Design method of Logical Topologies with Quality of Reliability in WDM Networks

Shin'ichi Arakawa   Junichi Katou   Masayuki Murata
Department of Information Networking
Graduate School of Information Science and Technology
Osaka University
1-3 Machikaneyama, Toyonaka, Osaka 560-8531, Japan
E-mail: {arakawa, j-katou, murata}@ics.es.osaka-u.ac.jp
Tel: +81-6-6850-6588; Fax: +81-6-6850-6589

Abstract

As the bandwidth capacity of WDM networks continues to grow rapidly, traffic loss caused by a failure of network components is becoming unacceptable. To prevent such traffic loss and thus enhance network reliability, a protection method that prepares backup lightpaths for each working path is now being developed. In this paper, we first introduce the concept of QoR (Quality of Reliability), which is a realization of QoS with respect to the reliability needed in a WDM network. We define QoR in terms of the recovery time from when a failure occurs to when traffic on the affected primary lightpath is switched to the backup lightpath. After that, we propose a heuristic algorithm that can be used to design a logical topology that satisfies the QoR requirement for every node pair. The objective is to minimize the number of wavelengths needed for a fiber in the logical topology to carry the traffic with the required QoR. We compare this algorithm with two existing algorithms and show that it enables more effective use of wavelength resources; with the proposed algorithm, up to 25% fewer wavelengths are needed than with the other algorithms.

keywords: WDM network, protection method, logical topology design algorithm, QoR (Quality of Reliability), layered graph

1 Introduction

WDM (wavelength division multiplexing) enables a large transmission capacity by multiplexing wavelengths on the fiber. An IP (Internet protocol) over WDM network, where IP packets will be directly carried over a WDM network, is now expected to provide the infrastructure for the next-generation Internet. However, currently available products for IP over WDM networks only provide a large bandwidth on a point–to–point link. That is, each wavelength on the fiber is treated as a physical link between conventional IP routers. This certainly increases the link capacity as the number of wavelengths multiplexed on the fiber grows, but is insufficient to resolve the network bottleneck that arises when there is an explosion of traffic demand since it only shifts the bottleneck to the electronic routers.

A promising way to alleviate such bottlenecks is to configure wavelength paths over the WDM physical network and to carry IP packets that directly use the wavelength paths. Here, the physical network is equivalent to an actual network consisting of optical nodes and optical–fiber links connecting two nodes. Each node in a wavelength–path network has optical switches directly connecting an input wavelength to an output wavelength, which means no electronic processing is necessary at the node. The incoming multiplexed signals are divided into each wavelength at the wavelength demultiplexer (demux). Each signal is then routed to an optical switch that switches incoming signals to a preconfigured outgoing port. Finally, signals routed to the wavelength multiplexer (mux) are again multiplexed and transmitted to the next node. The wavelength path can then be set up directly between two nodes via one or more optical switches. Hereafter, we will call the wavelength path directly connecting two nodes a *lightpath* (Figure 1). Viewing the network from an upper layer rather than the optical layer (e.g., from the IP layer), we can see that the nodes are directly connected via the lightpaths. By utilizing lightpaths, another topology is thus embedded over the physical topology (Figure 2), and this is called the *logical topology*.

The large transmission capacity of a WDM network means that a failure of network components can lead to a large traffic loss. To avoid this, *protection* and *restoration* methods are being developed [1–6]. Protection focuses on providing a fast recovery by switching the working lightpaths affected by the failure (hereafter, we refer to the working lightpath as the *primary lightpath*) to backup lightpaths prepared for the primary lightpath before a failure occurs [2]. By properly preparing backup lightpaths in advance, the protection method can guarantee 100% recovery from a failure if more than two components never fail at the same time (i.e., the single–failure assumption).

In contrast, a restoration method tries to dynamically discover the route and wavelength of available backup lightpaths after a failure occurs [2]. Therefore, the restoration method may be incapable of providing failure recovery if no unused wavelengths are available. Moreover, more time is usually needed to recover from a failure with the restoration method than with the protection method because of the signaling time needed by the restoration method to find backup lightpaths.

The means of determining the route and wavelength of primary/backup lightpaths is called a logical topology design method [1, 7, 8]. Most conventional methods for designing a logical topology using protection/restoration methods focus on minimizing the number of wavelengths used in the WDM network [2–4], or on minimizing the blocking probability when lightpaths are to be set up [5,6]. The blocking probability is the probability that a lightpath set-up request will be rejected because no lightpaths are available. Reducing the number of wavelengths needed may be possible by allowing backup lightpaths whose routes are disjoint with each other to share the same wavelength resources, but this means assuming a single failure [1]. Recent research has focused on providing QoS (Quality of Service) with respect to failure recovery in an optical WDM network [3,4]. QoP (Quality of Protection) was then introduced to realize QoS in an optical network [3], through a probabilistic failure recovery model where only a certain fraction of traffic, which can be specified by the user, is restored after failure. A different approach from [1,3,6] is to consider the possibility of two or more components failing at the same time (a multiple–failure assumption) and assume that each primary lightpath has its own reliability metric that can be determined from the failure probabilities of the network components [4]. Based on this approach, backup lightpaths are partially configured for the primary lightpath according to the specified probability. However, in these QoP–based lightpath configuration methods, the failure-recovery quality is guaranteed only probabilistically. That is, these methods are aimed at improving the effective usage of network resources, but at the cost of a 100% guarantee of failure recovery.

In this paper, we introduce QoR (Quality of Reliability) as a new QoS metric that is aimed at providing highly reliable lightpaths. In QoR, both the time needed to recover from a single failure and 100% failure recovery is guaranteed, because building a highly reliable network is increasingly more important than using network resources efficiently, especially as the number of wavelengths rises with advances in WDM technology. In other words, the approach here is that we should build a logical topology by effectively using the available wavelengths in a way that guarantees the failure-recovery time and guarantees 100% failure recovery. In [9], we proposed two heuristic algorithms that can be used to design the logical topology while satisfying the QoR requirements of each connection. In this paper, we will propose a more effective method, and compare these three algorithms in terms of the number of wavelengths needed to design a logical topology consistent with QoR requirements.

Our paper is organized as follows. We begin with a brief introduction to current protection and restoration methods and discuss the existing research with respect to the quality metrics for fault tolerance functionality. In Section 3, we introduce QoR (Quality of Reliability), and describe a method to satisfy the required QoR in Section 4. We also propose a heuristic algorithm that can be used to design a logical topology that satisfies QoR requirements in Section 4. In Section 5, we compare and evaluate the three proposed algorithms for designing the logical topology, and conclude our paper in Section 6.

2 Fault Tolerance Methods in WDM Networks

2.1 Protection Method

The protection method [1, 10] is a fast recovery method realized through mechanical switching in the optical domain. For each primary lightpath, backup lightpaths are determined and statically configured beforehand, and wavelengths for the backup lightpaths are reserved. There are two protection methods: path protection and link protection. In path protection, a backup lightpath is prepared between the source and destination nodes (Figure 3(a)). In contrast, in link protection a backup lightpath is prepared for each link of the primary lightpath (Figure 3(b)). In either case, when a network component fails along the primary lightpath, the corresponding backup lightpath is activated and traffic on the primary lightpath is switched to the backup lightpath. The protection method thus guarantees 100% reliability for primary lightpaths under the single–failure assumption. That is, whatever failure occurs, the lightpath can be restored and the lightpath bandwidth will never be reduced by a failure. However, since the protection method reserves wavelengths for backup lightpaths, the effectiveness of wavelength usage falls, and there is a trade–off between fast recovery and effective usage of wavelength resources.

Accordingly, several methods aimed at using wavelengths more effectively have been proposed [1–6]. One promising method is *shared protection*, where two or more primary lightpaths can share the same backup lightpath as long as the primary lightpaths are disjoint [1]. Figure 4 illustrates the idea of shared protection. In Figure 4, three primary lightpaths (denoted as $P1$, $P2$ and $P3$) are shown. $P1$ is placed between nodes A and B, and $P2$ and $P3$ connect node pairs CD and FD, respectively. Backup lightpaths $B1, B2$, and $B3$ protect the primary lightpaths $P1$, $P2$, and $P3$, respectively. Primary lightpaths $P1$ and $P2$ both traverse intermediate node E. Furthermore, backup lightpaths $B1$, $B2$, and $B3$ are configured to use the link connecting node pair XY in this example. Here, $B1$ and $B3$ share the same wavelength $\lambda1$, whereas $B2$ uses $\lambda2$. Note that $B1$ and $B2$ must use different wavelengths on the link since the corresponding primary lightpaths ($P1$ and $P2$) both use node E. If we assume that two or more components may fail at the same time, though, we cannot employ the shared protection method. This is because the shared protection method assumes that backup lightpaths whose primary lightpaths are disjoint will never be activated at the same time, hence the shared wavelength on the link will never create a conflict between the sharing backup lightpaths.

2.2 Restoration Method

A restoration method is an alternative way to recover from failures at the optical layer. In a restoration method a backup lightpath is dynamically determined when a failure occurs. Once the backup lightpath is found, the traffic on the primary lightpath affected by the failure is switched to the backup lightpath. Unlike the protection method, the restoration method does not take up any wavelength resources for backup lightpaths before the failure. Therefore, the wavelengths are used more effectively than with the protection method. However, the restoration method will fail to set up a backup lightpath if available wavelength resources are not found. This means that the restoration method cannot provide a 100% guarantee of failure recovery. Moreover, since the backup lightpath is determined only after a failure occurs, the restoration method needs more time to restore a lightpath after a failure.

2.3 Quality Metrics in Existing Fault Tolerance Methods

Several researchers have discussed methods to design logical topologies with protection [1,3,4]. Most of the existing protection methods try to minimize the number of wavelengths when designing the logical topology or to maximize the total throughput within the network. The shared protection method is an effective way to further reduce the number of wavelengths needed under the single–failure assumption.

Wavelength resources can also be used more effectively if we introduce several classes of guarantee with respect to the probability of failure recovery [3]. The conventional protection method only guarantees complete failure recovery (i.e., a single class with a 100% guarantee). Likewise, another guarantee class with a smaller probability of failure recovery can be offered [4]. That is, backup lightpaths are provided for only the connections requesting a higher class of protection, and thus a higher probability of failure recovery.

In this paper, we introduce a new metric to define QoS with respect to the reliability provided by the optical layer. This metric, which is based on the maximum recovery time defined as the maximum time between failure occurrence and the time at which traffic is switched to the backup lightpath, is QoR (Quality of Reliability). The QoR can be used to guarantee the maximum recovery time according to user requests and provide a 100% guarantee that a backup lightpath will be available.

3 QoR (Quality of Reliability) and Recovery Time Modeling

3.1 QoS Classification based on Maximum Failure Recovery Time

In the QoR definition, the class is associated with the maximum recovery time. By specifying a QoR class, we can guarantee a corresponding maximum recovery time upon failure for each connection. In the QoR system we propose, QoR_1 (the highest class) guarantees the minimum failure recovery time. QoR_∞ provides no lightpath protection, and the actual failure recovery may be left to the upper-layer protocol (e.g., IP). More specifically, $QoR_{\,n}$ guarantees the maximum recovery time associated with class n, denoted as $RT(QoR_n)$. One of its simplest forms is

$$RT(QoR_n) = a + b * f(n), \tag{1}$$

where a, b, and $f(n)$ are determined by the network administrator based on the network environment. By configuring $f(n)$, a QoR class can be represented in an arithmetic or geometric progression, or any other form. In the numerical evaluation of Section 5, $f(n)$ is simply set as

$$f(n) = n - 1 \tag{2}$$

and $a = D_{min}$ is the minimum recovery time, which includes the time needed to switch from the primary lightpath to the backup lightpath. $b = D_{scale}$ is the step–width of the recovery time, which includes the processing time to propagate the failure information and to reserve wavelengths at each node of the backup lightpath. The function $RT(QoR_n)$ should be appropriately determined for a given network environment, but specification of only a class–dependent recovery time is not sufficient and we can consider a more precise form of the recovery time. The node–pair dependent recovery time is discussed in Section 3.2.

3.2 QoR Specification for Each Node Pair

There may be no route that can be used to configure backup lightpaths in a way that guarantees the maximum recovery time specified in the QoR class. Figure 5 shows an example of such a case. In Figure 5, there are two routes from node A to F. One is $[A \to B \to C \to D \to E \to F]$, and the other is $[A \to G \to H \to F]$. The propagation delay of the first route is 25 ms in total, while that of the second route is 44 ms. In this situation, if node pair AF requires a QoR class with a maximum recovery time of 20 ms, no lightpath route would provide the required recovery time. The recovery time would include the time needed to propagate the notification of a failure, and this would take more than 20 ms regardless of the route assigned to the primary lightpath.

Thus, the QoR concept should be extended to allow the network administrator to specify the QoR class for each node pair ij. This means the network administrator will begin by examining the smallest possible recovery time for node pair ij, which will be determined by including the propagation delay between the nodes of ij, the node delay for lightpath switching, and so on. This minimum time will be set as the recovery time for the highest class for node pair 12, which is represented as $QoR_{12}(1)$. The recovery times of the lower classes, $QoR_{12}(2)$, $QoR_{12}(3)$, $\ldots$ will then be determined. In the example shown in Table 2, the original QoR classes are defined by Eq. (1). First, $QoR_{12}(1)$ for node pair 12 is mapped to QoR_3. Then, the network administrator decides to map $QoR_{12}(n)$ to QoR_{n+2}. The network operator should make decisions for all node pairs. The mapped QoR_{ij} will then be provided to end users, and an end user using node pair ij can choose the preferred class from $QoR_{ij}(\cdot)$.

3.3 Modeling Recovery Times

In this section, we describe the behavior of the protection method and explain how the recovery time is determined. As shown in Figure 6, a primary lightpath L is protected by several backup lightpaths P_x $(1 \leq x \leq B)$. Here, B is the number of backup lightpaths for primary lightpath L, and is at most equal to the number of intermediate nodes that the primary lightpath traverses. We also define *segment* x as a part of the primary lightpath between the source and destination nodes of P_x (denoted as S_x and D_x, respectively). Using this notation, we will describe the protection method and show how the recovery time is modeled in this method.

To provide QoR as described earlier, we need to set up several backup lightpaths in such a way that the maximum recovery time of each segment provided by the backup lightpaths does not exceed a threshold value. For this purpose, we can modify a SLSP (Short Leap Shared Protection) method [10]. In the original SLSP, several backup lightpaths are configured for each primary lightpath, so that any two neighboring backup lightpaths overlap (Figure 7). Unlike the shared protection method, SLSP enables recovery from a node failure. For example, if a failure occurs at node D, node C will switch the traffic to the backup lightpath directly connected to node H.

The quality metric is realized by specifying the maximum length of the backup lightpath such that its length will be shorter than the threshold [10]. However, when SLSP is used only the length of the backup lightpath is specified. In contrast, we wanted to allow users to specify the maximum recovery time for the primary lightpath L. Such a QoR can be realized by allocating backup lightpaths in a way that ensures the maximum recovery time of each segment is smaller than that segment's threshold. Positioning two neighboring segments so that they overlap also enables recovery from a single-node failure.

The recovery time is modeled as shown in Figure 6. When a failure occurs at segment x, the nodes next to the failed component send information to the nodes that precede it to notify them of the failure. When the failure information arrives at node S_x, node S_x reserves wavelengths on the prepared backup lightpath P_x by sending a reservation signal to D_x through nodes $k, k+1, \ldots k+H_x$. Here, H_x is the hop count of backup lightpath P_x. When the activation is completed, node S_x switches the traffic on the primary lightpath onto P_x. As we see from the above, the recovery time when a failure occurs in segment x consists of three factors;

- Delay needed to propagate the failure information to node S_x
- Configuration time needed to reserve wavelengths at each node of backup lightpath P_x
- Switching time needed to move the traffic from the failed primary lightpath to backup lightpath P_x

Thus, the maximum recovery time when a failure occurs in segment x (denoted as RT_x) is

$$RT_x = \sum_{k=S_x}^{\alpha} d_{k(k+1)} + D_{node} \times (H_x + 1) + D_{conf}, \tag{3}$$

where D_{node} is the wavelength reservation time needed at each node along P_x, and D_{conf} is the switching time at node S_x. In Eq. (3), d_{ij} is the propagation delay between nodes i and j. α is the maximum hop count that the failure information has to traverse in segment x. That is

$$\alpha = \begin{cases} D_x - 1, & D_x \leq S_{x+1}, \\ S_{x+1} - 1, & S_x < S_{x+1} < D_x. \end{cases} \tag{4}$$

The maximum recovery time for primary lightpath L, $RT_{max}(L)$, is the maximum of RT_x for each segment x, and thus,

$$RT_{max}(L) = \max_{1 \leq x \leq B} \{RT_x\}. \tag{5}$$

4 Logical Topology Design Algorithms for Satisfying QoR Requirements

In this section, we describe three heuristic algorithms for designing logical topologies that satisfy the QoR requirements. The objective in designing the logical topology is to minimize the number of wavelengths when the traffic volume and QoR requirements for each node pair are given. In essence, all three algorithms work as follows.

Step 1: For each node pair ij, we set a metric β_{ij} based on $QoR_{ij}(\cdot)$, which is used to determine the order of node pairs assigned to lightpaths.

Step 2: In descending order of a metric β_{ij}, the route and wavelengths are assigned.

The route of a backup lightpath is assumed to be configured on the shortest hop route between the source node S_x and destination node D_x, and the route is disjoint with the links or nodes of its primary lightpath L except S_x and D_x. The backup lightpath is set up based on the hop count because the failure recovery time is highly dependent on the number of hops in the recovery model as shown in Eq. (5).

Before explaining how the wavelength is allocated for backup lightpaths, we should mention that wavelength conversion is not taken into consideration here, so the same wavelength must be used for each lightpath (i.e., a wavelength continuity constraint). When a backup lightpath is set up to protect one segment of L, the same wavelength on L must be assigned to the backup lightpath since the backup lightpath will become part of the primary lightpath after a failure (Figure 8). However, when the source and destination nodes of the backup lightpath are identical to those of L, the wavelength of the backup lightpath does not have to be the same as that assigned to the primary lightpath because in this case the backup lightpath does not share any links with the primary lightpath.

In what follows, we will describe two previously proposed algorithms [9], and then explain a new algorithm.

4.1 First–Fit Algorithm

The First–Fit algorithm first determines the routes of the primary and backup lightpaths. This is a combinational optimization problem to determine routes for the best set of a primary lightpath and backup lightpaths. To simplify the algorithm, the primary lightpath is routed by selecting the route with the smallest propagation delay between nodes, while the backup lightpath is set on the route that has the minimum hop count on the link/node disjoint path.

After the routes of all the primary/backup lightpaths are determined, a wavelength is assigned to each lightpath based on a First–Fit (FF) policy [11]. The FF policy works as follows. When the algorithm discovers that several wavelengths $\{\lambda_{i_1}, \lambda_{i_2}, \ldots, \lambda_{i_n}; i_1 < i_2 < \ldots < i_n\}$ are available for the lightpath, we select the wavelength with the lowest index (i.e., λ_{i_1} is selected). Note that the wavelength assignment depends on whether the source and destination nodes of the backup lightpath are identical with those of the primary lightpath. That is,

- If the nodes are identical, different wavelengths can be assigned to the primary lightpath and the corresponding backup lightpath. Therefore, the algorithm first searches for an available wavelength for the primary lightpath. The wavelength for the backup lightpath is then determined independently of the wavelength assignment for the primary lightpath (see Figure 3(a)).

- If a backup lightpath only partially protects the primary lightpath, a primary lightpath and the set of backup lightpaths must be assigned the same wavelength to satisfy the wavelength continuity constraint (Figure 3(b)).

4.2 Max–Shared Algorithm

In the Max–Shared algorithm, routes of the primary lightpath and a set of backup lightpaths are determined, and then wavelengths are assigned to those lightpaths. The routing algorithm for primary and backup lightpaths is the same as for the First–Fit algorithm, i.e., finding the minimum propagation delay for the primary lightpath and the minimum hop count for the backup lightpaths. The difference from the First–Fit algorithm is in the wavelength assignments. In the Max–Shared algorithm, all available wavelengths are examined for possible assignment to both the primary and backup lightpaths, and the best one is chosen. During the evaluation of each wavelength, we count the number of links which are newly used for the backup lightpath and set the count as the cost of the wavelength. Only when the source and destination nodes of a backup lightpath are the same as those of the primary lightpath, the wavelength for the backup lightpath is assigned independently of the primary lightpath. Note that we then select a wavelength with minimum cost, if several wavelengths are available for the backup lightpath.

The Max–Shared algorithm should enable more effective use of wavelength resources compared to the First–Fit algorithm. This is because the Max–Shared algorithm assigns a wavelength to each set of primary and backup lightpaths that is selected from all possible wavelengths to maximize the number of wavelengths that are shared with other lightpaths while the First–Fit algorithm does not try all available wavelengths.

4.3 Logical Topology Design Algorithm based on a Layered Graph

A layered graph consists of a set of wavelength graphs $G_n (1 \leq n \leq W)$, each of which corresponds to the graph for wavelength λ_n [2]. Wavelength graphs are independent of each other if wavelength conversion is not allowed. The layered graph enables us to determine both the route and the wavelength of the lightpath at the same time by calculating the shortest route for each wavelength. Figure 9 shows an example of a layered graph where the number of wavelengths is set to W. In Figure 9, solid lines in each wavelength graph G_n indicate that the wavelength λ_n is free on that link, whereas dotted lines indicate the wavelength is already being used for primary or backup lightpaths. The metric for each edge of G_n is the propagation delay of the corresponding link. To determine the wavelength to be assigned to each set of primary and backup lightpaths, we introduce a cost C^n for each wavelength λ_n, which denotes the number of links where the wavelength λ_n on the link is newly utilized by the set of primary and backup lightpaths. The proposed algorithm works as follows.

```
Step 0: Initialize $w$, representing the number of wavelengths needed to construct the logical topology, to 0.
Step 1: For each possible lightpath between nodes $i$ and $j$, perform Steps 2 through 4.
Step 2: Update $w$ by calculating the number of wavelengths already used by some links.
Step 3: From $\lambda_1$ to $\lambda_{w+1}$, perform the following steps. (Assume that $\lambda_n$ is currently chosen in the following steps.)
    Step 3.1: Check whether a route consisting of only unreserved wavelengths exists between node pair $ij$ on graph $G_n$. If such a route does not exist, the primary lightpath cannot be set up. If so, go back to Step 3 and check the next wavelength on $G_{n+1}$. Otherwise, assume to set up the primary lightpath, denoted by $L_{ij}$ on the route using $\lambda_n$, and update the metric of edges on $G_n$. That is, delete the corresponding links on $L_{ij}$ from $G_n$, and set the cost of the primary lightpath $C_p^n$ to the number of deleted links.
    Step 3.2: Based on SLSP, a set of backup lightpaths $\{P_1, P_2, \ldots, P_k\}$, each of which should satisfy the $QoR_{ij}$ requirements, can be derived. For this purpose, the route of the backup lightpaths are determined such that the backup lightpaths are disjoint to the primary lightpath $L_{ij}$ and the hop count of the route is minimal. To satisfy these two conditions, calculate $C_r^n$, the cost for assigning wavelength $\lambda_n$ to the backup lightpath $P_r$ ($1 \leq r \leq k$), and determine the set of backup lightpaths for $L_{ij}$.
        Step 3.2.1: When the source node and destination node of $P_r$ is identical to those of $L_{ij}$, $P_r$ can be tentatively assigned to each wavelength $\lambda_i$ ($1 \leq i \leq w+1$). If the backup lightpaths are partially configured at $L_{ij}$, perform Step 3.2.2 only for graph $G_n$ because the backup lightpath partially protecting the primary lightpath must be assigned the same wavelength as the primary lightpath.
        Step 3.2.2: If the backup lightpath $P_r$ can be set up on wavelength graph $G_e$, set the cost of $P_r$ by counting the number of links that are newly used on $G_e$, and set it to $C_e$. After checking all wavelengths (i.e., $G_1$ through $G_{w+1}$), select $e'$ where the cost $C_{e'}$ of the corresponding $G_{e'}$ is minimal. Then, set $C_{e'}$ to $C_r^n$.
    Step 3.3: Set $C^n \leftarrow C_p^n + \sum_{r=1}^{k} C_r^n$. Here, $C^n$ is the cost of wavelength $\lambda_n$ for setting up both the primary and backup lightpaths between nodes $i$ and $j$. Go back to Step 3.
Step 4: Select $a$ such that $C^a$ is a minimum value of $\{C^1, C^2, \ldots, C^{w+1}\}$, and assign wavelength $\lambda_a$ to $P_a$ and $P_r$ (which is partially protecting $P_a$). Then, assign $\lambda_{e'}$, which is precalculated in Step 3.2.2, to the path protection backup lightpath.
```

The algorithm calculates the cost of assigning the primary and backup lightpaths for each wavelength in Step 3.1 and Step 3.2, respectively. In Step 3.3, we calculate the cost C_r^n for each backup lightpath r on λ_n, where the cost means the number of newly used wavelength resources. Step 3 determines the actually used wavelength that minimizes the cost of assigning both the primary and backup lightpaths, and sets up the lightpaths using λ_a. Note that the above algorithm counts the number of wavelengths needed, w. However, when the number of wavelengths is set to W, Steps 3.1 through 3.4 are performed from λ_1 to λ_W.

5 Numerical Evaluations and Discussions

5.1 Network Models

We used a 14–node NSFNET model (Figure 10) and a traffic matrix given in [12] to evaluate the three algorithms. The traffic matrix in [12] contains relative values of the amount of traced traffic on NSFNET in 1992. Hence, we introduced a traffic scale factor γ and used the traffic matrix multiplied by γ as actual traffic demand. (We assumed the appropriate unit for the traffic matrix [12] would be Gbps.)

The bandwidth of each wavelength was set to 10 Gbps and a connection whose requested bandwidth exceeded 10 Gbps was assigned multiple lightpaths to carry the traffic. When two or more lightpaths were assigned to a connection, we set the routes of these lightpaths on the same routes.

We also used a randomly generated network with 21 links that were placed randomly within the 14–node network. Note that the numbers of links and nodes were the same as for NSFNET. The propagation delay for a link was also given randomly and ranged from 0.7 ms to 11.2 ms, which are the shortest and longest propagation delays of links in the original NSFNET. A traffic matrix for the network was randomly selected between 0.0004 and 21.030, the minimum and maximum values in [12].

In the following subsections, we use the values of $D_{min} = 10\text{ms}$, $D_{scale} = 2\text{ms}$, $D_{node} = 1\text{ms}$, and $D_{conf} = 0\text{ms}$.

5.2 Evaluation Results and Discussion

First, we will look at the number of wavelengths needed with each algorithm when every node pair ij requests the same QoR_{ij}. More specifically, in the current example, the network administrator prepares QoR_{ij} classes that are dependent on node pair ij. For example, consider node pair $3,4$ in NSFNET (Figure 10). If the primary lightpath is set to the route $[3 \to 4]$ and a backup lightpath is set to $[3 \to 1 \to 2 \to 5 \to 4]$ between node pair $3,4$, the maximum recovery time is 6.8 ms. If lightpaths are set on different routes, the maximum recovery time will be more than 6.8 ms. Therefore, 6.8 ms is the minimum of the maximum time that can be guaranteed for node pair $3,4$. Here, if D_{min} and D_{scale} are set to 5 ms and 1 ms, respectively, the maximum recovery time guaranteed in QoR_2 is 6 ms and that in QoR_3 is 7 ms. Accordingly, $QoR_{34}(1)$ is set to QoR_2.

In the current example, however, all node pairs are assumed to request the same class to simply show the relationship between QoR_{ij} and the number of wavelengths needed with each algorithm. The horizontal axis in Figure 12 shows the class number that all node pairs request. The vertical axis shows the number of wavelengths needed to set up all the primary and backup lightpaths to fulfill the requests. To obtain this figure, we used the NSFNET network model (Figure 10), and a traffic scale factor γ of 1. The proposed algorithm, based on the layered graph, enabled the wavelength resources to be used more effectively than with the other algorithms, especially when QoR_{ij} was high (e.g., $QoR_{ij} = 1$ or 2). When QoR_{ij} is high, more backup lightpaths must be configured throughout the network to realize the required recovery times. In this situation, the layered graph algorithm can determine routes for each primary and backup lightpath in a way that requires fewer additional wavelength resources. Note that a solid line without points represents the result when no backup lightpath is prepared for a primary lightpath (labeled as Non–Protection in each figure), or the result when only one backup lightpath is configured for each primary lightpath based on the layered graph, which guarantees 100% reliability (labeled as 100% Guarantee in each figure). The number of wavelengths needed with our QoR was at most 100% more than what was needed with no protection in this experiment. Moreover, the number of wavelengths needed with the three algorithms was at most 50% more than the result for a 100% guarantee. In Figures 12, 13, 14, and 15, the number of wavelengths needed for the 100% guarantee exceeded the number needed with the layered graph algorithm at lower QoR_{ij}. This is because even for the lower QoR_{ij}, the number of backup lightpaths configured by the layered graph algorithm slightly exceeds the number needed for the 100% guarantee. As a result, the layered graph algorithm requires fewer wavelengths than in the 100% guarantee case. This tendency was also observed when the algorithms were applied to a randomly generated network (Figure 13).

When the traffic volume was increased ($\gamma = 2$ in Figure 14 and $\gamma = 5$ in Figure 15), the layered graph algorithm still enabled the most effective use of wavelength resources. We then limited the number of wavelengths, W, to 20. QoR_{ij} was configured as in the previous evaluations. The number of blocked connections due to a lack of available wavelength resources and the total amount of traffic volume on the blocked connections are shown in Figures 16 and 17, respectively, for the NSFNET model with $\gamma = 1$. No significant difference was observed among the three algorithms when $W = 20$. However, when the number of wavelengths was set to 50, the advantage of the layered graph algorithm became significant in terms of the number of blocked connections and the amount of blocked traffic, as shown in Figures 18 and 19, respectively. This was because the greater number of available wavelengths made it easier to find available wavelength resources for the backup lightpaths that could be shared with other backup lightpaths. In other words, more wavelengths enable more wavelength sharing, and the advantage of the layered graph algorithm becomes increasingly significant as the number of wavelengths rises. Note that there was no blocking in the case of no available backup lightpaths when the number of wavelengths was set to 50.

6 Conclusion

In this paper, we have introduced QoR (Quality of Reliability), which is a concept related to QoS that concerns reliability in a WDM network. QoR can be used to guarantee a maximum recovery time set according to a user request and provide a 100% guarantee that backup lightpaths will be available. By extending QoR, we can specify QoR for each node pair ij as QoR_{ij}. We have described a heuristic algorithm based on QoR_{ij} that can be used to design a logical topology with a protection method that satisfies QoR_{ij} requirements. The objective of this algorithm is to minimize the number of wavelengths needed to carry the overall traffic and provide fault tolerance within QoR requirements. Numerical results have shown that the algorithm, which is based on a layered graph, enables more effective use of wavelength resources than is possible with other algorithms, especially as the requested traffic volume grows. The algorithm also allows more connections to be carried when using a limited number of wavelengths.

Several topics remain for future work. One is to obtain guidelines for determining the classification of QoR and the specification of QoR_{ij} that take the network environment into consideration. Also, while we have assumed in this paper that the traffic between a node pair will request the same QoR_{ij}, different classes of QoR_{ij} might be requested between a node pair in an actual network. Therefore, this work needs to be extended to obtain a logical topology design algorithm that can accommodate multiple classes of QoR_{ij} even for the same node pair ij. The upper layer of the WDM layer is also of interest for future work. In this paper, we have considered fault tolerance only with respect to the WDM layer. However, the effectiveness of the restoration functionality of the IP layer, for example, should also be considered to create more reliable networks.

References

[1] S. Ramamurthy and B. Mukherjee, “Survivable WDM mesh networks, part I – Protection,” in *Proceedings of IEEE INFOCOM ’99*, vol. 2, (New York, NY, USA), pp. 744–751, Mar. 1999.

[2] V. Anand and C. Qiao, “Static versus dynamic establishment of protection paths in WDM networks,” *Journal of High Speed Networks*, vol. 10, no. 4, pp. 317–327, 2001.

[3] O. Gerstel and G. Sasaki, “Quality of protection (QoP): A quantitative unifying paradigm to protection service grades,” in *Proceedings of Opticomm 2001*, (Denver, CO, USA), Aug. 2001.

[4] C. V. Saradhi and C. S. R. Murthy, “Routing differentiated reliable connections in WDM optical networks,” in *Proceedings of Opticomm 2001*, (Denver, CO, USA), Aug. 2001.

[5] M. Kodialam and T. V. Lakshman, “Dynamic routing of locally restorable bandwidth guaranteed tunnels using aggregated link usage information,” in *Proceedings of IEEE INFOCOM 2000*, vol. 2, (Tel Aviv, Israel), pp. 902–911, March 2000.

[6] G. Mohan and A. K. Somani, “Routing dependable connections with specified failure restoration gurantees in WDM networks,” in *Proceedings of IEEE INFOCOM 2000*, vol. 3, (Tel Aviv, Israel), pp. 1761–1770, March 2000.

[7] R. Ramaswami and K. N. Sivarajan, “Design of logical topologies for wavelength-routed all-optical networks,” in *Proceedings of IEEE INFOCOM ’95*, vol. 3, (Boston, MA, USA), pp. 1316–1325, April 1995.

[8] B. Mukherjee, D. Banerjee, S. Ramamurthy, and A. Mukherjee, “Some principles for designing a wide-area WDM optical network,” *IEEE/ACM Transactions on Networking*, vol. 4, pp. 684–695, Oct. 1996.

[9] J. Katou, S. Arakawa, and M. Murata, “Design method of logical topologies in WDM network with quality of protection,” in *Proceedings of Workshop on OPTICAL NETWORKING*, (Sydney, Australia), Nov. 2001.

[10] P.-H. Ho and H. T. Mouftah, “A framework of a survivable optical Internet using short leap shared protection (SLSP),” in *Proceedings of 2001 IEEE Workshop on High Performance Switching and Routing*, (Denver, CO, USA), pp. 21–25, May 2001.

[11] H. Zang, J. P. Jue, and B. Mukherjee, “A review of routing and wavelength assignment approaches for wavelength-routed optical WDM networks,” *Optical Network Magazine*, vol. 1, pp. 47–60, Jan. 2000.

[12] R. Ramaswami and K. N. Sivarajan, “Design of logical topologies for wavelength-routed optical networks,” *IEEE Journal on Selected Areas in Communications*, vol. 14, pp. 840–851, June 1996.

List of Figures

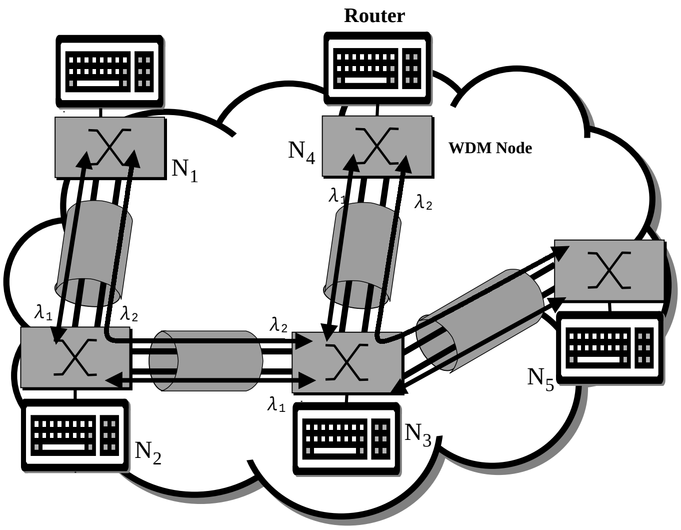


Figure 1: WDM Path Network

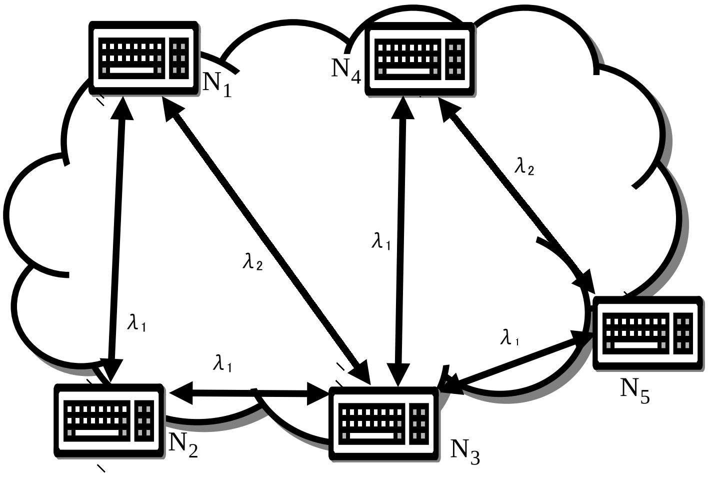
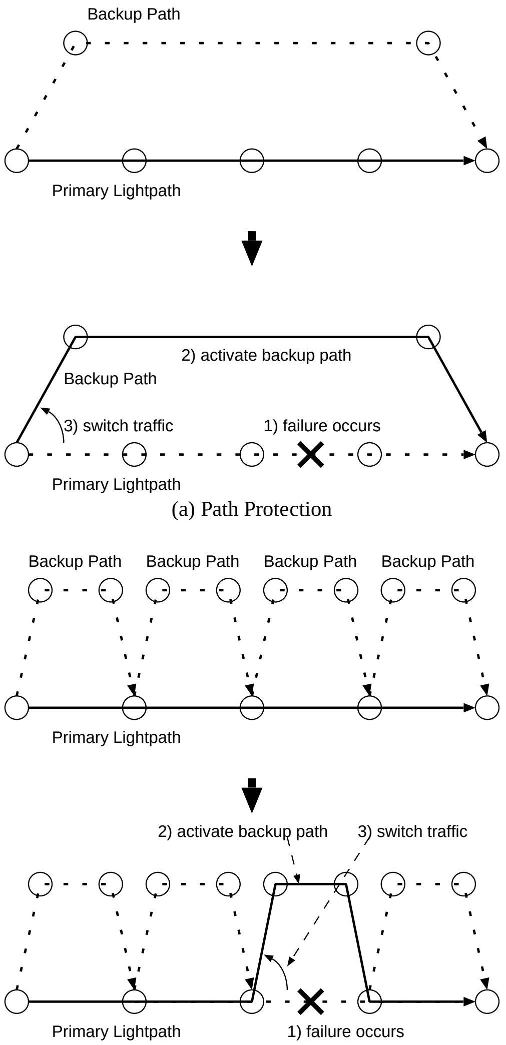


Figure 2: Logical Topology viewed from the IP Layer



(a) Path Protection

(b) Link Protection

Figure 3: Protection Method

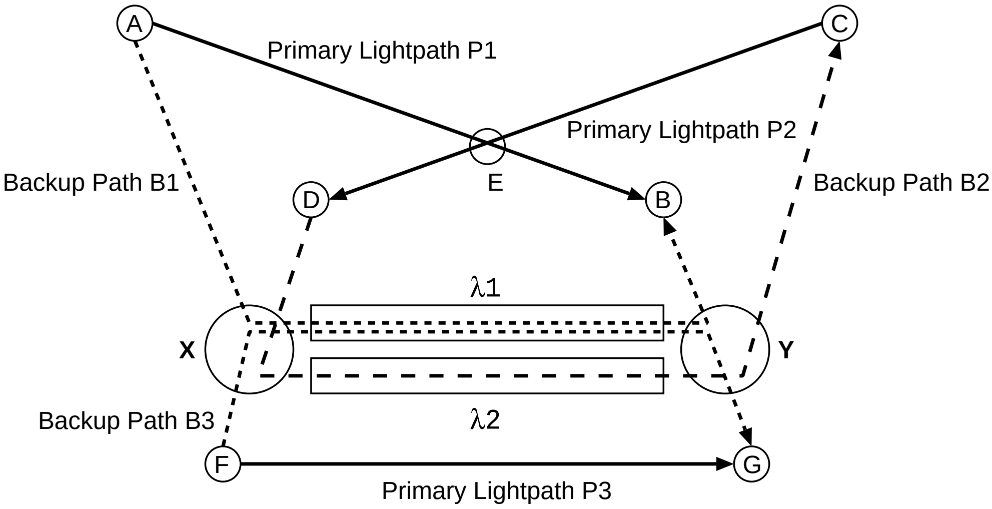


Figure 4: Shared Protection Method

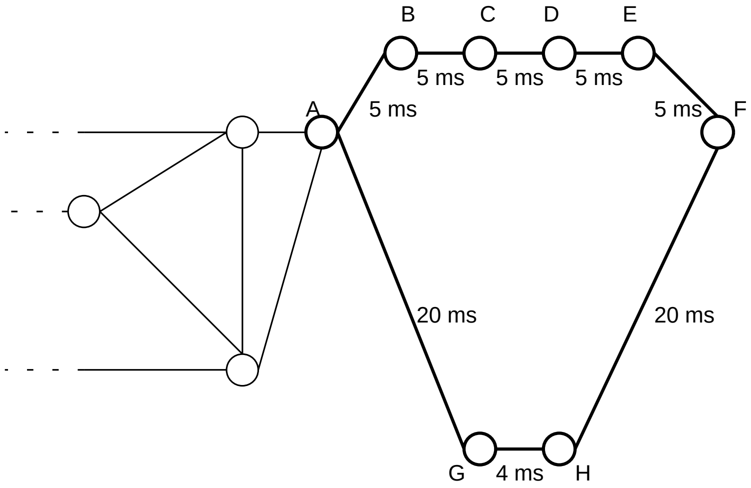


Figure 5: Example Topology

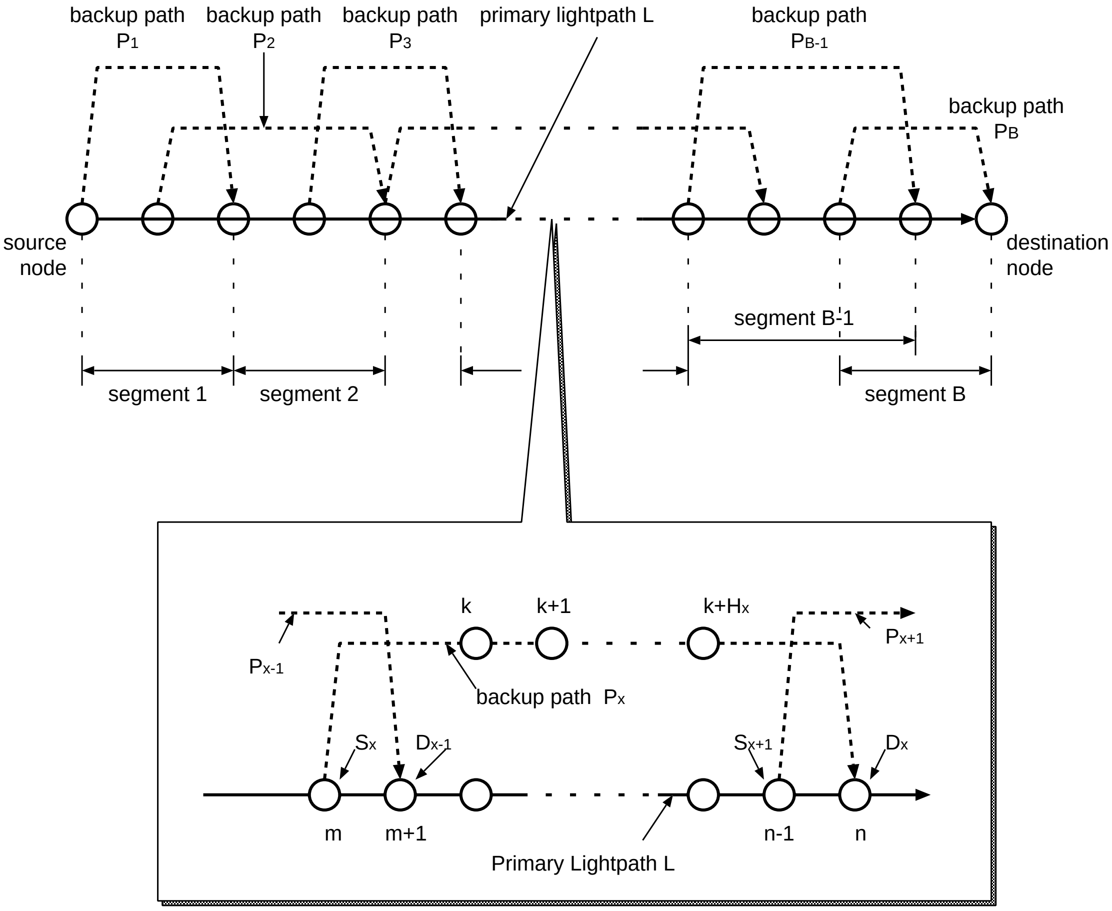


Figure 6: Primary Lightpath protected by Several Backup lightpaths P_x $(1 \leq x \leq B)$

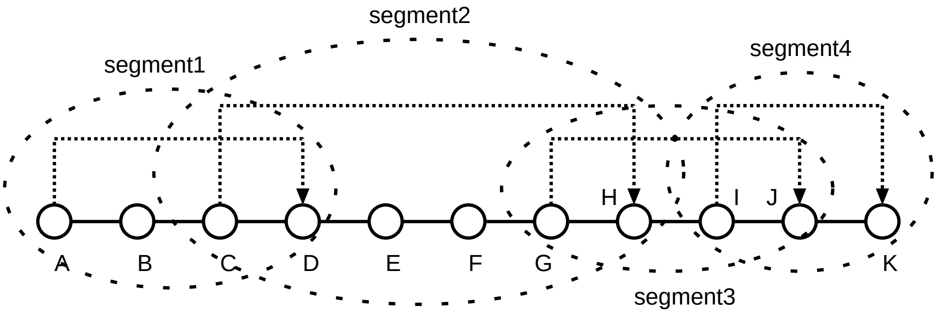


Figure 7: Illustrative example of SLSP

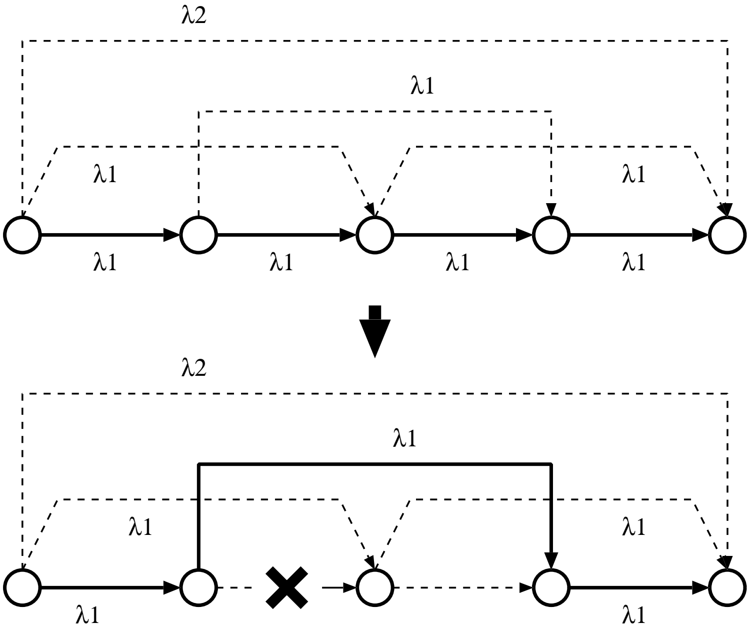


Figure 8: Wavelength Continuity

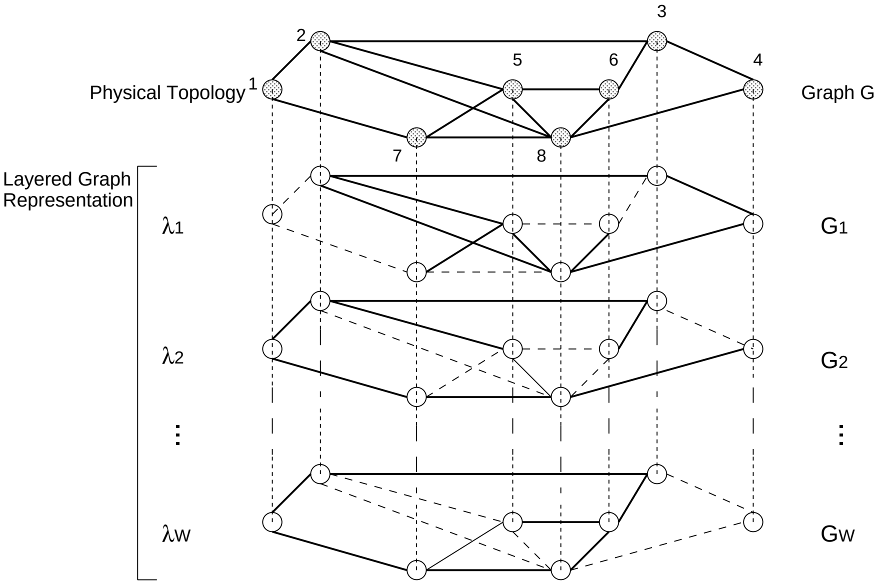


Figure 9: Example of a Layered Graph: The number of wavelengths = W

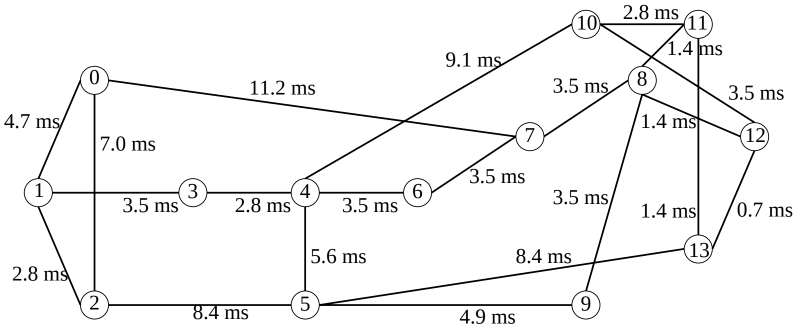


Figure 10: 14–Node NSFNET

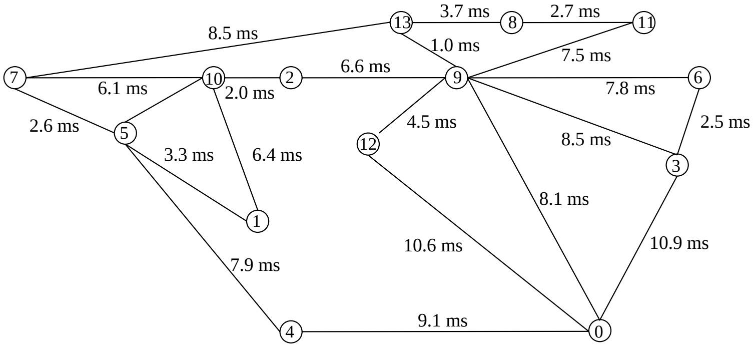


Figure 11: 14–Node Random Network

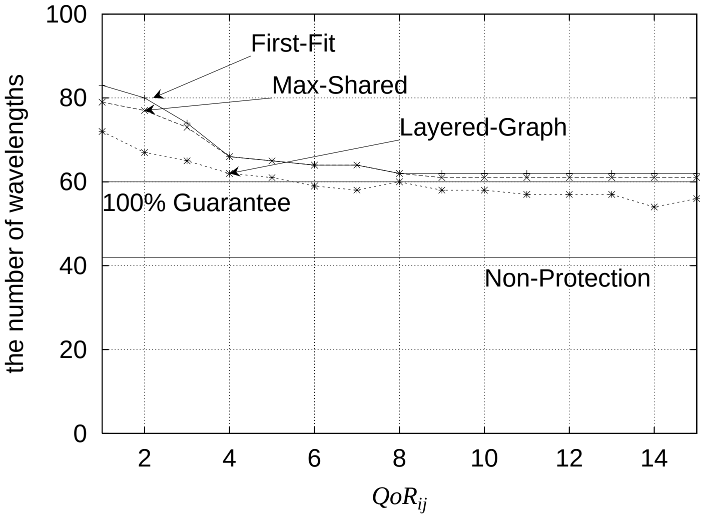


Figure 12: QoR_{ij} vs the Number of Wavelengths in NSFNET: $\gamma = 1$

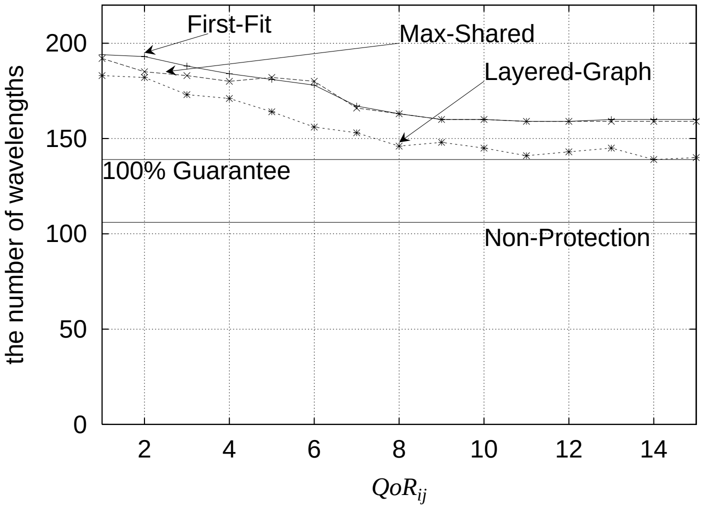


Figure 13: QoR_{ij} vs the Number of Wavelengths in a Random Network: $\gamma = 1$

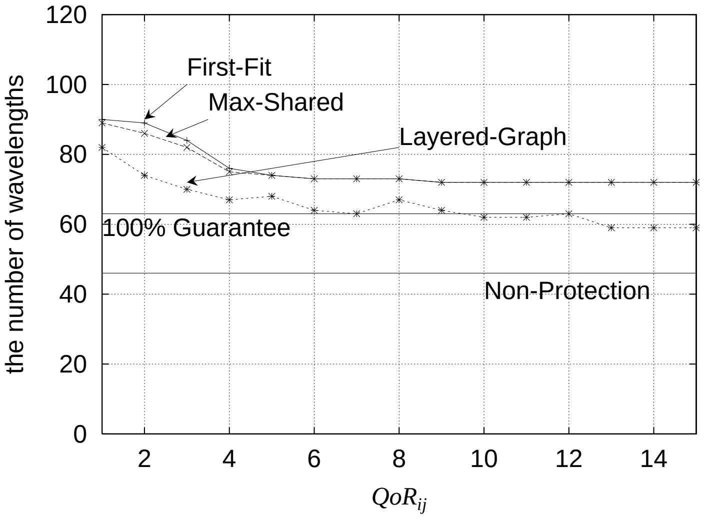


Figure 14: QoR_{ij} vs the Number of Wavelengths in NSFNET: $\gamma = 2$

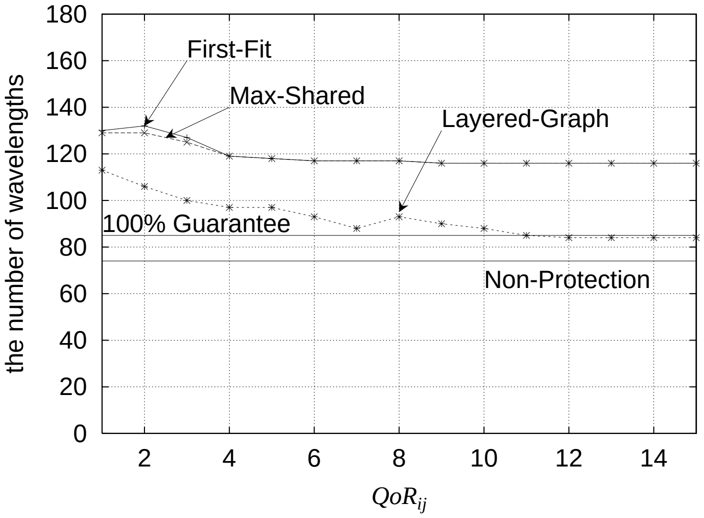


Figure 15: QoR_{ij} vs the Number of Wavelengths in NSFNET: $\gamma = 5$

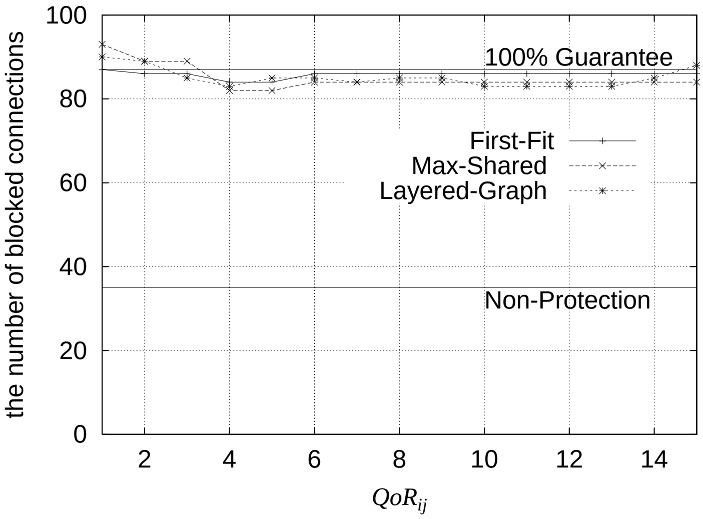


Figure 16: Number of Blocked Connections in NSFNET: $W = 20$

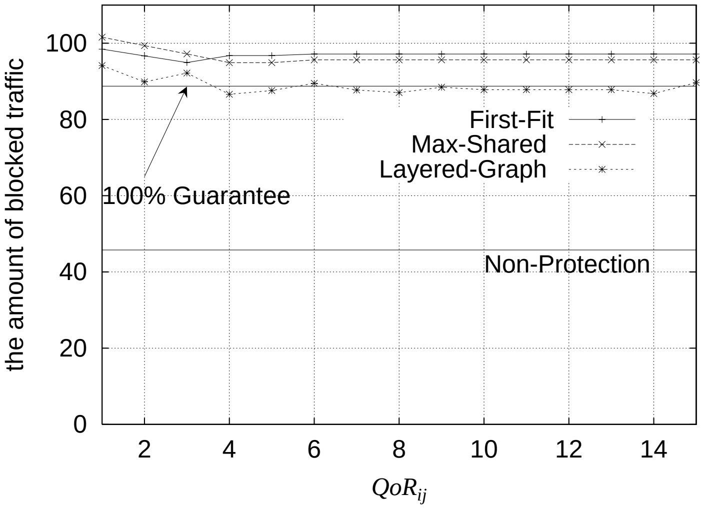


Figure 17: Amount of Blocked Traffic in NSFNET: $W = 20$

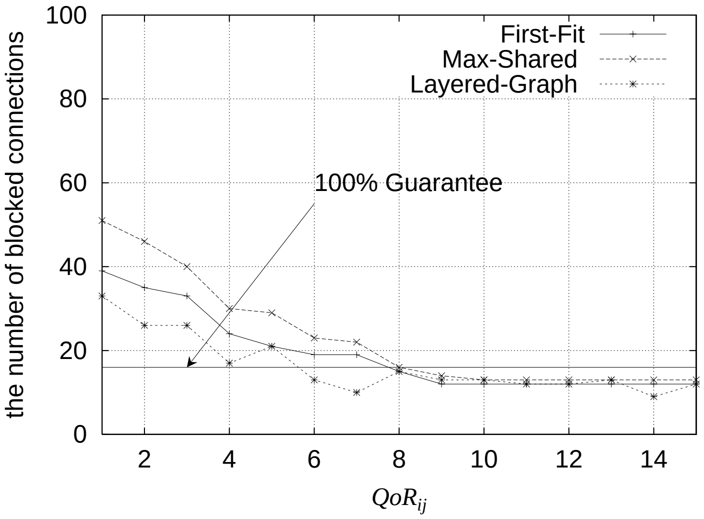


Figure 18: Number of Blocked Connections in NSFNET: $W = 50$

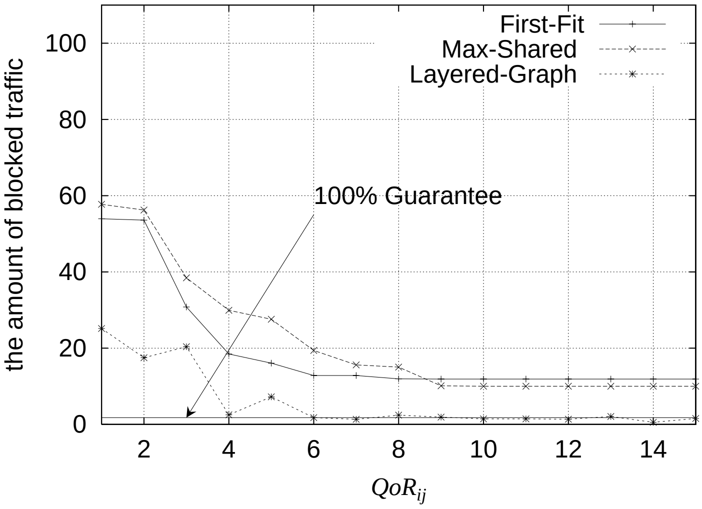


Figure 19: Amount of Blocked Traffic in NSFNET: $W = 50$

List of Tables

Table 1: QoR (Quality of Reliability)

QoR$_1$	failure recovery within D_{min}
QoR$_2$	failure recovery within $(D_{min} + D_{scale})$
QoR$_3$	failure recovery within $(D_{min} + 2D_{scale})$
$\vdots$	$\vdots$
QoR$_n$	failure recovery within $(D_{min} + (n-1)D_{scale})$
$\vdots$	$\vdots$
QoR$_\infty$	no lightpath protection provided

Table 2: QoR dependent on Node Pair

QoR	Maximum Recovery Time	QoR_{12}		QoR_{ij}	
QoR_1	D_{min}	—		—	
QoR_2	$D_{min} + 1 * D_{scale}$	—		$QoR_{ij}(1)$	
QoR_3	$D_{min} + 2 * D_{scale}$	$QoR_{12}(1)$		$QoR_{ij}(2)$	
QoR_4	$D_{min} + 3 * D_{scale}$	$QoR_{12}(2)$	$\cdots$	$QoR_{ij}(3)$	$\cdots$
QoR_5	$D_{min} + 4 * D_{scale}$	$QoR_{12}(3)$		$QoR_{ij}(4)$	
$\vdots$	$\vdots$	$\vdots$		$\vdots$	
QoR_∞	No Protection Lightpaths	$QoR_{12}(\infty)$		$QoR_{ij}(\infty)$	

Table 3: Traffic Matrix for Random Network

	0	1	2	3	4	5	6	7	8	9	10	11	12	13
0	0.000	6.014	16.019	16.596	7.874	7.979	9.556	20.655	17.433	16.887	16.318	3.662	8.016	21.928
1	10.809	0.000	8.875	16.940	17.114	4.149	10.389	1.429	12.390	9.286	14.597	0.614	9.435	23.283
2	6.535	18.131	0.000	1.331	6.372	10.558	21.717	12.767	17.530	5.591	20.742	17.462	2.246	4.555
3	10.349	18.561	22.590	0.000	8.741	16.489	9.399	17.612	23.805	2.514	12.137	10.195	18.315	0.528
4	19.477	8.912	1.138	4.912	0.000	8.195	22.045	13.420	23.898	18.793	14.354	21.615	7.561	22.260
5	3.207	18.679	15.722	19.825	13.611	0.000	2.072	14.386	12.201	1.189	21.251	11.976	9.178	21.057
6	4.866	21.311	21.628	23.178	12.215	17.105	0.000	8.090	3.729	12.394	6.662	1.775	16.190	20.936
7	10.944	6.544	18.552	8.881	4.804	12.135	3.561	0.000	20.522	7.960	7.548	12.970	12.723	19.745
8	14.156	0.354	22.097	23.330	11.787	2.964	11.021	9.415	0.000	2.142	23.233	16.897	0.608	2.962
9	5.291	21.642	19.109	21.477	18.579	20.430	18.397	3.511	5.311	0.000	13.577	15.642	23.244	10.099
10	13.978	6.792	13.446	17.077	16.913	17.978	17.428	15.011	7.688	5.215	0.000	17.971	18.705	5.007
11	20.109	8.318	21.900	11.093	1.657	3.191	8.736	20.762	15.044	3.315	7.572	0.000	23.817	6.822
12	12.880	13.394	12.840	2.504	23.489	17.194	9.293	3.315	10.272	2.206	21.289	18.076	0.000	7.593
13	4.977	13.667	1.564	14.059	18.670	12.049	22.373	16.570	23.139	0.030	10.137	22.251	11.169	0.000