SPARE CAPACITY MODELLING AND ITS APPLICATIONS IN SURVIVABLE IP-OVER-OPTICAL NETWORKS

D. Harle , S. Albarrak, F. Ali
Department of Electrical and Electronic Engineering,
University of Strathclyde, U. K
{d.harle,Sbarrak, fuead}@eee.strath.ac.uk

KEYWORDS

IP over optical networks, survivability, pre-allocated restoration, pre-emption.

ABSTRACT

As the interest in IP-over-optical networks are becoming the preferred core network architecture, survivability has emerged as a major concern for network service providers; a result of the potentially huge traffic volumes that will be supported by optical infrastructure. Therefore, implementing recovery strategies is critical. In addition to the traditional recovery schemes based around protection and restoration mechanisms, pre-allocated restoration represents a potential candidate to effect and maintain network resilience under failure conditions. Pre-allocated restoration technique is particularly interesting because it provides a trade-off in terms of recovery performance and resources between protection and restoration schemes. In this paper, the pre-allocated restoration performance is investigated under single and dual-link failures considering a distributed GMPLS-based IP/WDM mesh network. Two load-based spare capacity optimisation methods are proposed in this paper; Local Spare Capacity Optimisation (LSCO) and Global Spare Capacity Optimisation (GSCO).

1. INTRODUCTION

Optical networks have become the choice of core backbone communications networks worldwide because of their superiority in terms of transmission range and quality coupled with the potentially huge amount of data that can be carried. At the user end, IP (Internet Protocol) network is the consensus choice because of its flexibility and interoperability. Furthermore, more applications have become IP based; suggesting that IP-over-optical networks are expected to be the network architecture for next-generation networks [1]. Survivability has been identified as one of the critical issues in this network. Particularly, at the optical layer, any failure will have significant consequences which can lead to a considerable loss of data and, hence, revenue. Therefore, it is critical that such networks are robust and resilient especially in terms of recovering from failures [2].

Integrating survivability strategies into such networks are one of the major concerns for the network service providers. Survivability strategies in optical networks can be broadly classified as *protection* and *restoration*. Protection refers to recovery schemes where backup resources are pre-computed and reserved in advance. The alternative mechanism, restoration, relies on the dynamic discovery of the backup resources for each disrupted connection [3]. In general, dynamic restoration schemes are more efficient in utilising network resources since no capacity is allocated in advance; thus providing more resilience against different types of failure. In contrast, protection schemes have faster recovery times and, moreover, recovery is guaranteed. However, these backup resources can be thought to be wasted if no failures occur and these resources are not required to carry traffic.

Consequently, *a pre-allocated restoration* scheme has been proposed that combines the best of both protection and restoration schemes. Here, additional capacity specifically for survivability purposes is embedded in the network. Under normal conditions, the additional capacity is not seen by the routing algorithms, suggesting that there is no need for survivable routing calculations to be involved [4]. Furthermore, this technique is more flexible in terms of resource utilisation and coping with various failure scenarios.

The rest of the paper is organised as follows; Section 2 presents the problem discussion. The model implementation and characteristics are described in Section 3. Section 4 presents the model performance and simulation results, and finally, Section 5 concludes this paper.

2. PROBLEM DISCUSSION

Nowadays, many of the network service providers are attracted by the pre-allocated restoration technique. The reason is that it is a simple and flexible technique in terms of implementation, resource utilisation and coping with various failure scenarios; as a result, there is no need for survivable routing algorithms to be involved under no-failure condition. Moreover, the improvement of optical layer functionality has also made it possible to implement this technique, whereby most functions are facilitated through a GMPLS-based distributed control plane rather than a centralised management unit. From the resource utilisation perspective, the spare capacity embedded in the network is significantly less than that required by protection techniques.

Even though this technique is simple and flexible enough for the next generation network (NGN) where IP is run directly over optical networks and lightpaths are established and deleted on-demand, there are still several issues worth being considered by network operators. These issues are:

- **Spare Capacity Allocation**

The NGN data plane is an overlay model with three topologies; link, lightpath, and label switching path (LSP) topology. Therefore, it is important to provide efficient methods to allocate the spare capacity within each topology. A well-known method used within the LSP topology is called bypass or backup tunnels [4-5]. In this method, a span tunnel is reserved to reroute the traffic under failure conditions. Adapting this method, previous work [6-7] suggested and investigated three methods to allocate spare capacity in the link and lightpath topology; lightpath partitioning, link partitioning and the pre-allocated lightpath method. In the ‘lightpath partitioning’ method, the spare capacity is allocated within all active lightpaths whereby the total lightpath capacity is partitioned into two parts; working capacity and restoration capacity. Using ‘a link partitioning’ method, the spare capacity is allocated within all links whereby the link wavelengths are partitioned into two parts; working wavelength and restoration wavelengths. In the ‘pre-allocated lightpaths’ method, some lightpaths are pre-provisioned in the network to form the spare capacity.

- **Spare Capacity Optimisation**.

Under any of the allocation methods, providing a flexible reconfiguration mechanism to optimise the spare capacity is essential. This can be classified as either static or dynamic mechanism. In the former, static spare capacity is embedded in the network using an off-line calculation algorithm based on the static traffic demand. In the latter, the amount of such capacity is calculated and adjusted on-line based on the current network conditions. The static technique is not suitable for the NGN where the traffic changes in dynamic fashion. Thus, this work supports dynamic spare capacity reconfiguration. Two load-based spare capacity optimisation methods are proposed in this paper; Local Spare Capacity Optimisation (LSCO) and Global Spare Capacity Optimisation (GSCO).

In the former, the term “local” refers to the fact that only local port capacity information is considered in the optimisation. Therefore, each node is autonomously responsible for adjusting its port capacity based on the amount of generated traffic within each port. The main idea is to ensure that the generated traffic within any port can be rerouted through other ports. This constraint is presented in equation (1).

$$WC_i \le \sum_{j=1}^{n} SC_j \qquad i \ne j \qquad (1)$$

Where WC_i represents the generated traffic in port i, SC_i represents the spare capacity in port j, and n indicates the number of ports.

In the GSCO method, it is assumed that the optimisation is achieved by a centralised link-failure agent. The agent works on the principle that the optimisation will be applied at a slower time scale than that of per-connection reconfiguration. Therefore, the agent can be triggered periodically or by a node whose link capacities experience prescribed and significant change.

The main idea is that the agent maintains a small database which describes the existing spare capacity and the total load for each pair passing through the corresponding link. Based on this information, the agent emulates some link-failure scenarios and investigates the level of spare capacity in each link. Consequently, the spare capacity in the network can be reconfigured. It is assumed that the agent operates in the background and therefore no service interruption occurs.

- **Implementation**

In order to implement the spare capacity allocation methods and optimization mechanisms, several scalability concerns need to be considered. With respect to the signalling protocol, it is essential to take into consideration the increasing messaging complexity and the compatibility with the GMPLS signalling protocols. From a routing perspective, the scalability can be viewed from the required routing information to achieve both routing calculation and shared spare capacity between IP and optical layer.

- **Spare Capacity Utilisation**

There is no doubt that network capacity is a premium in any network infrastructure. Thus, the additional capacity created for the survivability purpose may be thought to be wasted should no failure occur. Therefore, network service providers can capitalise from this circumstance by accepting low priority traffic to utilise the additional capacity. However, in a QoS-enabled IP/WDM network, it is important to provide available and reliable services to the end users; especially for the high priority class users since a large portion of revenue comes from this type of user. Preemption techniques can be viewed as one of the efficient ways to achieve this objective. A preemption technique consists of a control admission policy which decides on which connections are to be dropped when resource scarcity is experienced, or a recovery process has to take place due to failure occurrences in the network. The spare capacity utilisation issues will be considered in the future work.

3. NETWORK MODELLING

This work uses the OMNeT++ (Objective Modular Network Testbed in C++) simulator as discrete-event simulation software platform which is a public-source simulator with a generic and flexible architecture, whose primary application area is the simulation of communication networks. OMNeT++ is an object-oriented modular whereby each module in the network is implemented as an object. Thus, it supports hierarchically nested modules with flexible module parameters. These models then communicate with each other using messages passed through channels.

3.1 Network Structure

The network structure considered by this work is the IP/WDM network architecture. The model is developed in such a way that a distributed mesh network topology is implemented under GMPLS control protocols. It consists of a set of nodes connected by a set of paired fibre links. Internally, each node consists of an edge router connected to an optical cross connect (OXC) as illustrated in Figure 1. The network structure comprises of control and data planes. The data plane must be an overlay model with three topologies; link, lightpath and label switching path (LSP) topology. The control plane in both the edge routers and OXCs consists of three units; the signalling, the routing, and the recovery/preemption units. The functionalities of the signalling and routing units are implemented using standard GMPLS protocols [8-9].

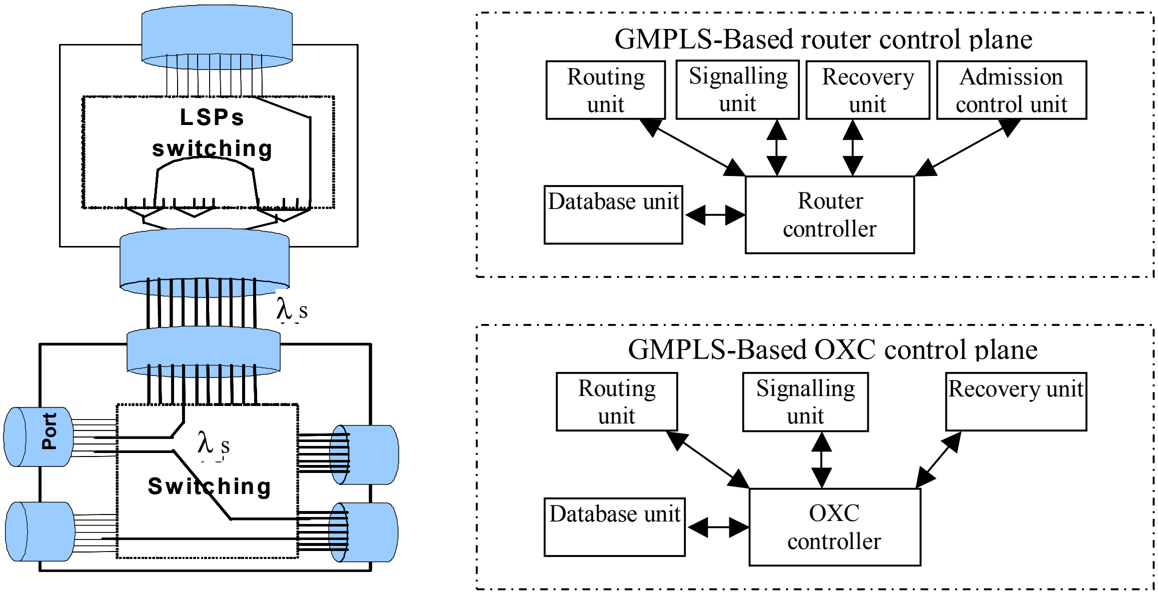
Each layer has a controller model responsible for controlling and scheduling all required functions in the node. Moreover, it must also deliver messages to remote nodes through dedicated control channels, using GMPLS standard protocol messages implemented by the ***cMessage*** class. These messages could be generated locally by the signalling unit or passed over to other nodes. The suggested approach in this paper is to implement an admission control (AC) unit to manage LSP requests at the edge routers. The admission control has full awareness of the situation when multiple identical requests associated with a source-destination pair, and a class of service arrives simultaneously at an edge router [10].

3.2 Routing Protocol Unit:

This model adopts the source-based explicit routing concept and the constraint-based shortest-path-first algorithm. The former attempts to provide an explicit route at the source nodes; therefore, this route cannot be modified during the signalling phase. The latter provides an efficient method to compute a new request route. The IP routing unit determines the explicit route based on the amount of available capacity in each lightpath. In the optical layer, it determines the explicit route, based on the number of free wavelengths in each link.

The network nodes must require particular information in order to efficiently implement their functionality. Specifically, three data tables are maintained in each node:

- Wavelength routing table: contains the information that describes the status of wavelengths at each port. This information supports the OXC control plane to make a decision as to whether a required connection can be established or not. Moreover, the occupied lightpath identification fields support the OXC control plane in order to achieve one of two tasks: to find a



(a) : Data plane structure

(b) : control plane structure

Figure 1: proposed network node structure

new sub-path from the OXC to the destination of a lightpath, or to notify the responsible nodes when failures are detected.

- Lightpath information table: maintains the information about all lightpaths generated from, or terminated on, the corresponding OXC. This information enables the control plane, to change or modify the lightpath route in order to improve network performance or to recover from failures.
- Network Physical topology table: contains the information about the entire network link connectivity. This information enables the routing unit to calculate the appropriated route for a new request. In practice, routing protocols are responsible for collecting table entries for each OXC. However, this model does not consider this issue. The network topology is built and modified automatically using functionality provided in the ***cTopology*** class features offered by Omnet++.
- Control channel topology table: contains the information that describes the control channel connectivity. The main reason for creating this table is the requirement by GMPLS standards that control message exchanges made independently from the data plane via control channels. It is assumed that the control plane topology is identical with the network topology.

Similarly to the OXCs, routers also require certain information to efficiently implement their functions. Three tables implemented at each node are described as follows:

- Forwarding table: It contains the forwarding information including: ***in_port***, ***in_label***, ***out_port***, ***out_label*** and the identification of LSPs that pass through the existing router. This information supports the data plane in forwarding packets and supports the control plane in finding a new sub-path for any LSP or in notifying the responsible nodes when failures are detected.
- Logical topology: This table contains the information regarding the existing lightpaths including: the source, destination, capacity and type of lightpaths. This information supports the routing unit to calculate the appropriate route for a new request. Typically, such tables are maintained in each router and updated via routing and signalling protocols. However, in this model, routers retrieve such information from a global file.
- LSP information table: maintains the information about all LSPs generated from, or terminated on the corresponding router. This information supports the control plane in changing or modifying the lightpath route in order to improve network performance or to recover from failures.

These tables can be updated either by signalling or routing protocols. The signalling protocol enables updating tables to maintain local information such as wavelength routing, lightpath information, forwarding and LSP information tables. On the other hand, tables that maintain global information including the link resource availability and logical topology tables are updated by means of the routing protocol.

The routing units at the IP layer determine the shortest path based on the amount of available capacity in each lightpath. At the optical layer, the routing units determine the shortest path based on the number of free wavelengths in each link.

3.3 Signaling Protocol Unit:

From the signalling perspective, once the path for a request (lightpath or LSP) is successfully computed, this model employs the destination-initiated reservation (DIR) method using the GMPLS signalling protocol in both IP and optical layers. Based on the DIR method, a connection request is forwarded from the source to the destination and collects the resource information on its way. The destination then selects the appropriate label and sends a reservation request to the source; all intermediate nodes, including the source, attempt to find and reserve the required resource. The request will be blocked if there are no available resources along its route. It is assumed that no repeat behaviour is considered.

At the IP layer, connections in the form of LSPs are requested and terminated randomly. The edge routers will make a request for a lightpath at the optical layer in order to accommodate the LSP connections by using the lightpath-create-first policy [10]. Based on this policy, the edge routers will search for a direct lightpath within the existing lightpath topology. If no available lightpath is found, the routers will attempt to provision a new lightpath to accommodate new LSP requests. On each lightpath setup failure, the routers will attempt to find a route within the existing lightpaths. In such cases, an LSP could travel through multiple lightpaths on its way from source to destination.

One of the critical issues in a distributed GMPLS-based data plane is contention between messages when multiple provisioning processes begin simultaneously. One of the solutions for such problem is to apply a retrial method where, when the connection provisioning process fails, the provisioning process is repeated. Another efficient solution is to apply a prioritization method based on the type of control messages. For instance, the reservation messages have higher priority than path messages. Moreover, within the same class of message the suggested prioritization method is the *master and slave* method. This method relies on the fact that each link is at least connecting two nodes. One of these two nodes is set as a master node and another is set as a slave node. Therefore it allows the master node to take higher precedence when the contention occurs. Note that, a lightpath is considered as a link by the logical IP layer.

3.4 Delay Time Components:

This model implementation also considers three delay components; the propagation delay, the transmission delay, and the nodal processing delay. The propagation delay represents the delay for the first bit propagates from a source to a destination and is a function of the link propagation speed and the link length. The transmission delay represents the time needed to send in data onto a link and calculated as a function of the link capacity and the message size. The nodal process delay describes the time between the node receiving a message through the input port and the time when the message is sent to the output port, including the time take to analyse a message, to calculate a new route and to perform wavelength switching.

4. PERFORMANCE RESULTS

This section presents results for a number of simulation-based experiments. The performance metrics of interest are the spare capacity ratio, the restoration ratio and the blocking probability. The restoration ratio gives the ratio of the number of restored connections over the number of failed connections in the network. The spare capacity ratio is defined as the ratio of the total available spare capacity over the total network capacity. The blocking probability presents the ratio of the number of rejected connections over the number of requested connections in the network. The offered load presents the traffic load expressed in Erlangs which is defined as the product of mean arrival rate and the mean connection holding time. The network topology adopted in this work is the NSFnet network topology (14 nodes and 22 links). It is assumed that each link is bi-directional and supports 8 wavelengths with capacity 10 Gb/s. LSP connections are requested and terminated randomly, with requests generated following a simple Poisson process. The LSP parameters include the source, the destination, and the bandwidth, selected randomly based on a uniform distribution. The LSP capacity varies in a continuous range from 1Mb to 2.5 Gb. For simplicity, the message length is fixed at 256 bytes and the nodal process delay is 1ms. The length of links is chosen as the distance in [11].

The mean failure inter-arrival time is 5 time units (time unit equal 50s) and the mean repair time is one time unit. These parameters are chosen to be much less than the values in the reality in order to test the model within reasonable simulation time and to process multiple failure events. Links selected for failures are obtained using a uniform distribution. The dual link failure scenario considered in this work is when two random links fail simultaneously. The path-level recovery (end-to-end recovery) is applied because it provides better resource utilisation than link-level recovery. The recovery process begins at the optical layer which attempts to recover any failed lightpath. If the lightpath can not be recovered, the IP layer will be in charge to attempt recovering the LSPs that travel through the failed lightpath.

Two restoration schemes are investigated; multilayer restoration and multilayer pre-allocated restoration. In the pre-allocated restoration, it is assumed that the spare capacity is allocated based on the lightpath partitioning method [6-7] and the spare capacity is optimised using either the LSCO method or GSCO method.

Figures 2 and 3 present the restoration ratio and spare capacity ratio respectively. The experimental results show that the restoration ratio improves significantly when the two optimisation methods are applied. The improvement is clearly evident, in particular, for the case of medium and high load values. Additionally, the figures show that there is a trade-off between the amount of spare capacity embedded in the network and the restoration ratio performance. While the restoration ratio improves under the optimisation methods, the amount of spare capacity increases significantly. Moreover, the experimental results demonstrated clearly that the GSCO method achieves better performance than the LSCO, in which the restoration ratio of GSCO exceeds that of LSCO under single-link failures. The reason is that the GSCO method includes not only the local generated traffic

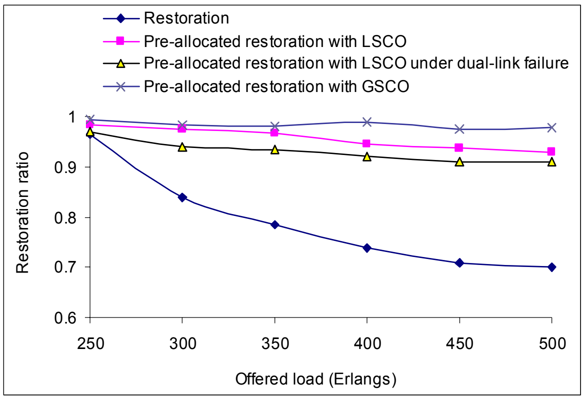


Figure 2: restoration ratio comparison for restoration and pre-allocated restoration with the two optimisation methods.

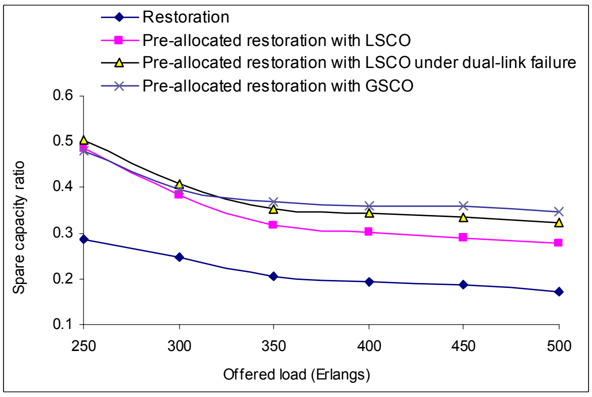


Figure 3: spare capacity ratio comparison for restoration and pre-allocated restoration with the two optimisation methods.

but also the generated traffic between all pairs in the network.

The LSCO performance is investigated under single and dual-link failure. the experimental results show that the required spare capacity under dual-link failure is higher than that under single-link failure. The reason is that under dual-link failures, the LSCO method ensures that the generated traffic within any port can be rerouted though at least two other ports.

In Figure 2 which shows the relative spare capacity ratio, it can be seen that the spare capacity ratio decreases when the load increases, in particular, for the low and medium load values. The reason is that the spare capacity ratio relies on the number of existing lightpaths. Therefore, when the load increases, the number of existing lightpath is also increased.

Further to the failure condition performance, this work is also interested into the effect of deploying the optimisation method on the normal network operation. Figure 4 presents the blocking probability when the two methods are applied under single-link failure. The blocking probability considers only normal LSP requests and does not include the restoration LSP requests. The results show that the blocking probability increases when only two methods are applied. This result is expected whereby a specific amount of the network capacity is hidden from the routing unit under no-failure conditions. On the other hand, the figure shows that the LSCO method achieves slightly lower blocking probability than GSCO. The reason is that, with the LSCO method, the amount of reserved capacity is lower.

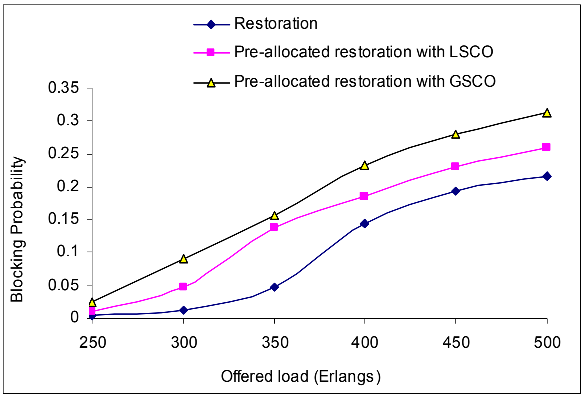


Figure 4: blocking probability comparison for restoration and pre-allocated restoration with the two optimisation methods

5. CONCLUSION

This paper presents a comprehensive overview of the pre-allocated restoration technique. The prime focus was given to the spare capacity embedded in the network for survivability purposes by outlining the key requirements including the capacity allocation, optimisation implementation and utilisation. In order to investigate and study all of these requirements, a distributed model was implemented considering a GMPLS-based IP/WDM structure. Two load-based spare capacity optimisation methods were proposed in this paper; Local Spare Capacity Optimisation (LSCO) and Global Spare Capacity Optimisation (GSCO). The simulation results show that the model performance in terms of the restoration ratio improves significantly when the proposed methods are applied. Additionally, the figures show that there is a trade-off between the amounts of spare capacity embedded in the network and the restoration ratio performance

REFERENCE

[1] E. Mannie, "Generalized Multi-Protocol Label Switching ({GMPLS}) Architecture,'' IETF RFC 3945, Oct. 2004.

[2] J. Zhang and B. Mukherjee, "A Review of Fault Management in WDM Mesh Networks: Basic Concepts and Research Challenges,'' in IEEE Networks Magazine, Mar. 2004.

[3] D. Colle et al., "Data-centric optical networks and their survivability,'' in IEEE Journal on Sel. Areas in Comm., vol.20, no.1, pp. 6-20, Jan. 2002.

[4] W.D. Grover, "The protected working capacity envelope concept: an alternate paradigm for automated service provisioning," in IEEE Communications Magazine, vol.42, no.1, pp.62-69, Jan 2004.

[5] M. Kodialam, T. Lakshman and S. Sengupta, "A Simple Traffic Independent Scheme for Enabling Restoration Oblivious Routing of Resilient Connections," in IEEE INFOCOM 2004.

[6] S. Albarrak and D. Harle, "Pre-Allocated Restoration Technique in a Distributed GMPLS-Based IP/WDM Mesh Network," 2nd IEEE International conference on information and communcation from theory to application, Damascus, Syria, , April 24 - 28, 2006

[7] S. Albarrak and D. Harle, "Spare Capacity Allocation in a Distributed GMPLS-Based IP/WDM Mesh Network," International Symposium on Performance Evaluation of Computer and Telecommunication Systems (SPECTS'06), Canda ,July 31, 2006.

[8] J. Lang, "Generalized Multi-Protocol Label Switching (GMPLS) Signaling Resource ReserVation Protocol-Traffic Engineering (RSVPTE) Extensions," January 2003.

[9] R. Braden, L. Zhang, S. Berson, S. Herzog, and S. Jamin, "Resource ReSerVation Protocol (RSVP) -- Version 1 Functional Specification," September 1997.

[10] S. Albarrak and D. Harle, "An Edge Admission Control in a Distributed GMPLS-Based IP/WDM Network," IV GMPLS Workshop, Spain, 21st, April, 2005.

[11] Jian Wang , Sahasrabuddhe, L., and Mukherjee B., "Path vs. subpath vs. link restoration for fault management in IP-over-WDM networks: performance comparisons using GMPLS control signalling, " in IEEE Communications Magazine,Vol.40, No 11, pp.80-87, Novemer 2002.