Enhancing MPLS QoS routing algorithms by using the Network Protection Degree paradigm.*

Eusebi Calle, Jose L Marzo, Anna Urra, Pere Vila
Broadband Comm. and Distributed Systems
Institut d'Informàtica i aplicacions (IiiA)
Universitat de Girona, 17071 Girona, SPAIN
e-mail: {eusebi, marzo, aurra, perev}@eia.udg.es

***Abstract*- IP based networks still do not have the required degree of reliability required by new multimedia services, achieving such reliability will be crucial in the success or failure of the new Internet generation. Most of existing schemes for QoS routing do not take into consideration parameters concerning the quality of the protection, such as packet loss or restoration time.**

In this paper, we define a new paradigm to develop new protection strategies for building reliable MPLS networks, based on what we have called the Network Protection Degree *(NPD)*. This *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*), to determine the impact on the network in case of failure.

Having mathematical formulated these components, we point out the most relevant components. Experimental results demonstrate the benefits of the utilization of the *NPD,* when used to enhance some current QoS routing algorithms 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 MultiProtocol Label Switching (*MPLS*) networks. MPLS fault restoration mechanisms usually establish backup Label Switch Paths (*LSPs*). With these backups, traffic can always be re-routed when a failure occurs. MPLS 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 LSPs 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 Sensitivity 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.

* This work has been partially supported by Special Action (Spanish Ministry Science and Technology)TIC2002-10150-E.

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 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 $LFP << 1$.

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:

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

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

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=Number of links of the LSP *(2)*

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

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

k = Number of links of the LSP *(3)*

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

$$LSP\_NLP = \sum_{i=1}^{k} LPR_i$$

k = Number of links of the LSP *(4)*

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)*).

$FSD\_FP = (LSP\_FP_1, LSP\_FP_2, \ldots LSP\_FP_N)$ *(5)*

$FSD\_NLP = (LSP\_NLP_1, LSP\_NLP_2, \ldots LSP\_NLP_N)$ *(6)*

Where: N = *Number of LSPs in the network*

These arrays allow defining different strategies to evaluate the *FSD*. With *(5)* the number of LSPs out of an 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. 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:

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

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:

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

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

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

Fig 1 shows the most common used MPLS protection methods (global and local backups). The advantages and disadvantages of these, and other, mechanisms are widely discussed in the literature [1], [2],and [3]. In our previous work [6], and [7], Packet Loss and Recovery Delay are considered as well as packet reordering and resource consumption. Basically, Local Backups offers a solution respect to Packet Loss and Recovery Time problems of the Global Backup. Nevertheless, when the number of links to protect in the path is elevated Local Backups are not suitable, due to elevated resource consumption. In order to formulate *FID* for each protection method we have assumed the following simplifications:

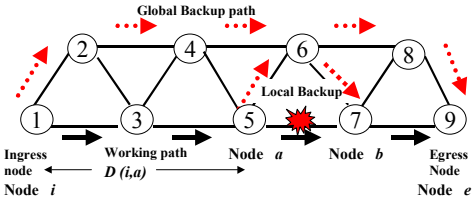

Fig.1. Global and Local LSP Backup Paths.

1) The fault detection time, T_{DET}, depends on several factors (such as the level of the network where the fault is detected, or the performance of the switch components). However, these aspects affect all protection mechanisms equally. Moreover, the switchover time, T_{SW} , is negligible with respect to the notification time, T_{NOT} , and to the backup establishment time, T_{BE}. For the purpose of simplification, they have not been considered in *FID* formulation.

2) Most of currently proposals consider inevitable the packet loss at the failed link P_{FL}. However, there are some recent approaches that propose the utilizations of buffering and tagging techniques to avoid such loss [9]. Whether or not these techniques are used, in both cases packet loss is still negligible in relation to the total amount of packet loss, hence they are not considered in this work

3) The most significant elements, in terms of delay, of Packet Loss and the Recovery Delay (deriving from *(4)* and *(5)*) are the notification time, T_{NOT}, and the backup establishment time, T_{BE}. However, further analysis of T_{BE} implies a better analysis of the diverse routing algorithms because T_{BE} is proportional to the time needed to get a new route.

The first element to look at is $T_{NOT.}$. T_{NOT} is proportional to the propagation time for the message, T_{PR}, and the distance from the node where the fault is detected (*a-node*) to the responsible of the switchover (*i-node*) (see fig. 1). Although this distance, *D(i,a)* , should be expressed in a real metric (meters, Km, etc.), *D(i,a)* is in fact expressed in terms of the number of hops for the purposes of simplification. Therefore, the calculation for fault notification is:

$$T_{NOT} = D(i,a) * T_{PR} \qquad (11)$$

Then, the *FID* is obtained using *(7),(8)* and *(9)*:

$$FID = f\ (D(i,a) * T_{PR}\ ,\ D(i,a) * T_{PR} * R_{TR}) \qquad (12)$$

As expected, packet loss is proportional to the restoration time which depends on distance (*D(i,a)* as defined) and on the propagation time $T_{PR.}$.

In conclusion, the greater the distance, (or, the greater the propagation time), the worse the impact of a failure is. Reducing the propagation time of the fault notification would reduce the impact. Unfortunately this depends on the physical topology which is, for a given network, a static

parameter, and therefore difficult to modify. Thus, any effort to minimize the impact of failure should be aimed at trying to reduce the distance from the node where the fault occurs and the node, which carries out the switchover.

III. NETWORK PROTECTION DEGREE APPLICATION.

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

$$NPD = f(FSD, FID) \qquad (13)$$

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.

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(i,a)*) 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.

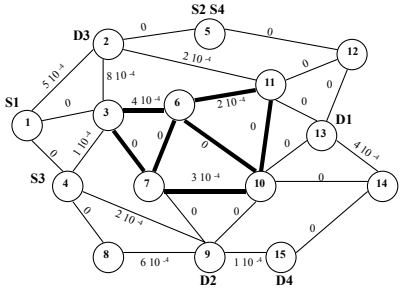

Fig 2 . Network Topology

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(i,a).* In this case, the objective is to reduce not only the failure probability, but the failure impact (minimizing the distance D(i,a), as explained in section 2.2). Each link of a LSP is weighted by the product of the distance *D(i,a)* by the *LFP*. With the total sum of these values, the LSP with the lowest value is selected.

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

IV. EXPERIMENTAL CALCULATION OF *NPD*.

In this section, the *NPD* is evaluated in two network scenarios. For these experiments we used the same topology, (see Fig. 2), as in several other studies such as [5], or [6]. The capacity of the links is 12 and 48 (bolded lines) units. But these capacities are scaled by 100, in order to experiment with thousand of LSPs. Each link is bi-directional (i.e., it acts like two unidirectional links of half of that capacity). There are 15 nodes and 28 links. There are four Ingress-Egress node pairs (see fig.2).

Link Failure Probabilities *(LFPs)* are assigned according to figure 2. There are 11 links to be protected, which represents a 40.7 percent of the network. In all simulation experiments described in this paper, LSP requests arrived randomly, at the same average rate for all node pairs. We assume that all links are long live (i.e., "static case"). For each experiment, 20 trials with 3000 LSP demands were conducted. The bandwidth allocation for the LSPs is uniformly distributed between 1, 2 and 3 units. Results have been obtained by implementing the QoS routing algorithm proposed in previous section.

Case a: Number of links to be protected: figure 3.a) shows an analysis of the average of the number of links to be protected (*NLP*) per LSP. Charts show that all routing schemes with protection (*PWSP* algorithms) have similar *NLP* results. In the case of applying a WSP, the *NLP* per LSP sharply increases (about 35 % more). This leads us to state that: a) WSP routing increases the probability of failure (due to a major number of links with a certain failure probability), and b) it increases the resource consumption if these links are protected with backups.

Case b: Failure impact degree: In this case we have analyzed the reduction in the *FID*, based on distance (*D(i,a)*). Fig 3.b) shows the distribution of LSPs with links to be protected at different distances. Results, as expected,

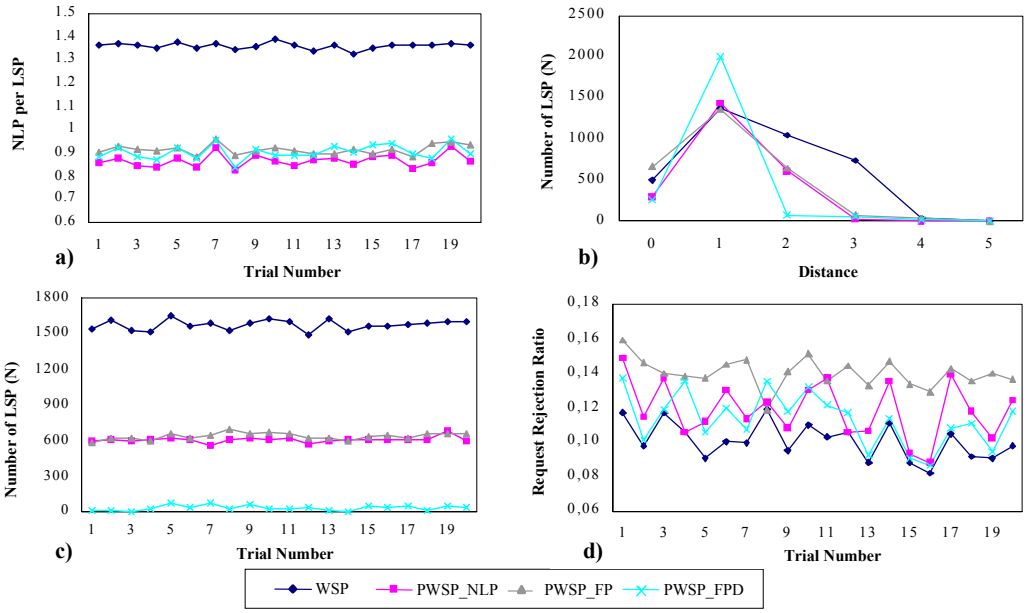

Fig. 3. a) Number of links to be protected. b) Failure impact Degree Analysis. c) Failure impact Degree Analysis. d) Request Rejection Ration

shows that *PWSP_FPD* has the best performance, allocating the major number of links to be protected at distance 1. Again, WSP shows the worst behavior distributing a big number of links to be protected at distances *D(i,a)>1*.

Case c: Optimizing the Network Failure Degree: Fig. 3 shows the number of LSPs out of a pre-set *NPD* threshold. The *NPD* (formula [13]) is evaluated in terms of notification distances (formula [12]) giving the *FID* value and failure probabilities (formula [5]) to evaluate the *FSD*. We have computed those LSPs with distances *D(i,a)>1* (large *FID*) and $LSP\_FP>2\cdot10^{-4}$ (large *FSD*). In this case the best option, once again, is the *PWSP_FPD*. However *PWSP_NLP* and *PWSP_FP* shows a similar protection degree better than the WSP.

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 3.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(i, a)* 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. Nov 2000.

[3] R. Guerin, D. Williams, A. Orda. "QoS Routing 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". QofIS'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" to appear in IEEE Communications Magazine, October 2003.

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