6

MULTIPLE FAULT TOLERANCE RECOVERY MECHANISMS

6.1 INTRODUCTION

The recent advances in fiber optic transmission and switched routing techniques dramatically facilitate the increment of link capacity and the provision of several classes of service over the same communication link. The introduction of MPLS as part of the Internet forwarding architecture to address the need of future IP-based Networks [RVC01][CDF+99] will contribute significantly, among other advantages, to the application of traffic engineering (TE) techniques and quality of service (QoS) provision mechanisms.

An adverse consequence of this increase in link capacity is a higher degree of complexity of network survivability. A link failure implies the rerouting of a huge amount of traffic with different QoS classes. In [IG00] the authors assure that fiber cable cuts are surprisingly frequent and serious.

For this reason, the need for rapid restoration mechanisms in an end-to-end label switching technology like MPLS obliged the research community to find different mechanisms to reroute traffic around a failure point in a fast, reliable and efficient way.

Protection schemes in MPLS networks can be classified as link protection, node protection, path protection and segment protection [ACE+02]. Path protection is used to protect a Label Switched Path (LSP) from failure at any point along its routed path except for failures that might occur at the ingress and egress Label Switching Routers (LSRs). The path protection scheme establishes an alternative LSP, either before or after failure detection. Segment protection only needs to protect the portion of the LSP that belongs to a defined segment protection domain. Segment protection will generally be faster than path protection because recovery generally occurs closer to the fault [ACE+02]. Link protection is carried out to protect the link between two adjacent nodes. Node protection addresses the protection of all links connected to the node. For the sake of better understanding of the following sections we will repeat some important concepts in the explanation.

There are two possibilities for establishing an alternative LSP in MPLS-based networks: i) Local repairs using alternative LSPs from point of failure and ii) Global repairs using ingress-to-egress alternative LSPs [OSMH01][Swa99][SH02].

The alternative LSP may be calculated on demand using dynamic restoration or may be pre-calculated and stored for use when the failure is detected using preplanned restoration[SH02] [OSMH01][HK00][CO99]. Usually the alternative LSP is established based on link protection or path protection techniques. The pre-established alternative LSP is better for critical traffic than the alternative LSP established on demand after the occurrence of failure [OSMH01] [HK00].

The dynamic restoration scheme searches, decides, and generates the alternative (backup) LSP dynamically upon failure. When a failure occurs nodes use message flooding to locate the backup routes that can bypass the failed routes. In order to

reduce the number of messages generated and to improve restoration speed, some algorithms restrict message broadcasting to a limited number of hops.

The preplanned algorithm permits many LSPs to be restored at the same time because only one message is generated per LSP. The preplanned restoration scheme preassigns an alternative LSP to each protected LSP before failure occurs. Several schemes have been proposed for selecting the best route(s) from several candidates based on different criteria [KL00][AWK+99][SWW01].

The key concept of the preplanned restoration scheme is the simplification of the restoration process that must be performed after a failure occurs; the goal is rapid and reliable restoration. One more advantage of the preplanned scheme is the ability to efficiently support explicit routing, which provides the basic mechanism for traffic engineering. The major drawback of preplanned alternative LSPs is that they allow less flexibility against multiple or unexpected points of failure. Furthermore, network resource utilization may not be optimal since alternative LSPs are pre-defined.

Our previous proposals for protection mechanisms in Chapter 3 and Chapter 4 assume a single link/node failure addressing basic performance metrics such as packet loss, packet reordering and average packet delay. In this chapter we propose a new protection mechanism for multiple link/node failures within a protected LSP. Multiple link failure on an LSP can be expected to occur during natural and human made disasters on the core networks [CKMO92] [Kuh97]. The cascade effect due to a problem in some part of the network can also be considered as multiple link failure on an LSP in the core networks [THS+94][RM01]. In this work we consider an LSP that goes through several MPLS autonomous systems with different policies or recovery mechanisms. We also consider each segment protection domain as an abstract of an autonomous system.

6.2 RELATED WORK

Published work about multiple link/node failure protection schemes for a particular protected path are practically limited to single link failures that accommodate more than one LSP. Note that any single node or link failure can produce several LSP failures if multiple LSPs have been routed over a failed link or through the node. We consider this a single link failure, but most of the proposals refer to this as multiple failures [CKMO92][KCO+90]. Most of the papers about protection mechanisms refer normally to a single node/link failure. Multiple failures within an LSP can be produced when more than one link, node, or combination of both node and link failure occur.

Using the notion of the Shared Risk Link Group (SRLG), the authors in [BS01] consider as a single failure when all links belonging to that SRLG fail simultaneously. In their proposal they consider multiple failures to be when a single link failure occurs in different LSPs of the MPLS domain (multiple failures in an MPLS domain). Moreover, the main objective of their proposal is to allow the sharing of bandwidth among backup LSPs for restoration mechanisms. The same multiple failures concept is presented in [CJVM01] with a complicated and costly (in terms of time and resources) algorithm called dynamic multilevel MPLS fault management. In this proposal the mechanism starts with global repair and changes to local repair according to the reported failure condition. The improved version of this proposal is presented in [MCSA]. This method periodically updates the network information, in contrast to computing the LSP dynamically on-line. The concept of QoS protection (QoSP) is introduced to select which restoration method is suitable to establish the backup path in the backup decision module (BDM). The most interesting observation in the reported results is that local repair and the reversing method are more suitable in most cases. These results agree with our approach for combining local, global and reversing methods.

In [KL01][KKL+02], the concept of sharing the backup path is used, like the previous proposal [BS01]. But unlike that one, the proposal can be used for multiple link

failure on a protected LSP. The disadvantage of this proposal is that it needs to set up (N-1) bypass tunnels to assure the protection of any combination of link failures on the protected LSP. Despite this, the proposal does not guard the protected LSP from multiple node failures.

In [OSMH01] the authors consider that transferring the protected traffic to the recovery path is enough to take care of multiple failures. This consideration also assumes that no fault can occur in the restored path (alternative LSP) during or after the recovery process.

Using the segment protection domain technique the traffic is rerouted close to the failure point, reducing blocking problems. Local rerouting using a stacking technique in an MPLS domain may produce a backhauling problem, i.e., failure recovery may cause the stream to traverse the same links twice in opposite directions [ADH94][MFB99]. In this case all protected LSP traffic around the failed link is rerouted by pushing the corresponding reroute LSP label onto the stack of labels for packets on the protected LSP without regard to their source and destination nodes. This may result in backhauling because packets can pass through the egress LSR to reach the node at the other end of the failure, and then back from this node to the egress LSR using the primary LSP segment (i.e., the LSP portion from point of failure to egress LSR) increasing the length of the protection path (see Figure 6.1). Note that in MPLS the LSRs see only the label carried by the packet on the top level of stack and this has only a local significance.

In our previous work in Chapter 3 and Chapter 4, we propose methods for path protection and restoration mechanisms using pre-established alternative LSPs setup at the same time as the protected LSP, giving a solution for problems like packet loss, re-ordering and packet delay, which take place during a link/node failure. In this chapter we focus on handling multiple failures in a protected LSP. The motivation of this study is to overcome multiple failure in a protected LSP. Here we propose a new mechanism able to handle a single failure based on Segment Protection Domain

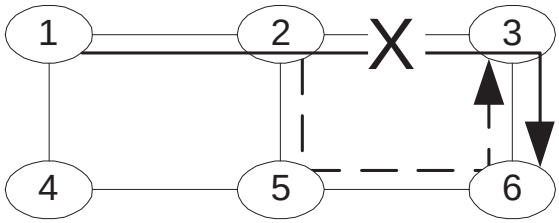

Figure 6.1 Backhauling problem. Ingress LSR is node 1, egress LSR is node 6, protected LSP: 1-2-3-6 (solid line), Local repair LSP (tunnel) for link failure 2-3 is: 2-5-6-3 (dashed line), protection LSP is: 1-2-5-6-3-6, and the arrows indicate the returning direction of the traffic

(SPD), local and global repairing methods; and, an extension of that mechanism to cope with multiple failures on the protected LSP in the MPLS network.

6.3 DESCRIPTION OF THE PROPOSED MECHANISM FOR SINGLE FAILURE

A protection domain is defined as the set of LSRs over which a working path and its corresponding alternative path are routed. Thus, a protection domain is bounded by the ingress and egress LSRs of the domain. The segment protection domain (SPD) is when a protection domain is partitioned into multiple protection domains, where failures are solved within that segment domain. In other words, the entire MPLS domain is the sum of many MPLS segment protection domains. SPDs may be established according to network administration policies, by an autonomous system. The SPD in this chapter is an abstraction of an MPLS autonomous system. In cases where an LSP traverses multiple protection domains, a protection mechanism within a domain only needs to protect the segment of the LSP that lies within the segment protection domain (SPD).

As stated in the former proposals (Chapter 3,4), the capacity reserved for the pre-planned alternative LSPs may be used by low priority LSPs with the caution that any low priority LSPs routed over this link will be preempted if the resource is needed by a high priority LSP as a result of a failure in the protected LSP.

The combination of path protection with segment protection and local repair activation is proposed in this chapter as a solution for multiple fault protection in a protected LSP, and single failures benefit from this proposal as well, in terms of full restoration speed.

In this proposal we combine the main benefits of segment protection (i.e., it is usually faster than path protection because recovery generally occurs closer to the fault) with the benefits of path protection to establish the optimal alternative path from ingress-to-egress in the entire MPLS network domain.

Another advantage of the segment protection scheme is related to blocking problems. Suppose that the failure occurs in a path used by clients with restricted service level agreements (SLA) (i.e., rigorous QoS demands). If the restoration/protection mechanism tries to reroute these important flows to the previously established alternative LSPs far away from the location of the failure, this can produce blocking problems in the other nodes (LSRs), which have not been involved in the failure.

For simplicity in the following example we consider only link failures. However, our proposal can also be used for node failure restoration without any additional modification.

In Figure 6.2 the MPLS domain is divided into three SPDs. Although Figure 6.2 seems to be a simple network topology, it represents the abstraction of a much more complicated concatenation of autonomous systems (AS) represented as segment protection domains (SPD). Note that each link in the figure may traverse one or more LSR, which are not shown in the figure. Border LSRs are in charge of rerouting in case of failure.

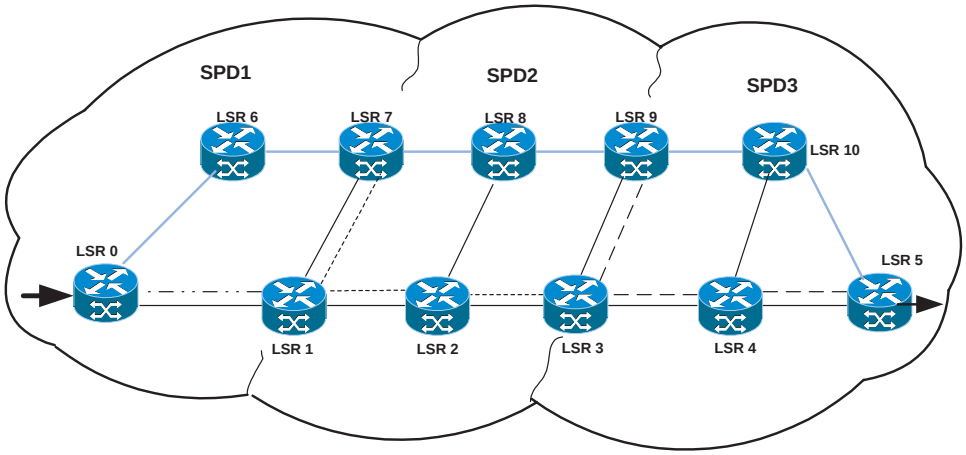

Figure 6.2 MPLS domain

We establish the primary LSP, and using explicit routing we set up the backward and alternative LSPs for path protection in each segment protection domain. The concatenation of the protected LSPs and backward LSPs for the SPDs makes the protected LSP and backward LSP for the entire MPLS domain respectively. The alternative path for the entire MPLS domain is made by concatenation of some portions of SPDs alternative LSPs.

A protection domain is denoted by specifying the protected LSP and the alternative LSP (protected LSP, alternative LSP)[OSMH01]. Using this definition and notation the entire MPLS protection domain (MPD) and all paths in Figure 6.2 are represented as follows.

Ingress LSR 0, Egress LSR 5.

Protected LSP (Primary LSP): the set of LSRs 0-1-2-3-4-5 (solid lines)

Preplanned Alternative LSP: the set of LSRs 0-6-7-8-9-10-5 (dim lines)

MPLS protection domain (MPD): (0-1-2-3-4-5, 0-6-7-8-9-10-5)

Segment Protection Domain 1: (0-1, 0-6-7-1)

Segment Protection Domain 2: (1-2-3, 1-7-8-9-3)

Segment Protection Domain 3: (3-4-5, 3-9-10-5)

Backward LSP for SPD1: the set of LSRs 1-0 (dash-dotted line)

Backward LSP for SPD2: the set of LSRs 3-2-1 (dotted lines)

Backward LSP for SPD3: the set of LSRs 5-4-3 (dashed lines)

During the recovery process the protection LSP is formed by concatenation of the following two portions: the backward LSP starting from the LSR that detects the failure (alert LSR), and the preplanned alternative protection LSP. Note that the use of the backward LSP for protected traffic is transitory (i.e., only during the recovery period). It is used to transport the packets routed on the faulty LSP from the LSR that detects the fault to the LSR responsible for redirecting this traffic. This minimizes packet losses.

Within a segment protection domain any kind of protection technique may be applied independent of other segment domains.

To illustrate the mechanism let us consider the segment protection domain1 (SPD1) in Figure 6.2. Assume a link failure between LSR0 and LSR1. If the link protection scheme is applied the recovery path for entire SPD1 will be formed by the set of LSRs 0-6-7-1. If the path protection scheme is applied, the recovery path for entire SPD1 is formed also by the same LSRs 0-6-7-1.

We apply the same approaches to segment protection domain2 (SPD2) for a link failure between LSR1 and LSR2. In case of link protection, the recovery path for the entire SPD2 (i.e., link protection plus the remaining path segment within SPD2) will

be formed by the set of LSRs 1-7-8-2-3. In case of path protection, the recovery path for entire SPD2 will be formed by the set of LSRs 1-7-8-9-3.

In the case of SPD3 for a link failure between LSR3 and LSR4, applying the link protection scheme the recovery path for the entire segment domain will be formed by the set of LSRs 3-9-10-4-5, while for the path protection scheme the result is the set of LSRs 3-9-10-5. In this case the path protection scheme provides a shorter recovery path than link protection.

As we stated before, our proposal combines the path protection scheme with the segment protection scheme, plus local repair techniques using the preplanned alternative LSP for protected LSPs in the entire MPLS domain. Once the preplanned alternative LSP for entire MPLS domain is setup, the segment protection for each SPD works in combination with this preplanned alternative LSP. This is possible because the alternative path for the entire MPLS domain is made by concatenation of some portions of SPD alternative paths. The first intersection point for both protections (i.e., the path protection for the entire MPLS domain and each segment protection domain) will be the merging point of the traffic rerouted by each SPD into the preplanned alternative LSP. This scheme uses link or path protection within the SPD to forward the packets to the egress LSR (LSR5) of the entire MPLS domain instead of forwarding to the corresponding segment domain egress LSR.

Let us apply the proposal to the previous example, Figure 6.2. If the link between LSR0 and LSR1 fails, the LSR0 reroutes the traffic using the alternative path of SPD1. The first intersection point for the alternative path of SPD1 (0-6-7-1) and the preplanned alternative path for the entire MPLS domain (0-6-7-8-9-10-5) is LSR0. From this merging point the traffic rerouted by SPD1 uses the preplanned alternative LSP. Then, the recovery path for the entire MPLS domain will be formed by LSRs 0-6-7-8-9-10-5. For a failure on link LSR1-LSR2 in SPD2, using the same principle, the first intersection between (1-7-8–9-3) and (0-6-7-8-9-10-5) is LSR7. Then, the recovery path for the entire MPLS domain is formed by LSRs 0-1-7-8-9-10-5. Finally for failure on link LSR3-LSR4 in SPD3, the alternative paths (3-9-10-5) and (0-6-7-

8-9-10-5) coincide on LSR9, and the recovery path will be formed by the set of LSRs 0-1-2-3-9-10-5 (see Table 6.1).

Faulty link	Link protection	Path protection within SPD	Proposal
LSR0-LSR1 in SPD1	0-6-7-1-2-3-4-5 7 links	0-6-7-1-2-3-4-5 7 links	0-6-7-8-9-10-5 6 links
LSR1-LSR2 in SPD2	0-1-7-8-2-3-4-5 7 links	0-1-7-8-9-3-4-5 7 links	0-1-7-8-9-10-5 6 links
LSR3-LSR4 in SPD3	0-1-2-3-9-10-4-5 7 links	0-1-2-3-9-10-5 6 links	0-1-2-3-9-10-5 6 links

Table 6.1 Comparison of restoration path length for single failure for MPLS protection domain (from ingress LSR0 to egress LSR5)

In Figure 6.2, the original end-to-end protected LSP length is 5 links (0-1-2-3-4-5). In Table 6.1, we present the comparison of the recovery path length from the ingress LSR to the egress LSR for single failures. Our proposal provides a shorter recovery path length compared with other approaches. The approach of applying segment protection with global path protection is better than applying segment protection or path protection separately. Moreover, as pointed out by numerous research papers, usually local repair may lead to the use of a non-optimal alternative LSP compared to the possible alternative LSP which can be established from the ingress LSR to egress LSR (Table 2.1). But, using our proposal we reduce the possibility of establishing non-optimal alternative LSPs from the point of failure to the egress LSR because we merge the packets rerouted to the alternative LSP (made by the local repair decision) into the preplanned alternative LSP (calculated by global repair). The use of this label merging technique [RVC01] allows the proposed scheme to avoid the backhauling problem.

6.4 DESCRIPTION OF THE PROPOSED MECHANISM FOR MULTIPLE FAILURES ON AN LSP

In the previous section we described the use of our proposal for a single failure. Here we present the explanation of the proposal for multiple failures. Multiple failures are considered to be the result of multiple single failures in the protected LSP. Applying the same principle used for single failures described in the previous section we are able to extend single failure protection to handle multiple failure protection.

According to the proposal in [OSMH01], the authors offer the possibility of handling multiple failures in an LSP by redirecting traffic from failed LSPs to the alternative LSP, but this approach has the disadvantage of excessive packet losses (i.e., all traffic on the protected path between the ingress node and the far extreme of the failed node/link). The node next to the failed link signals the event to the upstream nodes. Upon the reception of the failure signal the ingress node reroutes the traffic over the pre-established alternative LSP.

To illustrate how our proposal works, we will compare its behavior with Makam's and Haskin's. As an example, we consider a multiple failure on the protected LSP (LSR0-LSR1-LSR2-LSR3-LSR4-LSR5) as a combination of 3 link failures: LSR4-LSR5, LSR2-LSR3 and LSR0-LSR1.

Makam's proposal loses all the packets circulating on the LSP, and the ingress LSR (LSR0) redirects the incoming traffic to the alternative LSP. The same happens with Haskin's proposal in this condition. But, if we consider only the failures between LSR4-LSR5 and LSR2-LSR3 for the MPLS domain formed only by SPD2 and SPD3 (i.e., the LSP formed from LSR1 to LSR5), Haskin's proposal at least recovers packets traversing on the link LSR1- LSR2, while Makam's proposal loses all packets on the LSP plus additional packets sent to the already failed LSP before the notification message reaches the ingress LSR (LSR1).

In our proposal, if RFR is not used we lose only the packets on the failed link because the ingress LSRs in each segment protection domain (LSR0, LSR1 and LSR3) redirect the traffic to the alternative LSP. When link LSR4-LSR5 fails, LSR3 (being the ingress LSR of SPD3) redirects traffic through LSR3-LSR9-LSR10-LSR5. When link LSR2-LSR3 fails, LSR1 redirects traffic to the alternative LSP for SPD2 (LSR1-LSR7-LSR8-LSR9-LSR3). Furthermore, if we apply the proposal presented in Chapter 4 (Reliable and Fast Rerouting), we do not lose any packets.

Note that we assume that the multiple failures are produced at the same time. It is evident this is not the worst condition. The worst condition is produced when the sequence of link failure is LSR4-LSR5, and then LSR2-LSR3 and finally LSR0-LSR1. More precisely, the worst condition occurs as follows. Once the link LSR4-LSR5 has failed and the notification message in case of Makam's scheme or the reverse packet in case of Haskin's proposal is approaching LSR2, just before it reaches LSR2 the link LSR2-LSR3 fails.

Other situations are an intermediate of these extreme conditions. For example, if the link LSR0-LSR1 fails first, and link LSR4-LSR5 fails later, both Haskin's and Makam's schemes behave equally. They lose all packets traveling from LSR1 to LSR4 in addition to the packet losses on the faulty links.

Based on the segment protection approach, if we try to protect the entire protected path (i.e., from LSR0 to LSR5) from a link failure in each SPD (i.e., multiple link failure within the protected path) the recovery path length increases with (repeated link or path protection) within SPDs.

One important observation is that the recovery path length always increases when the link protection scheme is used. On the other hand, the path protection scheme does not always increase the length of the recovery path. The length of the protection path is considered to be a main quantitative measure of the quality of a protection scheme [BR02]. The protection path length can be used as an indication of the delay that the rerouted traffic will experience after a link failure. In addition to the delay,

Faulty links	Link protection	Path protection	Proposal
1-2 and 3-4 in SPD2 and SPD3	0-1-7-8-2-3-9-10-4-5 9 links	0-1-7-8-9-3-9-10-5 8 links	0-1-7-8-9-10-5 6 links
0-1, 1-2 and 3-4 in SPD1, SPD2 and SPD3	0-6-7-1-7-8-2-3-9-10-4-5 11 links	0-6-7-1-7-8-9-3-9-10-5 10 links	0-6-7-8-9-10-5 6 links

Table 6.2 Comparison of restoration path length for multiple failures for MPLS protection domain (from ingress LSR0 to egress LSR5)

the length of the protection path reflects the amount of resources required to protect an LSP.

In Table 6.2 we summarize the restoration path length used by link protection, path protection and our proposal for the entire MPLS domain (end-to-end) for multiple failures based on the network scenario of Figure 6.2. We can observe that our proposal needs only 6 links for a recovery path, performing better than separate link and path protection approaches. The protected LSP length is equal to 5 links. Note that the fact that the proposal recovery path length is one link more than the protected link length is not due to the proposed mechanism. It is simply because the possible alternative LSP found to protect the original protected LSP is one link more than the original (i.e., 6 links).

6.5 SIMULATIONS AND RESULTS

The objective of this simulation is to compare numerically the behavior of this proposal with the reference proposals: Haskin's and Makam's.

The MNS source code was modified to simulate these mechanisms: Haskin's [HK00], Makam's [OSMH01] and our proposal. The failures of links between LSR4-LSR5 and

LSR0-LSR1 are used as the separated single link failures. For multiple failures we use the failures between LSR4-LSR5 and LSR2-LSR3. The simulation scenario is the one shown in Figure 6.2.

We use CBR traffic with the following characteristics: packet size = 1600 bits and source rate= 400Kbps. In all cases path protection is applied for the entire MPLS domain, thus satisfying the requirement of Haskin's and Makam's proposals.

We measured packet loss, packet re-ordering and repeated packets at the egress node (LSR5) for a single failure, multiple failures with path protection, and multiple failures with combined path and segment protection. The figures show all simulation results: packets lost and disordered during the recovery period.

In reference to the simulation results behavior, we use 100% packet loss and packet re-ordering in the the LSR4-LSR5 link failure situation because in this situation there is maximum packet loss for Makam's scheme and maximum packet disorder for Haskin's scheme in the simulation results. The results presented in the figures are proportionally identical when the LSP length, the LSP bandwidth, the packet size and the source rate are varied. Note that both Haskin's and Makam's proposals use path protection schemes establishing the preplanned alternative LSP from the ingress LSR (LSR0).

In the following figures the proposal includes RFR with buffering at the LSR in order to avoid packet losses. It is labelled as "proposal +".

Figure 6.3 shows the results for a single failure without segment protection. Makam's scheme [OSMH01] uses a notification message to the ingress node after a failure to reroute traffic from the ingress LSR to a previously established alternative LSP, resulting in high packet loss and no packet re-ordering . Whereas, Haskin's [HK00] returns packets from the faulty point to the ingress LSR and there reroutes them to the alternative LSP together with the incoming traffic, resulting in minimum packet loss, and maximum packet disorder proportional to the distance (number of LSR) between the ingress LSR and alert LSR.

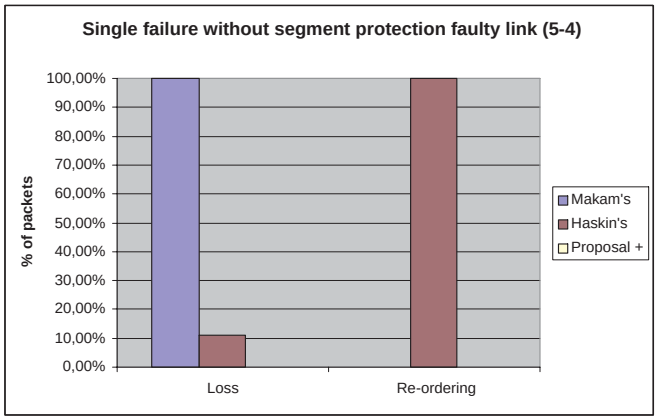

Figure 6.3 Performance comparison results during recovery period for packet losses, packet disorder

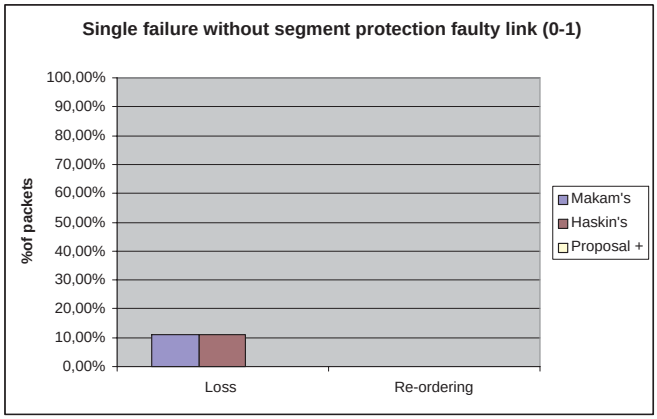

Figure 6.4 Performance comparison results during recovery period for packet losses, packet disorder

Figure 6.4 shows the results for a single failure without segment protection (failed link LSR0-LSR1). Both Haskin's and Makam's behave the same (they lose only the packets on the failed link). Note that in both figures (Figure 6.3 and Figure 6.4) our proposal does not experience packet loss or disorder.

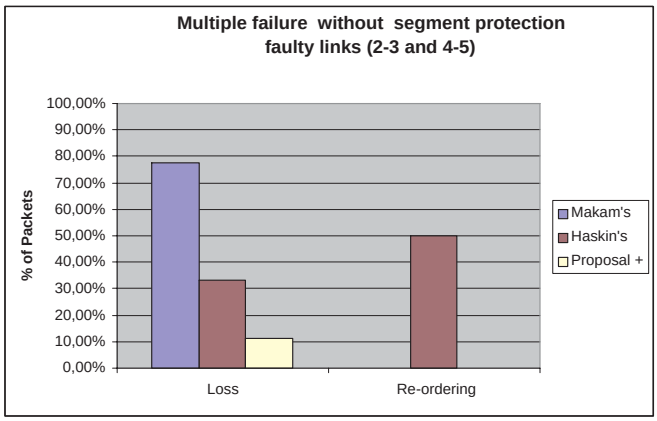

Figure 6.5 Performance comparison results during recovery period for packet losses, packet disorder

In Figure 6.5 the results for multiple failure without segment protection (failed links LSR2-LSR3 and LSR4-LSR5) are depicted. The packet loss for Makam's scheme decreases with respect to the result in Figure 6.3 and increases with respect to the result in Figure 6.4 because the point of failure is closer to and farther from the ingress node (responsible to redirect the traffic) respectively. This is translated as less and more time that the notification signal takes to reach the ingress LSR (LSR0).

The packet loss increases for Haskin's. This is due to the fact that the LSP segment between the two extreme points of failure in the protected LSP becomes disconnected. Haskin's scheme recovers the packets traversing in the portion of the LSP between the ingress node and the point of failure (LSR0-LSR1-LSR2), and loses packets on the links formed by LSR2-LSR3-LSR4-LSR5. In this case our proposal begins to lose packets. Although we include the RFR proposal, we recover only the lost packets on the links formed by LSR2-LSR3 and LSR3-LSR4 from the LSR2 local buffer. We lose packets circulating on link formed by LSR4-LSR5. This is because we specified the buffer size equivalent to the packets circulating in two downstream links. Note that we can increase the buffer size to avoid the packet losses.

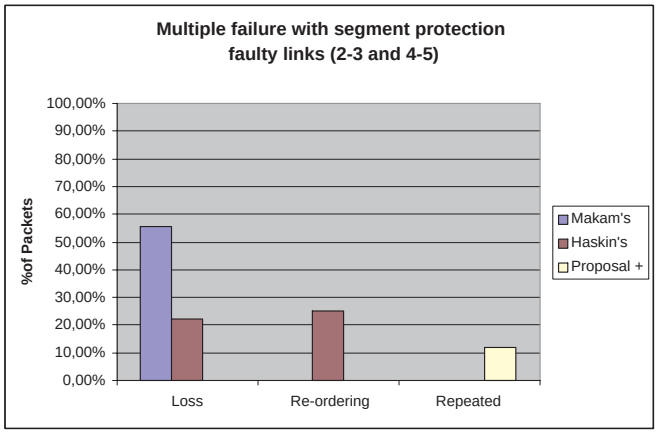

Figure 6.6 Performance comparison results during recovery period for packet losses, packet disorder and repeated packets

Figure 6.6 shows the results for multiple failures applying the combination of path protection with segment protection. The packet loss for Makam's scheme as well as the packet re-ordering for Haskin's experience an important reduction, improving the main drawback of each scheme. This is because the rerouting of traffic is performed close to the failure points, improving their performance. Our proposal using RFR performs better than the others by avoiding both packet loss and packet disorder.

We did extensive simulation with different scenarios and traffic patterns and the results show basically the same behavior. Results presented in the chapter are representative of the behavior of the proposal. Based on these results we believe that the combination of path and segment protection with the local repair method is the best option as a protection mechanism against multiple/single failure for protected traffic on MPLS-based networks. The most complex element of our proposed scheme is to set up all of the alternative LSPs required.

6.6 SUMMARY

The proposed mechanism covers many of the aspects of IP-QoS provision. The proposal provides protection from multiple link/node failure in a protected LSP on an MPLS-based network using a combination of path protection with segment protection and local repair. Rerouting of traffic is performed close to the failure point, increasing the restoration speed and providing a significant reduction of the LSP blocking problem. At the same time it provides better recovery (protection) in terms of path length. As a result, we achieve better network resource utilization and shorter delays for rerouted traffic.

The criteria for partitioning an MPLS domain into several segment protection domains may be established according network administration policies.

The main open issue is how to compute the alternative LSP for each segment protection domain (SPD), and then to identify the merging point in order to select the shortest path. The routing algorithm must establish a global protected LSP and a global alternative LSP for the entire MPLS domain. For each SPD, the algorithm will also establish a global alternative with a merge point with the global alternative for the entire MPLS domain. Several of the proposed routing algorithms might be adopted to find all possible LSPs.