2

REVIEW OF RELATED WORK

2.1 OVERVIEW

Multiprotocol Label Switching (MPLS) fuses the intelligence of routing with the performance of switching and provides significant benefits to networks with a pure IP architecture as well as those with IP and ATM or a mix of other Layer 2 technologies. MPLS technology is key to scalable virtual private networks (VPNs) and end-to-end quality of service (QoS), enabling efficient utilization of existing networks to meet future growth. The technology also helps to deliver highly scalable, differentiated end-to-end IP services with simpler configuration, management, and provisioning for both Internet providers and end-users. However, MPLS is a connection-oriented architecture. In case of failure MPLS first has to establish a new label switched path (LSP) and then forward the packets from the fault point or another node (i.e., in case the fault point is not a candidate to redirect the traffic) to the newly established LSP. For this reason MPLS has a slow restoration response from a link or node failure on the LSP.

In recent years new services and applications were developed with strong real-time connection-oriented characteristics. Such services include Voice-over-IP or the Real Time Streaming Protocol (RTSP)[SRL98]. Also in the transport layer new protocols were developed to support real-time services, like Real Time Protocol (RTP) [SCFJ96]. To meet quality-of-service requirements IETF introduced IntServ [BCS94] [SPG97][Wro97], RSVP [BZB+97] and DiffServ [DCea02] [HBWW99][BB+98][NBBB98] [Bla00] in the Internet service models.

The failure of a major link or backbone router may have severe effects on these services and protocols. After the rerouting is completed the services may experience a degradation of their quality of service, since the alternative route can be longer or more congested. Note that traffic not directly affected by the failure but diverted over an alternative route is also affected by this degradation.

On the other hand, the duration of the interruption due to a link or node failure is in most cases too long for real-time services and multimedia applications to maintain their sessions. At the same time, QoS flows could experience an unacceptable reduction of their QoS on the alternative route, and therefore not be able to be reestablished.

Multimedia applications typically have strict requirements regarding delay, delay jitter, throughput, and reliability bounds. Real-time network services are designed to guarantee these performance parameters to applications that request them. IntServ and DiffServ are added as new Internet services methods to provide these performance guarantees.

For these new services and applications advanced rerouting mechanisms have to be developed in order to provide fast rerouting, so that the sessions will not impaired. Additionally, the design of internet architecture and capacity planning should take alternative routes into account for IP-flows with quality of service guarantees.

From the above consideration one can conclude that resilience is a clear requirement for current and future IP-based networks. Resilience refers to the ability of a network to keep services running despite a failure. Unfortunately, since the Internet was designed for maximum connectivity and robustness, mechanisms for the fast recovery of traffic affected by network failures are not well considered. This is basically due to the limitation of the hop-by-hop destination-based IP routing. Moreover, in IP-based networks some convergence problems may occur when IP routers dynamically update routes to restore connectivity.

One of the challenges of a path-oriented routing protocol such as MPLS is service guarantee during failure. For this reason the ability to quickly reroute traffic around a failure or congestion point in a label switched path (LSP) can be important in mission critical MPLS networks to ensure that guarantees for quality of service to the established LSP will not be violated under failure conditions. In MPLS-based networks when an established label switched path becomes unusable due to a physical link or node failure data may need to be rerouted over an alternative/backup path to minimize these LSP service interruptions.

In this thesis we address the inherent problem of MPLS as connection-oriented architecture to recover from a network component failure.

2.2 SUMMARY OF PREVIOUS WORK ON PATH RECOVERY

Restoration schemes on networks are generally divided into two main categories: Centralized or Distributed schemes. Each of these schemes can be divided into preplanned or dynamic modes of restoration. These repair modes in turn can each use one of two methods of repair activation: Local or Global restoration.

2.2.1 Centralized Recovery

The centralized restoration scheme uses a centralized management system to perform the restoration functions, such as failure detection, selection of alternate route, redirection of flows to the established alternative path, etc. The centralized scheme has the advantage of always getting all network information available, including during failure, so it is easier to optimize restoration paths. As a result, it can make effective utilization of spare resources, and it may decrease network resources required compared to the distributed restoration scheme.

On the other hand, restoration speed is relatively slow with the centralized scheme due to the communication delay between the centralized controller and LSRs, and the concentration of processing load on the centralized controller. Therefore, centralized control may not satisfy the restoration speed requirement.

2.2.2 Distributed Recovery

To alleviate the negative impact of the centralized mode for restoration, some proposals consider the distributed restoration mode. In the distributed restoration scheme, each node in the network is capable of handling failures. The fastest detection occurs at the local end of a link failure using the distributed restoration method.

Grover's Self-Healing network algorithm is the first distributed network restoration algorithm for digital cross-connection system (DCS) based fiber networks proposed in [Gro87] and detailed in his PhD thesis dissertation [W.D89]. Self-healing implies failed path restoration with a distributed network element control mechanism. When a network failure occurs, failed paths are rerouted by processing and message transmission between local network elements without the intervention of a centralized control system. Self-healing schemes can be categorized into self-healing networks (SHN) for mesh networks where no topological restriction exists and self-healing rings (SHR) for ring networks.

Following Grover's publication other distributed network restoration algorithms for DCS-based fiber networks were proposed by Yang and Hasegawa [YH88] and by Chow et al.[CBMS93].

The first method ([YH88]) is called FITNESS, and uses the same relationship principle between adjacent nodes to the fiber cut link as the SHN algorithm ([Gro87])(i.e., sender and chooser relationship). FITNESS, however, reduces the potentially large number of request messages that may be generated in SHN by requesting the aggregate maximum bandwidth that is allowed on a restoration route.

In the second [CBMS93], unlike previous methods, the two nodes adjacent to the fiber cut perform nearly symmetrical (identical) roles during the restoration process. The algorithm is based on a Two-Prong approach. In this approach the restoration is initiated from both nodes with each sending a restoration request message labelled in a different "color". When the intermediate nodes receive a single color labelled requesting message they forward the message on all links which contain spare channels. A node, upon receiving two different color labelled request messages, will make appropriate cross connections between the links over which the two different requests were received. Once the cross connection has been made the request message will be forwarded over the newly connected link to the next node in the restoration path.

All the above proposals start the restoration mechanism after the occurrence of failure. Schemes that try to restore after the presence of failure are known as dynamic restoration schemes. At the same time they activate the repair locally (i.e., use the local repair scheme).

On the other hand, Automatic Protection Switching (APS) and Self-Healing Ring (SHR) [Wu95] use a set of working and backup links to switch traffic from the failed links to pre-assigned/preplanned backup links. These schemes provide high speed restoration of the network.

One of the advantages of the preplanned restoration scheme over the dynamic restoration scheme is the restoration speed. The dynamic restoration scheme uses many messages during the restoration process between restoration pair nodes to locate backup routes, to establish paths, and so on. The preplanned restoration scheme, on the other hand, can complete restoration by passing messages along each pre-established backup link. This simplification of the message transmission process and the reduced number of messages allows higher restoration speeds than the dynamic restoration scheme.

The previous proposals were designed for synchronous transfer mode (STM) networks such as digital cross-connection restoration or self-healing rings. The studies of self-healing concepts at the ATM-layer began in 1990. An extensive survey of work is presented in [Wu95] and [Kaw98]. Restoration mechanisms for ATM networks are presented in [KST94] [KO99] [KT95] [ADH94] [KKT94] and the implementation scheme is presented in [SHT90].

The restoration mechanisms proposed in the MPLS network use the same general protection principles as ATM. In MPLS networks, since an LSP traverses a fixed path in the network, its reliability depends on the links and nodes along the path. Traditionally IP networks have carried only best-effort traffic. However, new applications requiring guarantees are using the IP network infrastructure. This makes it highly desirable to incorporate the faster repair mechanisms.

In [GS00] and [She99] MPLS network restoration mechanisms are proposed. Both address the restoration mechanism using local repair. The fastest detection occurs at the local end of a link failure. Schemes that try to mend connections at the point of failure are known as “local repair” schemes.

In the [GS00] proposal the authors focus on two types of protection: one-to-one (1+1) backup tunnel creating a second separate LSP for every protected LSP tunnel. And one-to-many (1: N) where a single LSP is created which serves to backup a set of protected tunnels using the label stacking advantages.

In [She99] the author considers the problems of engineering reliability of router-router links and fast recovery of MPLS LSPs. Specifically, the problem of fast failure detection and notification of affected MPLS LSPs is addressed.

Local repair has performance advantages in maintaining connectivity but at the expense of efficiency (more hops, more bandwidth, more end-to-end delay).

In [HA00] extensions to CR-LDP and RSVP-TE for setup of pre-established recovery tunnels are proposed. In this proposal after a switchover of traffic to the recovery LSP the authors allow the traffic to merge onto the protected LSP at the merging node downstream of the fault without causing any extra resource reservation.

A path protection mechanism for MPLS networks is proposed in [OSMH01]. The extension of CR-LDP to provide signaling support for establishing protected/working and backup LSPs is proposed in [OSM+01]. In [OSM+01] the authors propose the introduction of an Explicit Route Protection ER-Hop type; the Path Switch LSR (PSL) and the Path Merge LSR (PML) to allow the identification of the end-points of a protected path or path segment; and the Path Protection Type Level Value (TLV) to the Label Request message to help the configuration of a protection domain and Path Protection Error Codes in the CR-LDP. The authors also presented the extension of RSVP-TE for MPLS path protection in [OSM+02].

Several methods have been proposed to reroute traffic in MPLS. There are two schemes for MPLS restoration currently under consideration within IETF giving different approaches to the label switched path (LSP) restoration problem in MPLS-based networks. The first is the fastest MPLS rerouting mechanism available, called the MPLS Fast Rerouting mechanism proposed by Haskin and Krishnan [HK00] and the second is a slower but less complex mechanism proposed by Makam et al. [OSMH01] known as RSVP-based Backup Tunnel. A comparison of different MPLS protection and rerouting mechanisms can be found in [FM01].

2.3 MPLS RECOVERY MODELS

Several IETF drafts and a framework proposal are being discussed in the MPLS working group (MPLS WG) to handle the slow recovery from network component failure as a main disadvantage of MPLS, like any connection-oriented technology. In case of a network failure a new LSP tunnel could be set up for a group of failed LSPs to route the traffic around the failed network element. The IETF MPLS WG defines two recovery models: rerouting, and protection switching or fast rerouting.

Some definitions that will be used throughout the following sections and chapters follows:

Downstream: The direction of data moving from an ingress LSR to an egress LSR. Or, with respect to the flow of data in a communication path: at a specified point, the direction toward which packets are received later than at the specified point.

Upstream: The direction of data moving from an egress LSR to an ingress LSR. Or, the direction from which traffic is expected to arrive.

Primary or protected LSP: The path that carries traffic before the occurrence of a fault.

Backward LSP: The path on which traffic is directed by a recovery mechanism in the upstream direction from the point of failure to a rerouting point.

Alternative LSP: The path by which traffic is rerouted to the destination node after the occurrence of failure.

Protection path: A set of links and nodes traversed by the packet in a protected flow after a failure is detected. During the recovery time the protection path may vary according the recovery scheme used, but after the recovery time the new path is the alternative LSP.

Alert LSR or alert node: The LSR or node that detects a fault.

Recovery period: The duration of time from the detection of the fault until the protected LSP is completely eliminated. In other words, the interval of time between the detection of failure and the time when the last packet sent by the ingress LSR on the protected LSP is rerouted to the alternative LSP.

2.3.1 Rerouting

Rerouting is a technique that can be used in both Label Switching and Packet Switching networks. Rerouting is defined as the establishment of a new path or path segment on demand for traffic restoration after the occurrence of a fault. Thus it is a recovery mechanism in which the recovery path or path segment is created dynamically after the detection of a fault on the working path. For this purpose, an alternative or backup path apart from the primary path used by current traffic is needed. The primary and the backup paths should be totally disjoint. Network components mainly consist of links and nodes. As a node failure causes the failure of the adjacent links connected to the node, we use link failure as a network failure.

When a link on the primary path fails the restoration process starts automatically. A complete rerouting technique is described in the frameworks presented in [SH02][LCJ99] and consists of several steps. The main steps that the rerouting method must accomplish are fault detection, fault notification, alternative path computing, and rerouting of traffic from the primary path to the alternative path.

Fault Detection: The network must be able to detect link failures. Link failure detection can be performed by dedicated hardware or by software in the end nodes of the failed link.

Fault Notification: Nodes that detect a link failure (alert nodes) must notify certain nodes. Which nodes are actually notified depends on the rerouting technique. The alert node initiates the failure restoration process according to the applicable

restoration method to determine the failed paths and create and send a notification message requesting a search for alternative routes to the upstream node.

Alternative Path Computation: The upstream node performs the computation of an alternative path upon the reception of the notification message. If this node is not responsible for redirecting the traffic then it relays the notification message to the corresponding upstream node.

Reroute traffic to alternative/backup path: This process detours the traffic to the backup path instead of sending traffic on the primary, failed path. This process completes the restoration of the network after a link failure.

Traffic reverting: This is the process that returns traffic back from the alternative path to the primary path after the failed link has been repaired. When the traffic reverting mode is used, the mechanism must detect the complete repair of the failed link, notify the related nodes in the network, and reroute the traffic from the backup path to the primary path as soon as the path becomes available.

2.3.2 Fast Rerouting or Protection Switching

The Fast Rerouting or Protection Switching recovery mechanism pre-establishes the alternative protection path before the occurrence of the fault. The criteria to establish the pre-established/pre-planned alternative path are based on network routing policies, the restoration requirements of the protected traffic, and administrative considerations. When a fault occurs the LSR responsible for detouring the traffic switches the protected traffic from the primary path to a pre-established alternative path. Since the protection switching model pre-establishes a recovery path before the occurrence of a fault, the recovery time is shorter than the rerouting model.

We will focus our contribution on fast restoration schemes. Currently there are two schemes for MPLS restoration under consideration within IETF.

2.3.3 Rerouting Strategies

As explained above, fast rerouting uses pre-established alternative LSPs. When a fault is detected, the protected traffic is switched over to the alternative LSP. Setting pre-established alternative paths results in a faster switchover compared to establishing new alternative paths on-demand [HK00][SH02][MSOH99][OSMH01][Swa99]. However, because the fast rerouting alternative LSP is established at the time the protected LSP is setup, it may lead to the use of non-optimal alternative LSPs due to changes in the network. At setup time the alternative LSP was compliant with the QoS requirement and was the best alternative path, but when a failure occurs network conditions may have changed and there may be a different optimal alternative LSP.

Global optimization algorithms that can be computed at the ingress of the LSP have been proposed to alleviate this drawback [Swa99]. The combination of both fast rerouting and optimal path computation would be the best solution for service restoration. Chapter 7 deals with a new proposal that combines both approaches.

There are two possibilities for repair activation: global repair and local repair.

Global repair: Global repair is activated on an end-to-end basis, as shown in Figure 2.1. That is, an alternative LSP is pre-established or computed dynamically from ingress to egress nodes of the path to be protected. Note that when a dynamic approach is used in global repair a failure signal is propagated to the source (ingress LSR) before a new route can be established, which wastes valuable time because the failure notification has to traverse the entire network (MPLS domain).

Local repair: Local repair aims to fix the problem at the point of failure or within a very short distance from the failure, thereby minimizing total packet loss.

The techniques proposed for local repairs in MPLS networks are splicing and stacking [Swa99].

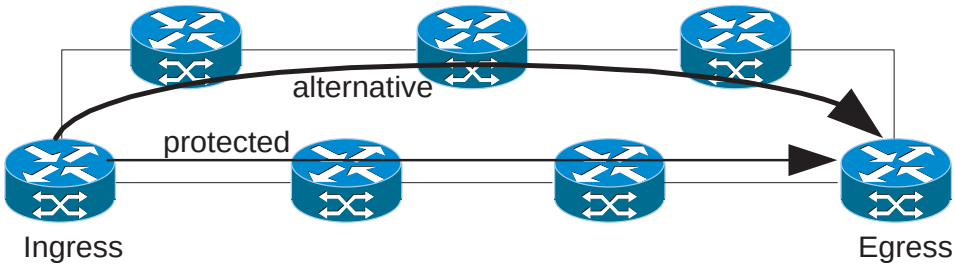

Figure 2.1 Global repair

Splicing: In this case an alternate LSP is pre-established from the point of protection to the egress LSR via an LSP that bypasses the network elements being protected. Upon detection of a failure, the forwarding entry for the protected LSP is updated to use the label and interface of the bypass LSP. Figure 2.2 illustrates the splicing repair technique in an MPLS domain.

The worst case requires as many alternative LSP candidates as the number of LSRs along the protected LSP minus one.

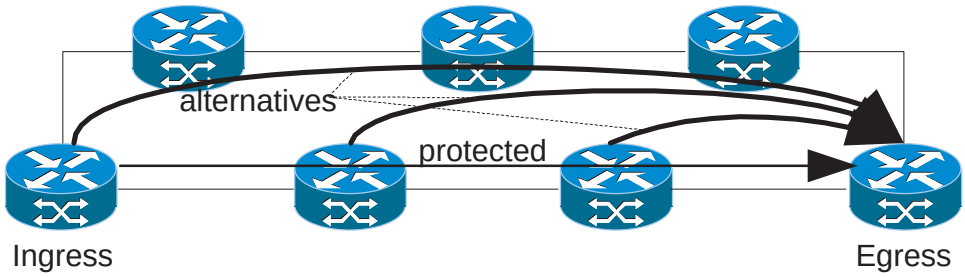

Figure 2.2 Local repair using splicing technique

When we refer dynamic restoration, this corresponds simply to splicing dynamic rerouting as illustrated in Figure 2.3.

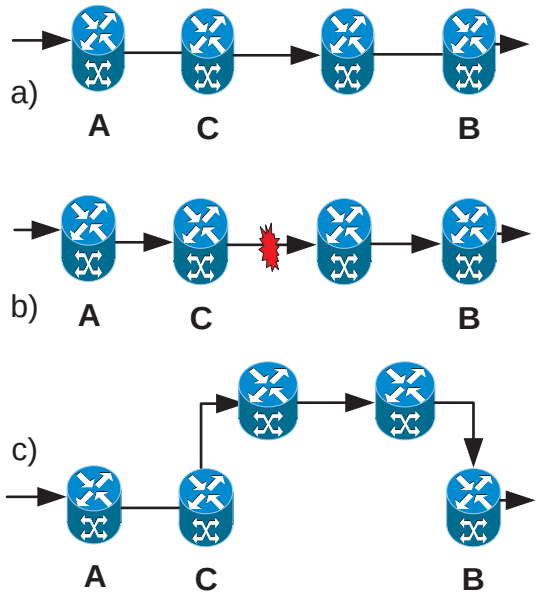

Figure 2.3 Dynamic rerouting steps, using local repair splicing technique

Stacking: In this case a single LSP is created to bypass the protected link; when a fault occurs the bypass LSP is a replacement for the faulty link. This LSP can be used as a hop by another LSP. This is done by pushing the bypass label onto the stack of labels for packets flowing on the rerouted LSP. Figure 2.4 illustrates the stacking repair technique within an MPLS domain.

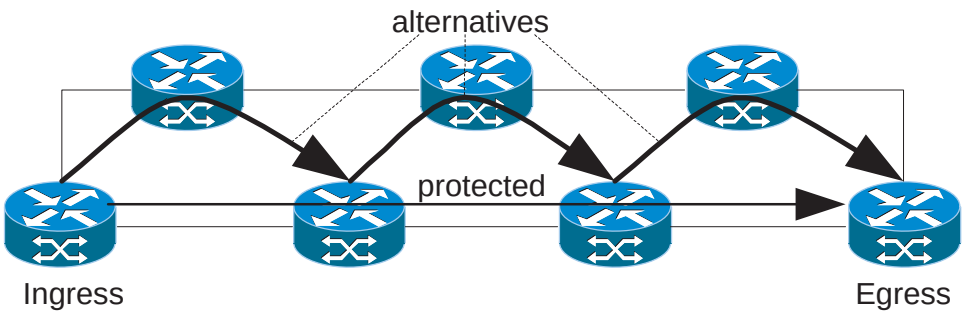

Figure 2.4 Local repair using stacking technique

Restoration and repair Method	Resource Requirement	Speed of Repair	Packet Loss	Packet Re-ordering	Protection Path (length)
Dyn. Local Repair	No	Slow	Minimum	Minimum	Might not be the SP available
Dyn. Global Repair	No	as above + FIS	High	Minimum	Path is shortest available
Fast re-routing Local	Yes, if not shared	Fast	Minimum	Minimum	May not be the optimal
Fast re-routing Global	As above	Fast, depends on FIS	High	Minimum	Better than the above
Fast re-routing with Reversing backup (Haskin's)	As above, plus backward LSP during recovery time	As above	Minimum	High	As above

Table 2.1 Comparison table for repair techniques, SP: shortest path, FIS: failure indication signal

If local repair is attempted to protect an entire LSP, each intermediate LSR must have the capability to initiate alternative, pre-established LSPs. This is because it is impossible to predict where failure may occur within an LSP. A very high cost has to be paid in terms of complex computations and extensive signaling required to establish alternative LSPs from each intermediate LSR to the egress LSR. For this reason, we have chosen the combination of local and global repair strategies with reversing backup (backward) for our mechanism. Our approach is similar to the one adopted in [HK00].

In table 2.1 we try to summarize the main aspects of different combination of restoration and repairing methods used to protect traffic from network failures.

2.3.4 Haskin's proposal

In Haskin's proposal [HK00] the authors present a method for setting up an alternative LSP to handle fast rerouting of traffic upon a single failure in the primary/protected LSP in an MPLS network. Since the objective of the proposed work is to provide a fast rerouting protection mechanism, the alternative LSPs are established prior to the occurrence of a failure.

For the correct operation of this proposal the complete path during the recovery period is composed of two portions: the path from the egress LSR to ingress LSR in the reverse direction of the primary/protected path (Backward LSP) and the alternative path from the ingress LSR to the egress LSR (Alternative LSP). The alternative LSP must be completely disjoint with the primary LSP (Fig 2.5a).

The main idea of this proposal is to reverse traffic at the point of failure of the protected LSP using the Backward LSP. This provides a quick restoration comparable to the 50 milliseconds provided by a SONET self-healing ring, and at the same time minimizes alternative path computation. Fast protection switching is achieved without signaling since the reversing decision is made using locally available information at the node that detects a downstream link failure (alert LSR).

In this scheme the alert LSR, reroutes the incoming traffic in the reverse direction of the protected path using the backward LSP (Figure 2.5b). When the redirected traffic reaches the ingress LSR, it is switched to the previously established alternative LSP. Furthermore, when the ingress LSR detects traffic in the reverse direction it switches the traffic entering the MPLS domain directly to the alternative LSP (Figure 2.5c). Note that until the ingress LSR receives the first packet from the backward LSP packets continue to be sent via the already broken primary/protected LSP (Figure 2.5b). These packets will experience a two-way delay while traversing the backwards loop from the ingress LSR to the last LSR at the point of failure (alert LSR). Another problem of this scheme is that as packets arriving from the reverse direction are mixed with incoming packets, this results in packet disordering through the alternative LSP

during the restoration period. Finally, the scheme also loses packets circulating in the failed link at the time of failure.

Figure 2.5 illustrates steps followed by Haskin's restoration scheme.

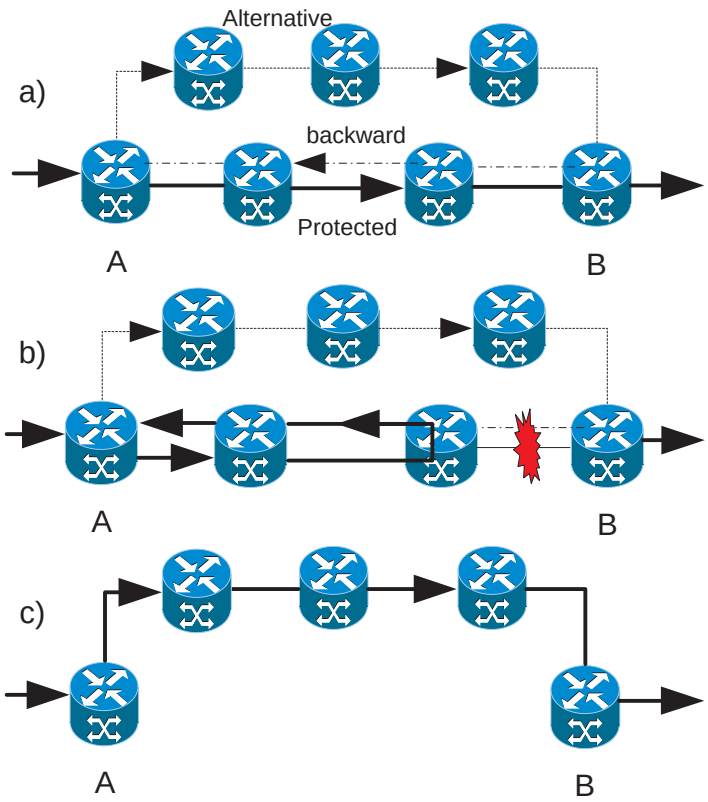

Figure 2.5 Haskin's scheme restoration process

2.3.5 Makam's Proposal

In this proposal [MSOH99] [OSMH01] [SH02] the authors consider the two recovery possibilities for the alternative LSP: pre-established (Figure 2.6) and dynamic recovery (Figure 2.7). The objective is to provide a path protection mechanism in MPLS networks. Unlike Haskin's proposal this scheme uses a fault notification mechanism (FIS) to convey information about the occurrence of a fault to a responsible node in

order to take the appropriate action (e.g., the ingress LSR is notified to switch traffic from the protected path to the alternative path).

Figure 2.6 illustrates steps followed by Makam's restoration scheme using fast rerouting.

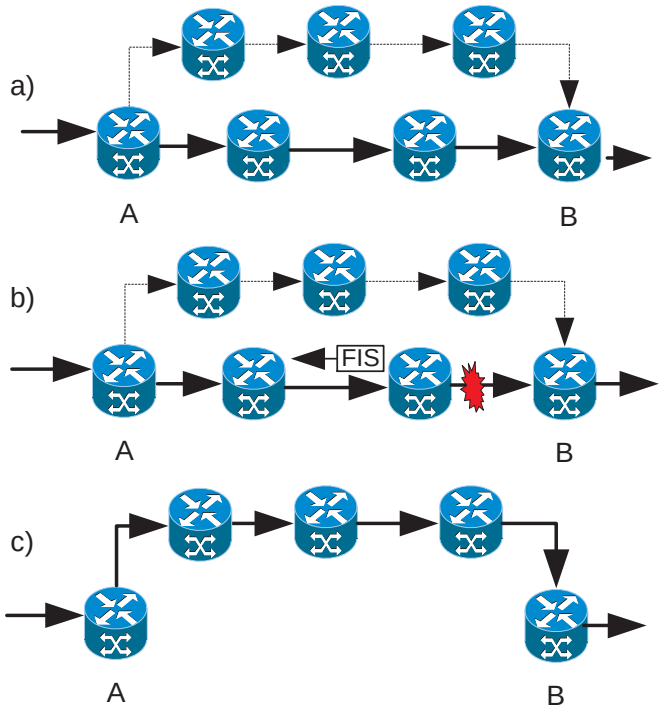

Figure 2.6 Makam's scheme using fast rerouting (preplanned)

When a link failure occurs on the protected path, the alert node signals the failure to the upstream nodes (i.e., the intermediate LSRs on a protected path between the ingress LSR and the alert LSR) as illustrated in Figure 2.6b and Figure 2.7b. The ingress LSR redirects the traffic over a *pre-established or pre-planned alternative LSP* (Fast rerouting method, Figure 2.6c) or *dynamically established alternative LSP* (rerouting method, Figure 2.7c) upon the reception of the failure notification signal.

In the case of using the pre-established alternative LSP, the traffic entering the domain is directly diverted to the pre-established alternative LSP by the ingress LSR after the arrival of the notification signal. This method provides better resource utilization than Haskin's scheme because the length of the protection path used during the recovery period is less than that of Haskin's proposal. However, the traffic that is in transit during the interval of time between the detection of the fault detected and the time the fault notification signal reaches the ingress LSR will be dropped by the alert LSR. Moreover, those packets that were circulating on the failed link at the time of the failure will also be lost.

When the dynamic method is applied, as it takes much longer to establish the alternative LSP, and the amount of dropped packets is larger than with the pre-established alternative LSP. Resource utilization is more efficient than the previously described scheme because updated network information is used. This scheme also provides more flexibility in the establishment of a new alternative LSP.

The main advantage of using a dynamic LSP is that an optimal alternative LSP may be established.

Figure 2.7 illustrates steps followed by Makam's restoration scheme using rerouting (Dynamic).

Table 2.2 shows the restoration and repairing method used by Haskin's, Makam's and the dynamic scheme (Figure 2.3).

2.4 PERFORMANCE EVALUATION METHODOLOGY

2.4.1 Simulation tools

The methodology used for performance evaluation in this thesis is a public domain network simulator version 2 (*ns-2*) originally from Lawrence Berkeley National Labo-

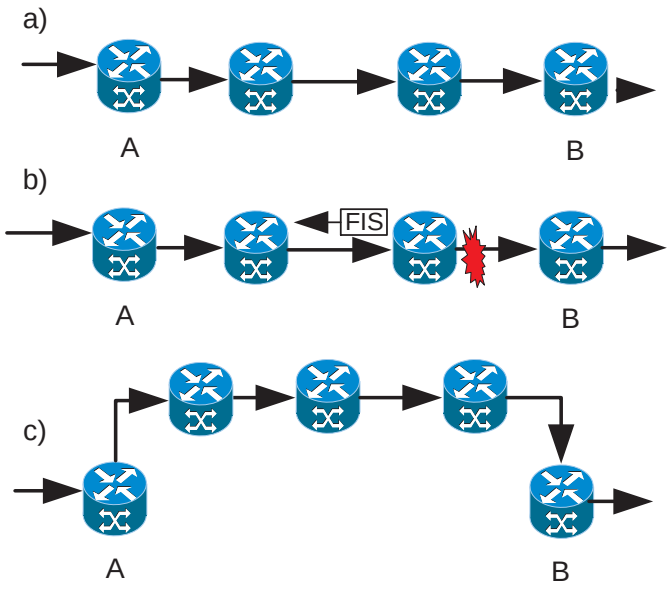

Figure 2.7 Makam's scheme using rerouting (dynamic)

	Haskin's scheme	Makam's scheme	Dynamic scheme
Restoration method	Fast Re-routing (Pre-planned)	Fast Rerouting or Rerouting	Rerouting (Dynamic)
Repairing method	Local	Global	Local

Table 2.2 Comparison of restoration and repairing methods for Haskin's, Makam's and Dynamic scheme

ratory (LBNL) [FVa][FVb] extended for MPLS networks called MPLS Network Simulator (MNS) contributed by Gaeil and Woojik [GW99][GW00][GW01a].

The *ns*-2 is considered the standard simulation tool widely used by the network research community to validate its new proposals. Therefore, the use of *ns*-2 as the evaluation tool has many advantages.

1. It is a well proved standard network simulation with sufficient documentation.
2. It is maintained and updated by contributions from many people from different network research groups.
3. The basic function and parameters in the simulator are calibrated properly. Therefore, the simulation results derived from different proposals using the same simulation conditions are feasible for evaluation. This allows easy and better comparison tools between different proposals for network researchers.

NS-2 is an event-driven simulator designed for IP based networks. In NS-2, a node consists of agents and classifiers. An agent is a sender/receiver object of protocol and a classifier is the object that is responsible for the packet classification used to forward packets to the next node. For the purpose of making a new MPLS node from an IP node, the authors introduce 'MPLS classifier' and 'LDP agent' into the IP node.

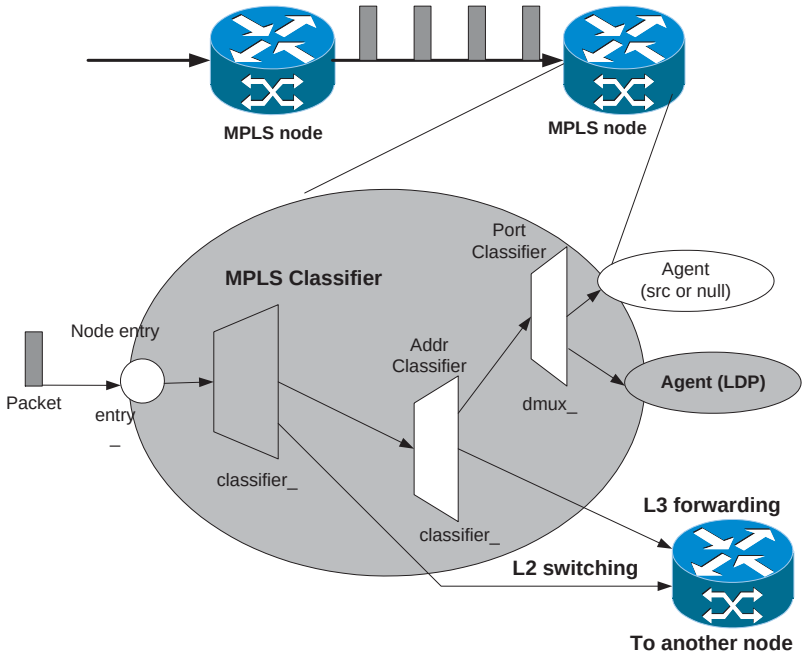

Figure 2.8 Architecture of MPLS node in MNS [GW99]

The simulated MPLS node handles the packets arriving in a three step process. First, it classifies them into labeled and unlabeled packets using the 'MPLS classifier'. Note that this principle is the same that the IP node uses to classify incoming packets into multicast and unicast using a "Multicast classifier". The MPLS classifier is responsible for the label swapping operation for labeled packets, and if it is an unlabeled packet but an LSP for the packet is prepared, the classifier executes a label push operation. Otherwise it sends the packet to the "Addr Classifier". Second, the Addr Classifier executes IP forwarding by examining the packet destination address. Third, if the next hop for the packet is itself, the packet is sent to "Port Classifier". Figure 2.8 shows the sequence of operations that an MPLS node performs on receiving a packet.

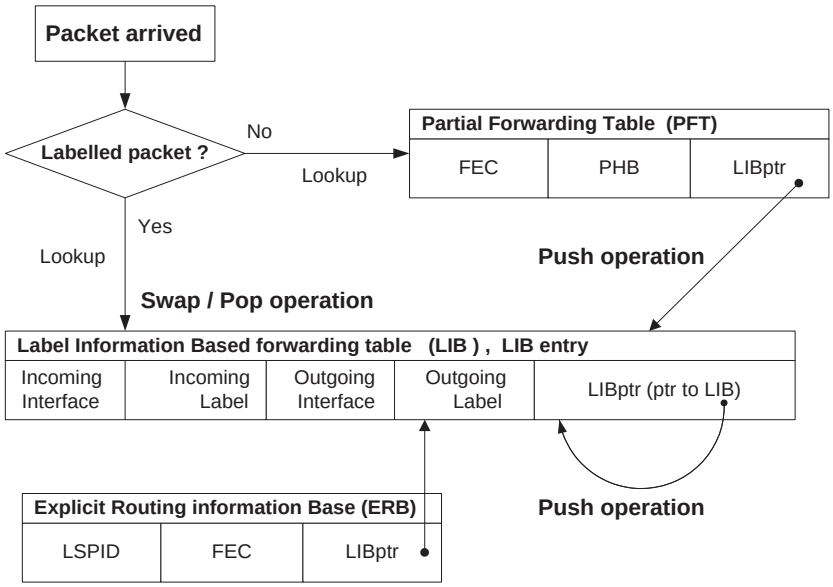

Figure 2.9 Entry tables in an MPLS node for MPLS packet switching

An MPLS node in MNS handles three information tables to forward packets using LSP: Partial Forwarding Table (PFT), Label Information Based forwarding table (LIB) and Explicit Routing information Base (ERB). PFT is a sub-set of the forwarding table and consists of FEC to NHLFE (FTN) mapping. The LIB table has information for LSPs, and ERB has information for Explicit Routing Label Switched

Path (ER-LSP). Figure2.9 shows the structure of these tables and the simple algorithm for forwarding packets [GW99].

Figure 2.10 illustrates the simple switchover mechanism used in MNS using the above tables when a link on the protected LSP fails. Note that the protected LSPs have a pre-established backup LSP using explicit routing.

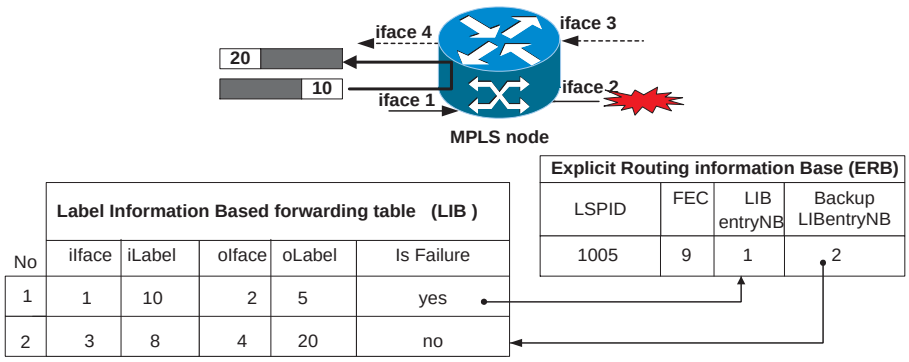

Figure 2.10 LSP restoration using backup LSP with switchover procedure

2.4.2 Performance criteria

Several criteria to compare the performance between different MPLS-based recovery schemes are defined in [SH02]. The most important are: packet loss, additive latency, re-ordering, recovery time, full restoration time, vulnerability, and quality of protection.

Packet loss: Recovery schemes may introduce packet loss during switchover to a recovery path. It is a critical parameter for a restoration mechanism. Throughput rates achieved for the service are seriously affected by packet losses. In real-time applications (e.g., VoIP, Multimedia, etc.) losses may interrupt the connection. Recovery schemes must guarantee minimal or no packet losses during the restoration period.

Latency: Latency represents the amount of time it takes a bit to traverse a network. The latency value is used as an indicator of the quality of the network connection: the lower the latency the better the connection. It is also referred as to end-to-end delay. For real-time applications, such as streaming video and audio, latency variation over time, or delay jitter, is also an important indicator of the network's quality.

Re-ordering of packets: The recovery mechanism may introduce packet disordering. The action of putting traffic back on a preferred path may introduce packet reordering by the ingress node when sending packets through an alternative LSP. This is also not desirable. While data transfers may handle disordered packets, streaming data usually do not.

Recovery time: The time required for an alternative path to be activated and begin carrying traffic after a fault. It is the time between the failure detection and the time when the packets start flowing through the alternative LSP.

Full restoration time: The time between the failure detection and the time all traffic is flowing through the alternative LSP.

Vulnerability: The time that the protected LSP is left unprotected (i.e., without backup) from possible network component failure. Once the alternative LSP becomes the primary LSP new alternative and backward LSPs should be established in order to protect it.

Quality of protection: Upon a failure the probability of a connection to survive the failure determins the quality of protection of the restoration scheme. The quality of protection range can be extended from relative to absolute. Relative survivability guarantee means that it is straightforward to assign different priorities to different connections and restore them based on their relative priority. Absolute means that the survivability of the protected traffic has explicit guarantees and therefore provides a better option for a service level agreement (SLA). The quality of protection of the protected LSP is absolute.

2.4.3 Simulation scenario

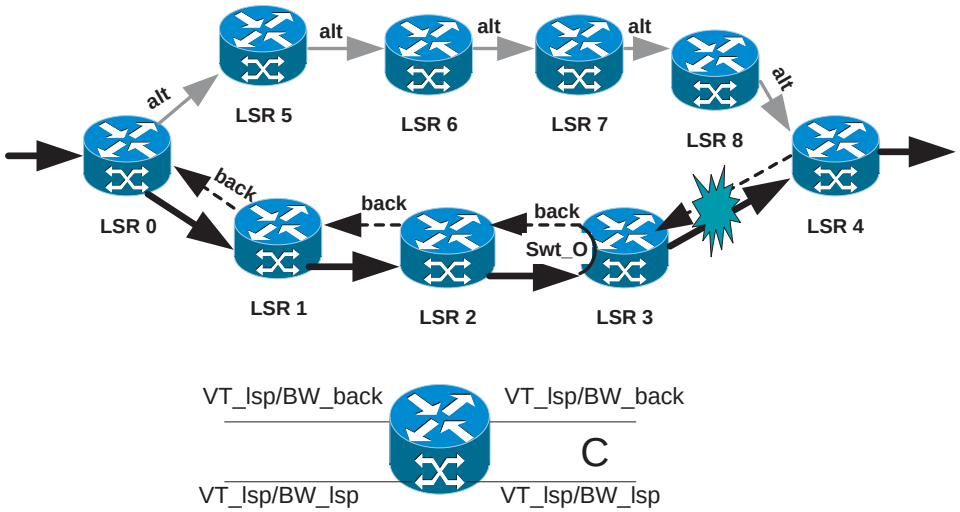

Figure 2.11 Simulation scenario

Figure 2.11 presents the basic simulation scenario used in this thesis, where C is the link capacity, B_{W_lsp} is the protected LSP bandwidth and V_{T_lsp} is aggregated protected flows. For a protected LSP, B_{W_back} is the backward LSP bandwidth and B_{W_alt} is the alternative LSP bandwidth.

The V_{T_lsp}, B_{W_lsp}, B_{W_back}, and B_{W_alt} are subject to:

$$V_{T\_lsp} \leq B_{W\_lsp} \tag{2.1}$$

$$B_{W\_back} \geq B_{W\_lsp} \geq V_{T\_lsp} \tag{2.2}$$

$$B_{W\_alt} \geq B_{W\_lsp} \geq V_{T\_lsp} \tag{2.3}$$

the worst case is when: $V_{T\_lsp} = B_{W\_lsp} = B_{W\_back} = B_{W\_alt}$.

In the simulations we vary the source rate, packet size, LSP length and the bandwidth of protected, backward and alternative LSPs to compare the performance for different restoration schemes.

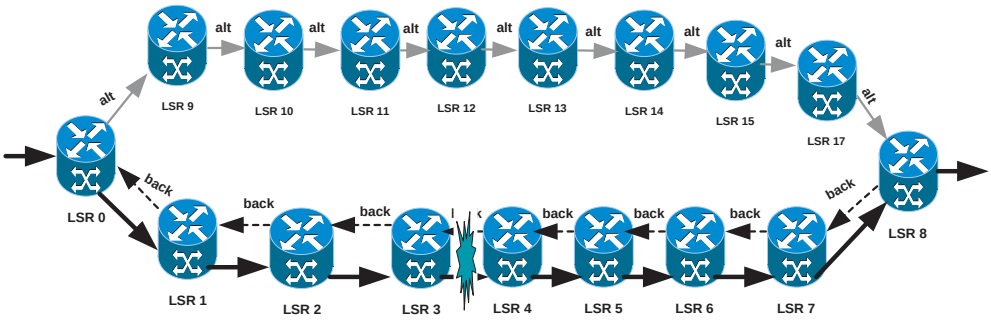

Figure 2.12 Network scenario

We use CBR traffic with a UDP agent generated by the network simulator NS-2 for the simulation. We use UDP traffic for our studies because the main interest is multimedia traffic for real-time requirements. We use CBR traffic due to the behavioral simplicity that it gives the simulation.

2.5 PERFORMANCE EVALUATION OF MPLS RECOVERY SCHEMES

The basic factors that affect the performance of the restoration mechanisms are packet loss, traffic recovery delay (Full Restoration Time) and packet disorder [BR02] [GJW02]. We use these performance measurement parameters to compare the above-mentioned proposals for MPLS restoration schemes for link/node failure. Other parameters will be considered later in other proposals.

Figures 2.13 and 2.14 present the comparison of the behavior of three approaches: Haskin's, Makam's pre-established, and classical dynamic using the local splicing technique (Figure 2.3). Results refer only to the restoration period and show % of packet loss and % of packets out of order due to the restoration mechanisms. The horizontal axis presents the place of the alert LSR within the protected LSP.

Performance evaluations based on the Figure 2.12 for these schemes. Figure 2.13 shows the comparison result for packet losses.

2.5.1 Packet losses

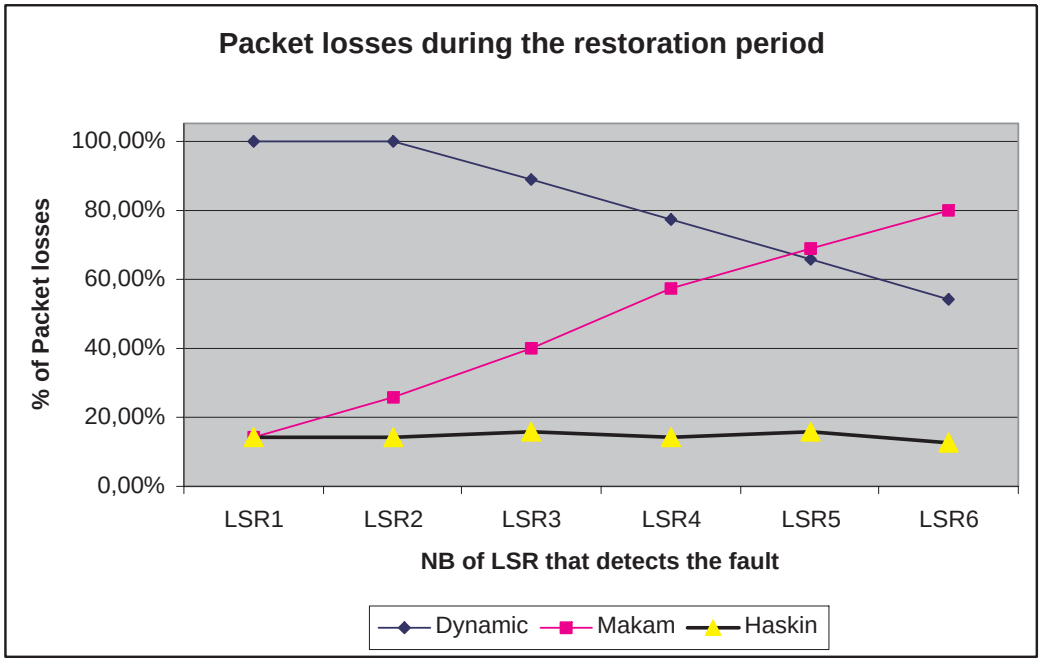

Figure 2.13 Packet loss performance comparison between path protection/restoration schemes in MPLS network

With the dynamic scheme packet losses increase in proportion to the distance between the alert LSR and the egress LSR, because of the set up time of an alternative LSP.

In Makam's scheme [OSMH01] packet losses increase in proportion to the distance between ingress LSR and an alert LSR that detects the failure, because of the delivery time of the fault notification message.

Haskin's scheme [HK00] only loses packets on the failed link or on the link adjacent to the failed LSR.

2.5.2 Packet Disorder

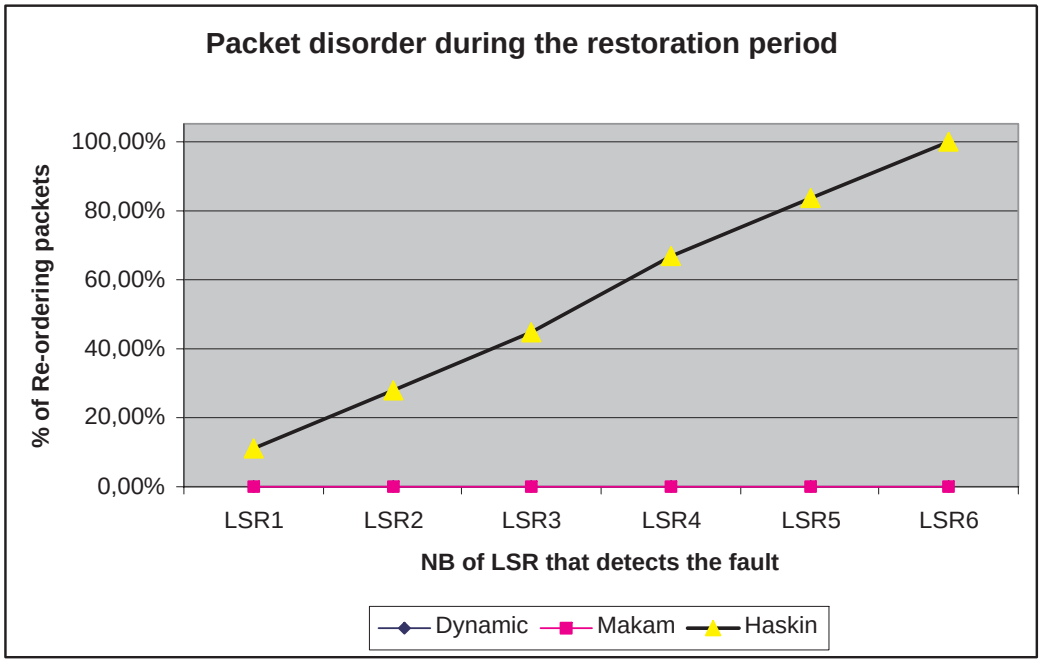

Figure 2.14 Packet disorder performance comparison between path protection/restoration schemes in MPLS network

Figure 2.14 presents the packet disorder result for the these schemes. In Haskin's scheme packet disorder increases in proportion to the distance between ingress LSR and the alert LSR. Note that the packet disorder that we consider here is the disorder produced during the restoration period which does not include the disorder produced by the retransmission of lost packets by a high level protocol (i.e., TCP).

Makam's and dynamic schemes do not introduce packet disorder but cause more packet losses.

Based on the discussion in this chapter we restrict ourselves to the combination of local repair action, reverse, and global restoration schemes with preplanned alternative LSPs. We use local repair action because of its advantage in terms of speed for switchover of traffic from the protected path to the backup path compared to global

repair action. Note that the choice of local restoration may lead to ta higher use of resources due to the length of the resulting protection path. For this reason we use the global restoration scheme, which provides the optimal available path (Table 2.1). We chose the reversing mode because, like local restoration it reports the minimum packet loss. However, unlike local restoration, in the reversing mode the resources are used only during the relatively short recovery period. Note that the reserved resources in the reverse backup path (backward LSP) can be used by low priority traffic. We also exclude the dual-fed path protection technique known as 1+1 because in this system only the transmitting node and receiving node affect recovery, and it consumes excessive network resources.

2.6 MOTIVATION

The effects of packet losses, packet delay and packet reordering on QoS provision are well known phenomena. These parameters are closely related. Chapter 5 provides some detailed explanations of these phenomena.

The main motivation of this thesis is to overcome the drawbacks of the previously proposed schemes for the restoration mechanism in MPLS networks during link/node failure or congestion. We focus mainly on the above problems: packet loss, packet delay and packet disorder.

Proposals in the following two chapters try to improve the performance of recovery schemes on packet loss, packet delay and packet disorder.