Optimal and Guaranteed Alternative LSP for Multiple Failures

Lemma Hundessa and Jordi Domingo-Pascual
Departament d'Arquitectura de Computadors
Universitat Politècnica de Catalunya (UPC)
C/ Jordi Girona 1-3, 08034. Barcelona, Spain
{hundessa, jordid} @ac.upc.es

Abstract—**Fast rerouting mechanisms are being studied in order to provide fault tolerance for LSP in an MPLS network in case of node or link failure. For QoS provision protected LSP are handled apart from non-protected LSP. Rerouting mechanisms when applied on protected LSP must take into account QoS requirements. This paper presents a mechanism that is able to handle multiple failures along an LSP while using an optimal alternative LSP. The rerouting decision is taken close to the point of failure reducing the restoration time. The use of pre-established alternative LSP also reduces the restoration time and avoids blocking when looking for an alternative path. The proposal is based on a hybrid approach of segment repair and path repair and provides a new alternative LSP using dynamic rerouting once the protected one has been rerouted. In this way there is always an alternative LSP for each protected LSP. The over all performance (recovery time, end-to-end delay, packet losses, and network resource utilization) is compared with existing protection mechanisms by simulation. The proposed hybrid approach, Optimal and Guaranteed Alternative Path (OGAP), avoids the possible use of a non-optimal alternative LSP to reroute the protected traffic and provides the flexibility of alternative route selection and setup as well as better resource utilization. Moreover, our proposal guarantees at least one alternative LSP at any time for the traffic on the protected LSP.**

Keywords: MPLS, Label Switched Path (LSP), QoS, Path protection, Segment protection, Alternative LSP, Multiple failure.

I. 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 needs of future IP-based Networks [1],[2] 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 [3] 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 out 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 [4]. Segment protection will generally be faster than path protection because recovery generally occurs closer to the fault [4].

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 [5], [6],[7],[8]. 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 [6],[7]. Several schemes have been proposed for selecting the best route(s) from several candidates based on different criteria [9],[10],[11].

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 [12] and [13] assume a single link/node failure addressing basic performance metrics such as packet loss, packet reordering and average packet delay. In this paper 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 [14],[15]. 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 [16],[17]. 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.

II. 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 [14],[18]. 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.

In [19],[20], the concept of sharing the backup path is used. 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, being N the number of nodes of the protected LSP. Despite this, the proposal does not preserve the protected LSP from multiple node failures.

In [6] the authors consider that transferring the protected traffic to the recovery path is enough to take care of multiple failures. This

0-7803-8784-8/$20.00 (C) 2004 IEEE

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 [21],[22]. 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, increasing the length of the protection path. 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 works [12],[13], 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 the recovery period of time. In this proposal we focus on handling multiple failures in a protected LSP. Here we propose a new mechanism able to handle a single failure based on Segment Protection Domain (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.

At the same time, we observe that the previously established alternative path may not be the optimal after the link/node failure. Because, it was setup based on the network information at moment of the protected LSP was established. As a result, this decision does not take in to consideration the network information changes. Moreover, after the restoration process, the restored LSP becomes unprotected.

The motivation of this paper is to overcome these problems and propose a new mechanism able:

i) To handle multiple faults in the MPLS network with failure/congestion situation,

ii) To establish the updated optimal alternative path and

iii) To maintain always at least an alternative LSP at any time for the protected LSP.

III. Description of the Proposed Mechanism for Single/Multiple 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. SPDs may be established according to network administration policies. The SPD in this proposal 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).

The combination of path protection with segment protection and local repair activation is proposed in this paper 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 strict 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 Fig. 1 the MPLS domain is divided into three SPDs. Although Fig. 1 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.

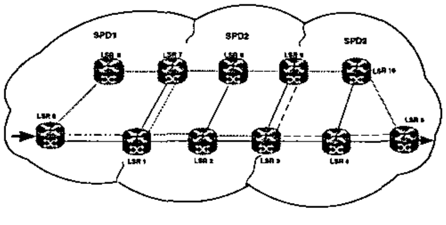

Fig. 1. MPLS domain

We establish the primary LSP, and 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, the backward LSP and the alternative LSP (protected LSP, backward LSP, alternative LSP). Using this definition and notation the entire MPLS protection domain (MPD) and all paths in Fig. 1 are represented as follows. Ingress LSR 0, Egress LSR 5.

Table I summarizes all the LSP established (protected, backward, alternative).

	SPD1	SPD2	SPD3	MPD
Protected LSPs	0-1	1-2-3	3-4-5	0-1-2-3-4-5 solid line
Backward LSPs	1-0 dash-dot. line	3-2-1 dotted line	5-4-3 dashed line	5-4-3-2-1-0
Alternative LSPs	0-6-7-1	1-7-8-9-3	3-9-10-5	0-6-7-8-9-10-5 dim line

TABLE I

MPLS protection domain (MPD), Segment Protection Domain 1,2,3 (SPD1,SPD2,SPD3)

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.

To illustrate the mechanism let us consider the segment protection domain1 (SPD1) in Fig. 1. 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 SPD2 with a link failure between LSR1-2, The recovery path results for link and path protection are LSRS 1-7-8-2-3 and LSRs 1-7-8-9-3 respectively. For SPD3 for a link failures between LSRs 3-4. The recovery path results for link and path protection are 3-9-10-4-5 and 3-9-10-5.

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, Fig. 1. 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 II).

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 II

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

In Fig. 1, the original end-to-end protected LSP length is 5 links (0-1-2-3-4-5). In Table II, 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. 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 [1] allows the proposed scheme to avoid the backhauling problem.

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.

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 (LSRs 0-1-2-3-4-5) 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, 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 LSRs 3-9-10-5. When link LSR2-LSR3 fails, LSR1 redirects traffic to the alternative LSP for SPD2 (LSRs 1-7-8-9-3). Furthermore, if we apply the proposal presented in [13] (Reliable and Fast Rerouting), we do not lose any packets.

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 [23].

In Table III 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 Fig. 1. We can observe that our proposal needs less links for a recovery path, performing better than separate link and path protection approaches.

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 III

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

IV. Proposed mechanism for optimal and guaranteed alternative Path (OGAP)

The preplanned protection scheme can have a risk that the preplanned alternative LSP will become out of date due to changes in the network. By out of date we mean that as network conditions evolve in time the preplanned alternative LSP may cease to be the optimal one. Moreover, after the restoration process, the restored LSP becomes unprotected.

To overcome these problems we propose to search for a new alternative LSP with updated network information concurrently while rerouting the traffic to the preplanned alternative LSP. Note that a long restoration time is a main problem of a dynamic restoration scheme but this does not apply to our proposal because the protected traffic is rerouted to the alternative LSP using the preplanned alternative LSP.

The idea behind this *hybrid approach* is to take advantage of the fast rerouting and the rerouting (dynamic) scheme [5]. At the same time our proposal provides a guarantee of an alternative LSP at any time for the protected LSP. We also consider the reversion operation. The reversion consists of rerouting the traffic from the alternative LSP to the original protected LSP once the failure has been repaired. Moreover, our proposal avoids the update of the alternative LSP each time the information database of the network changes. The update is done only when a failure occurs.

Fig. 2 presents the flow diagram of the proposed mechanism (OGAP). While no failure is detected in the protected LSP, each LSR continues carrying traffic through the protected LSP. Upon a failure the LSR which detects the failure (alert LSR) or one that receives protected traffic on the backward LSP looks for the preplanned alternative LSP in its label information base forwarding table (LIB). If the LSR is an ingress node for the SPD it should have an alternative LSP available. Otherwise, if the LSR is an intermediate node it must follow the RFR procedure described in [13]. If an alternative LSP is found, then it redirects the traffic from the affected protected LSP to the preplanned alternative LSP and it computes a new alternative path using the network conditions at that time.

If the path discovery and selection algorithm gives us a new alternative LSP we compare it with the one that was established previously as the preplanned alternative LSP. If the new alternative LSP is better than the preplanned one, the traffic will be redirected to the new alternative LSP without disruption of services (using the principle of *make-before-break*). The criteria for considering a path "better" may be based on the length of the path and other QoS parameters. The LSR maintains in its LIB the same preplanned alternative LSP as before, and proceeds to setup the backward LSP for the new protected LSP.

If the result is "not better" (i.e., the previously established preplanned alternative LSP is better than the new alternative LSP computed by the LSR after the failure) we assign the new alternative LSP as the preplanned alternative LSP and proceed to set up the backward LSP for new protected LSP.

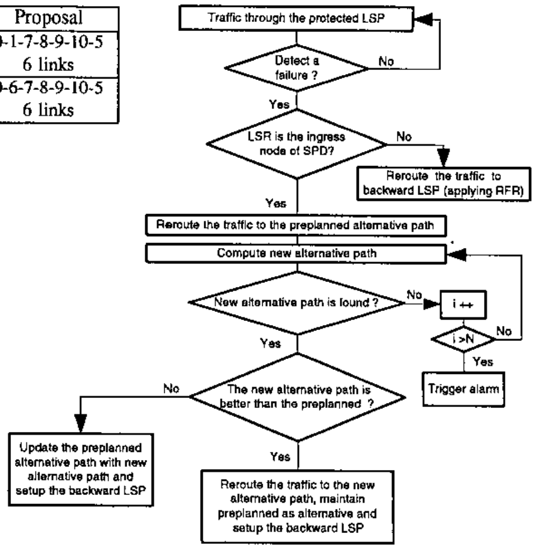
Traffic through the protected LSP
Detect a failure ?
No
Yes
LSR is the ingress node of SPD?
No
Reroute the traffic to backward LSP (applying RFR)
Yes
Reroute the traffic to the preplanned alternative path
Compute new alternative path
New alternative path is found ?
No
i ++
i >N
No
Yes
Trigger alarm
Yes
The new alternative path is better than the preplanned ?
No
Update the preplanned alternative path with new alternative path and setup the backward LSP
Yes
Reroute the traffic to the new alternative path, maintain preplanned as alternative and setup the backward LSP

Fig. 2. Flow diagram

If the routing algorithm is not able to find a new alternative path in the first attempt, we increment the iteration until its value (i) is greater than the control value established previously (N). This value (N) is determined by the network manager and it is a local implementation. If this iteration terminates without finding a new alternative path an alarm is sent to the network control manager to take appropriate measures.

Table IV summarizes the pros and cons of the different protection schemes for LSPs. Some parameters correspond to QoS provision and others to network resource utilization and feasibility.

The last column refers to the proposal presented in this paper combined with the previously proposed Reliable and Fast Rerouting mechanism (RFR) presented in [13].

RFR eliminates packet losses, including those circulating on the failed links, and packet disorder while imrproving the average delay time during the restoration period. This is achieved at a minimal cost of additional buffer (memory) that is far outweighed by the benefits.

Performance measurement	Haskin	Makam	OGAP	OGAP + RFR
Complexity	Low	High	Low	Low
Path placement	Restricted	Restricted	Flexible	Flexible
Restoration time	Fast	Slow	Fast	Fast
Packet Loss	Minimum	High	Minimum	None
Pkt Re-order	High	Minimum	High	None
Resource Req.	High	Low	Medium	Medium
Optimal path opt.	No	No	Yes	Yes
Protection for protected LSP	One Alternative	One Alternative	New Altern. Set-up	New Alt. Set-up

TABLE IV

Comparison of MPLS protection schemes

Although most of the concepts shown have been explained already, we would like to clarify some of them.

In the path placement row, unlike others, our proposal is flexible in the sense that the previously established alternative LSP can be changed to a new optimal alternative LSP computed using the rerouting (dynamic) scheme. Other proposals maintain the same alternative LSP set up during the establishment of the protected LSP to reroute the traffic.

The packet loss and packet reordering values in the last column are "none" because we incorporate in this proposal our Reliable and Fast Rerouting mechanism presented in [13].

Finally, in the last row we try to give the protection range not in terms of the amount of failure points on the protected LSP, but in the ability to handle further failures in the rerouted path. In our case as we establish a new alternative LSP to the rerouted path, our mechanism is able to handle further failures. For Haskin's and Makam's schemes, as they do not establish new alternative LSPs to the rerouted LSP, they only protect the first protected LSP (i.e., they handle only single failures).

V. 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 MPLS Network Simulator (MNS) [24] source code was modified to simulate these mechanisms: Haskin's [7], Makam's [6] 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 Fig. 1.

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 reordering 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, labelled as "proposal +".

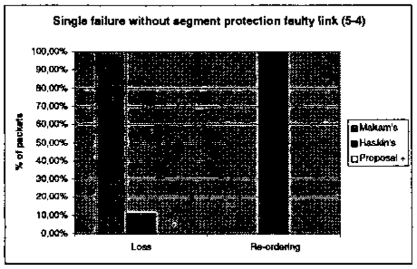

Fig. 3. Performance comparison results during recovery period for packet losses, packet disorder

Fig. 3 shows the results for a single failure without segment protection. Makam's scheme [6] 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 [7] 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.

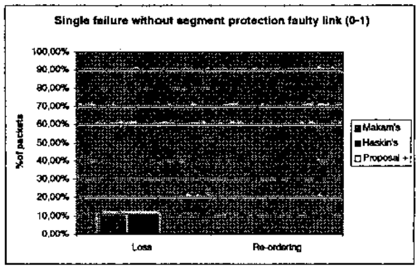

Fig. 4. Performance comparison results during recovery period for packet losses, packet disorder

Fig. 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 (Fig. 3 and Fig. 4) our proposal does not experience packet loss or disorder.

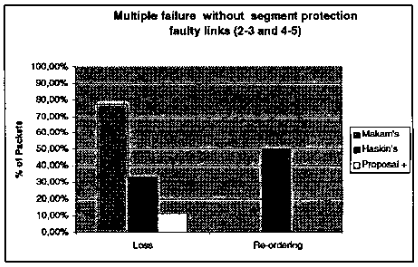

Fig. 5. Performance comparison results during recovery period for packet losses, packet disorder

In Fig. 5 the results for multiple failure without segment protection (failed links LSRs 2-3 and 4-5) are depicted. The packet loss for Makam's scheme decreases with respect to the result in Fig. 3 and increases with respect to the result in Fig. 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 losś 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 (LSRs 0-1-2), and loses packets on the links formed by LSRs 2-3-4-5. 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.

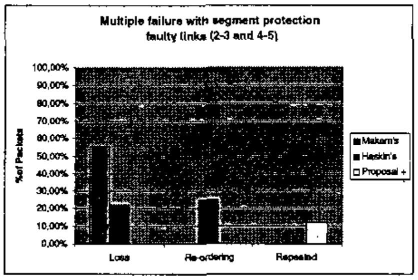

Fig. 6. Performance comparison results during recovery period for packet losses, packet disorder and repeated packets

Fig. 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 paper 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.

VI. 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.

One of the disadvantages of using a preplanned alternative LSP is that it may not be the optimal one when needed (i.e., at the time of failure). To overcome this disadvantage we propose a hybrid approach (OGAP) (i.e., preplanned and dynamic rerouting) capable of identifying and using the optimal alternative path based on recent network change information (i.e., after the fault was detected). This avoids the possible use of a non-optimal alternative LSP to reroute the protected traffic and provides the flexibility of alternative route selection and setup as well as better resource utilization. Moreover, our proposal guarantees at least one alternative LSP at any time for the traffic on the protected LSP.

This work has been partially funded by the MCyT under contract number FEDER-TIC2002-04531-C04-02 and CIRIT under contrat 2001-SGR00226.

References

[1] E. Rosen, A. Viswanathan, and R. Callon, "Multiprotocol Label Switching Architecture," *RFC 3031*, January 2001.

[2] R. Callon, P. Doolan, N. Feldman, A. Fredette, G. Swallow, and A. Viswanathan, "A Framework for Multiprotocol Label Switching," *Work in progress, <draft-ietf-mpls-framework-05.txt>*, Sep. 1999.

[3] Rainer R. Iraschko and Wayne D. Grover, "A highly efficient path-restoration protocol for management of optical network transport integrity," *IEEE Journal on Selected Areas in Communications, Volume: 18 Issue: 5*, pp. 779 –794, May 2000.

[4] D. Awduche, A. Chiu, A. Elwalid, I. Widjaja, and X. Xiao, "Overview and Principles of Internet Traffic Engineering," *RFC3272*, May 2002.

[5] V. Sharma and F. Hellstrand, "Framework for MPLS-based Recovery," *RFC 3469*, February 2003.

[6] K. Owens, V. Sharma, S. Makam, and C. Huang, "A Path Protection/Restoration Mechanism for MPLS Networks," *Work in progress, Internet draft <draft-chang-mpls-protection-03.txt>*, July 2001.

[7] D. Haskin and R. Krishnan, "A Method for Setting an Alternative Label Switched Paths to Handle Fast Reroute," *Work in progress, Internet draft <draft-haskin-mpls-fast-reroute-05.txt>*, November 2000.

[8] Thomas M. Chen and Tae H. Oh, "Reliable Services in MPLS," *IEEE Communication Megazine, Vol: 37 Issue: 12*, pp. 58 –62, Dec. 1999.

[9] M. Kodialam and T. V. Lakshaman, "Minimum Interface Routing With Applications to MPLS Traffic Engineering," *Proceedings of IEEE INFOCOM'00*, pp. 884 –893 vol.2, March 2000.

[10] G. Apostolopoulos, D. Williams, S. Kamat, R. Guerin, A. Orda, and T. Przygienda and, "QoS Routing Mechanisms and OSPF Extensions," *Internet,RFC 2676*, August 1999.

[11] S. Suri, M. Waldvogel, and P. R. Warkhede, "Profile-Based Routing: A New Frame work for MPLS Traffic Engineering," *In Proc. of Quality of Future Internet Services (QofIS)*, September 2001.

[12] L. Hundessa and J. Domingo, "Fast rerouting mechanism for a protected Label Switched Path," *Proceedings of the IEEE International Conference on Computer Communications and Networks (I3CN'01)*, October 2001.

[13] L. Hundessa and J. Domingo, "Reliable and Fast Rerouting Mechanism for a Protected Label Switched Path," *Proceedings of the IEEE GLOBECOM '02*, November 2002.

[14] T. Chujo, H. Komine, K. Miyazaki, and T. Ogura, "Spare Capacity Assignment for Multiple-Link Failures," *Proc. of the International Workshop on Advanced Communications and Applications for High Speed Networks*, pp. 191–197, March 1992.

[15] D. R. Kuhn, "Sources of failure in the public switched telephone network ," *Journal on Computer, Vol: 30 Issue: 4*, pp. 31–36, April 1997.

[16] D. Tipper, J.L Hammond, S. Sharma, A. Khetan, K. Balakrishnan, and S. Menon, "An analysis of the congestion effects of link failures in wide area networks," *IEEE Journal on Selected Areas in Communications, Volume: 12 Issue: 1*, pp. 172–179, January 1994.

[17] U. Ranadive and D. Medhi, "Some observations on the effect of route fluctuation and network link failure on TCP ," *Proceedings of the IEEE International Conference on Computer Communications and Networks (I3CN'01)*, pp. 460–467, October 2001.

[18] H. Komine, T. Chujo, T. Ogura, K. Miyazaki, and T. Soejima, "A distributed restoration algorithm for multiple-link and node failures of transport networks," *Proceeding of IEEE GLOBECOM '90*, pp. 459 –463, December 1990.

[19] M. Kodialam and T. V. Lakshaman, "Dynamic routing of locally restorable bandwidth guaranteed tunnels using aggregated link usage information," *Proc. of INFOCOM'01*, pp. 376–385 vol.1, April 2001.

[20] S. Kini, M. Kodialam, T. V. Lakshaman, S. Sengupta, and C. Villamizar, "Shared Backup Label Switched Path Restoration," *Work in progress, Internet draft <draft-kini-restoration-shared-backup-02.txt>*, April 2002.

[21] J. Anderson, Bharat T. Doshi, and S. Dravida P Harshavardhana, "Fast restoration of ATM Networks," *IEEE Jouranal on Selected Areas in Communications, Volume: 12 Issue: 1*, pp. 128 –138, January 1994.

[22] M. Medard, S.G Finn, and R.A. Barry, "WDM loop-back recovery in mesh networks," *Proc. INFOCOM'99*, pp. 752–759, Mar. 1999.

[23] R. Bartos and M. Raman, "Dynamic issues in MPLS service restoration," *Proc. of the Fourteenth IASTED International Conference on Parallel and Distributed Computing and Systems (PDCS)*, pp. 618–623, November 2002.

[24] A. Gaeil and C. Woojik, "MPLS Network Simulator (MNS)," *http://flower.ce.cnu.ac.kr/ fog1/mns/.*