

Evaluating the probability and the impact of a failure in GMPLS based networks.

Eusebi Calle, Jose L Marzo, Anna Urrea
Institut d'Informàtica i aplicacions (IIIÀ).
Universitat de Girona, 17071 Girona, SPAIN
e-mail: {eusebi, marzo, aurra}@eia.udg.es

Abstract-

In this paper, we define a new scheme to develop and evaluate protection strategies for building reliable GMPLS networks. This is based on what we have called the Network Protection Degree (*NPD*). The *NPD* consists of an a priori evaluation, the Failure Sensibility Degree (*FSD*), which provides the failure probability, and an a posteriori evaluation, the Failure Impact Degree (*FID*), which determines the impact on the network in case of failure, in terms of packet loss and recovery time.

Having mathematically formulated these components, experimental results demonstrate the benefits of the utilization of the *NPD*, when used to enhance some current QoS routing algorithms in order to offer a certain degree of protection.

I. INTRODUCTION

New network technology enables increasingly higher volumes of information to be carried. Various different types of mission-critical, higher-priority traffic are now transported over these networks. In this scenario, when offering better quality of service, the consequences of a fault in a link or node become more pronounced. A new concept of quality of protection is required.

Network reliability can be provided through different fault management mechanisms applied at different network levels and time scales. Although most concepts and methods discussed in this paper are applicable to different network technologies, which implement the logical path paradigm, our work focuses mainly on Generalized MultiProtocol Label Switching (*GMPLS*) networks [9]. *GMPLS* fault restoration mechanisms usually establish backups named Recovery Label Switch Paths [10], [11] and [12]. With these backups, traffic can always be re-routed when a failure occurs. *GMPLS* also provides suitable fault detection and fault recovery actuation, which allow effective utilization of backup paths. ([1], [2] and [7]).

A crucial aspect in the development of a fault management system is the creation and routing of backup paths. Several schemes have been proposed ([3], [4], and [5]) for routing new paths which guarantee certain QoS parameters (such as resource utilization or minimizing the request rejection ratio). However, most of these schemes do not take into consideration other aspects, such as network failure probability, or parameters concerning the quality of the protection, such as packet loss or restoration time.

We will discuss network protection, involving the creation of fast and suitable recovery mechanisms, in the context of these parameters and which of them have most influence. With this aim we propose new concepts for calculating a Network Protection Degree (*NPD*), such as the Failure Sensibility Degree (*FSD*) or the Failure Impact Degree (*FID*). A mathematical formalization is developed for each concept and several experiments are presented to support these formulations.

This paper is organized as follows: in Section II, the new Network Protection Degree concept is presented and formalized. In Section III and IV, the formulations, supported by experiments are discussed. Final Section summarizes and concludes the paper.

II. NETWORK PROTECTION DEGREE

In this section, we analyze the main components which define the Network Protection Degree (*NPD*). There are two main components of *NPD*: the Failure Sensibility Degree (*FSD*) and the Failure Impact Degree (*FID*). The *FSD* concerns the statistical analysis of network failure (this is an *a priori* analysis). On the other hand, the *FID* evaluates the impact on the network when the failure occurs (this is an *a posteriori* analysis). In this work, *FID* is expressed in terms of well-known parameters such as packet loss and recovery time.

In a real network, several technologies coexist: different wiring (or different physical layers) and different types of nodes (different providers, old and new equipment, etc.) all working together. This means that the actual probability of failure of any one of these elements is significantly different from any of the others. Although it is impossible in practice to determine which particular segment in a network will fail and when, the probability of failure can be calculated. A network operator can apply prediction techniques based on fault statistics. Eventually, a probability of failure can be explicitly assigned, manually, in order to decide upon a specific degree of protection. We will refer to this probability as 'Link Failure Probability' (*LFP*). In case of a new segment being set up, where there is no knowledge concerning failures, a high value *LFP* would initially be assigned. After a certain amount of normal functioning (no faults) a set of statistical information is obtained and the

initial LFP can be updated (hopefully decreased) to a more realistic value.

The mechanisms and methods for computing all the failure probabilities ($LFPs$) in a network are beyond the scope of this work. In the work we present here, we assume that knowledge of these probabilities is already known or readily available. Moreover, although their values may vary in time, this information is assumed to be stable.

A way to evaluate the FSD would be a useful tool for network providers, helping them to set the desired degree of protection for their customers and allowing them to guarantee QoS in terms of reliability and availability (depending on the SLA - Service Level Agreement). In section 2.1 we discuss using this information for calculating the sensibility to failure of an Label Switched Path (LSP). On the other hand, the impact to the network in the event of this path failing can be evaluated in terms of recovery delay and packet loss. The term Recovery Delay (T_{REC}) is defined as the period of time between the fault and the traffic restoration to the corresponding backup path. Packet Loss (P_{LS}) is defined as the total lost packets during the T_{REC} . Therefore, the Failure Impact Degree (FID) is calculated based on T_{REC} and P_{LS} .

In the following sections, a method for calculating FID and a study of the crucial factors when using backup protection mechanisms are presented. This provides us with a good knowledge about the segments of the network which are the most critical in case of failure.

2.1 Failure Sensibility Degree

The Failure Sensibility Degree (FSD) expresses the total probability of failure of the network. LSPs can cross through different links each with its own Link Failure Probability (LFP). Therefore, we assume in this work that all LFP 's are known (by calculation or heuristically) and they are also independent of each other. These values are normally very small; we assume that $LFP \ll 1$.

A LSP fails if any segment (i.e., an individual link or a combination of nodes and links) along the path fails. However, it is easier to evaluate the inverse probability, i.e., the probability that all the links involved work fine. Let consider the inverse probability of link failure as LFP^{-1} , (i.e. the probability that the link works fine). Therefore, the overall (LSP) probability of no-failure (the inverse of a LSP failure probability LSP_FP) is:

$$LSP_FP^{-1} = \prod_{i=1}^k LFP_i^{-1} = \prod_{i=1}^k (1 - LFP_i) \quad (1)$$

$k = \text{Number of links of the LSP}$

By simplifying all products and powers of LFP_i (as they are very small values by hypothesis) the product of this term is transformed into the following:

$$LSP_FP^{-1} = \prod_{i=1}^k (1 - LFP_i) \approx 1 - \sum_{i=1}^k LFP_i$$

$$k = \text{Number of links of the LSP} \quad (2)$$

But again, the LSP Failure Probability can be calculated as the inverse of LSP_FP^{-1} , therefore:

$$k = \text{Number of links of the LSP} \quad (3)$$

As expected, the total probability of failure of a LSP can be

$$LSP_FP = 1 - LSP_FP^{-1} \approx 1 - (1 - \sum_{i=1}^k LFP_i) = \sum_{i=1}^k LFP_i \quad \text{approximated}$$

by the sum of link failure probabilities.

It is also useful to assign a binary value to each segment to know whenever a link should be protected. This is defined as the Link Protection Requirements (LPR). This can be easily obtained by assign $LPR=0$ to those links with $LFP = 0$ and $LPR=1$ with $LFP > 0$. This allows us an easy calculation of the total LSP Number of Links to Protect (LSP_NLP). Hence, LSP_NLP is calculated as:

$$LSP_NLP = \sum_{i=1}^k LPR_i \quad (4)$$

$k = \text{Number of links of the LSP}$

In consequence, FSD can be defined as an array of the Failure Probability of all current LSPs (LSP_FP) in the network (formula (5)), or as an array Number of Links to be Protected per LSP (LSP_NLP) (formula (6)).

$$FSD_FP = (LSP_FP_1, LSP_FP_2, \dots, LSP_FP_N) \quad (5)$$

$$FSD_NLP = (LSP_NLP_1, LSP_NLP_2, \dots, LSP_NLP_N) \quad (6)$$

Where: $N = \text{Number of LSPs in the network}$

These arrays allow defining different strategies to evaluate the FSD . With (5) the number of LSPs out of a specific LSP_FP can be computed. With (6) we can determine, not only a failure probability expressed on the average of the number of links to be protected per LSP, but the protection requirements (number of links with backup requirements). In section IV several experiments to evaluate this second option are carried out.

2.2 Failure Impact Degree (FID)

In this Section, we show how we calculate the Failure Impact Degree (FID). As mentioned above, this metric concerns delays and packet loss in case of failure. Let us start with delays. It is well known that any protection mechanism based on the establishment of backup paths follows a set of steps for recovering faults (see section III). Each step needs a certain amount of time, i.e., the Recovery Delay (Time of Recovery T_{REC}), to carry on with the corresponding functions. This time consists of the following: Time for detecting the fault T_{DET} (for instance a signal from lower levels). Notification time T_{NOT} to inform (i.e, send a message to) the node responsible for switchover.

Time for backup setup, routing and signaling T_{BE} . Time for traffic switchover T_{SW} , from active path to backup path. Therefore, the T_{REC} can be evaluated by simple addition, as the following expression shows:

$$T_{REC} = T_{DET} + T_{NOT} + T_{BE} + T_{SW} \quad (7)$$

The Packet Loss (P_{LS}) is proportional to this T_{REC} and to the transmission Rate R_{TR} [8]. The packet loss in the faulty link (P_{FL}), that is to say, the packets lost when the link that was carrying them failed, should also be added to the equation. The resulting expression is:

$$P_{LS} = R_{TR} * T_{REC} + P_{FL} \quad (8)$$

Note the packets loss is not proportional to the T_{REC} in some network scenarios not contemplated in this paper. For instance, TCP will stop sending packets if no acknowledgements are received.

Therefore, it can be said that the Failure Impact Degree is a function, g , which depends on the packet loss and recovery time:

$$FID = g(T_{REC}, P_{LS}) \quad (9)$$

Other aspects such as the packet-reordering ratio [8] should be also added to evaluate the FID. In this paper we assume that major parameters are Packet Loss and Time to Recover the failures.

In the next section a review of the main fault management methods in GMPLS networks in order to evaluate the main features respect to the FID parameters (P_{LS} and T_{REC}) is presented.

III. FAULT MANAGEMENT METHODS

In this section a brief review of the mechanisms involved in the development of a backup protection method is provided. A specific protection architecture (GMPLS) is used to describe these methods. A discussion of the advantages and disadvantages of the backup methods is also provided, and the relationship between the recovery methods and the impact and the probabilities of a failure is introduced.

3.1 Creating a GMPLS recovery method.

Major protection methods begin with fault identification and end with link recovery. This chain of events involves various components:

a) First, a method for selecting the working and protection paths. If a QoS must be achieved, a QoS routing method should be used [4], [5], [6] or [7].

b) Once the paths are selected, a method for signaling their setup is required, (for instance, LDP/RSVP or CR-LDP/RSVP-TE in the case of MPLS).

c) Then, mechanisms for fault detection and notification: these convey information (about the occurrence of a fault) to the network entity responsible for taking the appropriate corrective action, for example, transmitting a FIS (Fault Indication Signal),

d) Finally, a switchover mechanism to move traffic from the working path to the backup path.

For providing certain protection features, two new sorts of nodes are necessary: a node responsible for the switchover function once the failure is identified and a node where the working and backup paths are merged. In MPLS, they are defined in [1] as Path Source LSR (PSL) switch router and Path Merge LSR (PML) respectively or the Bridge and Selector nodes in the GMPLS proposals [10].

3.2 GMPLS fault management methods.

The features of the main recovery methods are reviewed in this section.

a) The global backup path method

In this model (see Fig. 1(a)), an ingress node is responsible for path restoration when the FIS arrives. This requires an alternative, unconnected backup path for each working path. The ingress node is where the protection process is initiated, irrespective of the failure location along the working path.

The advantage of this method is that only one backup path per working path needs to be set up. Furthermore, it is a centralized protection method, which means only one LSR has to be provided with PSL /Bridge functions. On the other hand, this method has a high cost (in terms of time) as the FIS is sent to the ingress node. Furthermore, it implies higher packet losses during the switchover time.

b) Local backup path method

With this method, restoration begins at a point much closer to the fault (see Fig. 1(c)). It is a local method and does not necessarily involve the ingress node. The main advantage is that it offers a faster restoration time than the global repair model, as well as a significant reduction in the packet loss.

On the other hand, every node requiring protection has to be provided with a switchover function (PSL /Bridge). A PML /Selector needs to be provided too. Another drawback is the maintenance and creation of multiple backups (one per protected domain). This can lead to low resource utilization and increased complexity. An intermediate

solution establishes local backups only for segments with high reliability requirements.

c) Reverse backup path method

The main feature of this method is to reverse traffic close to the point of failure, back to the source switch (ingress node) of the path being protected via a Reverse Backup LSP (see Fig. 1(c)). As soon as a failure is detected, the LSR (Label Switch Router) at the ingress of the failed link reroutes incoming traffic to the backup LSP sending it in the opposite direction, back to the ingress node. Haskin [2] proposes to pre-establish the reverse backup path making use of the same nodes of the working path, thus simplifying the signaling process.

This method, like the local repair method, is especially indicated against the loss of sensitive traffic. Another advantage is the simplified fault indication, since the reverse backup transmits the FIS to the ingress node and the recovery traffic path at the same time. One of the disadvantages is poor resource utilization. Two backups per protected domain are needed. Another drawback, which it shares with the global repair model, is the time taken to send the fault indication to the ingress node.

e) 1+1 protection method

This method recovers the failure using the alternative-working path (see fig 1(d)). In this case the PML/Selector LSR monitors the best working path (for instance selecting the best signal). After a failure the PML/Selector detects that there is only one path, selecting this path as the working path.

This method is fast and there is not packet loss, but there is a high resource consumption due to the fact that both paths should be allocated a priori. In this method the

PSL/Bridge LSR have to be also setup to send the traffic over both paths.

d) Resource reservation and backup setup

Setting up a backup path can be done on a pre-established or on-demand basis. The resource allocation can be reserved or not reserved [1] (it is normally expressed in terms of bandwidth). Backup setup concerns the initiation of the recovery path setup. In the pre-established case, a recovery path is established prior to the link failure, whereas for the on-demand methods, the recovery path is established after the failure.

Resource allocation is pre-established if network resources are allocated before the failure. A backup path can be established with no (specific) bandwidth allocated. Another aspect to consider when defining more detailed resource reservation strategies is the method used to allocate bandwidth to LSPs. These are equivalent bandwidth allocated (same amount as the working path) or limited bandwidth allocated (less bandwidth than the working path).

f) Shared backups

A backup path can be shared by more than one working path. The resource reservation and the selected methods must take this into account. These mechanisms save a large amount of resources by maintaining the same level of protection for single failures.

3.3 Relationship between the impact and the probability of failure in the GMPLS recovery methods

Local methods and 1+1 methods are not affected by the impact in the occurrence of a failure in terms of packet loss and recovery time. Currently other methods, such as the

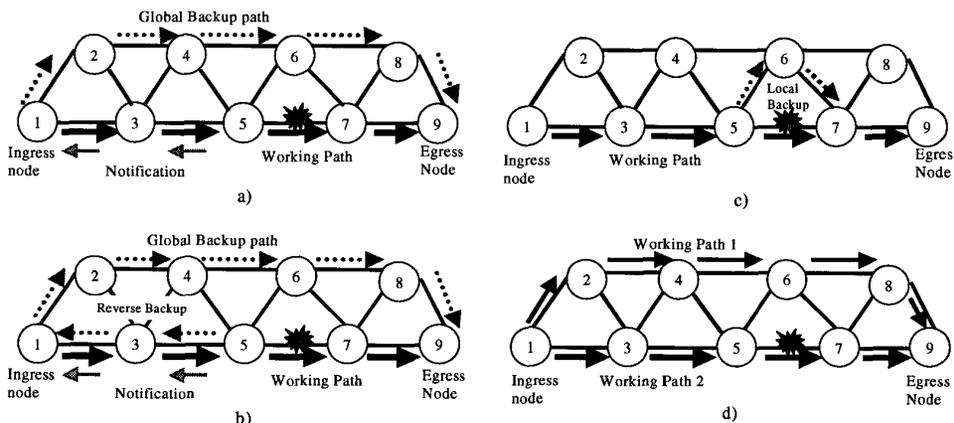


Fig. 1. Main fault management methods architecture.

reverse method are not usually applied. On the opposite global methods (pre-established or on-demand), are commonly used in several proposals [1], [4]. In this case the impact can only be reduced minimizing the distance between the node responsible of the failure detection and the node responsible of the switchover actions.

The use of an specific recovery method is beyond the scope of this paper. However the application of a recovery method, usually, involves a large number of resource consumption. In this paper we improve the network protection degree. In order to reduce these protection requirements we make use of the network protection degree components to enhance some current QoS routing algorithms, improving their protection without increasing the resource consumption.

IV. UTILIZATION OF THE NETWORK PROTECTION DEGREE.

In the previous section, we showed how we calculated the Network Protection Degree, *NPD*, which depends on the Failure Sensibility Degree, *FSD* (an *a priori* component) and the Failure Impact Degree, *FID* (an *a posteriori* component). In short, the protection Degree can be expressed as a function, *f*, of these two components:

$$NPD = f(FSD, FID) \quad (10)$$

We believe *NPD* will allow developers to create new or improve current QoS routing strategies. In [4] some QoS routing algorithms are defined and analyzed, such as Widest Shortest Path (*WSP*) or Shortest Widest Path (*SWP*). Both are based on resource optimization and load balancing. Recently, more complex approaches have appeared. [5], and [6], focused on resource optimization and the minimization of rejected requests. However, most of these algorithms do not consider network protection, at least not as a priority.

4.1 Enhancing QoS routing algorithms with the *NPD* paradigm.

By using the calculation of *NPD*, some of these methods can easily be enhanced. For instance, in order to enhance *WSP* we propose three new routing algorithms to add certain protection parameters in the route selection. Twice of them takes in consideration *FSD* formulation explained in section 2.1, in order to achieve LSPs with less failure probability and protection requirements. With the aim of considering the *FID* another routing algorithm integrating failure probabilities and distances (*D*) between the node detecting the failure and the node responsible of the switchover, has been developed.

In all these algorithms a pre-computation of a *k-WSP* algorithm is developed. Over the *k* set of possible LSPs different protection strategies are applied:

1) **PWSP_FP**, *Protected WSP considering the Failure Probabilities*; the LSP with the lowest failure probability *LSP_FP* is selected.

2) **PWSP_NLP**, *Protected WSP considering the Number of Links to Protect*; the LSP with the lowest Number of LSPs (*LSP_NLP*) is selected.

3) **PWSP_FPD**, *Protected WSP considering the Failure Probabilities and Distances (D)*. In this case, the objective is to reduce not only the failure probability, but the failure impact (minimizing the distance *D*, also reducing the time to notificate the failure). Each link of a LSP is weighted by the product of the distance *D* by the *LFP*. With the total sum of these values, the LSP with the lowest value is selected.

4) **PWSP_FPT**: *Protected WSP considering the Failure Probabilities and the traffic class*. In this case, the objective, based on the *PWSP_FP*, is to include the traffic class. This algorithm takes into account if the LSP should transport prioritized traffic (in terms of Low Impact Failure Degree). If the traffic should be protected the algorithm selects a path with low failure probability. Otherwise the algorithm does not consider the failure probabilities in order to choose the path. This mechanism enhances the *PWSP_FP*, due to the fact that paths with links with high failure probabilities are used for non-prioritized traffic, allowing a better network load balancing.

For all these algorithms, if there are several such paths with the same characteristics, one of them is randomly selected.

4.2 Routing Information

Routing protocols are used to communicate the resource properties and compute the paths. In this paper, all routing proposals need to maintain the information proposed in table 1. Tree databases are proposed in [13] in order to support the information and routing computation in the GMPLS control level.

Topology Database: Contains the information of the network graph.

TE Database: Contains information of the network constraints used by the routing protocols.

Existing Path Database: Contains information of the current working and backup paths.

In figure 2 depicts the routing process of a LSP request using the databases.

Case d: Request Rejection Ratio: Cases A, B and C have demonstrated that *PWSP* improves the *NPD*, expressed by the *FSD* and the *FID*. However it is important to remark that these algorithms do not deteriorate the number of requests accepted. Figure 4.d) shows that all these algorithms keep a Request Rejection Degree over 10-15%. Although, in this case, the best performance is offered by the *WSP*.

CONCLUSIONS

In this paper, we have proposed a new mechanism for evaluating the Network Protection Degree (*NPD*), which has two components: the Failure Sensibility Degree (*FSD*) and the Failure Impact Degree (*FID*).

Experiments have demonstrated the benefits of *NPD* application when used to improve the well-known routing algorithm *WSP*, which has been enhanced becoming a Protected *WSP*, *PWSP* in our study. This leads to a reduction in the *FSD* and *FID*, in terms of a reduction in the

number of protected links (*NPL*) and its probability of failure. Besides reducing the *NPL*, the resource consumption when using local backups is reduced. *PWSP* algorithms also reduce the impact in case of failure by decreasing the number of *LSPs* with critical (large) distances *D* and failure probabilities. In short, the presented formalization of the *NPD* paradigm should allow network and service providers to apply better QoS routing strategies that will improve the reliability of their networks.

REFERENCES

[1] Changcheng Huang, Vishal Sharma, Ken Owens, Srinivas Makam, "Building reliable MPLS Networks using a path protection mechanism", IEEE Communications Magazine, Mar 2002
 [2] D. Haskin, 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. Nov 2000.
 [3] R. Guerin, D. Williams, A. Orda. "QoS Routing

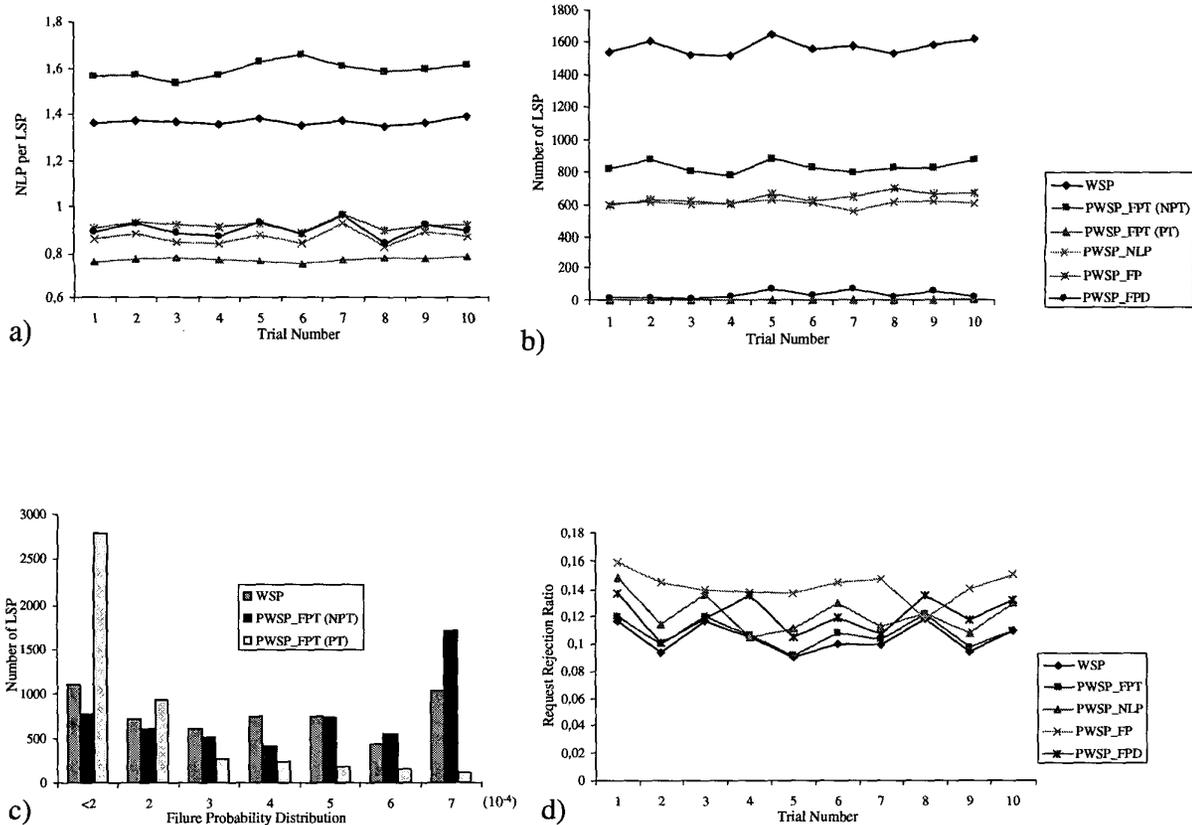


Fig 4. Experimental results a) Number of links to be protected. b) Number of LSPs with large distances (*D*) and failure probabilities. c) LSP failure probability distribution. d) LSP request rejection ratio.

- Mechanisms and OSPF Extensions". Proceedings of IEEE Globecom 1997.
- [4] M. Kodialam, T.Lakshman. "Minimum Interference Routing with Applications to MPLS Traffic Engineering". IEEE Infocom 2000.
 - [5] S. Subhash, M. Waldvogel, P. Warkhede. "Profile-Based Routing: A New Framework for MPLS Traffic Engineering". QoS'01.
 - [6] J. L. Marzo, E .Calle, C. Scoglio, T. Anjali "Adding QoS Protection in Order to Enhance MPLS QoS Routing". To appear in ICC 2003.
 - [7] J. L. Marzo, E. Calle, C. Scoglio, T. Anjali "QoS On-Line Routing and MPLS Multilevel Protection: a Survey" in preparation for IEEE Communications Magazine.
 - [8] L. Hundessa, J. Domingo-Pascual "Reliable and Fast Rerouting Mechanisms for a Protected Label Switched Path" Proceedings of Globecom 2002.
 - [9] E. Mannie et. al. "Generalized Multi-Protocol Label Switching (GMPLS) Architecture" Internet Draft. Work in progress. February 2003
 - [10] E. Mannie, D. Papadimitriou, D. S. Dharanikota, J. Lang , G. Li , B. Rajagopalan, Y. Rekhter "Recovery (Protection and Restoration) Terminology for GMPLS " Internet Draft. Work in progress. November 2002
 - [11] D. Papadimitriou, E. Mannie "Analysis of Generalized MPLS-based Recovery Mechanisms (including Protection and Restoration)" Internet Draft. Work in progress. January 2003
 - [12] J. P. Lang, B. Rajagopalan," Generalized MPLS Recovery Functional Specification" Internet Draft. Work in progress. January 2003
 - [13] Sudheer Dharanikota and Raj Jain, "Protection and Restoration in DWDM Networks: Recent Developments and Issues" Invited paper , SPIE conference 2003