A Novel Path Protection with Guaranteed QoS and Very High Availability for Real-time Applications in MPLS Networks

Mitsuo HAYASAKA†, Tetsuya MIKI†

†Faculty of Engineering, The University of Electro-Communications,
1-5-1 Chofugaoka, Chofu-shi, Tokyo, 182-8585 Japan
E-mail: †{mhysk, miki}@ice.uec.ac.jp

Abstract Real-time traffic will be a predominant traffic type in the next generation networks and 100% reliability and availability of networks will be required by real-time premium traffic (PT). It is believed that QoS guarantees could be better provided by the connection oriented networks such as Multi Protocol Label Switching (MPLS). These connection oriented networks are more vulnerable to network failures. Conventional path protections perform re-routing to cope with them. However, re-routing always causes packet losses and results in service outage. These losses are bursty in nature and highly degrade QoS of the real-time premium traffic. The novel path protection proposed in this paper recovers the bursty packet losses due to re-routing using forward error correction (FEC) path. Therefore, it can provide the network architecture with no service outage for such traffic. The numerical results show that the proposed method can achieve a very high availability for the real-time premium traffic in future IP/MPLS networks.

Keyword Path Protection, Forward Error Correction, Packet Loss Ratio, MPLS

1. Introduction

Real-time multimedia applications over the Internet such as VoIP, e-learning, telemedicine, e-commerce etc. grow rapidly and it can be expected that this trend continues in the future too. These applications demand guaranteed quality of service (QoS) with respect to delay, jitter, bandwidth and availability. It is believed that this can be better achieved by connection oriented networks than the connectionless networks, especially in the core. Connection oriented high speed networks such as MPLS [1] will be widely used in the future as they improve QoS by reducing the packet losses, delay jitter, bandwidth variations etc. It creates the Virtual Path (VP) called Label Switched Path (LSP) between the ingress and egress. The drawback in these networks is their potential vulnerability to network failures. According to reference [21], an e-commerce company with 99% availability (1% unavailability) will lose about $3.6 million annually due to network failures. Therefore, the focus of this study is to find a suitable solution to overcome the problems due to the network failures and increase the availability, especially for real-time premium traffic.

In the past, many Backup Path (BP) solutions for failures have been proposed such as 1+1 protection, 1:1 protection (extendible to m:n protection), and backup bandwidth sharing [2,3]. One major problem observed in these proposals is that they all perform re-routings during network failures. Re-routing always causes packet losses. These losses are bursty in nature and highly degrade QoS of the real-time applications. Therefore it is necessary to find proactive techniques to recover the bursty packet losses due to re-routings. The novel idea of path protection with forward error correction (FEC) path proposed in this article can be used for real time premium traffic that needs a guaranteed QoS. It combines a FEC path with conventional path protection methods using re-routings and recovers the packet losses due to re-routings by way of a FEC recovery technique. The numerical result shows that this is a promising proactive technique to provide a guaranteed QoS for real-time premium traffic that otherwise can lead to severe effects if 100% availability is not achieved.

The rest of this paper is organized as follows. An overview of MPLS is done in the next section. The problem description and the existing solutions are analyzed briefly in Section 3. In Section 4, we discuss the proposed method in detail. The performance of the proposed method is evaluated and the results are presented in Section 5. Finally this paper is concluded in Section 6.

2. An Overview of MPLS

MPLS is a connection-oriented model overlaid onto traditional connectionless IP networks. In contrast to the connectionless hop-by-hop routing in conventional IP, connection-oriented means traffic is sent between two end points after a connection (i.e. a pre-determined path) has been established. MPLS combines the best attributes of layer 2 switching technologies with the best attributes of the layer 3 routing technologies embedded in IP. The key component within a MPLS network, the label switched router (LSR), is capable of understanding and participating in both IP routing and layer 2 switching. Ingress is a node by which a packet enters the MPLS network, and egress is a node by which a packet leaves the MPLS network. The main functions of ingress are calculating the path through the MPLS network, initiating label switched path, classifying inbound traffic into forward equivalence classes that represents the binding of a group of packets or flows that require the same handling. The requests with the same destination egress and same QoS requirements are mapped to the same class by default, if no local policy is stated otherwise.

MPLS needs to have a signaling protocol to establish, maintain and terminate the communication sessions. MPLS uses Resource ReserVation Protocol with Traffic Engineering (RSVP-TE) [5] or Label Distribution Protocol (LDP) as a signaling protocol in the control plane. The control plane and the data plane of MPLS are logically separated, where the ‘call setup request’ is always accompanied by a ‘connection request’ in the recent router architectures [6]. MPLS uses in-band signaling, where the control messages are sent over the same links that carry data. In this paper, for all the discussions MPLS with RSVP-TE is considered since the Internet Engineering Task Force (IETF) encourages RSVP-TE over CR-LDP [7] as a control plane signaling protocol for MPLS. MPLS always creates a label switched path (LSP) using RSVP-TE before forwarding the traffic. In MPLS with RSVP-TE, a control plane session is always started before forming the LSP for data communication by exchanging PATH and RESV messages between ingress and egress. The ingress can send PATH messages explicitly enabling QoS routing and the egress will send a RESV message confirming the reservation of resources such as labels and bandwidth [8]. Therefore always the call setup time, the time taken to establish a LSP and start communications is round trip time (RTT) between the ingress and egress + the process time at each router. This varies from network to network, depending on the distance between the ingress and the egress.

RSVP takes a soft state approach to manage the reservation state of routers and hosts. This should be periodically refreshed by PATH and RESV messages. At the expiration of each ‘refresh timeout’ period, a refresh message is forwarded. The RSVP states are deleted by explicit TEAR messages or if appropriate refresh messages do not arrive before the expiration of ‘cleanup timeout’ interval [8]. RSVP also uses “hello protocol” to discover neighboring nodes and maintain the adjacencies with them. In other words it is used to detect node failures. Neighbor nodes periodically exchange HELLO messages with HELLO REQUEST and HELLO ACK objects. The periodicity is governed by ‘hello interval’ that can be configured on per neighbor basis. A RSVP ‘hello state timer’ value is decided and if it expires without receiving any hello messages the adjacency with the neighbor is lost. Furthermore the value of Src_Instance field must not be changed while the node is exchanging HELLO messages. If this value is changed or if it is zero the adjacency with neighbor is lost [5]. If the adjacencies are lost or the RSVP soft state is deleted the RSVP session is torn down resulting in termination of the corresponding data plane.

Each LSR maintains the “Next Hop Label Forwarding Entry” (NHLFE) in its routing tables, to forward labeled packets. Mapping packets to a forward equivalence class is done only once when they enter the MPLS network at the ingress. Therefore every ingress node maintains the class to NHLFE (FTN) to map each class to one or a set of NHLFEs, when unlabeled packets arrive at them. The ingress will always label them before they are dispatched. All other LSRs will maintain an “Incoming Label Map” (ILM) instead a FTN to map incoming labeled packets to NHLFEs.

3. Problem Analysis and Existing Solutions

Any of the network resources can fail at any time and therefore to provide a very high availability and reliability the network providers must be able to predict and plan for them.

3.1. Network Failures

The network failures can be due to many reasons such as hardware and software failures of equipment, link failures, service outages due to routine maintenance, temporary service outages due to very high congestion, protocol failures and failures of control functions etc. Since there are many reasons for network failures, the studies [9] have shown the following distribution in failure durations: about 10% of failures last for over 20 minutes, 40% of failures last between 1-20 minutes, and 50% of failures are very short lived, less than a minute. According to RFC 3469, the network failures of connection oriented networks such as MPLS are mainly classified into two types, namely link/path failures and degraded failures [10]. A link/path failure means a situation where the actual connectivity of the links/path between the ingress and egress is lost. Degraded failures that occur due to the links at lower layers are not in suitable quality for data transmission. Studies done on actual ISP networks have shown that almost 50% of total network failures are of degraded type and they explain the very short lived failures mentioned in [6]. One of the main reasons for degraded type failures is the control plane failures. The control plane of a connection oriented network performs the functions such as setup, termination and maintenance of the VPs in the data plane. Any failure in the control plane should not immediately affect the data plane communications since both planes are logically separated. Whenever the control plane session of a VP is failed, there will be temporary interruptions to the applications in the data plane due to the lack of maintenance functions. Usually these control plane failures are detected by the timers in the control plane; RSVP Hello State Timer in RSVP-TE and the Keep Alive Timer in LDP of the control plane of MPLS are two such examples. The values of these control plane timers are usually decided at the time of the formation of the control plane session by negotiating with the peers and usually they are in the range of 30-40s, but they can be as large as 60-90s.

All the control plane failures such as TCP teardowns of control sessions, control plane peer restarts, protocol failures in the control plane etc. are detected by these timers. If not for these timers, the control plane failure detection time can be as high as 2-3 minutes. Therefore the purpose of these timers is to reduce the convergence time after failures. Conventionally the timers are reset whenever Protocol Data Units (PDU) are received by the peers. If such a failure is detected, the corresponding data communications in the data plane are terminated and therefore it is necessary to do a re-routing to recover the terminated data communication. This will result in service outage and the QoS of real-time interactive applications are very much affected.

3.2. Existing Solutions

The existing solutions for network failures in connection oriented networks such as MPLS can be broadly classified into three types namely, local repair, path protection, and fast re-routing. The communication of signaling information in MPLS uses IP and therefore re-signaling a LSP due to failure will be time consuming. Furthermore a signaling protocol such as RSVP-TE concentrates more on the traffic engineering and therefore is less favorable for local repairs. Also network topologies are rarely full meshed and local repair might not succeed in MPLS and re-routing may need to be resolved at the ingress. In path protection, data is switched from failed LSP to a backup LSP at the repair point, conventionally at the ingress. It is said to be fast rerouting, when backup LSP can be pre-provisioned. As explained in [11], path protection is more efficient than local repair for connection oriented networks. Some such popular solutions for network failures in real-time applications are as follows. 1+1 protection, where the same data is transmitted both in the active and backup paths (AP & BP) simultaneously and at the receiver end the best channel is selected. 1:1 protection (extendible to m:n protection), where data is transmitted only via AP and BP is used only if a failure has occurred. Therefore when there are no failures in APs, the BPs can be used by some other non critical, best effort traffic. 1+1 has very fast recovery times but very inefficient with respect to the usage of bandwidth whereas 1:1 improves the bandwidth efficiency at the expense of the recovery time. Backup bandwidth sharing (BBS) is becoming increasingly popular due to the improved bandwidth efficiencies as a single BP can be shared by many link-disjoint APs [2,3].

One major problem in these conventional methods is that they all perform re-routings for network failures. Re-routing always causes packet losses. These losses are bursty in nature and highly degrade QoS of the real-time applications as the generation of such applications is also bursty. We have proposed Virtual Path Hopping (VPH) to reduce the number of re-routing [4]. The VPH concept identifies degraded type failures before the data plane communication session fails and the VP with a degraded failure is changed to a new VP by way of a VP hop. However, the problem of re-routing mentioned above still exists even for this proposal. Therefore it is necessary to find proactive techniques to recover the bursty packet losses due to re-routings.

4. Proposed Method

The main objective of this proposal is to provide network architecture with no service outage for real-time premium traffic (PT) even when network failures occur and re-routings are done to cope with them. In order to archive this target, forward error correction (FEC) technique that can recover bursty packet losses is discussed here. In FEC, the redundant packets, which are generated from original media packets by using an error correction code, are transmitted along with the media packets so that the lost original packets can be recovered using them [12,13]. This technique requires a redundant bandwidth that is called FEC overhead. When FEC with (n,k) block code is applied, where n is the total number of packets and k is the number of media packets, it adds (n-k) redundant FEC packets for every k media packets. Notation n and k are called the block length and the data length respectively. When there are packet losses, if any k packets of n block length are received at receiver end, all original media packets within n block length can be recovered using FEC. By applying this technique to conventional re-routing-based protection methods, the novel path protection scheme with FEC path is proposed.

4.1. Creation of Virtual Paths

In IP/MPLS the VP is called a LSP. The ingress nodes of IP/MPLS will have to play a major role in the implementation of the proposed method. When a request for a communication session arrives at the ingress, many link-disjoint VPs are decided between ingress and egress. In other words a link-disjoint VP-pool, which contains many VPs is decided for all ingress and egress pairs as shown in Fig 1. There are many algorithms proposed in the literature [14-18] to find link-disjoint paths between a pair of ingress and egress. It is beyond the scope of this paper to discuss them in detail. In this proposed scheme, all VPs in the VP-pool are ranked (from rank #1 to #N such that most suitable VP is #1) considering the delay parameter that each VP provides. Here, VP-pool of N VPs is considered. The best VP (rank #1) is the path whose delay is closer to the average delay of all VPs than any other VPs while the conventional schemes use the path with minimum delay as the best path. Since this minimizes the difference of link delays of each path, VPs with similar delays are activated and used first. Moreover, it helps to easily implement the concept of FEC path described in next section. Resources are not reserved for all VPs in the VP-pool since it is very inefficient, when it is decided. Resource reservation and allocation for VPs are done just before it is to be used by a certain communication session. In other words the VP-Pool shall only decide the different routes between ingress and egress that would satisfy the required QoS of the arrived traffic. When network failures occur, the PT is switched from the failed VP to another VP in the VP-pool.

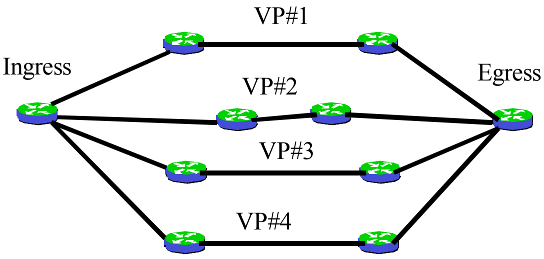

Fig. 1 Creation of virtual paths between ingress and egress

4.2. FEC Path

The traffic received at the ingress is divided into two types, namely PT and best effort traffic (BET). The PT is distributed among some active VPs (AVP) starting from the one ranked #1 VP at the ingress, as shown in Fig. 2. At the same time, the ingress creates FEC traffic by sending the PT in different AVPs through the exclusive-or (XOR) gate. This FEC traffic that consists of many FEC packets is sent via another AVP as another PT. The preplanned protection is only for PT. If an AVP fails, the affected PT is recovered by re-routing them to another activated VP. The packet losses during re-routing are recovered at the egress using FEC traffic. Generally, FEC is applied for an end-to-end communication treated as a flow in MPLS. If the burst length of packet losses in a flow increases, these packet losses are beyond the FEC recovery ability and cannot be recovered using FEC. However, in the proposed protection, even if their burst length in an AVP increases, they can still be recovered because FEC is generated from the PT in different AVPs and is sent via another AVP. Therefore, this proposal can provide a guaranteed QoS for the real-time PT even when network failures occur.

The ingress will calculate PT ratio (Pi), which is defined as the ratio of PT of *i*th AVP to total bandwidth of *i*th AVP. This proposal increases the number of AVPs with an increase of traffic and reduces it with the decrease of traffic. When the PT arrives at the ingress, it should be allocated to the AVP with minimum Pi. This helps to distribute PT among AVPs as much as possible and keeps the maximum Pi (max(Pi)) to a minimum value. This minimizes the spare capacity (SC) necessary to protect PT from failures as explained below. The SC to protect PT of an AVP is defined as the difference between the total capacity and bandwidth used by PT of an AVP. In this algorithm the SC to protect PT should be always large enough to recover a PT of max(Pi) * C; where C is the link capacity of *i*th AVP, (i.e., maximum PT in an AVP of the VP-pool).

Obviously the selected AVP should have enough vacant bandwidth (VBW) to accommodate newly arrived traffic flows. The VBW of an AVP is defined as the difference between the total bandwidth available and total bandwidth used by PT and BET of an AVP. On the other hand if the newly arrived traffic is BET, it is simply allocated to an AVP with enough VBW. If there is not enough VBW in the AVPs for newly arrived PT or BET, another VP in the VP-pool is activated. If no such VP is available to be activated and it is not possible to add any more VPs to VP-pool, the newly arrived traffic is dropped due to the lack of bandwidth. In order to carry out this kind of an allocation of traffic, ingress should know only very little information such as aggregate premium traffic and total capacity of each active VP. This is one of the advantages of this scheme and usually this information is available at each LSR through protocols such as extensions of Open Shortest Path First (OSPF) for traffic engineering [22].

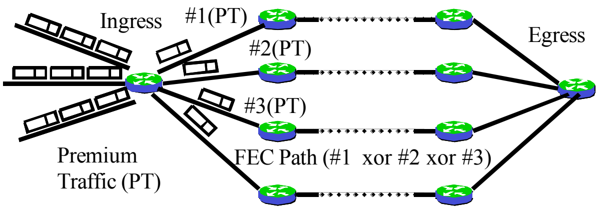

Fig. 2 Proposed path protection

For example, it is assumed that the VP-pool consists of N link-disjoint VPs each with a capacity of C, and there are n AVPs at any given time.

PT ratio of *i*th AVP;

$$P_i = \frac{PT\_in\_ith\_AVP}{Total\_BW\_of\_ith\_AVP} \; where(1 \le i \le n) \qquad (1)$$

Total PT in n AVPs;

$$C * \left(\sum_{i=1}^{n} P_i \right) \qquad (2)$$

Total available bandwidth after failure of one AVP;

$$C * (n-1) \qquad (3)$$

The available bandwidth for recovery of PT (SC to protect PT), if *j*th AVP fails (1 ≤ j ≤ n) is given by;

$$C\left(n - 1 - \left(\left(\sum_{i=1}^{n} P_i \right) - P_j \right) \right) \qquad (4)$$

Here the bandwidth used by the BET is not considered because the objective of this method is to provide guaranteed QoS and availability for PT. The maximum PT to be recovered is max(Pi).

For 100% restorability of PT;

$$C\left(n - 1 - \left(\left(\sum_{i=1}^{n} P_i \right) - P_j \right) \right) > C * \max(P_i) \qquad (5)$$

$$\therefore n > \max(P_i) + \left(\sum_{i=1}^{n} P_i \right) - P_j + 1 \qquad (6)$$

Here, A is defined as follows.

$$A = \max(P_i) + \left(\sum_{i=1}^{N} P_i \right) - P_j + 1 \qquad (7)$$

A service factor $T_{service}$ is considered to allow some extra bandwidth to make sure that the AVPs are not overloaded. In order to provide a guaranteed QoS for PT, the network load of PT in a path should be smaller. Generally, the QoS of PT is guaranteed at the expense of BET. When the network load of PT is increased, the QoS of PT is degraded because of the competition among the PT. Let $T_{service}$ be the maximum percentage of network load for PT where its QoS can be provided without degradation. Always n > A should be maintained and if n < A/ $T_{service}$, where 0 < $T_{service}$ < 1, another VP should be activated in the VP-pool in order to increase n by one. The PT ratio for every AVP is calculated by the ingress and these values are used to allocate PT to the AVP with minimum Pi as explained before. Whenever a new allocation of PT is done, the PT ratios are updated. The value of $T_{service}$ can be decided by the network administrator according to the needs of the network.

In addition, it can accommodate the delay jitter of PT in an AVP among AVPs. Basically, the delay jitter of PT is very small since it is treated as the highest priority traffic. Therefore, it is possible to consider the transmission delay of PT between ingress and egress is equal to the path delay. However, if the arrival of one of PTs in different AVPs at the egress is delayed, it can be accommodated using FEC traffic. This is because the delayed PT can be considered as bursty packet losses and is able to be regenerated using FEC traffic at egress. This is another advantage of this proposed scheme.

When the PT is distributed among several AVPs, FEC traffic is instantaneously created at ingress. Therefore, the special buffer for FEC recovery process is required at egress and its size depends on the difference of link delays in AVPs. The proposed method minimizes this delay difference considering the ranking of VPs as explained in Section 4.1 and therefore the required buffer size is also minimized.

5. Performance Evaluations

The performance of the proposed path protection is evaluated here. The real-time PT is distributed among k AVPs with a capacity of C and FEC traffic is sent to another AVP. Notation k should be more than 1. Let n be the total number of AVPs, there are n AVPs between a pair of ingress and egress.

5.1. Effective Packet Loss Ratio

The effective packet loss ratio is defined as the loss ratio of the lost packets that cannot be recovered even after using the FEC. It is assumed that there is a network failure in a month. The re-routing time (RRT) to change from AVP to another AVP mainly depends on the round trip time (RTT) between ingress and egress. More specifically;

$$RRT = RTT + \Pr ocess\_time\_at\_nodes + t \qquad (8)$$

where t is time to inform ingress about a failure occurrence after its detection and depends on the location of the failure. Therefore, it is clear that the re-routing time varies according to the networks used. Here, it is set to 100ms, 1s and 10s in order to observe the performance of proposed method according to the change of the re-routing time. In the proposed scheme, if any failure cannot be recovered by re-routing before the next failure occurs in another AVP, the packet losses due to re-routing cannot be recovered using FEC. Therefore, the effective packet loss ratio of proposed method is given by;

$$\sum_{i=2}^{k+1} {}_{k+1}C_i P_{loss}^i \left(1 - P_{loss}\right)^{k+1-i} \qquad (9)$$

where k is the number of AVPs used for PT and P_{loss} is the probability of failure occurrence during the re-routing time with the assumption of one failure in a month. Fig. 3 shows the effective packet loss ratios of conventional and proposed path protections according to the variety of the number of the AVPs used and the re-routing time. The target of packet loss ratio that should be provided by the networks is set to 10^{-9} [20]. All methods increase their loss ratios with the increase of the re-routing time. The proposed methods highly reduce the loss ratio compared to the conventional methods, and their loss ratios are less than the target value although it is the same as the target when the re-routing time and the number of AVP are 10s and 11 respectively. However, the loss ratios of all the conventional methods are more than the target. There is a huge improvement of the packet loss ratio, and these loss ratios can be ignored as they are very small. Since re-routings recover any network failures and the bursty packet losses due to re-routings are compensated, it can be concluded that the proposed network architecture can provide approximately 100% availability for real-time premium traffic even when network failures occur.

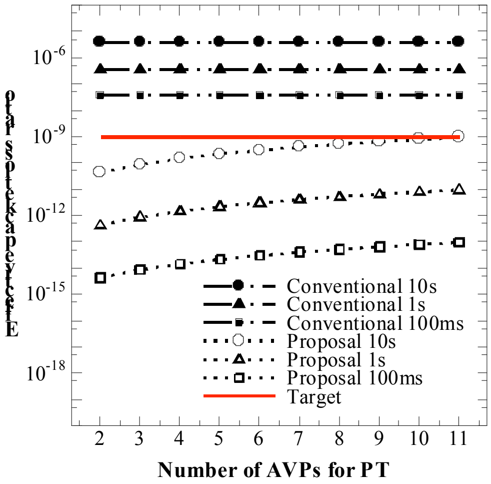

Fig.3 Effective packet loss ratio

5.2. Occupancy Ratio of FEC Traffic

The maximum occupancy ratio of FEC traffic to the total capacity of links used as AVPs is evaluated. It is an important factor that must be considered because this scheme requires the redundant bandwidth of FEC traffic that recovers the packet losses due to re-routings. The maximum occupancy ratio of FEC traffic in the proposed protection is given by;

$$\frac{T_{service}C}{nC} = \frac{T_{service}}{n} \qquad (10)$$

where n is the number AVPs and $T_{service}$ is the maximum percentage of network load for PT where its QoS can be provided without degradation. Here, $T_{service}$ is set to 30% as an example and therefore the network load of PT in each AVP is also 30% for the evaluation. Fig. 4 shows that the occupancy ratio of FEC traffic decreases with the increase of AVPs. The proposed protection can provide a very high availability and be implemented at the expense of these maximum ratios of BET. These ratios are less than 10% of total link capacity of AVPs for any number of AVPs and in practical, the occupancy ratio of FEC traffic is expected to be less than these ratios since they are upper boundaries. Therefore, the effect of FEC traffic can be considered as small.

5.3. Required Buffer Size At Egress

Finally, the required buffer size at egress to implement this scheme is evaluated by way of computer simulations. Let D_{diff} be the delay difference of each AVPs, the buffer size is given by;

$$T_{service} C D_{diff} \tag{11}$$

Different network topologies with nodes 20, 40, 50, 60 and 90 are simulated. The number of bi-directional links is set as 30% of the number of links in full-mesh networks. Random graphs are used to decide the network topologies. The link delays are randomly allocated from 1ms to 5ms as the weight of each link. The simulation results indicated similar patterns and therefore the results of the nodes with 50 and 90 are presented here. In all the simulations performed, the following simple algorithm is followed to decide the VP-Pool. This algorithm is followed because it is the similar QoS routing algorithms followed by MPLS-TE supported routers in the market today. First, prune off the links that do not have sufficient resources to support the requested QoS. Then the Dijkstra's [19] shortest path algorithm is performed on the remaining topology to find the paths. Once a VP is selected, those links are pruned off and the same procedure is performed for the balance part of the network to decide the next VPs in the VP-pool. If it is not possible to find link-disjoint paths, the least overlapped best VPs can be decided in a similar way to the algorithm in [14]. For simplicity and better comparability 10 ingress/egress pairs are decided and the maximum number of VPs is set as 10. Then, the average path delay among 10 VPs is calculated, and the paths with delay closer to the average are activated and used. The maximum delay difference of AVPs with the increase of number of AVPs for 50 and 90 nodes are summarized in Table 1 and 2, respectively. It is observed that the maximum delay difference is increased with the increase of AVPs used, but they are very small because of the new best path decided based on the average delay. Tables 1 and 2 also show the required buffer size according to these results and using (11). Here, it is assumed that each link capacity is 100Mbps and $T_{service}$ is 30%. They are also very small and therefore, the proposed protection is feasible.

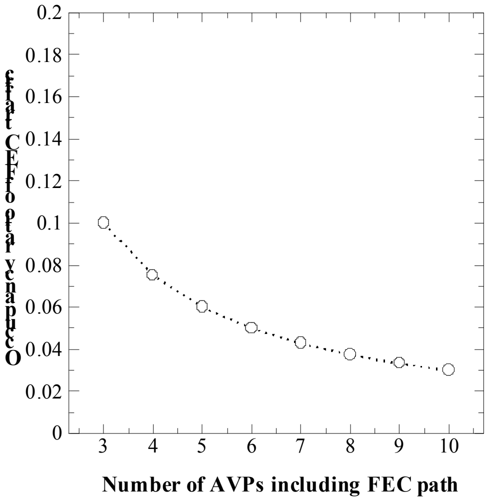

Fig.4 Occupancy ratio of FEC traffic to total link capacity of AVPs

If the maximum number of available AVPs is set as 8 and the PT and FEC traffic are distributed among these 8 AVPs, the required buffer size is around 10KB while reducing the occupancy ratio of FEC traffic and highly improving the effective packet loss ratio. This is a design example of proposed path protection. From these evaluations, it can provide reliable network architecture with no service outage for real-time premium traffic even when network failures occur.

Table1: Maximum Delay of AVPs and Required Buffer Size (50 Nodes, 100Mbps Link Capacity and 30% $T_{service}$)

Number of AVPs	Maximum delay difference of AVPs [ms]	Buffer size [KB]
2	1	3.75
3	1	3.75
4	2	7.44
5	2	7.44
6	3	11.25
7	3	11.25
8	3	11.25
9	4	14.88
10	5	18.75

Table2: Maximum Delay of AVPs and Required Buffer Size (90 Nodes, 100Mbps Link Capacity and 30% $T_{service}$)

Number of AVPs	Maximum delay difference of AVPs [ms]	Buffer size [KB]
2	1	3.75
3	1	3.75
4	1	3.75
5	1	3.75
6	2	7.44
7	2	7.44
8	2	7.44
9	3	11.25
10	4	14.88

6. Conclusion

The rapid expansion of premium real-time applications over the IP packet network demands guaranteed QoS with respect to delay, jitter, and bandwidth. The connection oriented packet networks can meet most of these QoS demands better in the future. Connection oriented networks are more vulnerable to network failures and it is a timely requirement to find a solution to achieve 100% availability for them. The re-routing is a solution for failures but causes bursty packet losses leading to service outage. According to the numerical results the effective packet loss ratio of proposed protection is highly reduced compared to conventional methods and very small. Therefore, it can be considered that it is negligible. The proposed network architecture recovers the packet loss due to re-routing at egress and can provide approximately 100% availability for real-time premium traffic. Also, the occupancy ratio of FEC traffic and the required buffer size at egress are very small and it is feasible. Therefore we can conclude that the implementation of FEC path in conjunction with conventional re-routing based protection in connection oriented networks can achieve the requirements of the future Internet applications.

The proposed path protection should be evaluated in the real network using real-time traffic, as future work of this study.

References

[1] E. Rosen et al., “Multi Protocol Label Switching Architecture”, IETF RFC 3031, Jan 2001.

[2] Yijun Xiong, Lorne G. Mason, "Restoration strategies and spare capacity requirements in self-healing ATM networks", IEEE/ACM Transactions on Networking, no. 1, Feb 1999 pp. 98-110.

[3] Li Li, Milind M. Buddhikot, Chandra Chekuri, Katherine Guo, “Routing Bandwidth Guaranteed Paths with Local Restoration in Label Switched Networks”, Proceedings of the 10th IEEE International Conference on Network Protocols 2002.

[4] M. Gamage, M. Hayasaka, and T. Miki, “Implementation of Virtual Path Hopping (VPH) as a Solution for Control Plane Failures in Connection Oriented Networks and an Analysis of Traffic Distribution of VPH”, Proceedings of 3rd International Workshop on QoS in Multi-service IP Networks (QoS-IP 2005), pp.124-135, Catania, Italy, February 2005.

[5] D. Awduche et al., “RSVP-TE: Extensions to RSVP for LSP Tunnels”, IETF RFC 3209, Dec. 2001.

[6] Osama Aboul-Magd, “The Documentation of IANA assignments for Constraint-Based LSP setup using LDP (CR-LDP) Extensions for Automatic Switched Optical Network (ASON)”, IETF RFC 3475, March 2003.

[7] L. Andersson, G. Swallow, “The Multi Protocol Label Switching (MPLS) Working Group decision on MPLS signaling protocols”, IETF RFC 3468, Feb 2003.

[8] R. Braden et al., “Resource ReServation Protocol (RSVP)”, IETF RFC 2205, Sept. 1997.

[9] Gianluca Iannaccone et al., “Analysis of link failures in a IP backbone” Proceedings of Internet Measurement Workshop 2002, http://www.icir.org/vern/imw-2002/imw2002-papers/202.pdf

[10] V. Sharma et al., “ Framework for Multi-Protocol Label Switching (MPLS)-based Recovery” , IETF RFC 3469, Jan 2003.

[11] Chancheng Huang, Vishal Sharma, Ken Owens and Srinivas Makam, “Building Reliable MPLS Networks Using a Path Protection Mechanism”, IEEE Communications Magazine, pp. 156-162, March 2002.

[12] J. Rosenberg and H. Schulzrinne, “An RTP Payload format for Generic Forward Error Correction,” RFC 2733, Dec. 1999.

[13] C. Perkins, “RTP: Audio and Video for the Internet,” Addison-Wesley, 2003.

[14] S. D. Nikolopoulos, A. Pitsillides and D. Tipper, “Addressing Network Survivability Issues by Finding the K best Paths through a Trellis

Graph", Proceediings of IEEE INFOCOM 1997.

[15] B. Szviatovszki, A. Szentesi and A.Juttner, "On the Effectiveness of Restoration Path Computation Methods", http//www.cs.elte.hu/~alpar/publications/proc/RestoPath.pdf

[16] Yuchun Guo, Fernando Kuipers and Piet Van Mieghem, "Link-Disjoint Paths for Reliable QoS Routing", http://www.nas.its.tudelft.nl/people/Piet/papers/dimcra.pdf

[17] Y. Bejerano et al., "Algorithms for Computing QoS paths with Restoration", http://citeseer.ist.psu.edu/cache/papers/cs/29147/http: zSzzSztiger.technion.ac.ilzSz~spalexzSzpubzSzTM-restoration.pdf/ bejerano02algorithms.pdf

[18] G. LIU, Y. Yang, and X. Lin, " Performance Evaluation of K Shortest Path Algorithms in MPLS Traffic Engineering", IEICE Trans. Commun., vol.E87-B, no.4, pp.1007-1010, Apr. 2004.

[19] Dijkstra's shortest path algorithm, http://en.wikipedia.org/wiki/Dijkstra%27s_algorithm

[20] Y.Sato and K. Sato, "Evaluation of Statistical Cell Multiplexing Effects and Path Capacity Design in ATM Networks," IEICE Trans. Commun., Vol.E75-B, No.7, pp.642-648, 1992.

[21] A. Autenrieth, and A. Kristadter, "Fault-Tolerance and Resilience Issues in IP-Based Networks," 2nd Int'l. Wksp. Design Reliable Commun. Net. (DRCN2000), Germany, Apr.2000.

[22] D.Katz, K. Kompella and D.Yeung, "Traffic Engineering (TE) Extensions to OSPF Version 2," RFC 3630, Sept. 2003.E. Rosen et al., "Multi Protocol Label Switching Architecture", IETF RFC 3031, Jan 2001.