Distance Adaptive Dynamic Routing and Spectrum Allocation in Elastic Optical Networks With Shared Backup Path Protection

Chao Wang, Gangxiang Shen, *Senior Member, IEEE*, and Sanjay Kumar Bose, *Senior Member, IEEE*

***Abstract*—This paper considers distance adaptive dynamic routing and spectrum assignment (RSA) for elastic optical networks with shared backup path protection (SBPP). Efficient heuristic algorithms based on spectrum window planes are proposed for implementing distance and modulation format adaptive RSA so as to maximize spare capacity sharing among multiple protection lightpaths. A differentiated sharable frequency slot cost was also defined for the first time to more efficiently share protection resource. Network performance is evaluated in terms of bandwidth blocking probability (BBP) through simulations. The proposed SBPP technique is effective in reducing BBP and improving spectral efficiency compared to conventional SBPP schemes and 1+1 path protection. The impact of transponder tunability on bandwidth blocking performance is also evaluated to show that a limited tuning range is sufficient to achieve a BBP performance close to that with full tunability.**

***Index Terms*—1+1 protection, bandwidth blocking, dynamic routing and spectrum allocation, elastic optical network, SBPP, spectrum window plane.**

I. Introduction

TRADITIONAL wavelength division multiplexing (WDM) networks adopt fixed-size bandwidth allocation per wavelength. This leads to capacity wastage when the traffic demand is less than the capacity of one wavelength. To overcome this issue, researchers have been working on next-generation optical transmission systems based on elastic optical transmission techniques such as coherent optical orthogonal frequency division multiplexing [1], [2]. An elastic optical network is more flexible in bandwidth allocation and uses the fiber spectrum more efficiently than a traditional WDM network. Networks of this type have been generating substantial research interest recently, with extensive studies dedicated to their design and performance evaluation [3]–[9].

Survivability is an important aspect for an elastic optical network that carries a large amount of traffic. Various protection techniques developed for traditional WDM networks can be extended to also protect this type of network. Among these techniques, shared backup path protection (SBPP) is considered promising because of its operational simplicity, fast restoration speeds, and high spare capacity sharing efficiency. SBPP is a failure-independent, path-oriented protection scheme where a protection route is predetermined and its required protection capacity is preplanned [10]. Multiple protection lightpaths can share the protection capacity if their corresponding working lightpaths do not share any common failures (e.g., link failures). However, the protection capacity is not cross-connected and a protection lightpath is made ready only when a failure on its corresponding working lightpath actually occurs.

Because of the above attractive features of SBPP, various studies have been done for SBPP elastic optical networks. These can be mainly divided into two categories, i.e., based on either the *static* or the *dynamic* lightpath traffic demand. For the case of static traffic demand, Kosaka *et al.* proposed an advanced RSA algorithm that employs a *path relocation scheme* and sets the cost of each shareable frequency slot (FS) to be a uniform small value so as to maximally share protection capacity [11]. Shen *et al.* developed integer linear programing (ILP) models for the SBPP elastic optical network and evaluated its performance [12]. Moreover, the impacts of transponder tunability and bandwidth squeezed restoration technique were evaluated. Other related works on the static traffic demand can also be found in [13] and [14]. For the case of dynamic traffic demand, Shao *et al.* proposed two protection capacity sharing policies, i.e., *conservative sharing policy* and *aggressive sharing policy* [15]. Tarhan and Cavdar proposed a strategy called primary first-fit modified backup last-fit to reduce spectrum fragmentations and increase FS shareability [16].

All these studies have successfully incorporated two important and unique constraints for elastic optical networks, i.e., *spectrum contiguity* and *spectrum continuity*. The former requires all the FS assigned to a lightpath to be spectrally neighboring. The latter implies that all the fiber links traversed by a lightpath must use the same set of FS.

However, it is interesting to observe that no studies have looked into the limitations that may arise due to physical layer impairments, even though these may force different modulation formats to be used by the working and protection lightpaths and may also require different numbers of FS to be assigned to them. For the same node pair, a protection lightpath would normally be longer than its corresponding working lightpath. In that case, the protection lightpath may have to be assigned with a less spectrally efficient modulation format and may then

Manuscript received January 4, 2015; revised March 7, 2015; accepted April 2, 2015. Date of publication April 8, 2015; date of current version June 3, 2015. This work was supported in part by the Chinese 863 Project (2012AA011302), the NSFC (61322109, 61172057), the NSF of Jiangsu Prov. (BK20130003, BK2012179), and the Science and Technology Support Plan of Jiangsu Province (BE2014855).

C. Wang and G. Shen are with the School of Electronic and Information Engineering, Soochow University, Suzhou 215006, China (e-mail: wangchao93180@163.com; shengx@suda.edu.cn).

S. K. Bose is with the Department of Electronics and Electrical Engineering, Indian Institute of Technology Guwahati, Guwahati 781039, India (e-mail: skbose@iitg.ernet.in).

Digital Object Identifier 10.1109/JLT.2015.2421506

0733-8724 (c) 2015 IEEE. Personal use is permitted, but republication/redistribution requires IEEE permission. See http://www.ieee.org/publications_standards/publications/rights/index.html for more information.

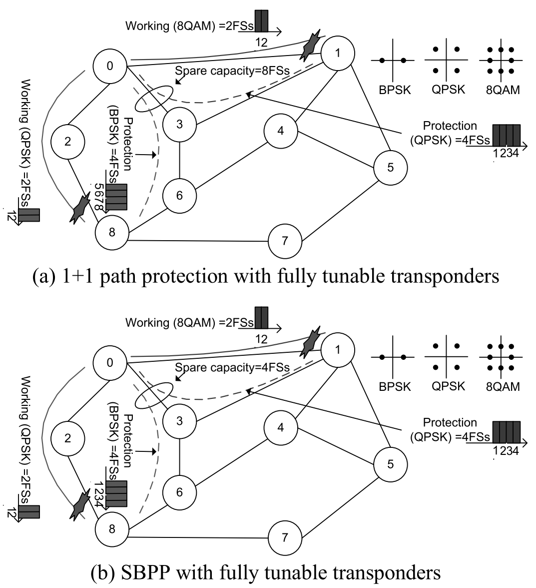


Fig. 1. Examples of distance adaptive SBPP and 1+1 path protection in elastic optical networks.

require more FS in order to achieve the same bandwidth as that of its corresponding working lightpath. Thus, for an SBPP elastic optical network, it is practical and necessary to also consider another important aspect, i.e., *lightpath physical distance*. We should adaptively assign different modulation formats and numbers of FS to a pair of working and protection lightpaths between a common node pair, respectively. This is illustrated in the example of Fig. 1, where the pair of working and protection lightpaths use different modulation formats and are assigned different numbers of FS because of the different physical distances associated with them.

It should also be noted that all the existing studies uniformly set a small cost for each sharable FS in order to achieve maximal spare capacity sharing. However, because the bandwidth of a protection lightpath consists of multiple FS and since each shareable FS can be shared by different number of protection lightpaths, an identical cost for each sharable FS may not be the most efficient option to achieve the best network performance. Differentiating the cost of each shareable FS based on their sharing status may provide a better alternative. This has been proposed and evaluated by us in this paper.

It may also be noted that for protection lightpath establishment, the approach followed by almost all the studies break up routing and spectrum assignment into two independent steps [13], [14], [16]. Using the K-shortest path algorithm, they first compute multiple offline routes that can be used for establishing the protection lightpath. Then, from these routes, they choose the one with the best spectrum sharing to establish the protection lightpath. Though this simplifies the process of establishing the protection lightpath, this method of breaking up the routing and spectrum assignment steps cannot achieve maximal spectrum sharing between the protection lightpaths. A more advanced strategy that integrates the two needs to be explored to see if that can give even better spectrum sharing. However, this is still an open problem for SBPP elastic optical networks and has been considered for the first time by us in this paper.

Based on the current research status of SBPP elastic optical networks, this paper makes the following key contributions. First, when implementing RSA, we incorporate the physical distance difference between a pair of working and protection lightpaths to differentiate between their assigned modulation formats and numbers of FS.

Second, rather than simply setting an identical small value as the cost of each sharable FS, we differentiate between them by setting the cost of each sharable FS as a function of the number of lightpaths that are sharing the FS; this is expected to provide better performance than the simplistic scheme based on an identical small cost.

Third, to maximize protection spectrum sharing, we develop an integrated RSA approach based on the concept of spectrum window planes (SWPs) to jointly choose the route and assign the spectrum for the lightpath.

A. Other Related Works

Apart from the research work reported on SBPP elastic optical networks, various related research have also been carried out for survivable elastic optical networks. These include link-based protection techniques, i.e., span restoration [17], p-Cycle [18], [19], and ring cover [18] techniques. In addition to the SBPP technique, other path-based protection techniques include 1+1 dedicated path protection [20], [21] and multipath provisioning [22], [23]. Other related works on survivable elastic optical networks are also reported in [24] and [25].

The rest of this paper is organized as follows. In Section II, we introduce the distance adaptive SBPP and 1+1 path protection techniques for the elastic optical network. In Section III, we describe the heuristic algorithms for the SBPP and 1+1 path protection techniques which integrate routing and spectrum assignment. In addition, we investigate the impact of elastic transponder tunability on the flexibility of spectrum assignment. In Section IV, we present numerical results and analyze network performance. Section V concludes the paper.

II. Distance Adaptive SBPP and 1+1 Path Protection

This section introduces the concept of SBPP in contrast to the usual 1+1 (dedicated) path protection technique in the context of the elastic optical network under the assumption that the working and protection lightpaths can be assigned with different sets of continuous FS (i.e., using fully tunable transponders). A transponder is *fully tunable* means that it can change the number of FS and modulation format of its supporting lightpath. With such an assumption, a pair of working and protection lightpaths can share a common transponder.

As shown in Fig. 1, when a link fails, both techniques can find a replacement path directly between the two end nodes of a working path. For example, if link (2–8) fails, working lightpath (0–2–8) is affected and a switch-over is carried out to direct affected working traffic onto a predefined route (0–3–6–8) for failure recovery. Similarly, if link (0–1) fails, working lightpath (0–1) is affected and a switch-over is carried out to

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/JLT.2015.2421506, Journal of Lightwave Technology

direct affected working traffic onto a predefined route (0–3–1) for failure recovery.

In an elastic optical network that employs different modulation formats depending on the actual physical distance of a lightpath, the working and protection lightpaths may use different modulation formats and may be assigned with different number of FS in order for them to support the same bandwidth. For example, to transmit the same bandwidth, the working lightpath between node pair (0, 1) is assigned with a higher level modulation format (e.g., 8QAM) and fewer FS (e.g., 2 FS) for its shorter distance and its corresponding protection lightpath is assigned with a lower level modulation format (e.g., QPSK) and more FS (e.g., 4 FS) for its longer distance. Similarly, to transmit the same bandwidth, the working and protection lightpaths between node pair (0, 8) may be assigned with the modulation formats of QPSK and BPSK and 2 and 4 FS, respectively.

Under the 1+1 protection technique, to achieve 100% failure recovery, the protection capacity on each protection lightpath should be dedicated to protecting its corresponding working lightpath. Thus, as depicted in Fig. 1(a), 8 FS (from 1 to 8) are reserved on the common link (0–3) that is shared by the two protection lightpaths. In contrast, the SBPP technique allows protection capacity sharing on the common links traversed by multiple protection lightpaths, as long as their corresponding working lightpaths do not share any common link. Since there is no common link shared by the working lightpaths (0–1) and (0–2–8), the protection capacity on common link (0–3) can be shared by their corresponding protection lightpaths under SBPP. This implies that only 4 FS (from 1 to 4) should be reserved on (0–3) to guarantee full protection for the two working lightpaths provided that links (0–1) and (2–8) do not fail simultaneously.

III. Distance Adaptive RSA Heuristic Algorithms for SBPP Elastic Optical Networks

In this section, we focus on efficient heuristic algorithms for distance adaptive dynamic SBPP-based lightpath service provisioning. We assume that optical transponders are fully tunable so that the working and protection lightpaths can be assigned with different available contiguous FS.

A. Preliminaries

We represent a general elastic optical network as $G(V, E)$, where V is the set of nodes and E is the set of (bi-directional) fiber links between node pairs. A request is represented by $CR(S, D, R)$, where S and D are the respective source and destination nodes and R is the bandwidth of the request.

We consider three modulation formats (i.e., BPSK, QPSK and 8QAM). Given a bandwidth R, we can easily find the required numbers of FS for a certain modulation format. The relationship is $F \cdot B \cdot SE \geq R$, where F is the number of required FS, B is the bandwidth of each FS in units of GHz, and SE is the spectrum efficiency (in units of bit/s/Hz) of the adopted modulation format. For BPSK, QPSK and 8QAM, the corresponding SEs are 1, 2, and 3 bit/s/Hz, respectively. These F FS are required to be spectrally contiguous along a lightpath if the sub-band virtual concatenation technique is not allowed. Because a pair of working and protection routes normally has different distances, different modulation formats and number of FS may be assigned to them.

TABLE I
FS Capacities and Optical Reaches for Different Modulation Formats [26]

Modulation Format	FS Capacity (Gb/s)	Transparent Reach (km)
BPSK	12.5	4000
QPSK	25	2000
8QAM	37.5	1000

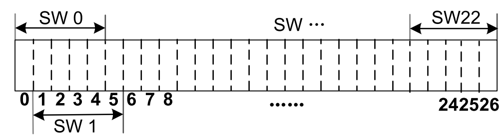


Fig. 2. SWs in a fiber link.

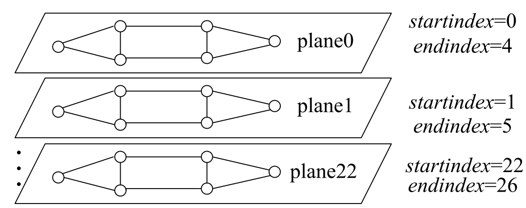


Fig. 3. SWPs in the n6s8 network.

For each modulation format, we assume a maximal optical reach as shown in Table I, in which the bandwidth of each FS is assumed to be 12.5 GHz and each row shows the FS capacity and transparent reach of each modulation format. BPSK has the longest transparent reach, but the lowest FS capacity. In contrast, 8QAM has the highest FS capacity, but the shortest transparent reach.[1]

For the heuristic algorithm, we introduce the concept of *spectrum window* (SW) as in [27], which is made up of a certain number of continuous FS. The size F of an SW may vary according to different user bandwidth requests. In the example of Fig. 2, assume a fiber has 27 FS. If $F = 5$, then the size of SW is five, and there are 23 SWs (i.e., SW0–SW22) in the fiber link.

Based on the concept of SW, we then define a concept called SWP as shown in Fig. 3. SWP is similar to the concept of waveplane [28] in the traditional WDM network. In a WDM network, each waveplane corresponds to a specific wavelength. Likewise, in an elastic optical network, each SWP corresponds to an SW. For each F-slot SWP, we use *startindex* and *endindex* to denote the index of its starting and ending FS, respectively. For example, in Fig. 3 plane 0 corresponds to SW0, its $startindex = 0$ and $endindex = 4$.

[1] It should be noted that we are employing a simplified model to decide the transparent reach for each lightpath based on the physical transmission distance. The proposed schemes can also be made to work with more advanced physical-layer transmission models if there are any. In addition, the data in the table is only for test purpose. The approaches proposed in the paper are general enough to support any transparent reach data that may be available.

DOI 10.1109/JLT.2015.2421506, Journal of Lightwave Technology

To establish a pair of working and protection lightpaths, we first need to find a pair of eligible working and protection routes on SWPs. If such a pair of routes can be found, the working and protection lightpaths can be established on corresponding SWPs by using the spectra of the SWPs. We divide the RSA algorithm for distance adaptive SBPP elastic optical networks into two steps, i.e., establishing the working and protection lightpaths subsequently. If a working lightpath cannot be successfully established, we will not subsequently search for a protection route.

B. RSA for Working Lightpath

We use two variables *w_route* and *w_index* to record the information of the working route and the starting FS index of the working lightpath, respectively. Next we introduce the detail of the RSA algorithm for the working lightpath below.

Algorithm 1 RSA for **working lightpath**

Input: $CR(S, D, R)$

for each modulation format (*MF*) with a specific *SE* (from 8QAM to BPSK in Table I) **do**
  Decide the number of FS for each SWP based on the modulation format as $F = \lceil \frac{R}{B \cdot SE} \rceil$;
  Create a corresponding list of SWPs, of which each has *F* FS;
  Remove all the links from each of the SWPs if corresponding SWs are not avaialbe, i.e., not all the *F* continuous FS are free;
  for each SWP (from the lowest to highest index) **do**
    Use Dijkstra's algorithm to find a shortest route R_w in hops;
    if R_w is found and the total distance of R_w is shorter than the transparent reach of the current *MF* **then**
      if $w\_route = NULL$ **then**
        w_route←R_{w}, *w_index*←*startindex of current SWP*;
      else
        if the hop length of R_{w} is smaller **than** that of *w_route* **then**
        w_route←R_{w}, *w_index*←*startindex of current SWP*;
        end if
      end if
    end if
    Move to the next SWP;
  end for
  if $w\_route =$ NULL **then**
    Move to the next *MF*;
  end if
end for

In the above algorithm, we consider all possible modulation formats from 8QAM to BPSK. For each of the modulation format, we decide the required number of FS, *F*, using $F = \lceil \frac{R}{B \cdot SE} \rceil$. We create a list of SWPs, of which each contains *F* continuous FS. We then remove all the SW links on each of the SWPs if any FS in the SW link has been used. Next we search for a route on each of the SWPs and if the distance of the found route is shorter than that of the transparent reach of the current modulation format, then the route is considered eligible. For each of the modulation formats, all the SWPs will be scanned to choose the shortest eligible route in hops (i.e., the LC strategy). If an eligible route is found for the current modulation format, we will terminate the searching process and assign the spectrum of the current SWP to the working lightpath. The request will be blocked if no eligible working route can be found after scanning all the modulation formats.

C. RSA for Protection Lightpath

If a working lightpath can be successfully established, we next search for an eligible protection route with the lowest cost. For this, two key aspects are considered, i.e., (a) deciding whether an SW link is available for the protection lightpath and (b) calculating the cost of each available SW link.

Because an SW link contains multiple FS, it is considered available for a protection lightpath only if all the contained FS are available for the protection lightpath. Under SBPP, there are two situations for an FS to be available for a protection lightpath: (1) the FS is free; or (2) the FS is sharable for the protection lightpath subject to the condition that the working lightpaths of all the protection lightpaths that share the FS do not share any common link. In both these cases, we must first ensure that the link containing the FS is not traversed by the working lightpath; this is required to ensure that the working and protection lightpaths are link-disjoint in nature; otherwise, all the FS on the link should not be used for protection lightpath establishment.

In the conventional SBPP scheme, a uniform small cost is typically set for each sharable FS in order to maximally share protection capacity [11]. However, the usage or sharing status of each FS in an SW can be different. Thus, an identical cost for each sharable FS may not be the most efficient option to achieve the best network performance. We propose to differentiate the cost of each shareable FS according to their shared status by protection lightpaths, given by equation

$$C_{\mathrm{SW}} = \sum\nolimits_{i=1}^{F} C_i \tag{1}$$

where C_i is the cost of the *i*th FS given by equation

$$C_i = \begin{cases} 1, & \text{if FS is free} \\ 1/(m+1), & \text{if FS is shareable} \end{cases} \tag{2}$$

where *m* is the number of protection lightpaths that are sharing the FS. If an FS is free, this cost is set to be 1.0, and if it is sharable, the cost is set to be inversely proportional to the number of protection lightpaths that are sharing the FS. It is expected to be more efficient to assign a smaller cost to an FS if it is shared by more protection lightpaths.

Knowing how to decide the availability of each SW and to calculate its associated cost, we next present the RSA algorithm for the protection lightpath. We use two variables *p_route* and *p_index* to record the information of the protection route and the starting FS index of the protection lightpath, respectively.

Algorithm 2 RSA for **protection lightpath**

Input: $CR\,(S, D, R)$, *w_route*

1: **for** each modulation format (*MF*) with a specific *SE* (from 8QAM to BPSK in Table I) **do**
2: Decide the number of FS for each SWP based on the modulation format as $F = \lceil \frac{R}{B \cdot SE} \rceil$;
3: Create a corresponding list of SWPs, of which each has *F* FS;
4: Remove all the links traversed by *w_route* from each SWP;
5: Remove all the links from each of the SWPs if corresponding SWs are not avaialbe, i.e., not all the *F* continuous FS are free or sharable;
6: **for** every SWP (from the lowest to highest index) **do**
7: Calculate cost C_{SW} of each available SW link on the SWP using (1) and (2);
8: Find a protection route R_p with the lowest cost via Dijkstra's algorithm;
9: **if** R_p is found and the total distance of R_p is shorter than the transparent reach of the current *MF* **then**
10: **if** $p\_route = NULL$ **then**
11: *p_route*←$\mathrm{R_p}$, *p_index*←*startindex of currnt SWP*;
12: **else**
13: **if** the cost of R_p is smaller than that of *p_route* **then**
14: *p_route*←$\mathrm{R_p}$, *p_index*←*startindex of currnt SWP*;
15: **end if**
16: **end if**
17: **end if**
18: Move to the next SWP;
19: **end for**
20: **if** *p_route* $=$ *NULL* **then**
21: Move to the next MF;
22: **end if**
23: **end for**

The above algorithm is very similar to the RSA algorithm for the working lightpath, except for the following two aspects. First, for the protection lightpath, the conditions of removing an SW link from its corresponding SWP are: (a) it is traversed by the working lightpath or (b) any one of the contained FS is *used* and *not sharable*. Second, for the protection lightpath, the SW link cost is calculated by equations (1) and (2), instead of simply the *hop number* as for the working lightpath.

Though extended from the traditional waveplane-based algorithm for a WDM network, the SWP-based algorithm does have important differences. First, the number of waveplanes is fixed for a given WDM network with a certain number of wavelengths. In contrast, the number of SWPs is not fixed and will depend on the required bandwidth (in Gb/s) between each node pair and the chosen route for lightpath establishment. For an elastic optical network with M FS per fiber, there are $M - x + 1$ SWPs for a lightpath with x FS. Note that x is different for different node pairs and different lightpath routes. Second, for the protection lightpath, each shared FS has different costs, which is also different from the cost of each shared wavelength in the WDM network. Thus, overall the proposed SWP-based algorithm is more complicated and needs to consider the relevant aspects carefully.

D. Complexity Analysis

The pseudocode of the *SBPP RSA* heuristic algorithm is shown in *Algorithms 1* and 2. In *Algorithm 1*, line 4 removes all unavailable SW links on each SWP, whose computational complexity is O (WM), where W is the total number of FS in each fiber link and M is the total number of links in a network. We note that the complexity of lines 5–17 is dominated by the complexity of the shortest path searching algorithm in line 6. With the possibility of scanning all the SWPs, its computational complexity is O $\left(WN^2\right)$, where N is the total number of network nodes. Thus, the overall computational complexity of lines 2–20 is O $\left(WM + WN^2\right)$. Meanwhile, we are considering multiple types of modulation formats in the *for*-loop in line 1. As a result, the overall computational complexity of *Algorithm 1* is O $\left(TW\left(M + N^2\right)\right)$, where T is the total number of available modulation formats. In *Algorithm 2*, the link cost calculation in line 7 is an additional step to *Algorithm 1*, whose computational complexity is O (WM). Thus, the computational complexity of lines 6–19 is O $\left(2WM + WN^2\right)$ and the overall computational complexity of *Algorithm 2* is also O $\left(TW\left(2M + N^2\right)\right)$.

E. Discussion

LC versus FF strategy: In the RSA algorithms for both the working and protection lightpaths, we have applied the LC strategy, i.e., scanning all the SWPs to choose the best eligible route. For a faster solution, we may alternatively apply the FF strategy that stops scanning the remaining SWPs once an eligible route is found.

Transponder tunability: Depending on the tunability of optical transponders at the two end nodes of a lightpath, the starting FS indexes of the working and protection lightpaths can be also different. In this study, we will consider three cases: (1) without tunability, which requires the starting FS indexes of working *w_index* and protection *p_index* lightpaths to be the same, i.e., $w\_index = p\_index$; (2) full tunability, which allows the working and protection lightpaths to have fully different starting FS indexes; (3) partial tunability, which requires the starting FS index difference of the working and protection lightpaths to fall within a certain tuning range *d*, i.e., $|w\_index - p\_index| \leq d$.

IV. Performance Evaluations and Result Analyses

We first compare the performance of the proposed heuristic algorithm with that of an ILP model that is specifically developed for the algorithm performance evaluation purpose. After convincing the efficiency of the proposed algorithm for the static lightpath traffic demand, we then consider to evaluate its benefit under dynamic lightpath traffic demand, under which we compare performance between different approaches and evaluate the impact of transponder tunability.

TABLE II
NUMBERS OF REQUIRED FS BY THE PROPOSED ALGORITHM AND THE ILP MODEL

Test network	Number of required FS	
	Proposed algorithm	ILP model
n6s8	70	69
COST239	49	48

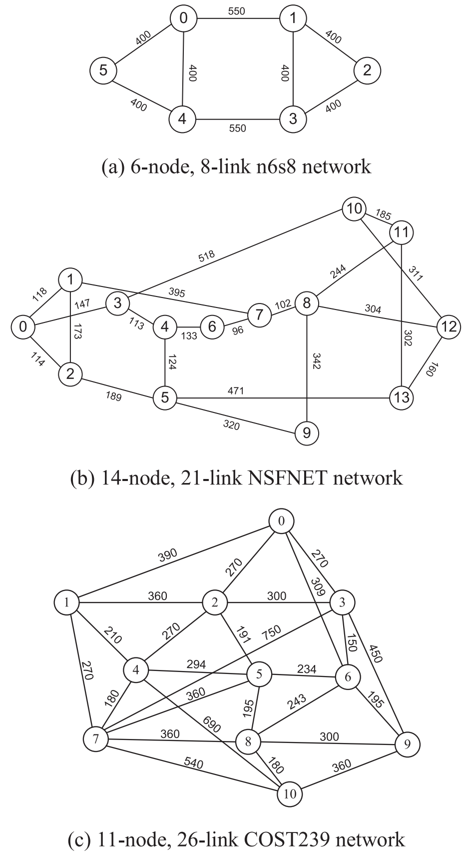
A. Performance Comparison Between Proposed Algorithm and ILP Model

To evaluate the optimality and efficiency of the proposed heuristic algorithm, we first consider the scenario of static traffic demand and compare its performance with an ILP model developed for performance evaluation purposes. With a static traffic demand, no lightpath services would be released and the performance criterion used for performance evaluation is based on the maximal number of FS required to accommodate all the lightpath demand units in the entire network. In addition, the ILP model was extended from that in [12], in which the constraints of transmission distance and modulation format are specifically taken into account. Note however that due to the page limit and because it is not the focus of this study, we do not present the model in the paper; readers can refer to our online file at [29].

Under the static lightpath demand, we assume that there is one bandwidth request between each node pair, which is uniformly distributed within a range from 10 to 400 Gb/s. We employ the proposed SWP heuristic algorithm to provision bandwidth between each node pair that supports SBBP protection. In addition, as per the observations from our previous study in [27], the performance of the demand serving algorithm is closely related to the sequence of served node pairs. We shuffle the node pair list many times (100 times in this study), and then for each shuffled node pair list, we run the heuristic algorithm to obtain the required number of FS, FS_i; we finally compare these obtained FS_i to choose the one with the smallest number, i.e., $FS_{\min} = \min_i \{FS_i\}$.

In the ILP model, the working lightpath is established along the shortest route R_w between a pair of nodes, and the correpsonding protection lightpath is established on one of the K-shortest routes that are link-disjoint from R_w. We considered all the link-disjoint K-shortest routes for our performance evaluation. We have employed the commercial software AMPL/Gurobi (version 5.0.0) [30] to solve the ILP model.

Table II compares the final required number of FS in the entire network for the two test networks, i.e., the n6s8 and COST239 networks as shown in Fig. 4. The MIPGAPs for the ILP solutions were set to be 1% and 3% for the two test networks, respectively. We were unable to obtain the ILP result for the NSFNET network because of the large size of the problem. In the table, we can see that the required numbers of FS by the two schemes are very close with one-FS differences, which therefore implies the efficiency of the proposed heuristic algorithm.



(a) 6-node, 8-link n6s8 network

(b) 14-node, 21-link NSFNET network

(c) 11-node, 26-link COST239 network

Fig. 4. Three test networks. (a) 6-node, 8-link n6s8 network. (b) 14-node, 21-link NSFNET network. (c) 11-node, 26-link COST239 network.

B. Test Conditions for the Simulation of Dynamic Traffic Demand

A dynamic lightpath traffic model is assumed in this study. Specifically, lightpath requests arrive according to a Poisson arrival process and their holding times follow a negative exponential distribution. When a lightpath service is released, we will set all the FS used by the working lightpath to be *free* and also check each of the protection FS shared by the protection lightpath. If there is no protection lightpath sharing the FS after releasing the current protection lightpath, we will set the FS to be *free*; otherwise, we remove the protection lightpath from the list of lightpaths that are sharing the FS. A total of 10^6 lightpath arrival requests were simulated for calculating the bandwidth blocking probability (*BBP*). We set the required bandwidths uniformly distributed within a range from 10 to 400 Gb/s. When a request is blocked, the bandwidth demanded by that request fails to get provisioned. Let *AR* represent the set of all arrival requests and *BR* represent the set of all blocked requests. Let a_k be the bandwidth required by the kth arrival request in *AR*. Then, as an important evaluation criterion, *BBP* is defined by

$$\mathrm{BBP} = \frac{\sum_{k \varepsilon BR} a_k}{\sum_{k \varepsilon AR} a_k} \tag{3}$$

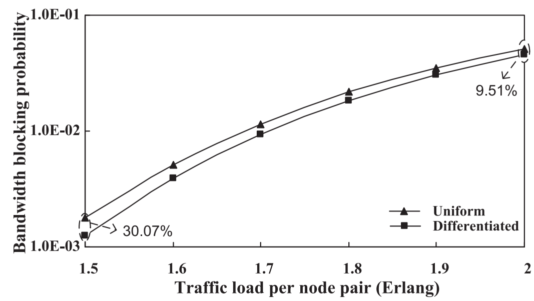
where the numerator sums all the blocked bandwidth and the denominator sums all the arrival bandwidth.

We consider two test networks: (i) the 14-node, 21-link NSFNET network and (ii) the 11-node, 26-link COST239 as shown in Fig. 4. The distance of each link (in km) is shown by the link. We assume that there are 400 FS in each fiber link in both of the networks with the bandwidth granularity of each FS being 12.5 GHz. In addition, three modulation formats (i.e., BPSK, QPSK, and 8QAM) are assumed to be used for both the working and protection lightpaths.

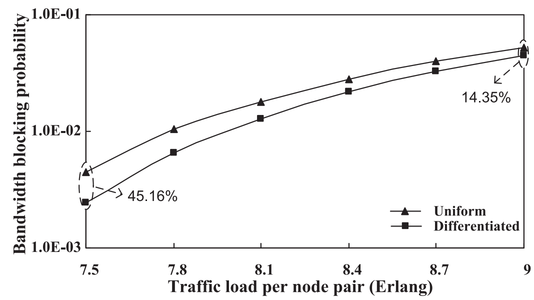
For performance comparison, we have also evaluated the fixed routing (FR) 1+1 path protection and SBPP techniques. For FR SBPP, we pre-calculate a set of fixed link-disjoint working and protection routes offline, and then choose a pair of routes from the set that can be used to establish the working and protection lightpaths. Specifically, we first find the shortest eligible working route to establish the working lightpath and then based on this working route find an eligible protection route that is link-disjoint from the working route to establish the protection lightpath. Here to choose a protection route, we may adopt either the FF or the LC modes. For the FF mode, we scan the list of protection routes (link disjoint from the working route) to choose the first eligible one for protection lightpath establishment. In contrast, for the LC mode, we choose a route that has the lowest cost for protection lightpath establishment. Once a pair of link-disjoint routes is decided, we assign suitable modulation formats to them, and use them to provision SBPP services allowing protection FS sharing on the protection route. FR 1+1 path protection is just a special case of the previous fixed route SBPP without spare capacity sharing on the protection lightpaths.

C. Performance Comparison of SBPP Under Different Sharable FS Cost Settings

The usage or sharing status of each FS in an SW can be different. Thus, an identical cost for each sharable FS may not be the most efficient option to achieve the best network performance. We propose to differentiate the cost of each shareable FS according to their shared status by protection lightpaths. Fig. 5 shows the results of the SBPP algorithm (i.e., *Algorithms 1* and *2*) with a uniform sharable FS cost (a very small value) and differentiated sharable FS cost (computed by (1) and (2)). In the legend, “uniform” corresponds to the case of the uniform FS cost and “differentiated” corresponds to the case of the differentiated FS cost. We can see that overall the BBP increases with the increase of network traffic load, and comparing the two cost settings, it is effective to consider the usage or sharing status of each FS when searching for a protection route. The differentiated cost can achieve a lower BBP than that of the uniform cost. Specifically, for the NSFNET network, the differentiated cost can maximally reduce BBP by 30% and for the COST239 network, the reduction of BBP is up to 46%. This result is reasonable since a smaller FS cost will be assigned when more protection lightpaths are sharing it, and this will encourage more future lightpaths to share this FS. From the spectrum usage efficiency point of view, we are trying to use those used FS as much as possible, and therefore can avoid or postpone using free FS for protection lightpath establishment.



(a) NSFNET



(b) COST239

Fig. 5. Performance comparison between the uniform and differentiated FS costs under the SBPP technique.

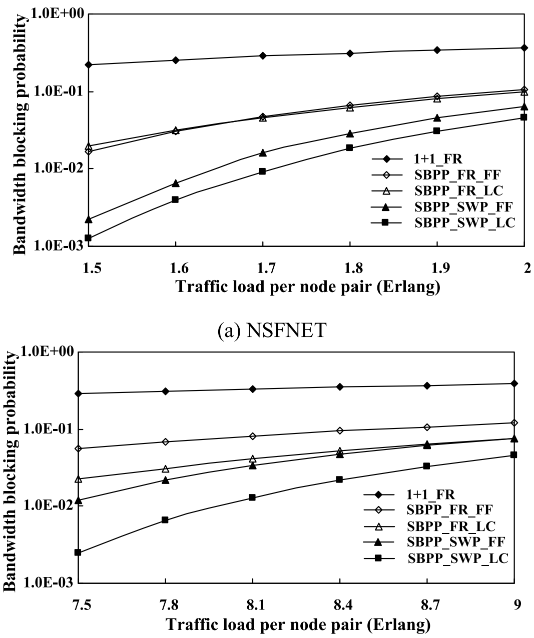
It is interesting to see that the COST239 network shows more BBP improvement than the NSFNET network. This is attributed to the different connectivity of the two networks. COST239 has a higher average nodal degree, and therefore has more opportunities for spare capacity sharing. An FS is shared by more protection lightpaths, which corresponds to a larger m in (2). The larger the number of sharing protection lightpaths is, the usage or sharing status of each FS has more differences. A uniform cost of a sharable FS cannot distinguish such differences, while (2) can better account for the differences of sharing status between different FS. This benefit becomes more in a network with a higher average nodal degree. Thus, the BBP improvement is stronger in a network with a higher connectivity.

D. Performance Comparison Among SBPP and 1+1 Schemes

In this section, we evaluate the performance of the proposed SWP-based SBPP algorithm in comparison with the FR SBPP algorithm in [13], [14], and [16] and 1+1 dedicated path protection. In the result figures, we use “SBPP_SWP” to represent the case of the SWP-based SBPP algorithm, “SBPP_FR” to represent the case of the FR SBPP algorithm, and “1+1_FR” to represent the case of the FR 1+1 path protection algorithm. In addition, we use “LC” and “FF” to represent the least cost and first fit strategies, respectively.

Fig. 6 shows the bandwidth blocking performance for various approaches. We have the following key observations.

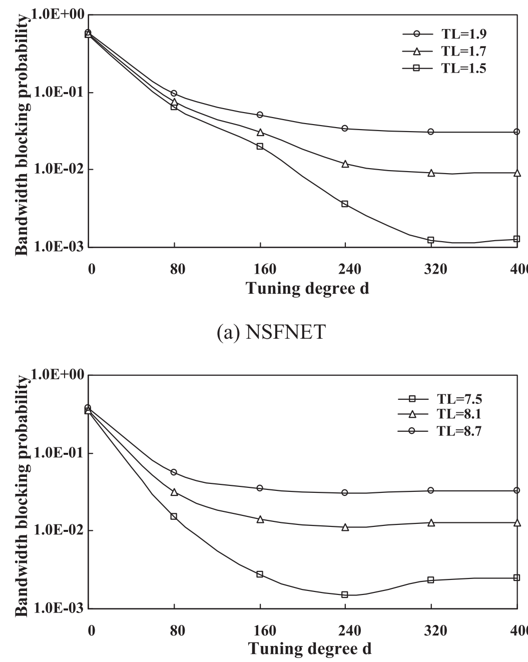
First, comparing the SBPP and 1+1 cases, we can see that SBPP shows a much lower BBP than that of 1+1 because SBPP allows protection capacity sharing among multiple protection lightpaths, while 1+1 does not. In addition, comparing results



(a) NSFNET

(b) COST 239

Fig. 6. Bandwidth blocking performance comparison between different approaches: SBPP_SWP, SBPP_FR versus 1+1_FR (FR: fixed routing; FF: first fit; LC: lowest cost).



(a) NSFNET

(b) COST239

Fig. 7. BBP change with an increasing transponder tunability (TL: Traffic load per node pair in Erlang).

of the NSFNET and COST239 networks, we see that the latter shows better performance improvement for SBPP versus 1+1. The improvement difference is attributed to the fact that COST239 has a higher average nodal degree, which increases spare capacity sharing opportunities and thus helps improve the overall bandwidth blocking performance.

Second, comparing the two SBPP schemes, we see that the SWP scheme can achieve much better performance than that of the FR scheme. The RSA algorithm in the FR scheme separates the steps of routing and spectrum assignment and moreover the candidate routes are found offline without knowledge on the current network resource usage status when used to provision SBPP services. In contrast, the proposed SWP algorithm integrates the routing and spectrum assignment steps. Whenever an eligible route is found on an SWP, the assigned FS are also decided to be the FS of the SWP. Moreover, the route searching process is online depending on the spectrum resource usage status, which can provide much more options than the FR scheme. All these factors thus enable the proposed SWP scheme to perform much better than the FR scheme.

Third, for the SWP scheme, we also compare two sub-cases, i.e., the LC and FF strategies. We can see that the LC strategy can achieve a lower BBP than the FF strategy for both the networks. This is also reasonable because the LC strategy scans all SWPs to search routes with the lowest cost, while the FF strategy stops scanning the remaining SWPs once it finds an eligible (but maybe not the best) route. The better performance of the LC strategy of course is at the cost of higher computational intensity than that of the FF strategy.

Fourth, for the FR scheme, we find that performance difference between the LC and the FF strategies is very small in the NSFNET network and larger in the COST239 network. COST239 has a higher connectivity, and therefore more different candidate routes between each node pair. The LC strategy in the FR scheme chooses the most efficient route from multiple candidate routes. Since more routes are considered in COST239, a better performance can be gained by the LC strategy. This therefore explains why the LC strategy performs better in the COST239 network.

E. Impact of Transponder Tunability

To evaluate the effect of transponder tunability, we evaluate bandwidth blocking performance with the increase of transponder tuning degree d. Fig. 7 shows BBP for the cases of the SBPP SWP-based algorithm (with the LC strategy). We can see that as the tuning range increases, the BBP decreases. This is attributed to the fact that a larger tuning range allows establishment of protection lightpaths on more different SWPs. In addition, we also observe a saturation phenomenon, i.e., when the tuning range reaches a certain value, further increase of the tuning range would not significantly improve the BBP. We can see that for NSFNET, the saturated tuning degree is in the region of $d = 320$, and for COST239, the saturated tuning degree is in the region of $d = 240$. Based on the above observation, an important implication can be made that a cheaper tunable transponder with a lower tunability may be sufficient to achieve a performance close to that of an expensive fully tunable transponder.

In addition, we notice that COST239 shows a lower saturated tuning degree than NSFNET. Again this is attributed to the higher average nodal degree of COST239. In a network with a higher average nodal degree, there are more candidate routes

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/JLT.2015.2421506, Journal of Lightwave Technology

between each pair of nodes. A larger number of routes increase the opportunity of finding an eligible protection lightpath whose starting FS index is close to that of its corresponding working lightpath. Thus, a smaller tuning degree is needed.

V. Conclusion

We consider distance adaptive dynamic routing and spectrum assignment for elastic optical networks under SBPP. An SWP-based RSA algorithm was proposed to efficiently establish working and protection lightpaths, in which a differentiated sharable FS cost was defined for the first time. Through simulation studies, we find that proposed SWP-based RSA algorithm can significantly improve BBP compared to the conventional FR RSA algorithm and 1+1 path protection. In addition, we see the benefit of using a differentiated sharable FS cost compared to the uniform FS cost in the SWP-based algorithm, i.e., the former can achieve better blocking performance than the latter. We also compared the LC and FF strategies to see that the former outperforms the latter at the cost of longer computation times. Finally, our results show that a tunable transponder with a wider tuning degree d can achieve a lower BBP as expected, and more interestingly, a limited transponder tuning range is sufficient to achieve a good BBP close to that of a fully tunable transponder.

Based on this work on the SBPP EON, subsequent interesting research work could include the signal regeneration, traffic grooming, and protection lightpath defragmentation issues. We plan to do this in our future research work. Specifically, when considering regeneration, the placement and sharing of regenerators will be an important problem. For the traffic grooming aspect, how to efficiently groom the protection capacity in an electronic layer onto a common protection lightpath will be a challenging problem. Finally, the spectrum defragmentation scheme can be extended to the protection lightpath to enhance SBPP lightpath blocking performance.

Acknowledgment

The authors would like to thank Prof. B. Mukherjee from UC Davis for his insightful discussion while preparing this paper.

References

[1] W. Shieh and I. Djordjevic, *OFDM for Optical Communications*. New York, NY, USA: Academic, 2010.

[2] W. Shieh, X. Yi, Y. Ma, and Q. Yang, "Coherent optical OFDM: Has its time come? [invited]," *J. Opt. Netw.*, vol. 7, no. 3, pp. 234–255, Mar. 2008.

[3] G. Zhang, M. D. Leenheer, A. Morea, and B. Mukherjee, "A survey on OFDM-based elastic core optical networking," *IEEE Commun. Surveys Tuts.*, vol. 15, no. 1, pp. 65–87, Feb. 2013.

[4] M. Jinno, H. Takara, B. Kozicki, Y. Tsukishima, Y. Sone, and S. Matsuoka, "Spectrum-efficient and scalable elastic optical path network: Architecture, benefits, and enabling technologies," *IEEE Commun. Mag.*, vol. 47, no. 11, pp. 66–73, Nov. 2009.

[5] G. Shen and M. Zukerman, "Spectrum-efficient and agile CO-OFDM optical transport network: Architecture, design, and operation," *IEEE Commun. Mag.*, vol. 50, no. 5, pp. 82–89, May 2012.

[6] K. Christodoulopoulos, I. Tomkos, and E. Varvarigos, "Elastic bandwidth allocation in flexible OFDM-based optical networks," *J. Lightw. Technol.*, vol. 29, no. 9, pp. 1354–1366, May 2011.

[7] M. Klinkowski and K. Walkowiak, "Routing and spectrum assignment in spectrum sliced elastic optical path network," *IEEE Commun. Lett.*, vol. 15, no. 8, pp. 884–886, Aug. 2011.

[8] Y. Wang, X. Cao, Q. Hu, and Y. Pan, "Towards elastic and fine-granular bandwidth allocation in spectrum-sliced optical networks," *J. Opt. Commun. Netw.*, vol. 4, no. 11, pp. 906–917, Nov. 2012.

[9] X. Wan, N. Hua, and X. Zheng, "Dynamic routing and spectrum assignment in spectrum-flexible transparent optical networks," *J. Opt. Commun. Netw.*, vol. 4, no. 8, pp. 603–613, Aug. 2012.

[10] W. D. Grover, *Mesh-Based Survivable Networks*. Upper Saddle River, NJ, USA: Prentice-Hall, 2003, ch. 6.

[11] S. Kosaka, H. Hasegawa, K. Sato, T. Tanaka, A. Hirano, and M. Jinno, "Shared protected elastic optical path network design that applies iterative re-optimization based on resource utilization efficiency measures," presented at the Eur. Conf. Opt. Commun., Amsterdam, The Netherlands, 2012, Paper Tu.4.D.5.

[12] G. Shen, Y. Wei, and S. K. Bose, "Optimal design for shared backup path protected elastic optical networks under single-link failure," *J. Opt. Commun. Netw.*, vol. 6, no. 7, pp. 649–659, Jul. 2014.

[13] K. Walkowiak and M. Klinkowski, "Shared backup path protection in elastic optical networks: Modeling and optimization," presented at the Int. Conf. Des. Rel. Commu. Netw., Budapest, Hungary, 2013, pp. 187–194.

[14] B. Chen, J. Zhang, Y. Zhao, J. P. Jue, J. Liu, S. Huang, and W. Gu, "Spectrum-block consumption for shared-path protection with joint failure probability in flexible bandwidth optical networks," *Opt. Switch. Netw.*, vol. 13, pp. 49–62, Jul. 2013.

[15] X. Shao, Y. Yeo, Z. Xu, X. Chen, and L. Zhou, "Shared-path protection in OFDM-based optical networks with elastic bandwidth allocation," presented at the Opt. Fiber Commu. Conf. Expo. Nat. Fiber Opt. Eng. Conf., Los Angeles, CA, USA, 2012, Paper OTh4B.4.

[16] A. Tarhan and C. Cavdar, "Shared path protection for distance adaptive elastic optical networks under dynamic traffic," in *Proc. Rel. Netw. Des. Model. Conf.*, Almaty, Kazakhstan, 2013, pp. 62–67.

[17] Y. Wei, G. Shen, and S. K. Bose, "Span-restorable for elastic optical networks under different spectrum conversion capabilities," *IEEE Trans. Rel.*, vol. 63, no. 2, pp. 401–411, Jun. 2014.

[18] Y. Wei, K. Xu, H. Zhao, and G. Shen, "Applying p-Cycle technique to elastic optical networks," in *Proc. Int. Conf. Opt. Netw. Des. Model.*, Stockholm, Sweden, 2014, pp. 1–6.

[19] F. Ji, X. Chen, W. Lu, J. J. P. C. Rodrigues, and Z. Zhu, "Dynamic *p*-Cycle protection in spectrum-sliced elastic optical networks," *J. Lightw. Technol.*, vol. 32, no. 6, pp. 1190–1199, Mar. 2014.

[20] M. Klinkowski, "An evolutionary algorithm approach for dedicated path protection problem in elastic optical networks," *Cybern. Syst.*, vol. 44, nos. 6/7, pp. 469–488, Aug. 2013.

[21] R. Goścień, K. Walkowiak, and M. Klinkkowski, "Joint anycast and unicast routing and spectrum allocation with dedicated path protection in elastic optical networks," in *Proc. Des. Rel. Commun. Netw.*, Ghent, Belgium, 2014, pp. 1–8.

[22] L. Ruan and N. Xiao, "Survivable multipath routing and spectrum allocation in OFDM-based flexible optical networks," *J. Opt. Commun. Netw.*, vol. 5, no. 3, pp. 172–182, Mar. 2013.

[23] A. Castro, L. Velasco, M. Ruiz, and J. Comellas, "Single-path provisioning with multi-path recovery in flexgrid optical networks," in *Proc. Ultra Mod. Telecommun. Control Syst. Workshops*, St. Petersburg, Russia, 2012, pp. 745–751.

[24] Y. Sone, A. Watanabe, W. Imajuku, Y. Tsukishima, B. Kozicki, H. Takara, and M. Jinno, "Bandwidth squeezed restoration in spectrum-sliced elastic optical path networks (SLICE)," *J. Opt. Commun. Netw.*, vol. 3, no. 3, pp. 223–233, Mar. 2011.

[25] A. N. Patel, P. N. Ji, J. P. Jue, and T. Wang, "Survivable transparent flexible optical WDM (FWDM) networks," presented at the Opt. Fiber Commu. Conf. Expo./Nat. Fiber Opt. Eng. Conf., Los Angeles, CA, USA, 2011, Paper OTuI2.

[26] A. Bocoi, M. Schuster, F. Rambach, M. Kiese, C. A. Bunge, and B. Spinnler, "Reach-dependent capacity in optical networks enabled by OFDM," presented at the Opt. Fiber Commu. Conf., San Diego, CA, USA, 2009, Paper OMQ4.

[27] A. Cai, G. Shen, L. Peng, and M. Zukerman, "Novel node-arc model and multiiteration heuristics for static routing and spectrum assignment in elastic optical networks," *J. Lightw. Technol.*, vol. 31, no. 21, pp. 3402–3413, Nov. 2013.

[28] G. Shen, S. K. Bose, T. H. Cheng, C. Lu, and T. Y. Chai, "Efficient heuristic algorithms for light-path routing and wavelength assignment in WDM networks under dynamically varying loads," *Comput. Commun.*, vol. 24, nos. 3/4, pp. 364–373, Feb. 2001.

[29] (2015). [Online]. Available: http://www.ontrc.org/Upload/DownFiles/2015362149366894.pdf

[30] AMPL+Gurobi, Linear programming optimization software package. (2015). [Online]. Available: http://www.gurobi.com/doc/30/ampl/

Chao Wang is currently working toward the Graduate degree at the School of Electronic and Information Engineering, Soochow University, Suzhou, China. His research interest includes optical network survivability.

Gangxiang Shen (S'98–M'99–SM'12) received the B.Eng. degree from Zhejiang University, Zhejiang, China, the M.Sc. degree from Nanyang Technological University, Singapore, and the Ph.D. degree from the University of Alberta, Edmonton, AB, Canada, in January 2006. He was a Lead Engineer with Ciena, Linthicum, MD, USA. He was also an Australian ARC Postdoctoral Fellow with the University of Melbourne. He is currently a Distinguished Professor with the School of Electronic and Information Engineering, Soochow University, Suzhou, China. He has authored and coauthored more than 80 peer-reviewed technical papers. His research interests include integrated optical and wireless networks, spectrum efficient optical networks, and green optical networks. He is a Lead Guest Editor of the *IEEE Journal on Selected Areas in Communications* (*J-SAC*) Special Issue on "Next-Generation Spectrum-Efficient and Elastic Optical Transport Networks," and a Guest Editor of the IEEE *J-SAC* Special Issue on "Energy-Efficiency in Optical Networks." He is an Associate Editor of the *Journal of Optical Communications and Networking*, and an Editorial Board Member of the *Optical Switching and Networking*. He is a Secretary for the IEEE Fiber-Wireless Integration Sub-Technical Committee. He received the Young Researcher New Star Scientist Award in the "2010 Scopus Young Researcher Award Scheme" in China. He received the Izaak Walton Killam Memorial Award from the University of Alberta and the Canadian NSERC Industrial R&D Fellowship.

Sanjay Kumar Bose (SM'91) received the B.Tech. degree from the Indian Institute of Technology Kanpur, Kanpur, India, in 1976, and the master's and Ph.D. degrees from Stony Brook University, Stony Brook, NY, USA, in 1977 and 1980, respectively. After working with the Corporate R&D Centre of the General Electric Co., Schenctady, NY, till 1982, he joined IIT Kanpur as an Assistant Professor and became a Professor in 1991. He left IIT Kanpur in 2003 to join the Faculty of the School of EEE, NTU, Singapore. In Dec 2008, he left NTU to join the Indian Institute of Technology Guwahati, Guwahati, India, where he is currently a Professor at the Department of EEE and the Dean at the Alumni Affairs and External Relations. He has been working in various areas in the field of computer networks and queueing systems and has published extensively in the area of optical networks and network routing. He is a Fellow of IETE, India, and a Member of Sigma Xi and Eta Kappa Nu.