and discarded the packets belonged to the same flow at first to minimize impacts to other flows.

V. CONCLUSION AND FUTURE WORK

In this paper, we investigated QoS architecture of mobile network and the current situation of IPv6 flow label. We proposed a flow label based QoS scheme, where flow label can be used to distinguish of packet flow and mobile network and IP carrier network can control the traffic more accurately and provide the finest granularity QoS. Experiment results show that our proposed QoS scheme is able to achieve better fine-grained control than existing ones.

Two services with several traffic flows are simulated on our experiment platform. In the future work we consider increasing the volume of traffic and new services. In addition we will research the performance of this scheme under mobility environment.

REFERENCES

[1] 3GPP TS 23.107, Quality of Service (QoS) concept and architecture, 2009.

[2] Dino Flore, LTE RAN architecture aspects, 3GPP IMT-Advanced Evaluation, 2009.

[3] 3GPP TS 23.401, General Packet Radio Service (GPRS) enhancements for Evolved Universal Terrestrial Radio Access Network (E-UTRAN) access, 2009.

[4] J. Rajahalme, A. Conta, B. Carpenter, and S. Deering, IPv6 flow label specification, IETF RFC 3697, March 2004.

[5] S. Amante, B. Carpenter, and S. Jiang, Rationale for update to the IPv6 flow label specification, IETF Internet draft, July 2011.

[6] S. Amante, B. Carpenter, S. Jiang, and J. Rajahalme, IPv6 flow label specification, IETF Internet draft, July 2011.

[7] Q.Hu and B. Carpenter, Survey of proposed use cases for the IPv6 flow label, IETF RFC 6294, June 2011.

[8] B. Carpenter and S. Amante, Using the IPv6 flow label for equal cost multipath routing and link aggregation in tunnels, IETF Internet draft, July 2011.

[9] B. Carpenter and S. Jiang, Using the IPv6 flow label for server load balancing, IETF Internet draft, October 2011.