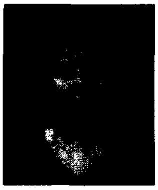
[12] T. Speakman, and L. Vicisano, Reliable Multicast Transport Building Block Generic Router Assist - Signalling Protocol Specification, IETF Internet Draft, July 2003.
[13] B.Cain, T.Speackman and D.Towsley, Generic Router Assit(GRA) Building Block-Motivation and Architecture, IETF Internet Draft, July 2001.
[14] Pingali, S., et al., A Comparison of Sender-initiated and receiver-initiated Reliable Multicast Protocols, SIGMETRICS 1994.
[15] Floyd, S., et al., A Reliable Multicast Framework for Light-weight Sessions and Application Level Framing, Proc. of ACM Sigcomm'95, pp.342-356, September 1995.
[16] B. N. Levine, S. Paul and J. J. Garica-Luna-Aceves, Organizing Multicast Receivers Deterministically According to Packet-Loss Correlation, In Proceeding of Sixth ACM International Multimedia Conference(ACM Multimedia 98), September 1998.
[17] B. N. Levine and J. J. Garcia-Luna-Aceves, A Comparison of Known Classes of Reliable Multicast Protocols, In Proceedings of International Conference on Network Protocol(ICNP'96), 1996.
[18] E.Kim, S.J.Koh, S. G. Kang and J. Choe, An ACK-Tree Creation Mechanism using Top-down scheme for Tree-based Reliable Multicast Transport Protocols, In Proceeding of International Conferencing on Internet Computing(IC2001),June 2001.
[19] S. McCanne, S.Folyd, NS(Network simulator), http://www-nrg.ee.lbl.gov/ns, 1995.

최 종 원

1984년 서울대학교 공과대학 컴퓨터공학과(학사). 1986년 서울대학교 컴퓨터공학과(석사). 1992년 미국 노스웨스턴대학교 EECS(박사). 1993년~현재 숙명여자대학교 정보과학부 교수. 관심분야는 인터넷 라우팅 및 멀티캐스트 프로토콜, 분산 알고리즘, 인터넷 응용



최 인 영

2000년 2월 강남대학교 이공대학 전자계산학과(학사). 2002년 2월 숙명여자대학교 컴퓨터과학(석사). 2002년 3월~2003년 5월 (주)에프아이디. 2003년 6월~현재 숙명여자대학교 컴퓨터통신연구실 연구원. 관심분야는 멀티캐스트 프로토콜, 센서네트워크, IPv6 기술

MPLS망에서 버퍼지연 문제가 발생하지 않는 무손실 Fast Rerouting 기법
(Packet Lossless Fast Rerouting Scheme without Buffer Delay Problem in MPLS Networks)

신상헌[†] 신해준[†] 김영탁[††]
(Sang-Heon Shin) (Hae-Joon Shin) (Young-Tak Kim)

요 약 본 논문에서는 MPLS(Multiprotocol Label Switching) 망에서 패킷 손실없이 장애를 복구하는 기존의 fast rerouting 기법 적용시 ingress 노드 버퍼에서 발생하는 누적 지연 문제를 해결하는 방안을 제안한다. 제안된 기법은 사용자 트래픽을 복구하기 위해서 사전에 설정된 대체 LSP(Label Switched Path)와 각 노드에 설치된 버퍼를 사용한다. Ingress 노드에서 발생하는 버퍼 지연 문제를 해결하기 위해서 본 논문에서는 두 가지 해결방안을 제안하였다. 첫 번째 방안은 대체 LSP가 보호되는 working LSP보다 일정기간동안 큰 대역폭을 가지도록 제어하는 것이다. 장애가 복구된 후, 대체 LSP에 설정된 대역폭은 working LSP와 동일하도록 재조정된다. 두 번째 방안은 세그먼트 기반의 장애복구 기법을 적용하여 보호되는 working LSP의 길이를 줄이는 것이다. 본 논문에서 제안한 방안들은 장애 복구후 ingress 노드에서 버퍼 지연 문제가 발생하지 않으며, ingress 노드에서 필요로 하는 버퍼의 크기도 기존 방안보다 작다는 장점을 가진다.

키워드 : 장애복구, MPLS, 경로 보호/복구, Fast rerouting, LSP, 버퍼 지연

Abstract In this paper, we propose a packet-lossless fast rerouting scheme at a link/node fault in MPLS (Multiprotocol Label Switching) network with minimized accumulated buffer delay problem at ingress node. The proposed scheme uses a predefined, alternative LSP (Label Switched Path) in order to restore user traffic. We propose two restoration approaches. In the first approach, an alternative LSP is initially allocated with more bandwidth than the protected working LSP during the failure recovery phase. After the failure recovery, the excessively allocated bandwidth of the alternative LSP is readjusted to the bandwidth of the working LSP. In the second approach, we reduce the length of protected working LSP by using segment-based restoration.

The proposed approaches have merits of (i) no buffer delay problem after failure recovery at ingress node, and (ii) the smaller required buffer size at the ingress node than the previous approach.

Key words : Fault recovery, MPLS, Path protection and restoration, Fast rerouting, Label Switched Path(LSP), Buffer delay

1. Introduction

MPLS has been developed as a key technology to enhance the reliability, manageability and overall QoS(Quality of Service) of core IP networks[1]. Recently, many restoration schemes have been proposed to restore link/node failures rapidly with pre-established backup paths in IP/MPLS over WDM (Wavelength Division Multiplexing) networks [2-5]. These proposals provide fast recovery capability using either optical layer protection or MPLS layer protection. The MPLS layer protection can achieve better network resource utilization than the optical layer protection although the optical layer protection can ensure fast recovery upon failure[2]. In order to ensure complete survivability, recovery schemes have to be deployed in both

---

† 비 회 원 : 영남대학교 정보통신공학과
shshin@yu.ac.kr
fishers@hitel.net
†† 종신회원 : 영남대학교 정보통신공학과 교수
ytkim@yu.ac.kr

논문접수 : 2003년 9월 29일
심사완료 : 2003년 11월 28일

layers[3]. Therefore, a reliable and efficient fault recovery mechanism at MPLS layer is required when there is a link/node failure.

Several schemes have been proposed for fast rerouting in MPLS network[4, 5]. An important issue in fast rerouting mechanisms is minimizing packet loss. Packet-lossless transmission is very important for loss-sensitive applications, such as highly interactive realtime remote control. Packet lossless restoration under a failure, however, usually requires an additional network resources(e.g. bandwidth or buffer) and may cause other problems. Thus, it is necessary to provide a stable and efficient fast rerouting mechanism without packet loss.

Haskin and Krishnan have proposed a fast rerouting scheme that uses an alternative LSP to provide a single failure protection[4]. The problem of Haskins mechanism is that packets suffer from a crank-back delay after the failure recovery, and packet loss/disordering during recovery period. RFR (Reliable and Fast rerouting) mechanism[5] eliminates both packet loss due to link/node failure and packet disordering during the restoration period. However, local buffer in each LSR(Label Switching Router) node is required in RFR, and especially a large buffer is required on the ingress node.

In RFR, the required buffer size of ingress LSR is proportional to the bandwidth of the protected working LSP and the length of path. The delay experienced by each packet at the ingress node buffer is proportional to the length of the crack-back path. If the transmission rate of user traffic is maintained continuously as in a CBR(Constant Bit Rate) traffic, the size of stored packet at ingress node buffer is not reduced even after a long time from the failure recovery. Therefore transmitted packets using the restored LSP will be suffered long end-to-end transfer delay time by the queuing delay in the ingress node buffer. Our simulation showed that this buffer delay is sometimes greater than 35ms in the U.S. sample network. We called it as *buffer delay problem* at ingress node.

In this paper, we propose a lossless fast rerouting scheme under a link/node failure without buffer delay problem. The proposed scheme uses a predefined, alternative LSP in order to restore traffic. We propose two restoration approaches: DRFR(Dynamic bandwidth RFR) and SRFR (Segment-based RFR). In DRFR, an alternative LSP has more bandwidth than the protected working LSP. After a failure recovery, the bandwidth of the alternative LSP is readjusted to the same bandwidth of the working LSP. In SRFR, it reduces the length of protected working LSP by using segment-based restoration. There is no buffer delay problem after failure recovery at ingress node even if the transmit rate of user traffic is CBR. Of course, we can integrated both approaches as an implementation.

The rest of this paper is organized as follows. In section 2, we briefly describe the related works for fast rerouting in MPLS network and analyze their characteristics. In section 3, we present the proposed schemes. In section 4, we evaluate and analyze the proposed packet lossless fast rerouting scheme, and finally we make conclusion in section 5.

2. Related Works

There are two basic methods for LSP recovery in MPLS network: (i) Rerouting and (ii) Fast rerouting(or protection switching)[6]. In rerouting, an alternative LSP is established on-demand, after a fault is occurred. Fast rerouting uses a pre-established alternative LSP that is prepared before the occurrence of a fault[6]. Comparing with rerouting, fast rerouting may rapidly restore service, but may have lower resource utilization because it has to preserve bandwidth of the backup path. For loss-sensitive time-critical applications, fast rerouting is essential because the packet loss due to an LSP failure is undesirable. Several fast rerouting mechanisms already have been proposed.

2.1 Fast Rerouting by Haskin

Haskin introduced a method for setting an alternative LSP with the objective to provide a single failure protection for quick restoration[4]. The traffic flowing through a working path from the source switch to the destination switch is protected by an alternative path. The alternative path consists of a parallel LSP from the source switch to the destination switch (we call it as *backup* LSP) and a reverse LSP from the destination switch to the source switch (we call it as *backward* LSP).

The main idea of Haskins method is to reverse traffic at the point of failure of the protected LSP back to the source switch of the protected LSP such that the traffic flow can then be redirected via a backup LSP. The major problem of Haskins mechanism is that packets suffer from a crank-back delay after failure recovery and packet loss/ disordering during recovery period[4].

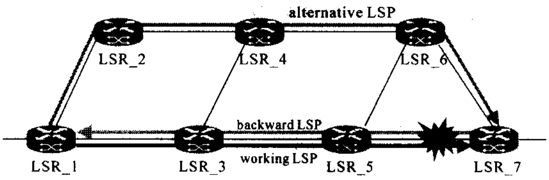
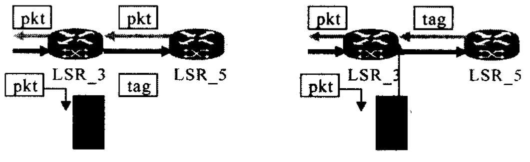


Figure 1 Haskins mechanism

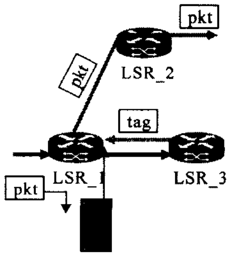
2.2 Reliable and Fast Rerouting(RFR)

RFR mechanism has been proposed to provide packet lossless path protection function against a link/node failure[5]. RFR is similar to the Haskins mechanism, but it uses local buffer in each LSR node to ensure packet lossless transmission even if failure occurs. And packet disordering during the restoration period is not occurred in RFR.

In RFR, each LSR along the protected path has a local buffer into which a copy of the incoming packet is saved while it is being forwarded along the protected path. When a fault is detected by an LSR, a switchover procedure is initiated and all packets in it's buffer are drained and sent back via the backward LSP. Any subsequent packet coming-in on the protected LSP is also sent back. As soon as each node of the backward LSP detects the first packet coming back, it forwards this packet along the backward LSP and stores the incoming packets in it's local buffer. Each LSR on the backward LSP successively sends back it's stored packets when it recognizes that the last packet is sent back from the downstream node. When all packets return to the ingress LSR and have been rerouted to the backup LSP, the restoration period is terminated[5]. Because in RFR each LSR requires a local buffer, it causes the buffer delay problem at the ingress node.



(a) Switchover (b) In intermediate LSR



(c) In ingress LSR

Figure 2 RFR mechanism

3. Dynamic bandwidth RFR and Segment-based RFR

We propose a packet lossless fast rerouting mechanism with a dynamically adjusted backup LSP. The goal of the proposed mechanism is to provide a packet lossless restoration function at a link/node failure and to solve the buffer delay problem at ingress node. We call the proposed mechanism as *DRFR(Dynamic bandwidth RFR)* and *SRFR(Segment-based RFR)*.

3.1 Dynamic bandwidth RFR(DRFR)

Packet storing at ingress LSR is unavoidable to ensure the path restoration without packet loss. The basic idea of DRFR is that a backup LSP is allowed to have excessive bandwidth than the protected (working) LSP during the failure recovery phase to prevent packets from being continuously accumulated at the ingress LSR after failure recovery. It means that a packet-drain speed is faster than the packet-storing speed at the ingress LSR buffer for a certain time period during the failure recovery phase. Therefore, the buffer will be emptied after the complete failure recovery and packets don't experience any further buffer delay.

Figure 3 shows the concept of DRFR. In DRFR, more bandwidth is assigned to the backup LSP than the protected LSP before a failure occurs as

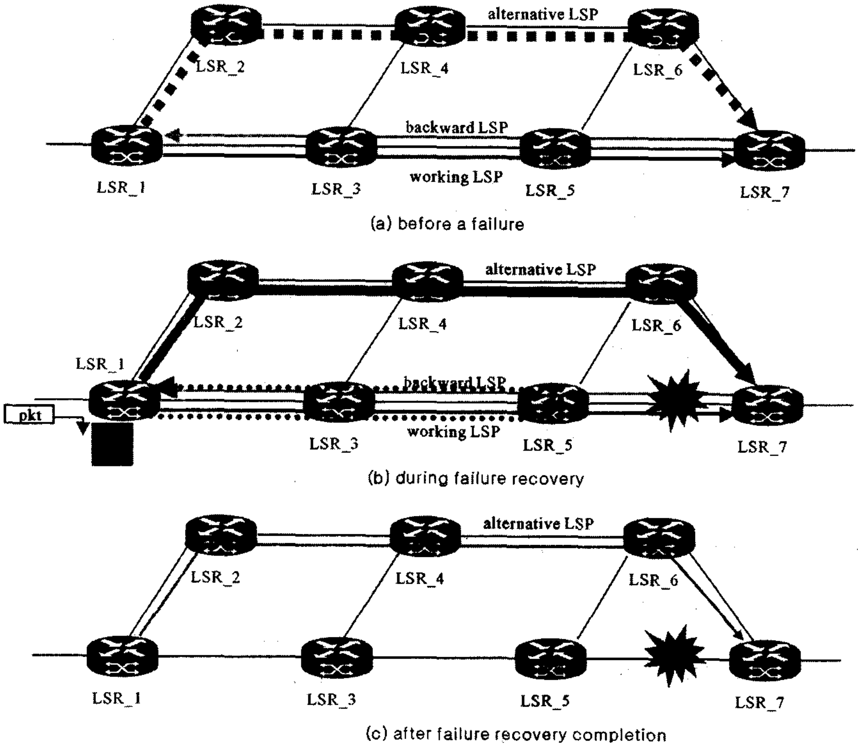


Figure 3 DRFR mechanism

in Figure 3(a). However, there is no need that the backward LSP has a more bandwidth than the protected LSP. If a failure occurs, packets are returned to the ingress LSR using the backward LSP similar to RFR. When the first packet coming back to the ingress LSR, the ingress LSR stops packet forwarding along the broken LSP and starts storing the incoming packets from the user. When all returned packets are rerouted, the packets stored in the ingress LSR buffer are forwarded via the backup LSP. Because the backup LSP has more bandwidth than the protected LSP, the ingress LSR buffer will be emptied rapidly even if the traffic rate from user is not reduced. From this time, the incoming packets from source are forwarded via backup LSP without buffering and the rerouting procedure is completed as in Figure 3(c).

After the completion of rerouting, the bandwidth of the backup LSP is readjusted because it temporarily has more bandwidth than the required bandwidth to transmit user traffic and it wastes network resource. In order to control the bandwidth, signaling message is sent from the ingress LSR to the egress LSR along the backup LSP, then the bandwidth of the backup LSP is adjusted to the same bandwidth of the protected LSP. In order to support this function, it is required to modify MPLS signaling protocol to adjust a bandwidth of the existing LSP. CR-LDP (Constraint-based routing Label Distribution Protocol)[7] or RSVP-TE(Resource ReSerVation Protocol Traffic Engineering)[8] is used as signaling protocol in MPLS network. Because CR-LDP and RSVP-TE have bandwidth negotiation concept and the bandwidth control scheme[9] with controlled bandwidth borrowing is studied currently, we expect that both of them can be easily applicable to DRFR. However, the specific signaling message format and procedure are beyond the scope of this paper.

3.2 Segment-based RFR(SRFR)

In RFR, the required buffer size of ingress LSR is proportional to the bandwidth of the protected working LSP and the length of path. The basic idea of SRFR is to reduce the length of protected path to avoid a very large buffer size required at ingress LSR. If only small size of buffer is used at ingress LSR, delay time experienced at buffer may not cause a serious problem.

Recently, several segment-based restoration schemes [10, 11] have been proposed. A segment restoration scheme subdivides an end-to-end working path into several segments. Each segment is assigned a protection domain for restoration after the working path is selected. It reduces the restoration time obviously compared with the path restoration scheme and lessens backup resource capacity compared with the link restoration scheme[11].

Basically, the fast rerouting and RFR both belong to the path restoration scheme. We applied a segment restoration scheme on RFR, and it makes SRFR as a segment-based restoration scheme. In SRFR, a length of working LSP to be protected by a segment is much shorter comparing with the total length of whole end-to-end LSP. Therefore, the required buffer size of the ingress LSR in each segment is much smaller than the ingress LSR buffer size for the whole end-to-end path. This is the reason why the buffer delay at a ingress LSR (in a segment) doesn't raise a serious problem, although a fault restoration procedure follows the principle of RFR.

Figure 4 shows the concept of SRFR. In Figure 4(a), the end-to-end whole LSP is not divided to segments. If a failure occurred, returned traffic should be buffered at ingress LSR. In Figure 4(b), the end-to-end LSP is divided into two segments. If a failure occurs, the returned traffic is buffered at the ingress LSR of segment 2. In this case, the volume of returned traffic to the ingress LSR of segment 2 is much less than Figure 4(a). In Figure 4(c), the end-to-end LSP is divided into three segments. If a failure occurs, the returned traffic is buffered at the ingress LSR of segment 3. The volume of returned traffic to the ingress LSR of segment 3 is less than in Figure 4(b). More segmentation enhance the performance(e.g. buffer size and delay) of SRFR, but it may increase the complexity of network management.

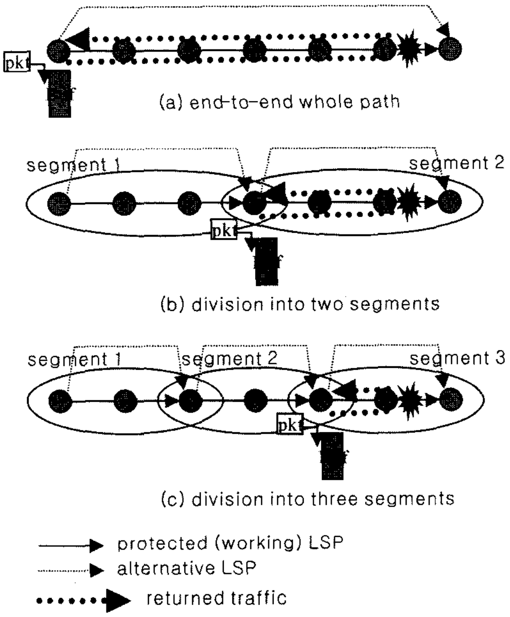


Figure 4 Principle of SRFR

It is possible that DRFR and SRFR are applied together for protecting LSP. We expect that the mixed version of DRFR and SRFR shows a better performance result, but it has more complex architecture than DRFR and SRFR.

4. Analysis and Result

4.1 Required buffer size

Local buffer in each LSR is required in RFR. In case of core LSR, the maximum size of this buffer needs to be about twice the number of packets that can circulate in a given link of the protected LSP. This buffer size is not too large to be implemented in each LSR and does not cause a serious problem. In case of edge LSR (or ingress LSR), the required buffer size is proportional to the bandwidth of the protected working LSP and the length of path. Therefore, the required buffer size in the ingress LSR is much larger than the core LSR. The required buffer size in ingress LSR is calculated as (1) [5]. $B_{ingress}$ is the buffer size in ingress LSR. T_{link} is link delay. Each link of real network has a different length and various T_{link} values exist. However, for convenience of derivation, it assumed that all links have a same T_{link}[5]. V_{T-lsp} is the source traffic rate. N is the number of nodes of the backward LSP excluding the ingress node. B_{W-lsp} is the LSP bandwidth.

$$B_{ingress} = 2 \times T_{link} \times V_{T\_lsp} \times \left(\frac{(N-1)V_{T\_lsp}}{B_{W\_lsp}} + 1 \right) \quad (1)$$

If user transmits traffic in CBR and the allocated bandwidth is fully used, the LSP bandwidth is same as the source traffic rate($V_{T-lsp}= B_{W-lsp}$). Thus, (2) is derived from (1).

$$B_{ingress} = 2 \times T_{link} \times B_{W\_lsp} \times N \quad (2)$$

Equation (2) depicts that the required buffer size at the ingress LSR is proportional to the bandwidth of protected working LSP and the length of path. Therefore, the required buffer size at ingress LSR increases according to the total bandwidth of the protected LSP. To show the required buffer size at ingress LSR, we use the U.S. sample network that has near mesh topology as shown in Figure 5. The distance of the longest link is 1,114 miles and the shortest link is 211 miles. In the U.S. sample network, one of the longest path is between Seattle and Miami. The required buffer size at ingress LSR according to LSP bandwidth is shown in Table 1.

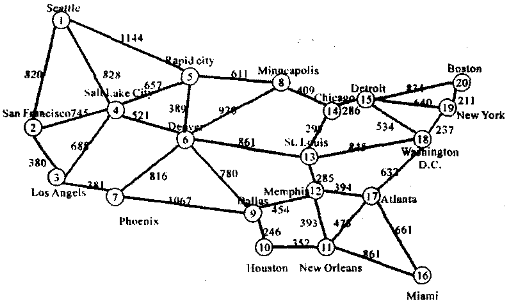


Figure 5 The U.S. sample network

Table 1 Buffer requirement at ingress node(RFR) for the Seattle-Miami LSP

LSP bandwidth (bps)	Buffer size (Bytes)
1.544M	6.8K
155M	685K
2.4G	10.96M
10G	45.11M
1T	4.4G

The required maximum buffer size at ingress LSR in DRFR is derived by (3) (when $V_{T-lsp}= B_{W-lsp}$). B_{B-lsp} is the bandwidth of backup LSP.

$$B_{DRFR} = 2 \times T_{link} \times B_{W\_lsp} \times \left(\frac{(N-1)B_{W\_lsp}}{B_{B\_lsp}} + 1 \right) \quad (3)$$

To compare with (2), let $B_{B-lsp}= kB_{W-lsp}$ (k is constant value).

$$B_{DRFR} = 2 \times T_{link} \times B_{W\_lsp} \times N \left(\frac{1}{k} - \frac{1}{N \times k} + \frac{1}{N} \right) \quad (4)$$

The required maximum buffer size at ingress LSR is reduced by factor of $(1/k-1/Nk+1/N)$ in DRFR. The reduction of buffer size is not a main goal of our work, but it is helpful. And note that buffer is required only during the rerouting procedure in DRFR, while in RFR buffer is used after the rerouting procedure.

The required buffer size at ingress LSR in SRFR is derived from (2). N_{seg} is the number of nodes of the backward LSP excluding the ingress node in a segment.

$$B_{SRFR} = 2 \times T_{link} \times B_{W\_lsp} \times N_{seg} \quad (5)$$

Because N_{seg} is much smaller than N, the required buffer size at ingress LSR in SRFR is smaller than RFR.

4.2 Delay Problem at ingress node

The main goal of our study is to solve the buffer delay problem at the ingress node and to provide a packet lossless restoration function under a link/node failure. In RFR, the delay which packets experience at ingress LSR buffer is calculated by (6).

$$D_{ingress} = \frac{B_{ingress}}{B_{W\_lsp}} = 2 \times T_{link} \times N \quad (6)$$

In DRFR, packets do not experience any delay at ingress LSR, because buffer is not used after the completion of fault recovery. There is no delay at ingress LSR($D_{DRFR}=0$).

In SRFR, the buffer delay at ingress LSR in a segment is formulated as (7).

$$D_{SRFR} = \frac{B_{SRFR}}{B_{W\_lsp}} = 2 \times T_{link} \times N_{seg} \quad (7)$$

4.3 Consideration for implementation

To implement the proposed scheme, a local buffer is required at each LSR node and MPLS signaling protocol should be modified. However, buffer requirements are within justifiable limites in RFR[5] and proposed schemes require much less buffer than RFR. And the proposed DRFR and SRFR require only limitted additional messages and control functions for fault recovery procedure. The proposed schemes don't require a big change in the framework of MPLS signaling protocol[7,8].

The DRFR requires the bandwidth modification of backup LSP to adjust the bandwidth of the backup LSP to the same bandwidth of the protected working LSP when the buffer of the ingress LSR is emptied. CR-LDP or RSVP-TE may be used as the signaling protocol in MPLS network. In CR-LDP, LSP modification is allowed when the LSP is already set up and active[13]. Bandwidth, traffic service class, route and setup/holding priorities of LSP can also be changed. In DRFR, the backup LSP is predefined before failure, and the backup LSP becomes an active status when we attempt to adjust the bandwidth. Therefore, bandwidth control function for DRFR can be implemented easily using CR-LDP. In RSVP-TE, the bandwidth modification of active LSP is not supported by standard yet. But, the bandwidth control scheme with bandwidth redistribution function is studied currently[9]. Redistribution of the resource(bandwidth) can be implemented by adding some messages without change of RSVP-TE signaling protocol architecture. We expect that both of CR-LDP and RSVP-TE can be easily applicable to DRFR.

In SRFR, it is necessary to divide a long end-to-end path into several sub-paths of short length. The partitioning is possible by logical path subdividing of each end-to-end paths, or by subdividing the topological network into several small subnetworks[11]. Network partitioning into several subnetworks has been researched from several years ago. A hierarchical connection management architecture is basic concept of network management system and the transport network is divided into several subnetworks with connection managers [14]. Therefore, we expect that an end-to-end working LSP can be easily divided into sub-paths by supporting of a hierarchical network management system.

4.4 Comparing of results

Figure 6 shows the compared result of the delay at ingress LSR buffer after fault recovery completion. For experiment, we used average length (946Km) of links in the U.S. sample network. Thus, the length of the protected LSP is expressed by the number of nodes that composed the LSP(e.g. the length of a path consists of 7 nodes is 5,676Km). And we supposed a worst case where a link failure is occurred at the last link of the protected LSP. SRFR-2 means that the end-to-end path is divided into two segments, and SRFR-3 means that the end-to-end path is divided into three segments.

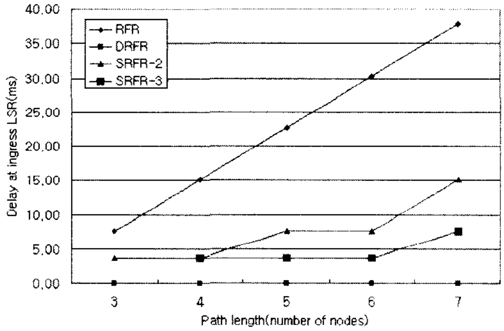


Figure 6 Delay comparison

In RFR, the delay at ingress LSR buffer increases linearly according to the path length of the protected LSP. When the number of nodes in the protected LSP is 3 (it means that the length of path is 1,892Km), the delay at ingress LSR is 7.57ms. When the number of nodes in the protected LSP is 7, the delay at ingress LSR is 37.84ms and it may injure seriously the quality of user service.

However, simulation result shows that delay of DRFR at ingress LSR is 0ms regardless of the number of nodes in the protected LSP. The reason is that buffer is not used after the completion of fault recovery unlikely with RFR. In DRFR, a packet-drain speed is faster than the packet-storing speed at the ingress LSR buffer during failure recovery procedure. Therefore, the buffer is empty after the complete failure recovery and packets don't experience any buffer delay at ingress LSR.

The quality of user service is not injured. This result satisfies our main objectives.

In SRFR, the delay at ingress LSR is much less than RFR, but is not zero. SRFR shows a performance between RFR and DRFR. And SRFR-3 shows better performance than SRFR-2. The reason is the segmentation of path. The end-to-end protected LSP is divided into two LSP segments in SRFR-2, and the same end-to-end LSP is divided into three LSP segments in SRFR-3. SRFR uses the same fault restoration procedure with RFR in the segmented LSP. Buffer is used similarly with RFR and packets experience buffer delay at ingress LSR after the completion of fault recovery. But, the length of protected LSP by a segment in SRFR-2 is the half of the whole end-to-end LSP and the length of protected LSP by a segment in SRFR-3 is 1/3 of the whole end-to-end LSP. Because the required buffer size of ingress LSR is proportional to the length of path, the used buffer size of ingress LSR in a segment is smaller than RFR and the buffer delay at a ingress LSR is much less. When the number of nodes in the whole end-to-end protected LSP is 7, the delay at the ingress LSR in SRFR-2 is 15.14ms, and the delay at the ingress LSR in SRFR-3 is 7.57ms. The delay is much less than RFR. The delay of SRFR-3 is less than SRFR-2. But, SRFR-3 has more complexity than SRFR-2, because more segments should be managed.

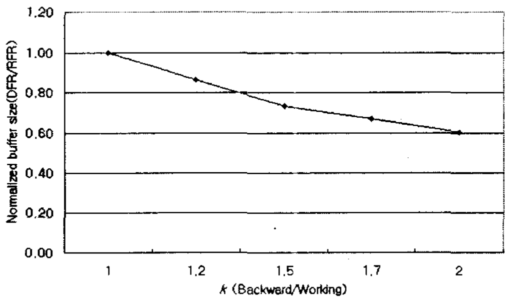


Figure 7 Ingress node buffer size ratio(DRFR/RFR)

Figure 7 shows the compared result of buffer size at ingress LSR between RFR and DRFR when the number of nodes in the backward LSP is 5. In Figure 7, the x-axis indicates a ratio of bandwidth between the backward LSP and the working LSP. It is same with k value of (4). When k is equal to 1, a backward LSP uses same bandwidth with a working LSP. When k is equal to 2, a backward LSP bandwidth is twice of a working LSP. The y-axis represents the normalized buffer size of DRFR compared with RFR.

In DRFR, the required maximum buffer size at ingress LSR is reduced according to the increased bandwidth of backward LSP. When k is 1, DRFR uses a same size of buffer with RFR at ingress LSR. The reason is that same time required with RFR for returning user traffic on the working LSP to ingress LSR when a backward LSP uses same bandwidth with a working LSP. If the bandwidth of backward LSP is larger than the working LSP, the required time for returning user traffic on working LSP to ingress LSR is reduced. It means that time for failure recovery is shorter than RFR and the volume of traffic to be buffered is less than RFR. When k is 1.5, DRFR requires a buffer only 73% of RFR during restoration period. When k is 2, DRFR requires a buffer only 60% of RFR during restoration period. This buffer is only used during the fault recovery phase. After the completion of fault recovery, buffer is not used in DRFR. Backward LSP bandwidth has a trade-off relationship with the required maximum buffer size at the ingress LSR.

5. Conclusion

This paper proposed a packet lossless fast rerouting scheme at a link/node fault in MPLS network. The goal of this paper is to solve the buffer delay problem that occurs in the existing schemes at ingress LSR when the user traffic rate is CBR. In this paper, we proposed two approaches: DRFR(Dynamic bandwidth RFR) and SRFR (Segment-based RFR). In DRFR, an alternative protection LSP has temporarily more bandwidth than the protected working LSP. After the failure recovery, the bandwidth of the alternative LSP is readjusted to the same bandwidth of the working LSP. In SRFR, it reduces the length of protected working LSP by using segment-based restoration. Through a series of analysis, we demonstrated that the proposed two approaches(DRFR and SRFR) do not cause that problem.

The extensions of MPLS signaling protocol are required in DRFR, but it shows more enhanced performance in aspect of delay than SRFR. SRFR does not require the modification of existing MPLS protocol architecture and has a shorter restoration period than DRFR and RFR. It is possible that the concept of DRFR and SRFR can be merged for a fast rerouting scheme to protect QoS-sensitive LSP.

References

[1] E. Rosen, A. Viswanathan and R. Callon, "Multiprotocol Label Switch Architeture," RFC 3031, January, 2001.

[2] Q.Zheng and G. Mohan, "An Efficient Dynamic Protection Scheme in Integrated IP/WDM Networks," ICC2003, 2003.

[3] Sophie De Maesschalck et al., "Intelligent Optical Networking for Multilayer Survivability," IEEE Communication Magazine, January 2002.

[4] D. Haskin and R. Krishnan, "A method for setting an alternative label switched paths to handle fast reroute," Internet Draft, July 2001.

[5] L. Hundessa and J. Domingo-Pascual, "Reliable and Fast Rerouting Mechanism for a Protected Label Switched Path," GlobeCom 2002, 2002.

[6] V. Sharma and F.Hellstrand, "Framework for MPLS-based Recovery," RFC3469, February 2003.

[7] B. Jamoussi et al., "Constraint-Based LSP Setup Using LDP," RFC 3212, January 2002.

[8] D. Awduche et al., "RSVP-TE: Extensions to RSVP for LSP tunnels," RFC 3209, December 2001.

[9] Chul Kim, Young-Tak Kim, "Controlled Bandwidth Borrowing with Extended RSVP-TE to Maximize Bandwidth Utilization," submitted to Journal of KICS, May 2003.

[10] Pin-Han Ho and Hussein. T. Mouftah, "A Framework for Service-Guaranteed Shared Protection in WDM Mesh Networks," IEEE Communication Magazine, February 2002.

[11] Hae-Joon Shin, Jae-Joon Jang, Young-Tak Kim, "Subnetwork-based Segment Restoration for fast fault Recovery in the MPLS network," Journal of KICS Vol. 27 No. 11, pp. 1046-1053, November 2002.

[12] D.A. Schupke, C.G. Gruber, A. Autenrieth, "Optimal Configuration of p-Cycles in WDM Networks," ICC2002, 2002.

[13] J. Ash et al., "LSP Modification Using CR-LDP," RFC 3214, January 2002.

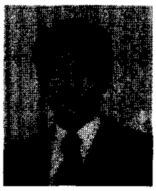
[14] Young-Tak Kim, "A Parallel & Distributed Routing Algorithm with a Hierarchical Connection Management Architecture for ATM/B-ISDN," GlobeCom98, 1998.

신상헌

1998년 2월 영남대학교 전자공학과 졸업 2000년 2월 영남대학교 전자공학과 공학석사. 2000년 3월~현재 영남대학교 정보통신공학과 박사과정. 관심분야는 Network Fault Restoration, Optical Network, NGI, MPLS/GMPLS

신해준

1997년 2월 영남대학교 전자공학과 졸업 1999년 2월 영남대학교 전자공학과 공학석사. 2003년 2월 영남대학교 정보통신공학과 공학박사. 관심분야는 Network Fault Restoration, High-speed Telecommunication Networking, NGI, MPLS/GMPLS, Optical Network



김영탁

1983년 2월 영남대학교 전자공학과 졸업 1985년 2월 한국과학기술원 전기 및 전자공학과 공학석사. 1990년 2월 한국과학기술원 전기 및 전자공학과 공학박사 1994년 8월 한국통신 통신망 연구소 선임연구원. 1994년 9월~현재 영남대학교 정보통신공학과 부교수. 관심분야는 High-speed Telecommunications Networking, Network Operation and Management, NGI, TINA, Active Networking Technologies