Enhancing Fault Management Performance of Two-step QoS Routing Algorithms in GMPLS Networks

Eusebi Calle, Jose L. Marzo, Anna Urra, Lluís Fàbrega
Institut d'Informàtica i Aplicacions (IIiA)
Universitat de Girona, 17071 Girona, SPAIN
e-mail: {eusebi, marzo, aurra, fabrega}@eia.udg.es

Abstract— **In this paper a novel methodology aimed at minimizing the probability of network failure and the failure impact (in terms of QoS degradation) while optimizing the resource consumption is introduced. A detailed study of MPLS recovery techniques and their GMPLS extensions are also presented. In this scenario, some features for reducing the failure impact and offering minimum failure probabilities at the same time are also analyzed. Novel two-step routing algorithms using this methodology are proposed. Results show that these methods offer high protection levels with optimal resource consumption.**

I. INTRODUCTION

Recent network technologies enable the transportation of a huge volume of information. As networks grow, the consequence of a failure becomes more pronounced. Network reliability is seen as a key requirement for the new QoS Internet.

Network reliability can be provided through different fault management mechanisms applied at different network levels and time scales. Currently, many of the proposed MPLS recovery methods, including their extension to other technologies (e.g., optical networks), provide fast restoration. This is normally carried out by using GMPLS. Local, global, segment and 1+1 backups are the most common techniques proposed. The selection of the working and alternative paths is a crucial step to offer the required QoS to traffic services. Some parameters, such as packet loss or recovery time, could be affected negatively if no suitable routing algorithms are used.

There are several novel routing methods that use traffic service characterization in order to offer suitable recovery techniques. Moreover, in case of high protection priority services, pre-established and pre-allocated protection methods must be selected. These methods offer a high protection level but in exchange for poor resource efficiency. The worst case occurs when the traffic is protected using 1+1 methods (for instance in optical networks). In 1+1 protection, major proposals use one-step routing algorithms to reduce the request rejection ratio.

Another important aspect in developing optimal recovery methods is taking into account some network aspects. Networks are updated and improved adding new node and link technologies. These technologies have different reliability values. However, the network failure probability computation cannot be evaluated using only the components' reliability values. Geographical and external components also affect this final value.

In this paper we propose a new methodology to minimize both the failure impact in the network (in terms of packet loss and recovery time) and the network failure probability. This methodology involves a pre-study of the network reliability (failure probabilities) and a post-process to select the suitable protection methods. The routing methods proposed in this paper follow this methodology using two-step algorithms. We also demonstrate that these algorithms reduce resource consumption, providing the same or better protection levels than other routing proposals.

II. FAULT MANAGEMENT METHODS

In this section a brief review of the mechanisms involved in the development of a backup protection method and the corresponding recovery cycle are presented. A discussion of the advantages and disadvantages of the backup methods is also provided. Both protection architectures (MPLS/GMPLS) are used to describe these methods. Some comments related to the difficulties of extending the MPLS fault management to optical networks are also analyzed.

A. The Fault Recovery Cycle

Protection methods begin with fault identification and end with link recovery. This cycle of events involves various phases:

a) a method for selecting the working and protection paths (routing algorithm);

b) a method for signaling these paths setup, (for instance, LDP/RSVP or CR-LDP/RSVP-TE);

c) a mechanism for fault detection (from lower layers or network monitoring techniques);

d) a hold off time, which is the waiting time before triggering the fault recovery process in case lower layers could overcome the fault faster enough (e.g., at SONET level);

e) a notification method that conveys fault information to the responsible network entity for taking the appropriate recovery action (for example, by transmitting a Fault Indication Signal);

f) a switchover mechanism to move traffic from the working path to the backup path.

This is the general cycle of events that describes the establishment and utilization of a protection method; however some recovery methods do not need all of these components, or they can change the sequence order. For instance, fault notification in local backups or switchover in 1+1 methods (see details in the next section) is not required. In the case of dynamic (non pre-established) fault management methods, steps a) and b) are moved after step e). The hold off time in the

This work has been partially supported by the Spanish Ministry Science and Technology (TIC2003-05567).

case of GMPLS over SONET can be set to 50 ms such that the SONET protection scheme can activate before the MPLS layer recovery mechanism is triggered. However, if the network is not able to recover faults at lower layers, the hold off time is not used [10].

The MPLS term Label Switched Router (LSR) is used in this paper to describe a circuit-switch node (optical cross-connects (OXCs) in optical networks). In order to provide 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, these two nodes are defined in [4] as the Path Source LSR (or PSL) and the Path Merge LSR (or PML) respectively. In GMPLS, they are known as Bridge and Selector nodes [5].

B. *Fault Management Methods Description*

1) *The Global Backup Path Method*

In this model, an ingress node is responsible for path restoration. This requires an alternative, unconnected backup path for each working path. The ingress node is where the protection process is initiated, irrespective of the actual location of the failure along the working path.

The advantage of this method is that only one backup path per working path needs to be set up. Only one LSR has to be provided with PSL/Bridge functions (see Fig. 1). 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.

In order to overcome the packet loss drawback, a reverse backup path can be established in the opposite direction of the working path (5-3-1 nodes in Fig. 1). This method reverses traffic from the point of failure back to the source (ingress node) via a reverse backup LSP. In [2], Haskin proposes to pre-establish the reverse backup path making use of the same nodes of the working path, thus simplifying the signaling process.

2) *Local Backup Path Method*

In this method, restoration begins at a point much closer to the fault (see Fig. 1). The main advantage is that it offers a faster restoration time than the global repair model, as well as a significant reduction in packet loss. On the other hand, every node requiring protection has to be provided with a switchover function (PSL). Merging nodes (PML) also have to be provided accordingly. Another drawback is the maintenance and creation of multiple backups (one per protected domain). That can lead to low resource utilization and high complexity.

3) *Segment Protection*

A hybrid solution between the local and global solution is to define protection segments, which are defined as a subset of links belonging to the working path. Segments can start or finish at the ingress/egress nodes avoiding PSL or PML setup at the intermediate nodes. This allows a reduction of resource consumption and notification times. In Fig. 1 a segment protection is shown (path 5-6-8-9). In this case if a failure occurs in link 7-9, node 7 transmits a fault notification to node 5 (PSL node). In Section III, some possibilities for protecting segments are introduced as well as their advantages and disadvantages.

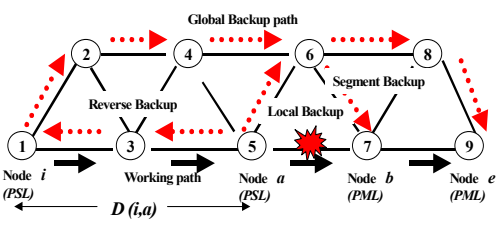

Figure 1. Fault management methods.

4) *1+1 Protection Method*

With this method the failure is repaired using the alternative working path. The traffic is sent in both paths (1-2-4-6-8-9 and 1-3-5-7-9 in Fig. 1) at the same time. In this case the PML/Selector LSR is monitoring the best working path (for instance selecting the path with the best signal). After a failure, the PML/Selector selects this single path as the working path. This method is fast and does not lose packets, but many resources are consumed since both paths need to be reserved a priori. Furthermore, a PSL/Bridge LSR also has to be set up to send the traffic over both paths simultaneously.

C. *Extending the MPLS Fault Management to Optical Networks*

In MPLS networks, the control and data planes share the same transmission media. Therefore, a single fault affects both equally. However, in optical networks the control and data planes can have different topologies, hence control messages can be sent through an "out-of-band" path (for instance, a dedicated wavelength). In other words, two OXCs that are neighbors on the data plane are not necessarily neighbors on the control plane. In this scenario, faults should be considered independent on each plane. Moreover, an LSP (in the MPLS domain) may have a reserved allocation of zero resources (such as bandwidth), but whenever a lightpath (in the optical domain) is routed, the corresponding wavelengths need to be reserved at the same time.

III. Failure Probability and Failure Impact

To define the degree of protection required for a given segment of a network, there are two main factors: firstly, working out, a priori, the probability of failure somewhere in the network; and secondly, predicting the a posteriori impact on traffic (in terms of recovery delay and packet losses) in the event of a failure.

A. *Failure Probability*

The exact failure probability of a given segment of the network (i.e., a protection domain) can be approximated based on certain information available before faults occur [3]. This calculation can begin based on known probabilities regarding certain aspects of transmission technology. This initial value can then be updated using actual failure statistics. As formulated in [3], the segment failure probability can be approximated as the sum of all the link fault probabilities. (Independent link faults and small probabilities are assumed.)

$$LSP\_FP = 1 - LSP\_FP^{-1} \approx 1 - (1 - \sum_{i=1}^{k} LFP_i) = \sum_{i=1}^{k} LFP_i$$

k = Number of links of the LSP. (1)

B. *Failure Impact (FI)*

Once the failure probability is known, the next aspect to be considered is how a failure affects the existing traffic in the network, i.e., the "failure impact". The guaranteed quality of

service (QoS) of this traffic is the crucial aspect for evaluating the failure impact, which we suggest dividing into two components: recovery time and packet loss. Other QoS components, such as increasing delay or packet reordering [8], are not considered in this work.

1) Recovery Time and Packet Loss

The recovery time is defined by the fault recovery cycle (as presented in Section II. This time consists of the following: a) time for detecting the fault T_{DET} (for instance a signal from lower levels); b) the Hold off time T_{HOF} (if necessary); c) the Notification time T_{NOT} to inform (i.e., send a message to the node responsible for the switchover); d) the time for backup setup, routing and signaling T_{BS}; and e) the time for traffic switchover T_{SW} from active path to backup path. Therefore, the Recovery Time T_{REC} can be evaluated by simply adding these components, as the following expression shows:

$$T_{REC} = T_{DET} + T_{HOF} + T_{NOT} + T_{BS} + T_{SW}. \quad (2)$$

The Packet Loss (P_{LS}) is proportional to this T_{REC} and to the transmission Rate R_{TR}. The packet loss in the fault link P_{FL}, (i.e., those packets being transported in the physical link at the moment of failure) cannot be avoided by the protection mechanisms presented in Section II. Nevertheless, there are some proposed mechanisms (such as the one presented in [8]) that overcome this drawback. The resulting expression is:

$$P_{LS} = R_{TR} \cdot T_{REC} + P_{FL}. \quad (3)$$

2) Reducing the Failure Impact

Table 1 sums up the options for reducing failure impact by reducing the time needed for each phase of the fault recovery.

TABLE I. THE FAULT RECOVERY CYCLE AND THE FAILURE IMPACT REDUCTION

Recovery phase	Features	Fault Impact Reduction
Fault detection (T_{DET})	Depends on the technology	Cannot be reduced
Hold off time (T_{HOF})	Depends on the lower layers	Setup (0-50 ms)
Notification time T_{NOT})	Depends on the D(i,a)*	Minimizing the D(i,a)*
Backup selection (T_{BS})	Depends on the routing and signaling method applied	Pre-establishing the backup
Switchover (T_{SW})	Depends on the technology	Cannot be reduced

* D(i,a) is further defined in this section, see also Fig. 1.

Reducing fault detection and switchover time depends on the technology used and this cannot be easily modified. Moreover, the establishment time of on-demand backup paths (once the fault is detected) depends on the routing and signaling methods used. In the case of pre-established backup paths, this delay can be avoided. In MPLS networks, a backup path can be pre-established with no allocated resources (bandwidth). This technique is also known as "fast restoration". In optical domains, the bandwidth (wavelength) must always be allocated.

The reduction of the notification time T_{NOT} is probably the most challenging aspect in designing the protection methods for a network. The notification time depends on the propagation time T_{PR} of the fault indication signal per link and on the distance D(i,a), which is defined as the number of links between the node detecting the failure (node a) and the node responsible of the switchover (node i).

$$T_{NOT} = T_{PR} \cdot D(i,a). \quad (4)$$

Since the propagation time only depends on the physical link technology, the reduction of T_{NOT} can only be achieved by reducing the distance (D(i,a)). Local backups achieve the optimal case: (D(i,a) = 0). The main drawback is that the distance D(i,a) is not known in advance because it is not yet known which link will fail. However, the link fault probabilities can be used to estimate these distances in a probabilistic manner.

C. Reducing the Probability and the Impact of a Failure

In this section, we present an analysis of the use of the proposed paradigms, such as fault probability, notification time and resource consumption. The objective is to design (and manage) networks in order to minimize fault probability and fault impact. This is not an easy goal, as there is sometimes a tradeoff between reducing the impact and reducing the probability. For instance, reducing fault probability may imply increasing the distance D(i,a), and therefore increasing the potential impact of a fault. On the other hand, reducing both simultaneously could imply excessive resource consumption. In addition, the class of traffic to be protected can also be crucial in making the right decision. In next section some of these aspects are analyzed and discussed.

1) Residual Failure Probability and Failure Impact values

In Sections III. A) and B) the failure probability and the failure impact have been defined. However, if some links/segments of the network are protected (by using a backup path), the residual probability and impact values can be reduced, or eliminated. For example, in a simple scenario (shown in Fig. 2.a) the working path contains two links with different failure probabilities. If this path is not protected, the Residual Failure Probability (RFP) of this path is the sum of the path link failure probabilities LSP_FP, formula (1). However, if the path is protected, using segment or local backups (Fig. 2.a and 2.b respectively), the residual failure probability will be zero. On the other hand, if the backup policy is to protect just one link, the residual failure probability is reduced to the value of the non-protected link.

The failure impact is evaluated as the degradation of the QoS after a failure occurs in a protected segment. This degradation is proportional to the failure recovery cycle. We propose evaluating this impact based on the notification distance D(i,a). Therefore, if the links are protected using local backups (D(i,a)=0) the failure impact is virtually zero (Fig. 2.b). If segment or global backups are used the impact depends on the distance D(i,a) of each link (to be protected) respect to the PSL node of the backup path.

2) Techniques for Reducing the Network Failure Probability and Impact

In this section, the reduction of the network impact and the failure probability are analyzed in some cases (using backup techniques). We assume that a two-step routing method is applied. For a given working path, the most suitable backup method is finally selected depending on its protection requirements.

Let us consider the case of a working path which has some adjacent links to be protected. These links can be protected by a segment backup (see Fig. 2.a). This protection technique eliminates the Residual Failure Probability (RFP = 0). However, the Failure Impact (FI) for the link with high failure

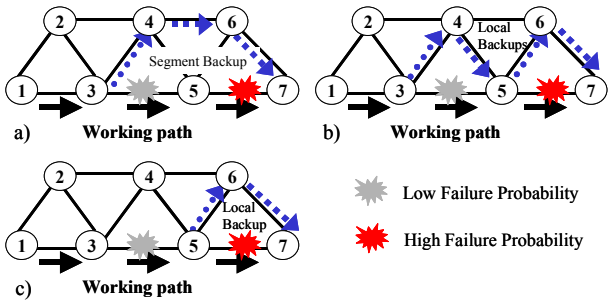

Figure 2. Adjacent links. Local protection vs Segment protection.

probability is equivalent to the distance (D (3,5) = 1). If the carried traffic is sensitive to the recovery time or the packet loss and there are links with high fault probability, the segment cannot be protected using segment backups. Hence, just local backup protection should be applied in order to avoid a large failure notification delay (Fig. 2.b). The FI is eliminated (FI=0) using two local backups. However, this case can result in large resource consumption. An intermediate solution can be achieved if only the link with high failure probability (link 5 – 7, see Fig. 2.c) is protected with a local backup. This case (case 2.c) eliminates the failure probability and impact for the link with high protection requirements. The amount of resources used in case 2.c) is also reduced. However, in this solution a link (with a certain failure probability) is not protected.

Now let us consider that the working route has some links to be protected, but they are separate, hence a segment backup cannot be used. In this case, the protection method to be applied depends on the level of the desired protection and on the traffic class. If the number of links to be protected is large, a global backup, which includes all links (high and low fault probabilities), can be used (Fig. 3.a). This involves eliminating the residual failure probability (RFP=0), but could increase the distance (as shown in Fig. 3.a), thus introducing greater packet loss and longer recovery times in the case of failure (a high FI). In this example, the distance for the high failure probability link is 2 (D(1,5)). For high levels of protection, local backups should be established for each link (Fig. 3.b). At least those with high fault probabilities should be protected in order to offer a balance between the final protection degree and resource consumption.

There are also hybrid cases where, depending on the fault link probabilities LFP and distances D(i,a) (for notification), a specific choice between local, segment or global protection should be made. Even a "no protection" policy may be chosen, depending on the traffic class.

Note that the selection of the most suitable protection

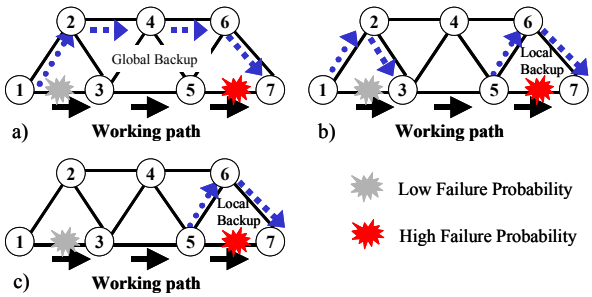

Figure 3. Separated Links. Local protection vs Global protection.

mechanism for every working path is not a simple task. Although all the information about traffic class, network available resources, etc., is known, a decision mechanism, more or less sophisticated, is desirable for selecting the most suitable protection mechanism. There are some proposals [1 and 9] aimed at mapping different traffic classes with the protection methods described in Section II. In the following section a discussion of current restorable QoS routing is presented and contrasted with some of the enhancing mechanisms described above.

IV. Restorable QoS Routing Solutions

In previous sections, the general cycle of events in fault protection methods was described. The first phase, which may be the most relevant, is the selection of the working path, and eventually the protection mechanism. In this section, some new routing algorithms are proposed to demonstrate, experimentally, aspects depicted in previous sections.

A. Restorable QoS Routing

Most current QoS routing algorithms consider protection issues as a secondary objective (if they are considered at all); normally, traffic is simply re-routed in the event of a failure. Some algorithms do consider restorable QoS routing, which is applied in a homogenous manner. This all new LSP request implies setting up a backup path. Most of them use path protection (global o 1+1). Although recently there have been more efforts made in this direction, few proposals involve the utilization of local/segment recovery paths, and fewer still use the most suitable protection method for each traffic class.

B. Two-step versus One-step Routing

The process of establishing the working and backup paths can be done in two steps by first calculating the working path (the shortest path meeting the QoS constraints) and then calculating the backup path (shortest disjoint path). In some cases, (see Fig. 4.a), the working path of the two-step algorithm blocks all the possible global backup paths. There are some proposals that establish the shortest cycle algorithm in order to avoid this disadvantage. However, as explained in Section III, it is more useful to take into account the working path properties (with respect to the failure probabilities) in order to select the working path with the optimum protection requirements. This allows us to select a path with less failure probabilities, and, in some cases, allows for better resource consumption (using local/segment backups or even no backups at all). Fig. 4.c) depicts a case where a two-step algorithm allows a working path with less failure probabilities to be selected. Furthermore, it can be protected with a segment

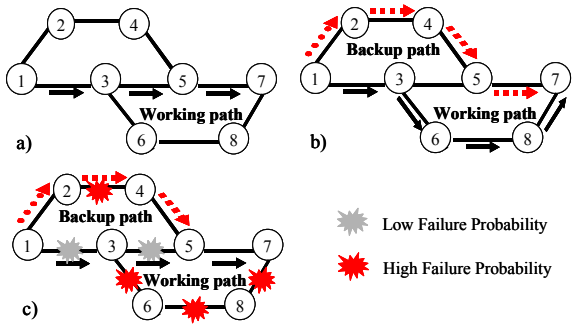

Figure 4. Disjoint routes computation.

backup path which results in less resource consumption than in case b).

V. EXPERIMENTAL RESULTS

In this section, to reduce the probability and the impact of a failure, we experiment with two modified routing algorithms, both based on the well-known K-Widest Shortest Path (K-WSP) [11]. These algorithms choose the path with the minimum number of links to be protected (in these experiments those links with LFP>$1 \cdot 10^{-4}$). This reduces the resource consumption (i.e. the bandwidth allocated to establish backup paths). In this paper, these algorithms are referred to as Minimum Residual Failure Probability and Impact (M-RPI) routing algorithms. In order to evaluate different failure impact values (in terms of notification distances), the first algorithm only uses Local backup paths (M-RPI-L) and the second one can create Segment backup paths (M-RPI-S) whenever the links to protect are correlative, providing different notification distances.

For this set of experiments the topology described in [3] has been used. Experiments are based on formulas (1) and (4) (failure probabilities and notification distances).

The first set of experiments is focused on evaluating the residual failure probability. Each point in the chart represents the network residual failure probability. This value is computed every 100 new LSP requests as the accumulation of all current LSP residual failure probability values. Results in Figs. 5.a) and 5.b), corresponding to the utilization of algorithms M-RPI-L and M-RPI-S respectively, show similar behavior. The Network Residual Failure probabilities for the protected traffic are accumulated close to zero, while the non protected traffic values are more dispersed across higher network failure probabilities.

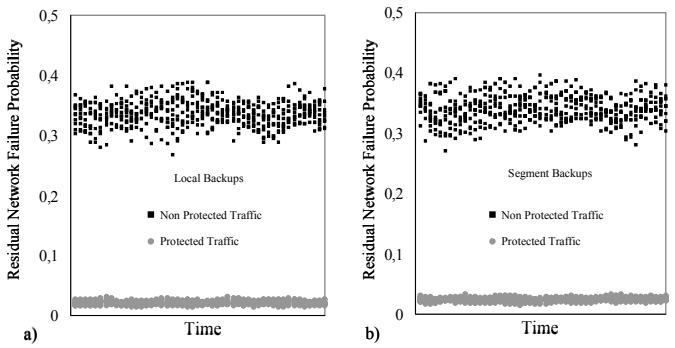

Figure 5. Network Residual Failure Probabilities results.

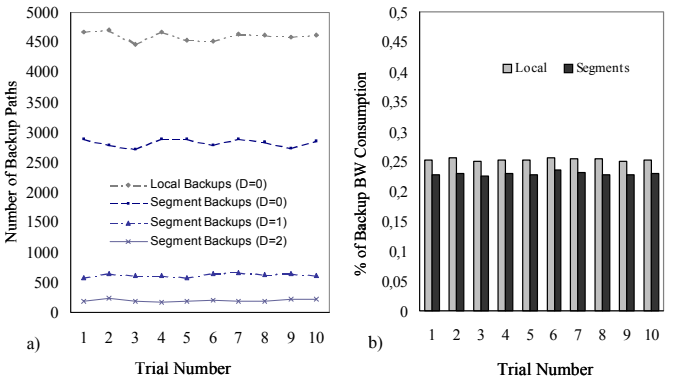

Figure 6. Resource Consumption and failure impact results.

However, using Local backups or Segment backups, the residual failure probabilities can be reduced in a similar manner, and the failure impact and resource consumption are affected in different ways. In Fig. 6.a) M-RPI-S distributes the protection of the network using segment backups with different notification distances (D=0, 1 and 2). In this experiment, major backups are local backups and there are a few backups with large notification distances. This can result in a high number of packet losses if a failure occurs in those LSPs with large D. On the other hand, using segment backups results in better resource consumption, which can be observed in Fig. 6.b).

VI. CONCLUSIONS

In this paper, we have proposed a new methodology that allows improvements of the GMPLS fault management based on reducing the failure probabilities and failure impact. This allows supporting traffic services with high network reliability requirements. Using this methodology, a new set of two-step K-WSP-based routing algorithms has been tested. Results show that there is a strong relationship between the residual failure probabilities and resource consumption. Local or segment backups can be used in order to reduce the residual failure probability. Local backups avoid notification distances while providing better protection in terms of packet loss and recovery times, but there is higher resource consumption than in segment backup protection. There is also a tradeoff between the number of the used resources, the selected protection mechanism (local, segment or global backups), and the residual failure probability and failure impact.

REFERENCES

[1] J. L. Marzo, E .Calle, C. Scoglio, T. Anjali, "Adding QoS Protection in Order to Enhance MPLS QoS Routing", In Proceedings of ICC 2003, Anchorage, Alaska.

[2] J. L. Marzo, E. Calle, C. Scoglio, T. Anjali, "QoS On-Line Routing and MPLS Multilevel Protection: a Survey". IEEE Communications Magazine, October 2003.

[3] Eusebi Calle, Jose L Marzo, Anna Urra "Protection Performance Components in MPLS Networks" Accepted in Computer Communications Journal, Elsevier 2004.

[4] V. Sharma, Metanoia, F. Hellstrand, "Framework for Multi-Protocol Label Switching (MPLS)-based Recovery", RFC: 3469, February 2003.

[5] D. Papadimitriou, E. Mannie, "Analysis of Generalized MPLS-based Recovery Mechanisms (including Protection and Restoration)". Internet draft. Work in progress. January 2003.

[6] J. P. Lang, B. Rajagopalan, "Generalized MPLS Recovery Functional Specification". Internet draft. Work in progress. January 2003.

[7] Changcheng Huang, Vishal Sharma, Ken Owens, Srinivas Makam, "Building reliable MPLS Networks using a path protection mechanism", IEEE Communications Magazine, March 2002.

[8] L. Hundessa, J. Domingo-Pascual, "Reliable and Fast Rerouting Mechanisms for a Protected Label Switched Path", Proceedings of Globecom, 2002.

[9] Hongwei Zhang, Arjan Durresi, "Differentiated Multi-Layer Survivability in IP/WDM Networks", 8th IEEE-IFIP Network Operations and Management Symposium (NOMS 2002).

[10] R. Rabbat, V. Sharma, N. Shinomiya, C. Su, P. Czezozowski, "Fault Notification Protocol for GMPLS-Based Recovery. Internet draft (work in progress). February 2003.

[11] R. Guerin, D. Williams, A. Orda, "QoS Routing Mechanisms and OSPF Extensions". Proceedings of Globecom 1997.