AN IMPROVED GMPLS SURVIVABILITY MECHANISM USING LINK DELAY-CONSTRAINED ALGORITHM

Anastasios Bikos[2], Christos Bouras[1,2] and Kostas Stamos[1,2,3]
[1]*Research Academic Computer Technology Institute, Patras, Greece*
[2]*Computer Engineering and Informatics Department, University of Patras, Patras, Greece*
[3]*Technological Educational Institute of Patra, Patra, Greece*

Keywords: GMPLS, Link failure probability, Link delay-constrained Algorithm, LSP routing, Path protection.

Abstract: It is widely accepted that GMPLS (Generalized MPLS) will be a key technology in the evolution of the next generation of reliable Internet Protocol (IP) backbone networks. Conventional GMPLS-based optical-switching network fault recovery only provides resiliency in terms of path segment selection instead of constraint-based calculation. This can create severe impact on the protocol's transport plane when a fault occurs to a link or path with many optical connections attached to it. This paper proposes the implementation of an improved GMPLS recovery algorithm based on the metric of optical link delay which is achieved through the pre or post selection of a safer and more stable protection path with fewer connections attached to it, and therefore with a lesser link delay metric compared to other possible paths. The improved recovery algorithm is evaluated using the network simulator ns-2 and more particularly a specialized simulator add-on for GMPLS, called ASONS (Automatically Switched Optical Network Simulator). The results indicate improved resiliency, increased fault avoidance, and reduced packet loss.

1 INTRODUCTION

As IP traffic becomes more and more massive, the optical switching network emerges as the most promising solution for meeting the modern backbone network needs. This has caused the introduction of GMPLS (Generalized Multi-Protocol Label Switching), as a reliable and stable optical framework, in order to meet those new standards and developments of telecom services (Dutta, 2008; Stern, 2009; Farrel, 2006).

While optical fiber medium using wavelength division multiplexing (WDM) offers tremendous transmission bandwidth to deliver high-traffic services cost effectively, faults such as the unavailability of optical links are still an important issue to resolve. Because the most massive amount of traffic is transmitted over the optical backbone network, a fault in the backbone may result in very important service degradation. This forces Internet Service Providers (ISPs) to include network reliability parameters in their Service Level Agreements and to design new protection strategies guaranteeing fast failure recovery times and high levels of reliability.

In this paper, we describe the design and performance analysis of a QoS-Constrained GMPLS Recovery algorithm, based on the ideas that have been presented in (Ortega, 2004) for MPLS, which is based on the dynamically changing optical link Delay Constraint, distributed by the IGP Routing Protocol. This makes the GMPLS fault recovery procedure able to adapt to the current network state and based on that condition it then becomes possible to post compute and configure the backup path. Finally, we evaluate the implementation of the currently existing GMPLS Protection Mechanisms, as well as an improved Restoration Mechanism, based on this new algorithm, under the network simulator ns-2 environment.

2 NETWORK SURVIVABILITY ISSUES AND RECOVERY SCHEMES

Next-generation optical communication technologies (DWDM/OADM/PXC) are expected to exceed aggregate capacities of hundreds of terabits per

Bikos A., Bouras C. and Stamos K..
AN IMPROVED GMPLS SURVIVABILITY MECHANISM USING LINK DELAY-CONSTRAINED ALGORITHM.
DOI: 10.5220/0003433900450050
In *Proceedings of the International Conference on Data Communication Networking and Optical Communication System* (DCNET-2011), pages 45-50
ISBN: 978-989-8425-69-0

second. As wavelength routing and all-optical switching paves the way for network throughput of such scales, network survivability assumes critical importance. A single loss of or damage to a fiber is a common means of a greater loss. A short network outage can lead to huge data loss, particularly in the backbone core. Thus, a connection being carried in the network also needs high protection and resilience. Survivability refers to the ability of the network to reconfigure and re-establish communication upon node and/or link failures.

Such network survivability can be classified into two general categories: pre planned protection and dynamic restoration. In pre-planned protection-based techniques resources are already planned, typically at the time of establishing a lightpath connection, to recover from network failures and hence recovery is faster.

During the normal operation phase these reserved resources remain idle. Upon the occurrence of failure, reserved resources are used to recover from the failure according to protection protocols. In contrast, in dynamic restoration, the resources used for recovery from failure are not reserved at the time of connection establishment, but are discovered dynamically using link state algorithms when a failure occurs. As it is obvious, dynamic restoration uses resources efficiently, but the restoration time is usually longer, because it requires the establishment of a new functional backup path. Moreover, 100% service recovery cannot be guaranteed as it is not guaranteed that the spare capacity is available at the time of failure (Dutta, 2008).

2.1 Problems with Conventional GMPLS Restoration Mechanisms

One of the most common problems of the existing fault recovery schemes in GMPLS networks is that they do not consider the already existing link load of a backup path when it has to be configured. A typical bad case scenario is when selecting an optical link which is a critical segment, or cut-edge, for many connections. It has been shown that a failure on this link has more overall impact on the network traffic (Changwoo, 2007). Figure 1 shows a related network situation where more connections cross through a particular optical link, which therefore acts as a bridge, than other links. As the number of connections increases in a particular link, so does the overall impact of a potential failure of the link.

It is well known that some links have higher failure probabilities, and this can be attributed to their physical situation and conditions. This Link Failure Probability Factor (LFP) is based on the type of physical link, the node characteristics and geographical distribution of the network segments. Since these parameters are outside of our control, we consider the LFP values for the network topology as given, and our purpose is to route backup paths so that traffic distribution across the network becomes as even as possible. Thus we can try to decrease the impact of new potential network faults in terms of affected connections.

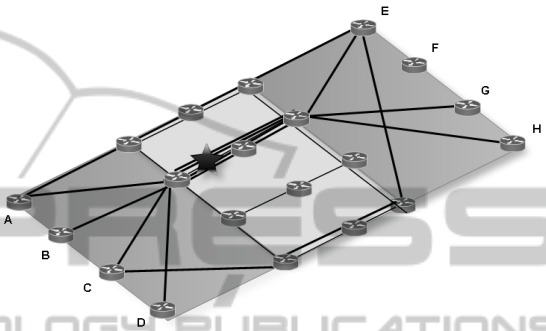

Figure 1: Link Failure in a Path with many connections (Changwoo, 2007).

3 LINK DELAY-CONSTRAINED ALGORITHM IMPLEMENTATION

Due to the previous problems that occur from traditional unconstrained Restoration Schemes in GMPLS networks, our proposed algorithm configures a backup path by searching for the optimal path through the link state algorithm, based on the delay parameter. The key concept of this improved algorithm is that the path selection procedure typically prefers links that carry fewer connections, and thus, given the Link Failure Probability Factors, distributes the impact of links failures on LSP more evenly.

3.1 Constraint-based Algorithm

The implementation of our mechanism, from now on called LDC (Link Delay-Constrained), is separated in two phases: The **Link Searching for Delay Constraint Procedure** and the **Modified Dijkstra Algorithm** which takes into account the filtered link information, with newer cost values, from the previous phase according to the least delay constraint. The delay metric can be calculated using

on the fly measurements.

3.1.1 Link Searching for Delay Constraint

We present the following pseudo code that searches for the optical link that satisfies the least link delay constraint among all its neighbouring ones. In particular, when it indeed finds this optimal link, it sets all its nearby links, except itself, with higher arc weight or cost (w(n, mi) >= 2), so that the Modified Dijkstra's Algorithm in the second phase will be able to calculate the optimal path based on these new link cost metrics, and thus re-update the whole routing table. The optimal link selected from this phase will continue to preserve the default cost value (c=1), thus it will remain first selection priority for the Dijkstra's Algorithm, in order to create the Protection Path.

```
L = All links except primary path links(l)
Function Link_Delay_Constraint_Search(L)
  FOR each node n
    Find link with min delay {lmin}
    FOR each link l of n
      IF l ≠ lmin
        Set weight value of link l = 2
      ELSE
        lmin = 1 {default link cost}
Return L
```

Figure 2: Link Searching for Delay Constraint.

3.1.2 Modified Dijkstra's Algorithm

The algorithm (Changwoo, 2007) receives the L value from the previous phase and then searches and selects a link to the destination t with the smallest number of connections within pool L. Afterwards, the optimal backup path is being configured. In any case, even if an optimal path segment to a specific node destination might not logically exist, due to the previous link delay cost update, the Dijkstra's Algorithm (Changwoo, 2007) will compromise to a path selection even with worse arc weight ($w \geq 2$).

4 REDUCING THE IMPACT OF THE LFP FACTOR WITH LDC

As discussed in the introductory section, in GMPLS-based networks the usual method of recovering a failure is the utilization of an alternative and disjoint path to the main working path. The general time process for the failure recovery procedure which applies to both pre planned protection and dynamic restoration is discussed in (Ortega, 2004).

Since the failure event point occurs, there is a time period when data packets are inevitably being lost due to the uncompleted switchover process, and until the normalization procedure finishes. If the survivability mechanism (either pre planned or dynamic) does not consider the load of traffic carried by each link of the potential protection LSP, the restoration can become prone to more recurrent faults and their associated costs. One such example, where the impact of Link Failure Probability greatly affects the future failure impact of the protection LSP is shown and described in Figure 3.

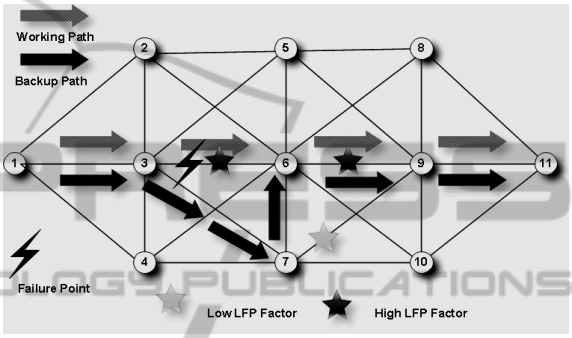

Figure 3 (a): Link Failure Probability in the Working Path with Conventional Resiliency.

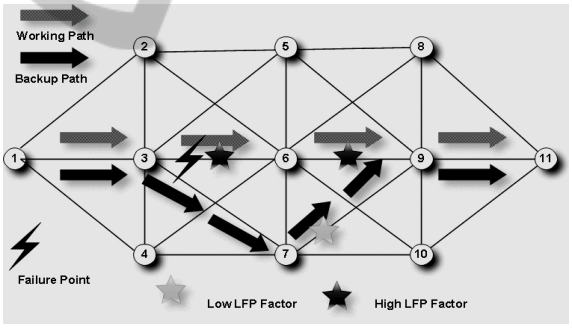

Figure 3 (b): Link Failure Probability in the Working Path with LDC Improved Resiliency.

Let as assume that the centralized optical links 3-6 and 6-9 act as bridges for the overall network traffic, thus contain a large number of optical connections, as most traffic passes through them. In Figure 3 (a) the working path (formed by the LSRs 1-3-6-9-11) contains the two links with high Link Failure Probability (3-6 and 6-9).Unfortunately this conventional method for path selection causes a high risk of increased service impact, should a possible link failure occur in the future. Indeed, when a failure event occurs between the nodes 3 and 6 (one of the two links mentioned earlier with high LFP Factor), the GMPLS conventional survivability

procedure configures a segmented backup Path that only avoids this faulty connection and does not consider any other constraint condition for some potential future failures on itself.

On the other hand, the LDC Survivability mechanism not only avoids the fault, but it actually configures a disjoint backup path that is both optimal and safe. Thus, it diminishes the impact of a further link failure (between the nodes 6 and 9), by choosing the optical link 7-9, which is conventionally not selected to be the minimum path segment by the Routing Algorithm.

This has great effect on the network's Resilience level both for dynamic or pre planned protection methods. In the first case, after the fault, the LDC link state algorithm adapts to the current network conditions and state (concerning the number of link connections) in order to select the optimal backup path. In the second case, again based on the same algorithm, we pre-select this optimal path with the advantage now of gaining in packet loss and switchover normalization time, compared to the post planned protection method which needs to establish a new lightpath. The results can be a more evenly distributed network topology and traffic as we can clearly see in Figure 4 (Compared to Figure 1).

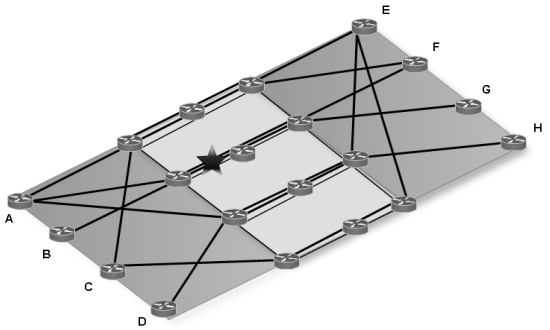

Figure 4: An evenly distributed network traffic (Changwoo, 2007).

4.1 Improved Restoration Mechanism using the LDC Algorithm

In this section we examine the issue of restoration and calculation of a backup path after the failure has occurred. Figure 5 illustrates the unconstrained selection of a backup path (dashed line) in case of failure. The particular path is in fact prone to more potential future failures compared to the LDC algorithm which takes into consideration the current load for each link in the topology graph to form the optimal path (bold line). The only difference with the previous schemes is that this procedure is being implemented a posterior, after the link failure event. The results can be increased fault avoidance and resiliency, and also a more evenly distributed network traffic across the network, without congested lines and nodes prone to new failures.

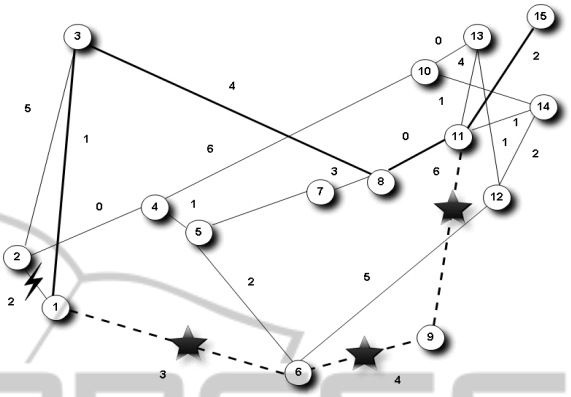

Figure 5: Post selecting an optimal backup path based on the LFP factor.

5 EXPERIMENTAL RESULTS ON NS-2

For evaluating the LDC algorithm we utilize the network simulator ns-2 environment (www.isi.edu/nsnam/) along with the ASONS simulator (An Automatically Switched Optical Network Simulator, www.telecom.ntua.gr/asons/). For our experiments we use an example network topology consisting of 14 nodes (figure 5). It consists of 14 nodes and 21 STM-64 (10Gbps) SDH Full-Duplex FiberLinks. We simulate real physical mile distances by using equivalent link delays. Each experiment lasts for 10 seconds, and the (sequential) failure events occur approximately at 5.0, 5.5, 6.0, 6.5 and 7.0 sec. The failure points are between nodes: 2-4, 4-5, 5-7, 7-8, and 8-11 respectively. Table 1 illustrates the parameters used.

Table 1: Network parameters for the experiments.

Network Parameters	Traffic Parameters (Exponential VBR)
Link BW : 10 Gbps **Link Delay :** 5×10^{-4} sec **Fiber Delay :** 1×10^{-3} sec **Network Load :** Exponential	**Traffic Rate :** 100Mb **Packet Size :** 100 Bytes

Table 2: The impact of Failure Notification Distance (relevant to the LFP Factor) and receiving Bandwidth Rate to Recovery Time (T_{REC}) and total Packet Loss (PLS).

Throughput (Mbps)	*Failure Notification Distance*							
	D(i,a) = 1		*D(i,a) = 2*		*D(i,a) = 4*		*D(i,a) = 0*	
	TREC	*PLS*	*TREC*	*PLS*	*TREC*	*PLS*	*TREC*	*PLS*
10^4	*23,5*	*1989*	*30,7*	*1992*	*42,1*	*3511*	*0,0*	*291*
10^3	*26,2*	*2695*	*33,3*	*4045*	*43,2*	*4112*	*0,0*	*300*
10^2	*26,6*	*2962*	*33,4*	*4858*	*45,6*	*4327*	*0,0*	*304*
10	*25,6*	*6948*	*36,1*	*9432*	*44,7*	*9878*	*0,0*	*334*

In Table 2, the influence of the Failure Notification Distance for different receiving traffic rates is being shown. It is illustrated in this experiment that these LSPs with higher Failure Notification Distance from the ingress node (the node responsible for the Failure Notification Procedure), are more likely to experience long recovery times and packet loss. More specifically, it is shown that T_{REC} is directly proportional to physical distance between the failure point and the ingress node. As D(i,a), or the number of successive hops between i (the ingress node) and a (the hop where failure occurs), increases relatively to the Traffic Throughput Rate, so does the propagation link delay (T_{REC}) in conjuction to the total amount of packet loss (PLS).The final case (D(i,a) = 0) is the most optimal since a local backup protection method is being selected.

5.1 Evaluating the GMPLS Protection Mechanisms using the LDC Algorithm

For implementing the improved Protection Mechanisms (using the LDC algorithm) we deploy 100 LSPs, in total, from nodes 1,2,3,6,9,10,12,13,14 to node 15 (egress destination node), as main working paths. After each disjoint link failure occurs, we compare the Default Protection state in the asons environment, which picks up the backup paths in an unconstrained manner, to the improved LDC based Mechanism, which preselects the optimal backup path(s) based on the least link-delay constraint., We utilize the algorithm to select a pre planned 1+1 backup path for each working path, as well as M≥1 protection paths for the M:N scheme.

The two other Protection Mechanisms (1:1 and 1+N) are equivalent to the previous ones, thus there is no need to further examine them.

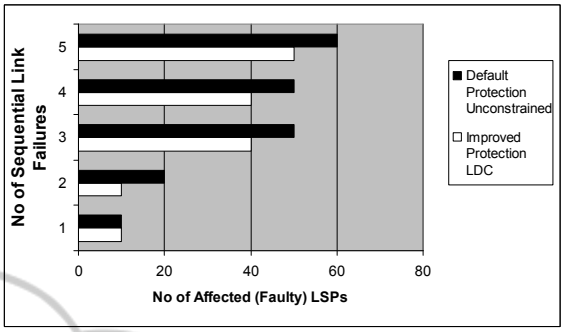

Figure 6: Comparing the LDC Protection Mechanism to the Default Unconstrained on the number of Damaged LSPs (1+1 case).

As we can clearly see in Figure 6, for the 1+1 case, the greater the number of sequential faults occurs the more is the amount of LSPs being affected from the source nodes to egress destination node. Yet, while this true for both implementations (the unconstrained and the metric-based), in the LDC case we manage to obtain more lightpaths unaffected by the network failures, thus retain traffic normality and increased resiliency. What is most important is that the total network traffic distribution is more evenly applied across the topology, after the utilization of the LDC algorithm. The results can be increased network fault avoidance as well as reduced packet loss, due to the unaffected and better protected LSPs. Figure 7 also illustrates the same effects for the M:N case.

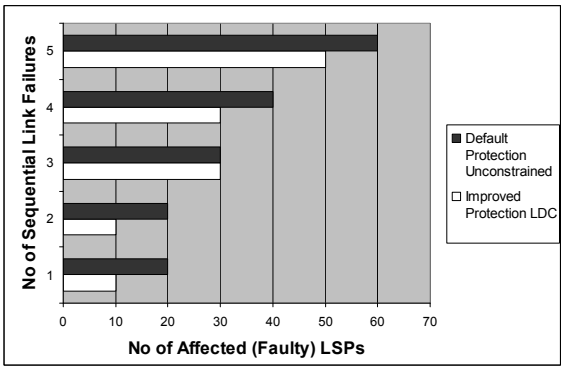

Figure 7: Comparing the LDC Protection Mechanism to the Default Unconstrained on the number of Faulty LSP's (M:N case).

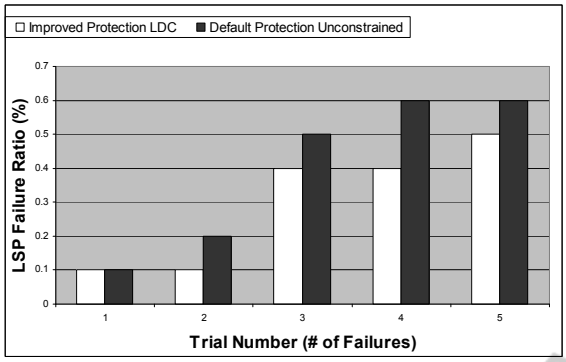

Figure 8: LSP Rejection Rate Analysis for the 1+1 case during adjacent link failures. LDC mechanism versus the default unconstrained.

Figure 8 demonstrates the percentage of LSPs being rejected as faulty for both Protection Mechanisms (LDC and Unconstrained) during successive link failures. It is important to notice that the LDC algorithm itself increases the total ratio of functional paths as more disjoint faults occur, contributing to better protected and fairly distributed network traffic. This happens because congested lines are being avoided, the total number of traffic cut-edges is further minimized, and finally a more even network topology in terms of traffic flow is achieved. Results in Figure 9 show similar behaviour.As the Trial Number increases and more failure events congest and aggravate the whole network flow, the LDC solution protects more paths than the conventional method offering higher resilience rate and traffic smoothness.

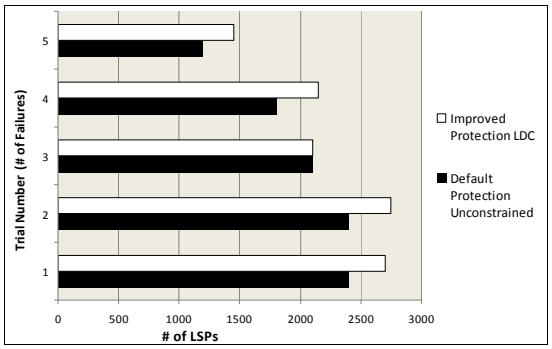

Figure 9: Number of Protected LSPs for the M:N case during adjacent link failures. Comparing the LDC mechanism versus the default unconstrained.

6 CONCLUSIONS – FUTURE WORK

This paper proposes the implementation of improved GMPLS Survivability mechanisms (both Protection and Restoration) through an efficient Constrained-based link-state Algorithm (LDC). This algorithm considers the delay metric on each link of the topology, a parameter which is directly related to the total number of connections the link has. By pre or post selecting a path with having less connections as the backup path, it achieves a higher safety level for the restoration case as well as faster recovery times and more delivered packets for the pre planned method. For further research prospects, there will need to be an investigation of a multi-constrained algorithm which takes for granted other metrics and QoS measurements, something that could provide even more stable and robust protection across the GMPLS networks.

REFERENCES

Calle, E.; Ripoll, J.; Segovia, J.; Vilà, P.; Manzano, M., 2010. *"A multiple failure propagation model in GMPLS-based networks",* November-December

Changwoo Nam, Kwangsub Go, Minki Noh, Seunghae Kim Hyuncheol Kim, Jaeyong Lee, Jinwook Chung, 2007. "LSA Expansion For Fault Recovery in GMPLS Network", *IJCSNS International Journal of Computer Science and Network Security*, VOL.7 No.10

Dutta R., Kamal A. E., Rouskas G. N., 2008. *"Traffic Grooming for Optical Networks: Foundations, Techniques, and Frontiers",* Springer.

Farrel A., Bryskin I., 2006. "*GMPLS Architecture And Applications"*, Morgan Kaufmann Publishers.

Maier M., 2008. "*Optical Switching Networks",* Cambridge University Press.

Minei I., Lucek J., 2005. *"MPLS-Enabled Applications Emerging Developments and New Technologies*", John Wiley And Sons Ltd.

Naoaki Yamanaka, Kohei Shiomoto, Eiji Oki, 2006. "*GMPLS Technologies Broadband Backbone Networks And Systems*", CRC Press.

Ortega E. C., 2004. "*Enhanced Fault Recovery Methods For Protected Traffic Services in GMPLS Networks*" Universitat de Girona, PhD thesis.

Stern T. E., Ellinas G., Bala K., 2009. "*Multiwavelength Optical Networks"*, Cambridge University Press.