# A Simple Integrated Provisioning and Protection Scheme in GMPLS-based Optical Networks

Ding, Zhemin and Mounir Hamdi,

Department of Computer Science, Hong Kong University of Science and Technology

**Abstract— This paper proposes an integrated provisioning and protection scheme in GMPLS-based IP over WDM networks, which takes into account the combined topology and resource availability knowledge on the IP and WDM layers. A GMPLS-based network architecture is discussed for possible implementation of the scheme. We adopt a clustering technique called Blocking Island Paradigm in this scheme to abstract network resources and reduce the searching space. An enhanced BIG network model is then developed. We demonstrate our scheme is a general framework, which can employ various provisioning and protection algorithms and improve their performances. In the simulation, we show the proposed scheme performs very well in terms of call blocking probability.**

## I. INTRODUCTION

A key problem in WDM optical networks is the network survivability since those networks carry high volumes of traffic and failures may cause severe consequences. Therefore it is important the networks should be fault tolerant. Fault tolerance refers to the ability of the network to reconfigure and reestablish communication upon hardware or software failure. Network survivability techniques can be classified as protection and restoration [1]. The technique that uses pre-assigned capacity to ensure survivability is called protection and the technique that re-routes the affected traffic on failed links/nodes by using existing capacity is called restoration. Most of the previous research on the survivability in WDM optical networks has focused on the recovery from a single link or node failure, which is due to the factor that it is easier to reroute the failed path one at a time. And also the possibility of multiple failures occurring at the same time is very low.

In the restoration methods, when a working path fails, a search is initiated to find a new backup path that does not use the failed components. However, the successful recovery can not be guaranteed in the restoration methods since the establishment of new backup paths may fail due to various factors such as resource shortage, limited path set-up time, etc. To overcome the shortcomings, the protection methods are proposed, in which the backup paths are reserved at the time of setting up the primary working paths. The protection methods can yield 100 percent successful recovery at the cost of more resource occupancy. Also it does not need the time consuming connection re-setup process. Typically there are three main architectures: 1+1, 1:1 and 1:N. 1+1 and 1:1 are commonly referred to as dedicated protection. In 1+1 protection, working path and backup path transmit the same data simultaneously and a selector is used on the receiving side to choose the best signals. In 1:1 protection, transmission occurs on the working path only, while the backup path may be either idle or used to transmit low-priority traffic. Upon the failure of the working path, the backup path will then be used. 1:N protection, also known as shared protection, allows a single backup link to be shared by N working paths. The single backup link provides protection against the failure of any one of the N working paths.

Based on the layered structure of WDM optical networks, survivability can be offered in the WDM layer or the higher layer. There are many protection schemes proposed in the optical domain [2] [3]. Usually WDM layer survivability responds to the link/node failure much faster than upper layers. It makes more efficient use of network resource and provides transparency: the protection is independent of the protocols used in the higher layer. It also has many disadvantages comparing to the upper layer protection (i.e. IP layer). The full survivability in WDM layer proves very expensive and the granularity is coarse (i.e. the granularity is the bandwidth of a full wavelength). On the other side, the traditional IP protection via layer 3 or IP rerouting is flexible and the cost is low. However, in IP protection, the working path and the backup path can only be set up in the logical (virtual) topology without the exact knowledge of lower layer resource availability. It is obvious both WDM layer

---

Author for correspondence: Dr. Mounir Hamdi, Email: hamdi@cs.ust.hk . This research is supported in part by a grant from the UGC-Hong Kong under the grant AoE/E-01/99.

0-7803-8956-5/05/$20.00 ©2005 IEEE.

protection and IP layer protection have pros and cons. With the development of new equipments and new network architectures, there is a convergence of WDM layer protection and IP layer protection. Motivated by this trend, we propose an integrated provisioning/protection scheme which takes into account the combined knowledge of both IP and WDM layers. In the proposed provisioning/protection scheme, we assume it protects single link failure and the bandwidth requirement of traffic requests can be a fraction of the wavelength bandwidth. We also assume similar control planes are employed in the GMPLS-based IP over WDM networks. The recent advances in *generalized multiprotocol label switching* (GMPLS) have provided the enhanced signaling and routing mechanism in both IP and WDM layer, which makes it possible for the implementation of our integrated scheme.

The rest of the paper is organized as follows. In section II, we introduce a network architecture based on GMPLS. The Blocking Island Paradigm and the integrated provisioning/protection scheme based on this paradigm are discussed in section III and IV. In section V, we present the simulation results. Section VI concludes the paper.

## II. A GMPLS-BASED NETWORK ARCHITECTURE

Based on different degree of information sharing and control sharing between IP layer and WDM layers, three interconnection models are defined in [4]: overlay model, augmented model and peer model. In overlay model, each layer is independent and the communication between two layers is handled in a “client-server” way. Augmented model allows certain information sharing between two layers to gain more efficiency and flexibility. In peer model, a single control plane is deployed and two layers are treated in a unified way.

In this paper, we assume a peer IP over WDM network model based on GMPLS. GMPLS is a generalized MPLS architecture to include Non-packet-based control planes, as well as the conventional packet networks. The signaling process is enhanced in GMPLS, which extends the base function of RSVP (resource reservation protocol) and LDP (label distribution protocol). LMPs (link management protocols) are also included in GMPLS for neighborhood discovery in optical networks.

There are many ongoing studies on either the IP protection or WDM layer survivability issues. Usually, they assume the two layers are not aware of each other. [5] proposes an integrated provisioning/protection scheme in IP over WDM networks. In [5], the logical topology is computed by an optimization approach (linear programming) based on a previously known traffic request matrix. The logical topology is not dynamically updated. In order to avoid high blocking probability, a periodical offline computation has to be carried out to update the virtual topology. In our scheme, the logical topology of IP layer is integrated with the optical layer. It is updated constantly according to the traffic requests to improve the network performance.

We define a network topology *G (V, L, W)* for a given IP/WDM network, where *V* is the set of all nodes; *L* is the set of bidirectional optical links and *W* is the set of wavelength per fiber link. Here we assume the number of wavelength on each fiber link is the same. Under the peer model assumption, network nodes are treated as integrated router/OXC nodes and there is only one control plane. While in practice, it is possible some nodes, which are only OXCs without the function of IP routers, remain one part of an IP/WDM network. Therefore we consider *V(R, O)* for a given set of nodes in an IP/WDM optical network, where *R* is the set of integrated router /OXC nodes, *O* is the set of OXC nodes. Nodes in *R* can multiplex or demultiplex traffic requests with any bandwidth granularity and do wavelength conversion. Nodes in *O* can only multiplex or demultiplex traffic requests with the bandwidth granularity of a whole wavelength and don’t have wavelength conversion capability. The transaction power of each node is only limited by the network resource availability. This assumption can be relaxed if the detailed transaction capability of equipments is given.

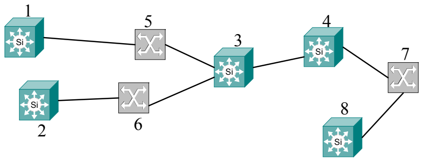


Figure 1: An example of IP over WDM network

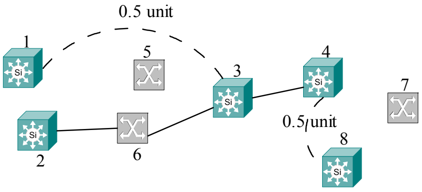


Figure 2: A new topology of the example network

An example of network topology is shown in Figure 1, where node 1, 2, 3, 4, 8 are integrated router/OXC nodes and node 5, 6, 7 are plain OXCs. Based on the GMPLS framework, an optical channel ($\lambda$-LSP) needs to be set up for each request and the required bandwidth is reserved on links of the $\lambda$-LSP path. The request to set up a $\lambda$-LSP can be defined as ($X_\mu$, $Y_\mu$, $\beta_\mu$) where $X_\mu$ and $Y_\mu$ are distinct nodes of the network; $\beta_\mu$ is the required bandwidth. Since this is a circuit switched network, the only QoS requirement we consider in this paper is bandwidth. Assume the bandwidth of a whole wavelength is 1 unit. A request $(X_\mu, Y_\mu, \beta_\mu)$ is to be routed from node $X_\mu \in R$ to node $Y_\mu \in R$ with the bandwidth requirement $\beta_\mu \leq 1$ unit. If an optical channel is set up to reach the destination and this path involves nodes of OXCs, some cut through arcs (lightpaths) may be created to meet the requirement. The IP layer network topology will be changed in this case. For example, in figure 1, a traffic request arrives, requiring the bandwidth of 0.5 unit from node 1 to node 8. To simplify the example, we consider each fiber has only one wavelength. Assume a LSP path (1->5->3->4->7->8) has been found from node 1 to node 8 along the wavelength $w_1$. Because OXCs can only multiplex and demultiplex traffic requests with the bandwidth request of a whole wavelength, new lightpaths are set up to directly connect integrated nodes. In figure 2, 2 new lightpaths (cut through arcs) are introduced to form a new topology. Notice only 0.5 unit bandwidth is consumed along the path. The residual 0.5 unit bandwidth is still available along the lightpath for future use. Those lightpaths are logical links in the IP layer. They can be released or re-setup according to traffic requests and resource availability.

## III. BIG NETWORK MODEL

In this section, we give a brief introduction on the Blocking Island paradigm, which is used as a framework in the proposed integrated scheme. The Blocking Island (BI) paradigm [6] provides an efficient way of abstracting resource (especially bandwidth) available in a communication network. An enhanced BIG (Blocking Island Graph) network model is proposed to represent IP over WDM networks.

BI clusters parts of the network according to the bandwidth availability. A *$\beta$-BI* for a node *x* is the set of all nodes of the network that can be reached from *x* using links with at least $\beta$ available bandwidth. For example, $N_1$ in Figure 3 (a) is a *40-BI* for node *V1*. We start with node *V1*. Then we add all the nodes which can be reached by links with at least 40 available bandwidth to form a *40-Blocking Island* $N_1$.

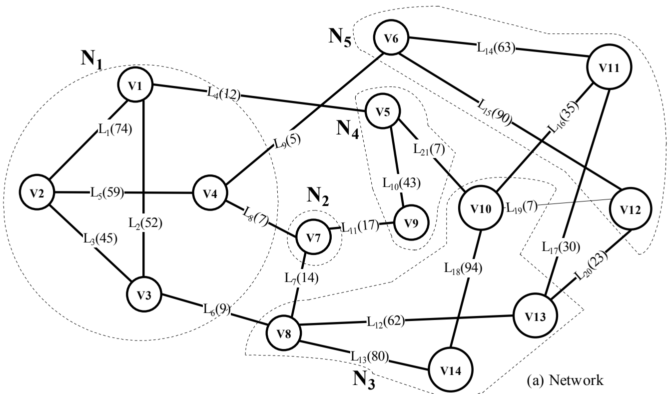
*$\beta$-BI* has some very useful properties. Below we list a few without proof (for a proof, please refer to [6]).

**Unicity**: there is one and only one *$\beta$-BI* for a node. Thus if *S* is the *$\beta$-BI* for a node, *S* is the *$\beta$-BI* for every node in this blocking island.

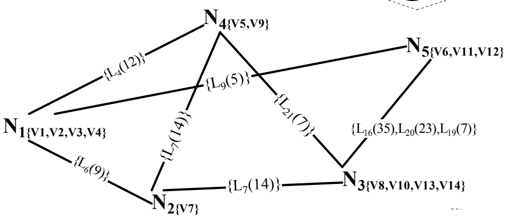
**Partition**: *$\beta$-BI* induces a partition of nodes in a network.

**Route existence**: give a request $d= (X_\mu, Y_\mu, \beta_\mu)$, it can be satisfied if and only if the node $x_u$ and $y_u$ are in the same *$\beta_u$-BI.*

**Inclusion**: If $\beta_i < \beta_j$, the *$\beta_j$-BI* for a node is a subset of the *$\beta_i$-BI* for the same node.



(a) Network



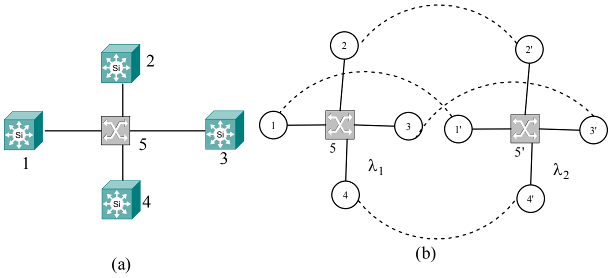
(b) 40-BIG

Figure 3: (a) The NSFNet topology. *$N_1$= {V1, V2, V3, V4}* is the 40-blocking island (*40-BI*) for node *V1*. The available bandwidth on a link is given in brackets. (b) 40-BIG

Using the concept of β-BI, we can construct a recursive decomposition of Blocking Island Graphs in decreasing order of *$\beta$s*, e.g. $\beta_1 > \beta_2 > \ldots > \beta_n$. We call this layered structure of Blocking Island Graphs a Blocking Island Hierarchy (BIH). For example, figure 3(b) is a 40-BIG. Based on figure 3(b), we can build a 20-BIG if necessary.

With the abstract technique, instead of studying the whole network topology, we focus our attention only on a small part. For example, given a traffic request (*$V_1$, $V_4$, 40*) in figure 3(a), according to the route existence property, the route is in *40-BI $N_1$*. In the $N_1$ Blocking Island, different routing heuristic can be employed to find the route. If the route is allocated, the available link capacity is decreased and the *BIH* may need to be modified. For example, in figure 3(a), if we assign a route *V1-->V3-->V2* with 40 bandwidth, the *40-BI $N_1$* will be split into two *40-BI*s: *(V1, V2, V4) and (V3).* Notice all the modification is actually localized and carried out only within the $N_1$ Blocking Island.

In order to apply the BI paradigm into the proposed scheme, we need to transform the network topology into a proper form. In [7], we propose a BIG network model to represent WDM optical networks. It is not appropriate to apply this model directly since there are some difference between the modeling of IP over WDM networks and WDM networks. In the original BIG model, we assume a single fiber network without wavelength converters. Each connection request needs to be allocated over a route and assigned one wavelength. It is modeled as a simplified blocking island graph with only one level of BIH. For IP over WDM networks, the integrated router/OXC nodes have the capacity of wavelength conversion. The traffic requests can require any fraction of wavelength bandwidth. And it will have multi-level layers of BIH according to different traffic requests.



(a)

(b)

Figure 4: (a) An example of IP/WDM network (b) Representation of the network by enhanced BIG network model

To accommodate those variations, we propose an enhanced BIG network model to represent the IP over WDM network. We assume a single fiber optical network and the set of wavelength on each fiber link is the same. Consider a network topology $G\ (V, L, W)$ for a given IP/WDM network, where $V=(R, O)$, $R$ is the set of integrated router/OXC nodes, $O$ is the set of OXC nodes; $L$ is the set of bidirectional optical links and $W$ is the set of wavelength per fiber link. The enhanced BIG network model can be obtained from a given network topology G as follows. Firstly we replicate the original topology of $G$ $|W|$ times. Each copy represents a wavelength and has the same topology as the original IP over WDM network. Then we check integrated node $r \in R$. In the enhanced BIG model, node $r$ has $|W|$ copies as ($r_1$, $r_2$ ...$r_{|W|}$). Virtual links $r_1r_2$, $r_2r_3$ ... $r_{|W|-1}\ r_{|W|}$ are then added to connect corresponding nodes. Notice since those nodes like ($r_1$, $r_2$ ...$r_{|W|}$) are actually the same node, the virtual links only characterize the link connectivity with unlimited bandwidth and have no weight (distance) in the routing and grooming computation. An very simple example is given in figure 4, where nodes 1,2,3,4 are integrated router/OXC nodes and 5 is the OXC node. 2 wavelengths $\lambda_1$ $\lambda_2$ per fiber is assumed.

Notice by converting the network topology into the enhanced BIG network model, we combine the WDM layer and IP layer into one network level. The previous independent RWA (routing and wavelength assignment) in WDM layer and the IP routing in the logical layer are transformed into one general routing problem in the BIG network model. In the next section, based on the enhanced BIG network model, we propose a simple and effective provisioning and protection scheme.

## IV. AN INTEGRATED PROVISIONING/PROTECTION SCHEME

In this section, we propose an integrated provisioning and protection scheme in IP over WDM network using the BI paradigm. The general idea of this scheme is very simple. Firstly we transform the network topology into the enhanced BIG network model. Unlike the scheme proposed in [5], where the virtual topology design is static and independent from the RWA process in the WDM layer, we treat RWA and IP layer routing in a unified way. We then build the BIH based on the BIG network model and incoming traffic statistics. Upon receiving a traffic request, we identify the proper blocking island in the BIH and check route existence. The working path and the backup protection path will then be searched in the blocking island instead of the whole network.

### BIH Construction

After the BIG modeling, we need to build more levels of BIH based on different traffic bandwidth requests to facilitate future resource allocation. The most primitive idea is to build a new level once there is a different traffic bandwidth request. Although this method can accurately abstract network resource availability and minimize the search space, the disadvantages are obvious: It may not be responding fast enough to handle large amount of the dynamic traffic. And too many levels also make the algorithm not scale well. Our idea is to pick up representative bandwidth according to incoming traffic statistics for a certain period.

### Blocking Island Assigning Procedure

After predefining the proper BIH, when new traffic request arrives, we pick up the closest BIG level in the BIH to apply routing heuristics. Consider a request $D_u= (X_\mu, Y_\mu, \beta_\mu)$ where $X_\mu$ and $Y_\mu$ are source node and destination node, $\beta_\mu$ is the required bandwidth, using the BI Routing Existence property we immediately know whether the request can be satisfied or not based on a $\beta_\mu$-BIG without any computing. As we stated before, the BIH building at disposal is not desirable because of the time and high maintenance cost. With the predefined limited levels of BIH, it is possible we don't have an exact match of BIG but we can still check the route existence of most requests much faster than a full network search. The route existence screening process is illustrated by an example. Assume a predefined $H$ level BIH $(\alpha_1,\ \alpha_2 ...\ \alpha_H)$, where $\alpha_i$ is the bandwidth level of the corresponding BIG level and $\alpha_1 < \alpha_2 < ... < \alpha_H$. If $\beta_\mu$ is equal to any predefined bandwidth value $\alpha_i$ the result can be obtained immediately.

If $\beta_\mu > \alpha_H$, we assign $D_u$ to $\alpha_H$-BIG. Then we check whether $X_\mu$ and $Y_\mu$ are in the same BI of $\alpha_H$-BIG. If the answer is no, the request is blocked. If yes, we have to do a further check on this BI using Dijkstra's algorithm or a link-state routing protocol.

If $\beta_\mu < \alpha_1$, we assign $D_u$ to $\alpha_1$-BIG. Then we check whether $X_\mu$ and $Y_\mu$ are in the same BI of $\alpha_1$-BIG. If the answer is yes, the route exists. If no, we have to do a further check on the whole network topology using Dijkstra's algorithm or a link-state routing protocol. This is the worst case in our screening process.

If $\alpha_1 < \beta_\mu < \alpha_H$, say $\alpha_i < \beta_\mu < \alpha_{i+1}$ $(1 \leq i \leq H-1)$, we first check whether $X_\mu$ and $Y_\mu$ are in the same BI of $\alpha_{i+1}$-BIG. If the answer is yes, the route exists. If not, we then check whether $X_\mu$ and $Y_\mu$ are in the same BI of $\alpha_i$-BIG. If they are in the same BI, we have to do a further check on this BI using Dijkstra's algorithm or a link-state routing protocol. If not, the request is blocked.

Consider all the scenarios, except in the worst case we have to check the whole network topology, normally, we can tell the route existence immediately or only need to do searching in a much smaller space. By analyzing the traffic statistics and carefully distribute the BI hierarchy, we can reduce the computation cost significantly and identify the bottleneck links more efficiently.

### BI Provisioning/Protection Scheme

After the network has been transformed into an enhanced BIG network with the corresponding BIH constructed, below we introduce the working path setup algorithm and backup path setup algorithm.

#### *1) Setup of the Working Path*

Given a traffic request

a) Update BIH after decreasing the link bandwidth occupied by other primary paths and removing the links in backup paths;

b) Assign the traffic request to a blocking island of the BIH;

c) A routing heuristic called *Minimum Splitting* (MS) [7] is employed to find the working path. The basic idea is to find a route which causes the minimum splitting of the original blocking island.

If the working path is available, the resource availability of each link and BIH are updated. The working path is set up as the primary active path. Concurrently the protection path allocation is started.

#### *2) Setup of the Backup Path*

Now we have a working path *P*.

a) Notice the backup path must be link-disjointed form the working path *P*. We need to remove links used in any working path or any backup path whose working path share common links with *P*. Then we update BIH;

b) Assign the traffic request to a blocking island of the BIH;

c) MS heuristic is employed to find the backup path.

Similar to the idea proposed in [5], when initiating the protection process, we can add a bandwidth fraction threshold *T* to provide differentiated reliability service, where *T* represents the fraction of traffic that needs to be protected.

### Complexity analysis

Define a network topology *G (V, L, W)* for a given IP over WDM network, where *V* is the set of nodes, *L* is the set of links and *W* is the set of wavelengths per fiber link. Assume the set of wavelengths on each fiber link is the same. After transforming into the enhanced BIG network, the number of nodes in the BIG network is $|VW|$ and the predefined BIH level is *H*. Assume $V=(R, O)$, *R* is the set of integrated router/OXC nodes, *O* is the set of OXC nodes. The number of links is equal to $|LW|+|R(|W|-1)|$, $|R(|W|-1)|$ is the number of added virtual links which are regarded as having unlimited bandwidth and no weight. The most common operation in the integrated algorithm is the Blocking Island construction. The $\beta$*-BI* for a given node *x* of a network can be obtained with a simple greedy algorithm. Starting with an initial set $\{x\}$, we recursively add every node to the set, if this node can be reached from any node in the set by a link that has at least $\beta$ available bandwidth. In the worst case, this construction process will examine all links. Therefore, the $\beta$-BI construction process is linear in $O(n)$, where n is the number of actual links in the network $(n=|LW|)$. The time of constructing one level of BIG is $O\ (mn)$, where m is the number of nodes and n is the number of links in the network $(m=|VW|,\ n=|LW|)$. The building time of BIH is $O\ (Hmn)$. Given a good distribution of BIH levels, usually the route existence check time is equal to the time of constructing one level of BIG. In the worst case, it has to compute the route in the whole enhance BIG network using Dijkstra's algorithm to decide whether the route is available or not. If the request can be satisfied, the running time is equal to the combination of 1) *K* alternate shortest paths; 2); Splitting cost computation 3) BIH update. That is $K*O(nlg(m))+K*O(Hmn)+O(Hmn)$, where *K* is a constant and *H* is a constant, so the algorithm running time is linear in $O(mn)$.

## V. SIMULATION RESULTS

In this section, we evaluate the performance of the proposed scheme via simulation in a random generated network topology. In the simulation, the lightpath requests are randomly generated among all node pairs. The wavelength continuity constraint is considered if it is not an integrated router/OXC node. We assume that the propagation delay on any link is the same (e.g. 50ms). Single-link failures are considered as the set of failure scenarios. We do not consider multi-failure scenarios. The network topology is shown in figure 5, consisting of 15 nodes and 29 links. 6 nodes are chosen as integrated router/OXC nodes.

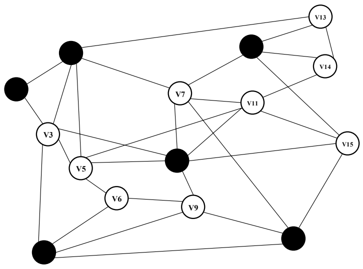


Figure 5: A random generated network topology

So we have 30 pairs of ingress/egress nodes. The traffic pattern is dynamic. Calls arrive at each ingress/egress node pair according to an independent Poisson process. The session holding time is exponentially distributed. The bandwidth requirement is uniformly distributed between 0.1 and 1 unit. We assume the protection ratio *T* is 0.8, which means the bandwidth of protection path is only 80 percent of the working path. In our simulation, extensive tests are carried out to ensure a steady state.

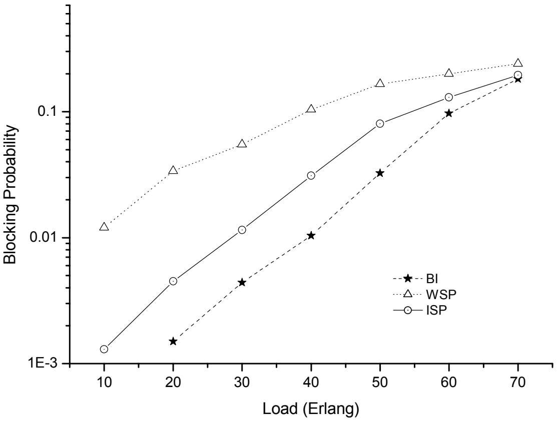


Figure 6: The call blocking probability with the number of wavelength 4

We compare the performance of our scheme (BI) with the WDM shared protection scheme (WSP) and an integrated shared protection scheme (ISP) proposed in [5]. The performance of those algorithms is compared in terms of two objectives. One is to maximize the number of successfully built primary path and the corresponding protection path based on the same network resources. In our simulation, we use blocking probability as the parameter. Under the same traffic load and network topology, the lower the blocking probability is, the better the performance is. The other objective is to minimize average propagation delay on primary lightpath.

Notice in ISP scheme, the lightpath is computed using the shortest path algorithm with first-fit wavelength assignment and the single-hop lightpath allocation is used to assign working path. In our scheme, we predefine the BIH with 0.1-BIG, 0.3-BIG, 0.5-BIG and 0.8-BIG. The simulation results are shown in figure 6 and figure 7 with the number of wavelengths 4 and 8 respectively. In both cases, our scheme outperforms the other two and has a much lower blocking probability. The WDM shared protection performs the worst because its bandwidth granularity is coarse (full wavelength protection) and has the wavelength continuity constraint.

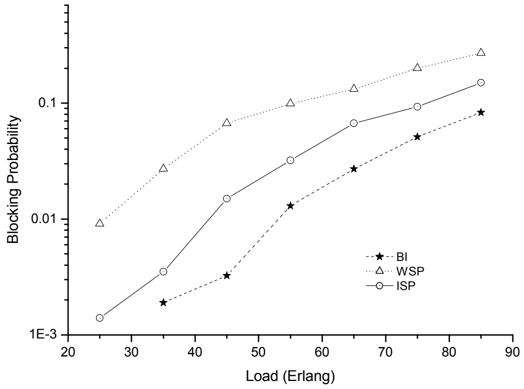


Figure 7: The call blocking probability with the number of wavelength 8

Figure 8 is the average propagation delay (APD) on primary lightpaths vs the traffic load. The wavelength is 4. With the increase of traffic load, the average propagation delay with ISP algorithm changes little, because the shortest path between a pair of nodes is always used as a primary path. The WDM shared protection scheme gives the largest propagation delay because the route is usually long due to wavelength constraint and coarse bandwidth granularity. In our algorithm, with the increasing traffic load, more and more alternate routes will be used and longer alternate routes may be used for conserving limited network resources, which in turn causes the higher average propagation delay. Notice usually our two objectives are contradictory. Under the same condition, the more lightpath requests a network can satisfy, the longer the average propagation delay becomes.

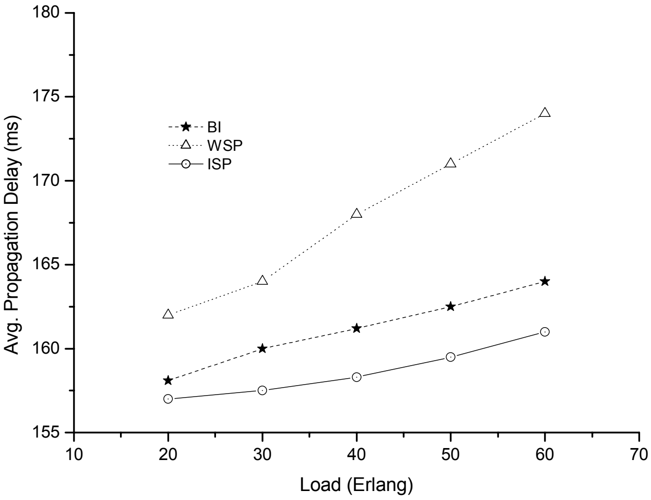


Figure 8: The average propagation delay of primary lightpaths with the number of wavelength 4

## VI. CONCLUSION

The primary contribution of this paper is to develop a dynamic and integrated provisioning/protection scheme in GMPLS-based IP over WDM networks. Using the proposed scheme, we are able to set up an efficient survivable IP over WDM networks. This scheme is proposed based on an abstraction technique called the Blocking Island Paradigm. We introduce the basic idea of blocking island and discuss the process of converting the network topology to the enhanced BI network model. The main advantage of our scheme is that it uses a combined view of IP layer and WDM layer to do IP routing and RWA a single routing domain. Also we show our scheme is a general framework which can reduce the searching space and accommodate various provisioning/protection heuristics. The simulation results prove its effectiveness.

## REFERENCES

[1] V.Sharma et al., Framework for MPLS-based recovery, IETF draft, *draft-ietf-mpls-recovery-frmwrk-03.txt*, July 2001.

[2] S. Ramamurthy and B. Mukherjee, "Survivable WDM Mesh Networks," *Infocom'99*, Mar. 99.

[3] E. Modiano, and A. Narula-Tam, "Survivable Routing of Logical Topologies in WDM Networks,"*OFC'01*, Mar. 2001.

[4] B. Rajagopalan *et al,* "IP over Optical Networks: Architectural Aspects," *IEEE Commun. Mag.*, vol. 38 no. 9, Sept. 2000, pp. 94-102.

[5] Y. Ye, *et al,* "A Simple Dynamic Integrated Provisioning/Protection Scheme in IP over WDM Networks", *IEEE Commun. Mag.*, Nov. 2001, pp. 174-182.

[6] C. R. Frei, "Abstraction Techniques for Resource Allocation in Communication Networks," *PhD thesis*, Swiss Federal Institute of Technology – Lausanne, 2000.

[7] D. Zhemin and M. Hamdi, "A Simple and Intelligent Routing and Wavelength Assignment Algorithm for All-Optical Networks," *SPIE Opticom,* 2001, pp. 210-226.