Vol. 48 No. 12 IPSJ Journal Dec. 2007

Regular Paper

Seamless Failure Recovery for Real-time Multimedia Applications in MPLS Networks

Mitsuo Hayasaka† and Tetsuya Miki†

The QoS provided by current best effort Internet is not good enough for real-time multimedia applications that are categorized as premium traffic. It is believed that QoS guarantees could be better provided by the connection oriented networks. Multi Protocol Label Switching (MPLS) is one such technology and these connection oriented networks are inherently more prone to network failures. Re-routing is a solution to cope with them. However, the re-routing always causes packet losses and results in service outage. Therefore, the QoS of the real-time premium traffic is highly degraded. The seamless failure recovery proposed in this paper can be used for real-time premium traffic that needs a guaranteed QoS. It applies an FEC technique to the conventional re-routing based path protection and seamlessly recovers the packet losses due to re-routing by way of an FEC recovery technique. The numerical and simulation results show that the proposed method can provide network architecture without service outage for real-time premium traffic while minimizing the service costs such as redundant traffic and additional buffer at edge routers.

1. Introduction

Real-time multimedia applications over the Internet such as VoIP, e-learning, Internet TV, telemedicine and e-commerce grow rapidly with the development of broadband networks. These emerging applications that are categorized as Premium Traffic (PT) demand guaranteed quality of service (QoS) with respect to packet losses, delay, jitter 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 IP/MPLS [1] will be widely used in the future as they improve QoS by reducing packet losses, delay jitter and bandwidth variations. 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. Therefore, the focus of this study is to find a suitable solution to overcome the problems due to network failures and improve the QoS of real-time premium traffic. Many Backup Path (BP) solutions for failures have been proposed in the past such as 1+1 protection, 1:1 protection (extendible to m:n protection), and backup bandwidth sharing (BBS) [2),3)]. Since 1+1 is very inefficient with respect to the usage of bandwidth, 1:1 and BBS are becoming increasingly popular due to the improved bandwidth efficiencies. Therefore, this paper focuses on these as the conventional methods. One major problem observed in both 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. We have proposed Virtual Path Hopping to reduce the number of re-routings [4]. However, the problem of re-routing mentioned above still exists, and therefore it is necessary to find proactive techniques to recover the bursty packet losses due to re-routings. The novel idea of seamless failure recovery using the forward error correction (FEC) path proposed in this article can be used for real-time premium traffic that needs a guaranteed QoS. It applies an FEC technique to the conventional re-routing based path protection and recovers the bursty packet losses due to re-routing by way of an 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. The problem description and the existing solutions are analyzed briefly in the next Section. In Section 3, we discuss the proposed method in detail. The performance of the proposed method is evaluated and the results are presented in Section 4. Finally this paper is

† The University of Electro-Communications

concluded in Section 5.

2. 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.

2.1 Network Failures

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 [5] 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, link/path failures and degraded failures [6]. A link/path failure mean a situation where the actual connectivity of the links/path between the ingress and egress is lost. Degraded failures occur due to the links at lower layers not being of suitable quality to guarantee data transmission. Studies done on actual ISP networks have shown that almost 50% of total network failures are of the degraded type and they explain the very short lived failures [7]. One of the main reasons for degraded type failures is the control plane failures. The control plane of a connection oriented network performs functions such as setup, termination and maintenance of the VPs in the data plane. In other words there will be a corresponding control plane session to each VP in the data plane. The control plane and the data plane communications of connection oriented networks can be separated according to recent router architectures [7]. Therefore any failure in the control plane should not immediately affect data plane communications. Whenever the control plane session of a VP fails, 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 Resource reSerVation Protocol for Traffic Engineering (RSVP-TE) [8] and the Keep Alive Timer in Label Distribution Protocol (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 formation of the control plane session by negotiating with peers, and usually they are in the range of 30–40 s, but they can be as large as 60–90 s.

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 could 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 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 outages and the QoS of real-time interactive applications are very much affected.

2.2 Existing Solutions

The existing solutions for network failures in connection oriented networks such as MPLS can be broadly classified into three types, local repair, path protection, and fast re-routing. The communication of signaling information in MPLS uses IP and therefore re-signaling an 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 repairs might not succeed in MPLS and re-routing may need to be resolved at the ingress. In path protection, data is switched from a failed LSP to a backup LSP at the repair point, conventionally at the ingress. It is said to be fast re-routing, when backup LSP can be pre-provisioned. As explained in Ref. 9), path protection is more efficient than local repairs for connection oriented networks. Some 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 is very inefficient with respect to the usage of bandwidth. Therefore, it highly limits the bandwidth to accommodate the real-time premium traffic in the network. In contrast, 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)]. Thus, 1:1 protection and BBS are improved methods of 1+1 protection and many studies have focused on them. Similarly, this paper focuses on these methods and considers them as the conventional methods.

One major problem in these conventional methods is that they all perform re-routings for network failures. When network failures occur, all traffic sent via the failed VP will be lost. Even if re-routing is done, all traffic intended to be sent via the failed VP will be lost until the BP is activated and re-routing is completed. Thus, re-routing always causes packet losses. These losses are bursty in nature and highly degrade the QoS of 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-routings [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. If these re-routing based protections can be provided with compensation of the bursty packet losses such as 1+1 protection, it is an attractive solution since the network failures can be recovered with no packet losses and improvement of bandwidth efficiency. Therefore it is necessary to find proactive techniques to recover bursty packet losses due to re-routing to improve the QoS of the real-time premium traffic.

3. 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 [10),11)]. This technique requires a redundant bandwidth that is called FEC overhead. When FEC with an (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 packet. Notations 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 the receiver end, all original media packets within the n block length can be recovered using FEC. 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. By improving this technique and applying it to the conventional re-routing-based protection methods, the seamless failure recovery using FEC path is proposed.

3.1 Creation of Virtual Paths

In IP/MPLS, the VP is called an 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 chosen between ingress and egress. In other words a link-disjoint VP-pool, which contains many VPs is chosen for all ingress and egress pairs as shown in **Fig. 1**. This VP-pool should contain at least three VPs to make this proposed method effective. There are many algorithms proposed in the literature [12)~16)] to find link-disjoint paths between a pair of ingress and egress. It is beyond the scope of this paper to discuss these in detail. Here, a VP-pool of N VPs has been considered. All VPs in the VP-pool are ranked (from rank #1 to #N such that the most suitable VP is

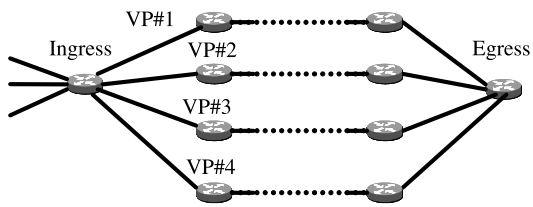

Fig. 1 Creation of virtual paths between ingress and egress.

#1) considering the delay parameter that each VP provides. The best VP (rank #1) is the path whose delay is closest 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 path delays of each path, VPs with similar delays are activated and used first. Moreover, it helps to easily implement the concept of the FEC path described in the next section. Resources are not reserved for all VPs in the VP-pool since it is very inefficient. The ingress only does path computations when the VP-pool is formed and it does not do any label bindings. Resource reservation and the establishment of label binding for VPs are done by exchanging PATH and RESV messages in RSVP-TE, just before they are to be used by the intended traffic. In other words the VP-Pool shall only decide the different routes between ingress and egress that would satisfy the required QoS of the arriving traffic.

When network failures occur, the ingress is informed about a failure occurrence after its detection. The ingress and egress pair will exchange PATH and RESV messages to activate the next available VP, and the PT is switched from the failed VP to another VP in the VP-pool. It is clear that the re-routing time (RRT) mainly depends on the round trip time (RTT) between the ingress and egress, or more specifically;

$$RRT = RTT + t \quad (1)$$

where t is the 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 depending on the networks used.

3.2 An FEC Path

The traffic received at the ingress is divided into two types, PT and best effort traffic (BET). The PT is distributed among some active VPs (AVP) starting from the rank #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 it to another activated VP. The packet losses during re-routing are recovered at the egress using FEC traffic. Therefore, in the proposed protection, even if their

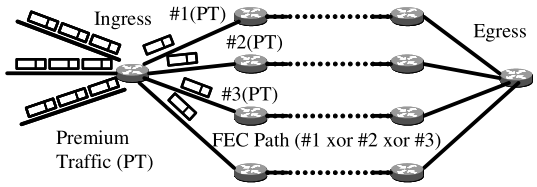

Fig. 2 Proposed path protection.

burst length in an AVP increases, these losses can still be recovered because FEC is generated from the PT in different AVPs and is sent via another AVP. In other words, the bursty packet losses due to re-routing can be treated as one packet loss within a block length in the FEC recovery process of the proposed method and can be recovered. This method overcomes the losses due to re-routing and this will highly improve the QoS of the PT even when network failures occur.

When the PT is distributed among several AVPs, FEC traffic is instantaneously created at ingress. Therefore, the special buffer for the FEC recovery process is required at egress and its size depends on the difference of path delays in AVPs. The proposed method minimizes this delay difference considering the ranking of VPs as explained in Section 3.1 and therefore the required buffer size is also minimized.

3.3 Traffic Allocation for Virtual Paths

It is assumed that the VP-pool consists of N link-disjoint VPs each with a bandwidth of B, and there are n AVPs at any given time ($3 \leq n \leq N$). The ingress will calculate PT ratio (P_i) which is defined as the ratio of PT of ith AVP ($1 \leq i \leq n$) to the total bandwidth of ith AVP and given by;

$$P_i = \frac{PT\_in\_ith\_AVP}{Total\_BW\_of\_ith\_AVP} \quad (2)$$

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 the minimum P_i. This helps to distribute PT among AVPs as much as possible and keeps the maximum P_i ($\max(P_i)$) to a minimum value. In other words, this minimizes the amount of the redundant FEC traffic because it depends on the maximum PT ratio among AVPs. Here, a service factor $T_{service}$ is considered to avoid QoS degradation for PT. 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 the network load for PT where its QoS can be provided without degradation. When the PT arrives at the ingress and if the total PT ratio assumed to allocate it to the path with $\min(P_i)$ is beyond the $T_{service}$, another VP should be activated in the VP-pool in order to increase n by one and allocate the newly arrived PT to it. If no such VP is available to be activated and it is not possible to add any more VPs to the VP-pool, the newly arrived PT is dropped due to the lack of bandwidth. Therefore, the maximum available bandwidth (MAB) that can provide a guaranteed QoS for PT is given by approximate $T_{service}B(N-2)$ since two VPs are required for the FEC path and the backup path. This is a limitation of the proposed method. This MAB is slightly degraded compared to BBS but is highly improved compared to 1+1 protection since the MABs of BBS and 1+1 protection are approximate $T_{service}B(N-1)$ and $\frac{T_{service}BN}{2}$, respectively. The PT ratio for every AVP is calculated by the ingress, and 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. On the other hand if the newly arrived traffic is BET, it is simply allocated to an AVP with the minimum network load. If there is not enough bandwidth in the AVPs for newly arrived BET, another VP in the VP-pool is activated. If no such VP is available in the VP-pool, the newly arrived BET is dropped due to the lack of bandwidth. This BET is preempted by PT, similar to the conventional 1:1 protection, if there is a network failure in an AVP that carries PT. In order to carry out this kind of an allocation of traffic, ingress only needs to know little information such as aggregate premium traffic and the total bandwidth 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 [18].

4. Performance Evaluations

The performance of the proposed path protection is evaluated and compared to conventional methods. The PT is distributed among k AVPs with a bandwidth of B 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.

4.1 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. The adverse effects of bursty packet losses due to re-routing are numerically evaluated here. In Ref. 19), it is assumed that the failure probability of a network in a month is set to 0.1 and less than this value. Here, it is set to 0.1 and 1.0 to evaluate the proposed method with a high probability of network failure. These values mean that there is a network failure in ten months and in a month, respectively. As described in Section 3.1, the re-routing time (RRT) to change from a failed AVP to another activated VP mainly depends on the round trip time (RTT) between ingress and egress. Therefore, it is clear that the re-routing time varies according to the network domains used. Here, it is set to 100 ms, 1 s and 10 s as examples of the RRT in order to observe the performance of the proposed method depending on changes of the RRT. Since these values are of a different order of magnitude and cover a wide range of RRT, the performance of the proposed method in the various network domains with different RRTs can be estimated using this evaluation. In other words, the proposed method is evaluated for the occurrence of bursty packet losses during 100 ms, 1 s and 10 s due to re-routing, and is compared to the conventional methods. 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 the proposed method is given by;

$$\sum_{i=2}^{k+1} {}_{k+1}C_i P_{loss}^i (1-P_{loss})^{k+1-i} \qquad (3)$$

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 failure probability of the network in a month. P_{loss} also indicates the probability of packet losses for the conventional methods. **Figures 3** and **4** show the effective packet loss ratios of the conventional and the proposed path protections depending on the variety of the number of the AVPs used and the re-routing time, where the failure probabilities of the networks is 0.1 and

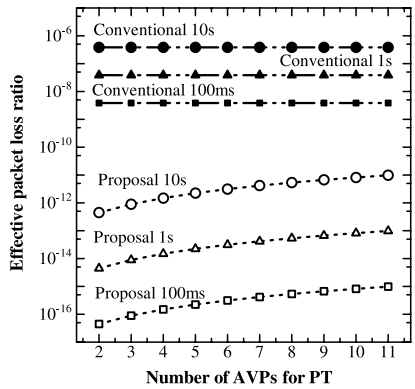

Fig. 3 Effective packet loss ratio for 0.1 failure probability in a month.

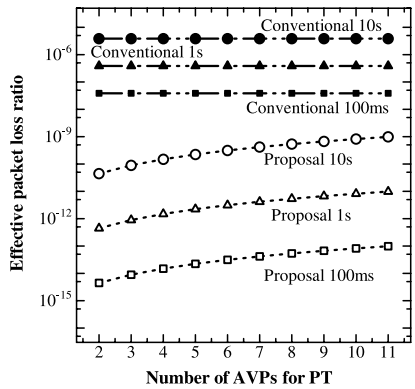

Fig. 4 Effective packet loss ratio for 1.0 failure probability in a month.

1.0 respectively. All methods increase their loss ratios with the increase of the re-routing time. The proposed methods highly reduce the loss ratio compared to conventional methods and their loss ratios are at least less than 10^{-11} and 10^{-9} for the failure probabilities of 0.1 and 1.0, respectively. There is a huge improvement of the packet loss ratio, and these loss ratios can be ignored because they are very small. Since re-routings recover any network failures and the bursty packet losses due to re-routing are compensated for this method, the proposed method can achieve availability of more than 99.999999999% or 99.9999999% for the failure probabilities of 0.1 and 1.0, respectively. Therefore, it can be concluded that the proposed network architecture can provide approximate 100% availability for real-time premium traffic even when network failures occur.

4.2 Occupancy Ratio of FEC Traffic

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

$$\frac{T_{service}B}{nB} = \frac{T_{service}}{n} \quad (4)$$

where n is the number of AVPs and $T_{service}$ is the maximum percentage of network load for PT where its QoS can be provided without degradation. In Ref. 20), the mean waiting time due to switching delay on an N × N packet switch are evaluated using Markov models, queueing theory, and simulation for both input and output queues, where the N indicates the number of input and output ports. It shows that the mean waiting time starts to increase when the percentage of network load exceeds 30%. Therefore, this percentage should not be greater than 30% especially for PT to avoid the QoS degradation because the switching delay causes delay and jitter. Here, $T_{service}$ is set to 10%, 20% and 30% as examples and therefore the network load of PT in each AVP is also these percentages for the evaluations. **Table 1** shows that the occupancy ratio of FEC traffic decreases with the increase of AVPs. The proposed protection can provide a very high availability and can be implemented at the expense of these maximum ratios of BET. These ratios are less than 10% of total link bandwidth of AVPs for any number of AVPs and in practical use, 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 to be small.

Table 1 Maximum occupancy ratio of FEC traffic to total link bandwidth of AVPs.

No. of AVPs for PT	$T_{service}$ 10%	20%	30%
3	0.033	0.067	0.100
4	0.025	0.050	0.075
5	0.020	0.040	0.060
6	0.017	0.033	0.050
7	0.014	0.029	0.043
8	0.013	0.025	0.038
9	0.011	0.022	0.033
10	0.010	0.020	0.030

4.3 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 AVP, the buffer size is given by;

$$T_{service} BD_{diff} \quad (5)$$

Different network topologies with nodes 10, 20, 30, 40, 50, 60, 70, 80 and 90 are simulated since there are various network domains comprised of the different number of nodes. The number of bi-directional links is set to 30% of the number of links in full-mesh networks as an example since the network topologies are rarely full-meshed. Random graphs [21] are used to decide the network topologies. In this graph, the link between nodes is randomly allocated when the number of nodes and links is given. Therefore different network topologies are able to be simulated for each number of nodes with the increase of the number of simulations. Here, 1,000 different network topologies are simulated for each number of nodes and the average of their results is presented. The link delays are randomly allocated from 1 ms to 5 ms as the weight of each link. Therefore, different paths with different path delays can be found between a pair of ingress and egress. The simulation results indicated similar patterns and therefore the results of nodes 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 similar to the 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 [17] 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 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 and best VPs can be decided in a similar way to the algorithm in Ref. 12). For simplicity and better comparability 10 ingress/egress pairs are decided and the maximum number of VPs is set to 10. Then, the average path delay among 10 VPs is calculated, and the paths with delay closest to the average are activated and used first. The maximum delay difference of AVPs with the increase of number of AVPs for 50 and 90 nodes are summarized in **Tables 2** and **3** respectively. It is observed that the maximum delay differences are increased with the increase of AVPs used, but they are very small because of the new best path decision based on the average path delay. Tables 2 and 3 also show the required buffer size calculated using Eq. (5) and the results of the maximum delay difference. Here, it is assumed that the $T_{service}$ is set to 30% and the link bandwidths are 100 Mbps, 1 Gbps and 10 Gbps. These buffer sizes are also very small and therefore, the proposed protection is feasible. If the maximum number of available AVPs is set to 8 as the design example of the proposed path protection and the PT and FEC traffic are distributed among these 8 AVPs, the required buffer sizes are about 10 KB, 100 KB and 1 MB for the link bandwidths with 100 Mbps, 1 Gbps and 10 Gbps respectively. In this scenario, the occupancy ratio of FEC traffic is reduced and the effective packet loss ratio is highly improved.

Table 2 Maximum delay difference of AVPs and required buffer size for 50 nodes.

No. of AVPs	Delay difference [ms]	Required buffer size [MB] for varied link bandwidth		
		100 Mbps	1 Gbps	10 Gbps
2	1	0.004	0.038	0.375
3	1	0.004	0.038	0.375
4	2	0.007	0.074	0.744
5	2	0.007	0.074	0.744
6	3	0.011	0.113	1.125
7	3	0.011	0.113	1.125
8	3	0.011	0.113	1.125
9	4	0.015	0.149	1.488
10	5	0.019	0.188	1.875

Table 3 Maximum delay difference of AVPs and required buffer size for 90 nodes.

No. of AVPs	Delay difference [ms]	Required buffer size [MB] for varied link bandwidth		
		100 Mbps	1 Gbps	10 Gbps
2	1	0.004	0.038	0.375
3	1	0.004	0.038	0.375
4	1	0.004	0.038	0.375
5	1	0.004	0.038	0.375
6	2	0.007	0.074	0.744
7	2	0.007	0.074	0.744
8	3	0.011	0.113	1.125
9	3	0.011	0.113	1.125
10	4	0.015	0.149	1.488

As described in Section 3, the proposed network architecture can be constructed if the edge routers of the ingress and egress pair are changed without any change of existing LSR in the core. Furthermore, this method employs single parity check code using exclusive-or operation, which is one of the simplest and fastest algorithms to create and process FEC. Therefore, the overhead of the FEC operation can be considered to be small. Thus, this method

implements an advantage of 1+1 protection in BBS while minimizing the overheads of service costs such as redundant traffic and additional buffer at Egress. Therefore, the proposed method can provide reliable network architecture with no service outage for real-time premium traffic even when network failures occur.

5. 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 high priority requirement to find a solution to achieve 100% availability for them. 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 the proposed protection is highly reduced compared to conventional methods and very small. Therefore, it can be considered to be negligible. The proposed network architecture recovers the packet losses due to re-routing at egress and can provide a guaranteed QoS for real-time premium traffic. Also, the occupancy ratio of FEC traffic and the required buffer size at egress are very small and 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 future real-time applications.

It will be interesting to evaluate the proposed path protection in the real network using real-time traffic, as future work of this study.

References

1) Rosen, E., et al.: Multi Protocol Label Switching Architecture, IETF RFC 3031 (Jan. 2001).
2) Xiong, Y. and Mason, L.G.: Restoration strategies and spare capacity requirements in self-healing ATM networks, *IEEE/ACM Trans. Networking*, No.1, pp.98–110 (Feb. 1999).
3) Li, L., Buddhikot, M.M., Chekuri, C. and Guo, K.: Routing Bandwidth Guaranteed Paths with Local Restoration in Label Switched Networks, *Proc. IEEE ICNP* (2002).
4) Gamage, M., Hayasaka, M., Sugawara, S., Terada, M. and Miki, T.: Virtual Path Hopping to overcome Network Failures due to Control Plane Failures in Connection Oriented Networks, *Proc. APCC2004* (Aug. 2004).
5) Iannaccone, G., et al.: Analysis of link failures in a IP backbone, *Proc. Internet Measurement Workshop* (2002). http://www.icir.org/vern/imw-2002/imw2002-papers/202.pdf
6) Sharma, V., et al.: Framework for Multi-Protocol Label Switching (MPLS)-based Recovery, IETF RFC 3469 (Jan. 2003).
7) Aboul-Magd, O.: The Documentation of IANA assignments for Constraint-Based LSP setup using LDP (CR-LDP) Extensions for Automatic Switched Optical Network (ASON), IETF RFC 3475 (Mar. 2003).
8) Awduche, D., et al.: RSVP-TE: Extensions to RSVP for LSP Tunnels, IETF RFC 3209 (Dec. 2001).
9) Huang, C., Sharma, V., Owens, K. and Makam, S.: Building Reliable MPLS Networks Using a Path Protection Mechanism, *IEEE Communications Magazine*, pp.156–162 (Mar. 2002).
10) Rosenberg, J. and Schulzrinne, H.: An RTP Payload format for Generic Forward Error Correction, RFC 2733 (Dec. 1999).
11) Perkins, C.: RTP: Audio and Video for the Internet, Addison-Wesley (2003).
12) Nikolopoulos, S.D., Pitsillides, A. and Tipper, D.: Addressing Network Survivability Issues by Finding the K best Paths through a Trellis Graph, *Proc. IEEE INFOCOM* (1997).
13) Szviatovszki, B., Szentesi, A. and Juttner, A.: On the Effectiveness of Restoration Path Computation Methods. http//www.cs.elte.hu/~alpar/publications/proc/RestoPath.pdf
14) Guo, Y., Kuipers, F. and Mieghem, P.V.: Link-Disjoint Paths for Reliable QoS Routing. http://www.nas.its.tudelft.nl/people/Piet/papers/dimcra.pdf
15) Bejerano, Y., Breitbart, Y., Orda, A., Rastogi, R. and Sprintson, A.: Algorithms for Computing QoS paths with Restoration, *Proc. IEEE INFOCOM* (2003).
16) Liu, G., Yang, Y. and Lin, X.: Performance Evaluation of K Shortest Path Algorithms in MPLS Traffic Engineering, *IEICE Trans. Commun.*, Vol.E87-B, No.4, pp.1007–1010 (Apr. 2004).
17) Cormen, T.H., Leiserson, C.E., Rivest, R.L. and Stein, C.: Introduction to Algorithms, 2nd ed., Section 24.3: Dijkstra's algorithm, pp.595–601, MIT Press and McGraw-Hill (2001).
18) Katz, D., Kompella, K. and Yeung, D.: Traffic Engineering (TE) Extensions to OSPF Version 2, RFC 3630 (Sep. 2003).
19) Gamage, M., Hayasaka, M. and Miki, T.: 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, *Proc. QoS-IP 2005* (Feb. 2005).
20) Karol, M.J., Hluchyj, M.G. and Morgan, S.P.: Input versus output queueing on a space-division packet switch, *IEEE Trans. Commun.*, Vol.COM-35, No.12, pp.1347–1356 (Dec. 1987).
21) Bollobas, B.: Random Graphs, 2nd ed., Cambridge University Press (2001).

(Received December 15, 2006)
(Accepted September 3, 2007)
(Online version of this article can be found in the IPSJ Digital Courier, Vol.3, pp.779–787.)

Mitsuo Hayasaka received B.E. and M.E. degrees from the University of Electro-Communications, Tokyo, Japan in 2000 and 2002, respectively. He is currently a Ph.D. student at the University of Electro-Communications, Tokyo, Japan. His research interests involve QoS controls of real-time multimedia communications, and reliable network architecture. He is a member of IEEE, IEICE and IPSJ.

Tetsuya Miki received a B.E. degree from the University of Electro-Communications, Tokyo, Japan in 1965, M.E. and Ph.D. degrees from Tohoku University, Sendai, Japan in 1967 and 1970, respectively. He joined the Electrical Communication Laboratories of NTT in 1970, where he was engaged in the research and development of high-speed digital transmission systems using coaxial cable, fiber-optical transmission systems including initial WDM technologies, fiber-to-the-home systems, ATM systems, network management systems, and broadband network architecture. He is currently a Professor at the University of Electro-Communications, Tokyo, Japan, and is interested in photonic networks, community networks, access networks, and dependable networks. Currently a fellow member of the IEEE and IEICE, Prof. Miki also served as vice-president of the IEEE Communications Society in 1998 and 1999 and as vice-president of IEICE in 2003 and 2004.