Photon Netw Commun (2007) 14:159–164
DOI 10.1007/s11107-007-0071-4

Multiple link failure recovery in survivable optical networks

Xiaofei Cheng · Xu Shao · Yixin Wang

Received: 6 September 2006 / Accepted: 24 May 2007 / Published online: 7 July 2007

Abstract Survivability is of critical importance in high-speed optical communication networks. A typical approach to the design of survivable networks is through a protection scheme that pre-determines and reserves backup bandwidth considering single/double link failure scenarios. In this article, a greedy algorithm is presented to reserve backup bandwidth considering multiple ($F > 2$) link (SRLG) failure scenarios. A bandwidth-saving joint selection scheme of working and protection paths is presented for protection against random multiple-link failures under dynamic traffic. Simulation shows that the algorithm can achieve maximum sharing of backup bandwidth for protection against random multiple-link failure with significant amount of bandwidth saving.

Keywords Survivability · Protection · Greedy algorithm

1 Introduction

With the explosive growth of the Internet and the emergence of new services, optical transport networks are being rapidly deployed to satisfy the high-speed transport capacity demand economically. Optical communication network employing dense wavelength division multiplexing (DWDM) technology has currently harnessed several Terabit/s bandwidths into one fiber. As the size and capacity of transport network increase rapidly, any failure in the transport network will result in a significant loss of data and service. Therefore, survivability for high-speed communication networks becomes critical.

The technologies for providing network survivability can be briefly classified, as either protection or restoration. Protection schemes reserve a backup path when the working path is established. Restoration schemes will find a suitable backup path dynamically from the pool of available resources when faults occur [1].

Many network applications are mission critical, and hence, require protection. The well-known protection mechanisms are 1+1/1:1 and 1:n protection [1]. In protection schemes, sharing of backup bandwidth provides significant saving of network capacity. Hence, many studies [1–10] focus on the algorithms and the schemes for sharing backup bandwidth among connections. In [1], the authors develop path-based and link-based ILP formulations under static traffic demand for designing protection against single-link failure. In [2], the authors present a joint working and protection path selection approach under dynamic traffic for protection against single-link failure.

In the single-link failure case, two-link disjoint working paths could share the same backup resources to save network capacity. Recently, there are some researches [3–10] on WDM network recovery schemes against double-link failure cases. In [3], the authors focused on double-link failure scenarios and presented a backup reprovision scheme to provide new backup lightpaths for connections that became unprotected due to the first failure. In [4], the authors presented a sub-graph routing strategy to tolerate double-link failure scenarios. In [5], the authors summarize backup capacity sharing rules in two-link failure scenarios and present a path-based integer-programming formulation for static traffic to optimize the total network capacity for protection against two-link failures. In [6], the authors present three pre-assigned backup capacity assignment for link-based protection against double-link failure. In [7,8], the authors present a link-based ILP formulation for determining the capacity for protection

X. Cheng (✉) · X. Shao · Y. Wang
Institute for Infocomm Research (IIR), 21 Heng Mui Keng Terrace,
Singapore 119613, Singapore
e-mail: chengxf@i2r.a-star.edu.sg

against dual failures under static traffic. In [9], the authors present a heuristic algorithm for selecting working and protection paths under dynamic traffic for protection against single and two random failures. However, these algorithms are not suitable for multiple ($F > 2$) failure cases.

Single- and double-link failure tolerance is useful to a network but the network may remain exposed to the risk of multiple-link ($F > 2$) failures. The occurrence of multiple-link failures is not uncommon in a practical network, e.g., single (or multiple) node failures will affect all links connected to the node and results in multiple-link failures. Due to the long (a few hours to a few days) [6] repair time for a physical link cut, it is possible that multiple-link failures occur during link repair. Reliability [10] of each component in an optical network decreases as its utility time increases. This increases the probability of a multiple-link failure case. Fire, flood, and earthquakes will also cause a large number of links and nodes damaged and result in multiple-link failure. As a network grows in size and complexity, both the possibility and impact of multiple-link failures increase. So protection scheme must be able to handle multiple-link failures ($F > 2$) especially for those high security and robustness transport networks (e.g., military fiber networks). Multiple-link failure recovery is a significant problem. In this article, we will present a path-based joint working and backup path selection scheme and a greedy algorithm to reserve backup bandwidth with maximize bandwidth sharing for protection against random multiple-link ($F > 2$) (SRLG) failure.

The remainder of this article is organized as follows. In Sect. 2, we will give a mathematical model for protection against random multiple link failures, and present a joint working and protection path selection scheme and a greedy algorithm to reserve backup bandwidth. In Sect. 3, we will study the performance of different algorithms and provide simulation results, which include both the total bandwidth consumption and the blocking probability. Section 4 concludes this article.

2 Multiple-link failure problems

Consider a network G with L bi-directional links and N nodes. F is the number of simultaneous link failures. In order to provide 100% guarantee for dynamic traffic, when a new connection request arrives at an ingress node, the ingress node would choose a working path (WP) and F link-disjoint backup paths (BP) between itself and the intended egress node from a pre-computed routing table. We use s and d to denote the source and destination nodes of the new connection. Let k denote the arrival sequence of a connection and w_k denote the bandwidth requirement of the kth connection. We make use of the following notations to describe the problem and the proposed solution.

A'_e: Set of connections whose working paths traverse link e.

B'_e: Set of connections whose backup paths traverse link e.

B_e: Backup bandwidth on link e for the set of connections in B'_e. Since sharing of protection bandwidth is allowed, $B_e \leq \sum_{k \in B'_e} w_k$.

R_e: Residue bandwidth of link e; i.e., $R_e = C - A_e - B_e$ where C is the total capacity of link e and A_e is the working bandwidth on link e.

$S_a^{\prime b}$: Set of connections whose working paths traverse link a and backup path traverse link b, i.e., $S_a^{\prime b} = A'_a \cap B'_b$.

$U_{a,b,c,\ldots n}^{\prime e}$: Set of connections whose working paths transverse any of the links $a, b, c \ldots n$ and whose backup paths traverse link e. In case of all links a,b,c,. . .n failures, all connections in $U_{a,b,c,\ldots n}^{\prime e}$ will be protected by link e.

C_e: Additional bandwidth needed on link e when a new connection is established.

$V\,(.)$: A function that returns the total bandwidth for all the connections in a set S, such that $V(S) = \sum_{k \in S} w_k$ where S is a set of connections.

Based on the above definition, we can get the following equation:

$$\begin{aligned} U_{a,b,c,\ldots n}^{\prime e} &= S_a^{\prime e} \cup S_b^{\prime e} \cup \ldots \cup S_n^{\prime e} \\ &= B'_e \cap (A'_a \cup A'_b \cup \ldots \cup A'_n) \end{aligned} \tag{1}$$

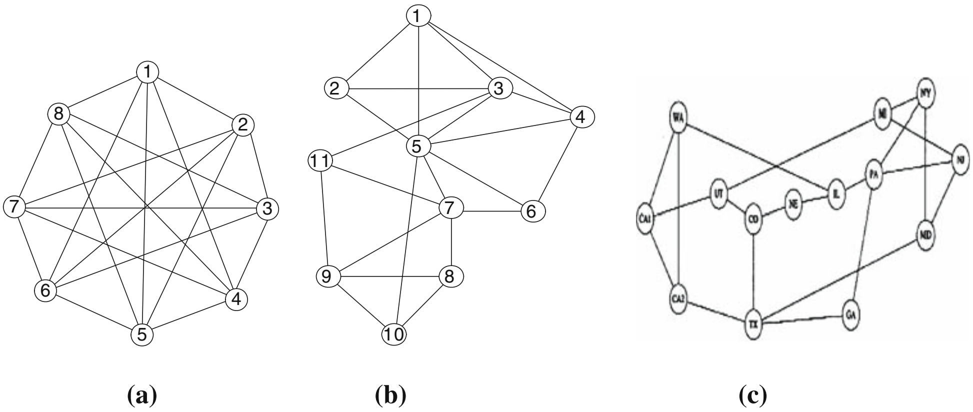
In order to provide 100% guarantee for network connections, total backup bandwidth reserved on link e should protect against random F-link simultaneous failure. Assume that F-link set is represented by $\{l_1, l_2, ..l_i..l_F | l_i \in L\}$. To protect against this F-link failure, the total backup bandwidth reserved on link e is $V(U_{l_1,l_2,..l_i..,l_F}^{\prime e})$. For the random F-link failure case, the total backup bandwidth on link e must be enough to cater for the worst case and is therefore given by:

$$\begin{aligned} B_e &= \max_{\substack{l_i \in L \\ i=1,2,\ldots F}} V(U_{l_1,l_2,\cdots l_F}^{\prime e}) \\ &= \max_{\substack{l_i \in L \\ i=1,2,\ldots F}} V(S_{l_1}^{\prime e} \cup S_{l_2}^{\prime e} \cup \ldots \cup S_{l_F}^{\prime e}) \end{aligned} \tag{2}$$

When a new connection k (bandwidth requirement: w_k) arrives, the ingress node will choose a working path (WP) and F link-disjoint backup paths (BP) from a list of pre-computed routes between the source and the destination (We assume the network is F+1-connected) to protect against F link failures. Our objective is to find a working path and F backup paths from pre-computed routing table with the minimal total additional bandwidth to carry the new connection:

$$\text{Minimize} \sum_{e \in WP \cup BP} C_e \tag{3}$$

Fig. 1 Simulation Network Topology (**a**) Topology A (**b**) Topology B, NJLATA(**c**) Topology C, NSFNET



For each link e of a candidate-working path, an additional bandwidth w_k is required to carry the new requested connection. For each link e of candidate backup paths, admission of connection k changes the sets A'_e, B'_e, $S'^e_{l_i}$ and $U'^e_{l_1,l_2,\cdots l_F}$. Denote the total backup bandwidth on link e before and after the admission as B_e and B_e^{new}, calculated according to Eq. 2, the additional bandwidth on link e of a candidate backup path for protection against random F-link failure, C_e $(0 \leq C_e \leq w_k)$ is given by:

$$C_e = \begin{cases} 0 & \text{if } B_e^{\text{new}} - B_e \leq 0 \\ B_e^{\text{new}} - B_e & \text{if } 0 < B_e^{\text{new}} - B_e \leq R_e \\ \infty & \text{if } B_e^{\text{new}} - B_e > R_e \end{cases} \tag{4}$$

Note that $C_e = \infty$ means that it is not feasible to set up the new connection with BP traverses link e.

Equations 2–4 give a protection scheme for protect against random F $(F > 2)$ multiple-link failure scenarios. However, the computation time for algorithm in Eq. 2 is O (L^F). The computation time increases exponentially with the number of simultaneous link faults F. It is not suitable for on-line resource reservation for dynamic traffic. To solve this problem, we present a greedy algorithm described below to calculate B_e instead of Eq. 2. We define a connection set operator:Δ, which is to update all relative connection sets, $S'^e_{l_i}$ $(l_i \in L)$ as follows:

$$\Delta(S'^e_l) \rightarrow \forall l_i \in L, S'^e_{l_i} = S'^e_{l_i} - S'^e_l = S'^e_{l_i} - (S'^e_{l_i} \cap S'^e_l) \tag{5}$$

The backup bandwidth reserved on link e for protection against F multiple-link failure is given by:

$$B_e = \sum_{n=1}^{F} \max_{\substack{l_i \in L \\ \Delta(S'^e_{\max}|_{n-1})}} V(S'^e_{l_i}) \tag{6}$$

$S'^e_{\max}|_{n-1}$ represents the connection set, $S'^e_{\max}$in the $n-1$ iterate step. It satisfies that:

$$\begin{array}{ll} S'^e_{\max}|_{n-1} = \emptyset & n = 1 \\ V(S'^e_{\max}|_{n-1}) = \max\limits_{l_i \in L}(V(S'^e_{l_i}|_{n-1})) & 2 \leq n \leq F \end{array}$$

In Eq. 6, we iterate F times to get the F sequential maximal bandwidth required on link e for protect against random single link failure scenarios. After each iteration time, a connection set update operation, $\Delta(S'^e_{\max}|_{n-1})$ is implemented to avoid iterate calculating a connection' bandwidth. The time complexity of the greedy algorithm, Eq. 6, is *O (LF).*

The detailed steps of greedy algorithm are described as follow:

- *Step 1*: Set $j = 1$. Find the relative connection set of link e, $S'(e)$, as given by

$$S'(e) = \left\{ S'^e_{l_i} | l_i \in L, S'^e_{l_i} \neq \Phi \right\} \tag{7}$$

- *Step 2*: Find in $S'(e)$ the $S'^e_{l_i}$ with maximum $V(S'^e_{l_i})$ and denote it as $S'_{\max}$. Calculate M (j)as given by:

$$M(j) = V(S'_{\max}) = \max_{S'^e_{l_i} \in S'(e)} V(S'^e_{l_i}) \tag{8}$$

- *Step 3*: Update every $S'^e_{l_i} \in S'(e)$ in Eq. 7 as follows:

$$S'^e_{l_i} = S'^e_{l_i} - S'_{\max}, \quad \forall S'^e_{l_i} \in S'(e) \tag{9}$$

  where$A - B = A \cap \overline{B}$.

- *Step 4*: Increment j. Repeat Steps 2 and 3 until M (1), M (2),. . .M(F) are found. We have then:

$$B_e = \sum_{j=1}^{F} M(j) \tag{10}$$

In a centralized network, a control node will maintain the connection set, $S'^e_{l_i}$ $(\forall l_i, e \in L)$ information. When a dynamic connection arrives, the control node will assign an optimal working and F backup path and reserve backup bandwidth according to Eqs. 3 and 4, and Eqs. 7–10. The connection set, $S'^e_{l_i}$ $(\forall l_i, e \in L)$ will be updated. In a distributed network, each node will maintain the connection set, $S'^e_{l_i}$ $(\forall l_i, e \in L)$.

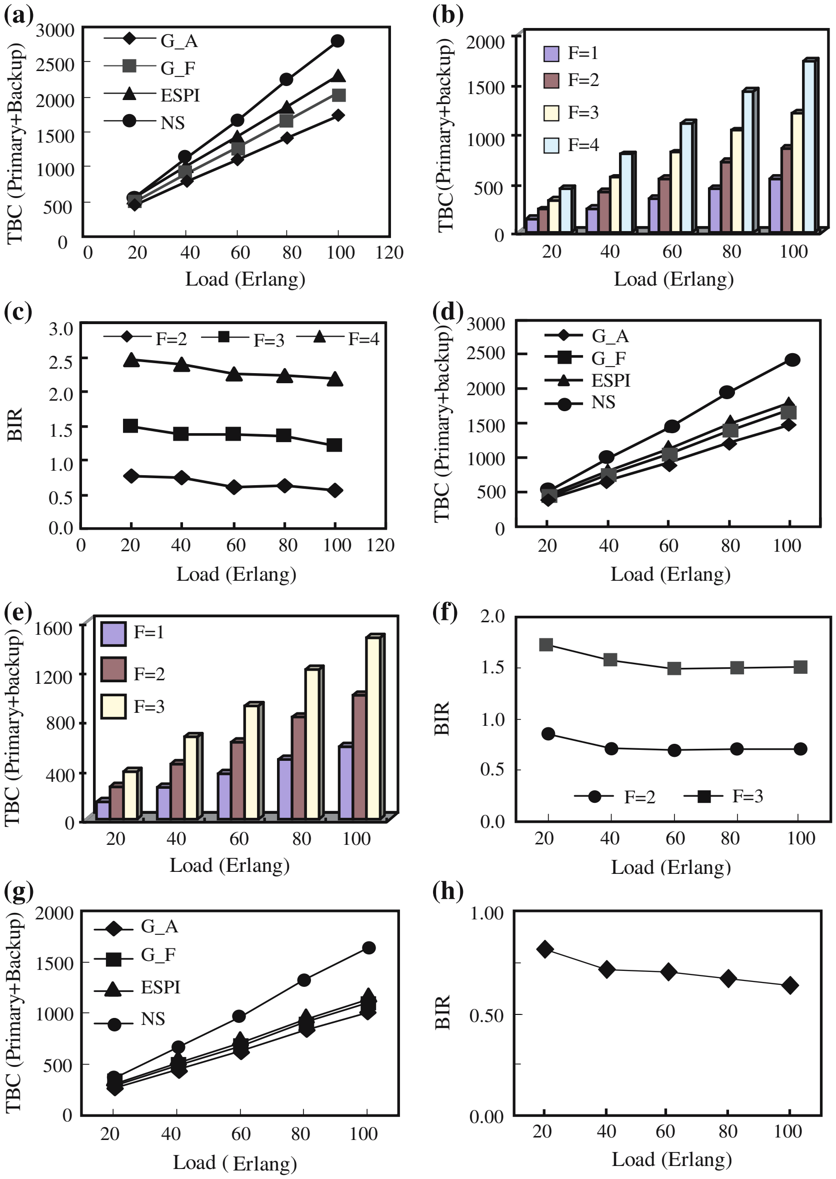


Fig. 2 Bandwidth consumption (**a**) Total bandwidth consumption in Topology A. (**b**) Total bandwidth consumption in Topology A using G_A algorithm. (**c**) Bandwidth increase ratio in Topology A using G_A algorithm. (**d**) Total bandwidth consumption in Topology B. (**e**) Total bandwidth consumption in Topology B using G_A algorithm. (**f**) Bandwidth increase ratio in Topology B using G_A algorithm (**g**) Total bandwidth consumption in Topology C. (**h**) Bandwidth increase ratio in Topology C using G_A algorithm ($F = 2$)

When a dynamic connection arrives, the ingress node will assign an optimal working and F backup paths and reserve backup bandwidth according to Eqs. 3, 4 and Eqs. 7– 10. Then, the connection set $S'^{e}_{l_i}$ ($\forall l_i, e \in L$) is updated and the updated information is broadcasted to all distributed nodes.

3 Simulations

We simulate different routing and bandwidth allocation schemes on three network topologies (Fig. 1). The average node degrees $\bar{d}$ of the network topologies are 5, 4 and 3, respectively. We studied the following four algorithms: (1) G_A algorithm: our greedy algorithm with alternate routing scheme. (2) G_F algorithm: our greedy algorithm with fixed (shortest path) routing scheme. (3) ESPI algorithm: extended sharing with partial information algorithm. (4) NS: shortest path with no backup bandwidth-sharing algorithm. In algorithm (3), the ESPI algorithm, we extend the SPI algorithm [9,11] to multiple-link failure scenarios. Backup bandwidth reserved on a link e is calculated as the following equation:

$$B_e = \sum_{n=1}^{F} V(A'_l) \quad \forall l \in L, \quad l \neq e \tag{11}$$

In our simulation, connection request follows a Poisson process and has an exponential holding time. Connection request arrival is uniformly distributed over all node pairs and a total of 10^6 connection requests are generated. The bandwidth requirement of each demand varied randomly from one to four units. In network bandwidth consumption comparison, we do not consider the connection blocking, link capacity is set to infinity, and hence, no connection request

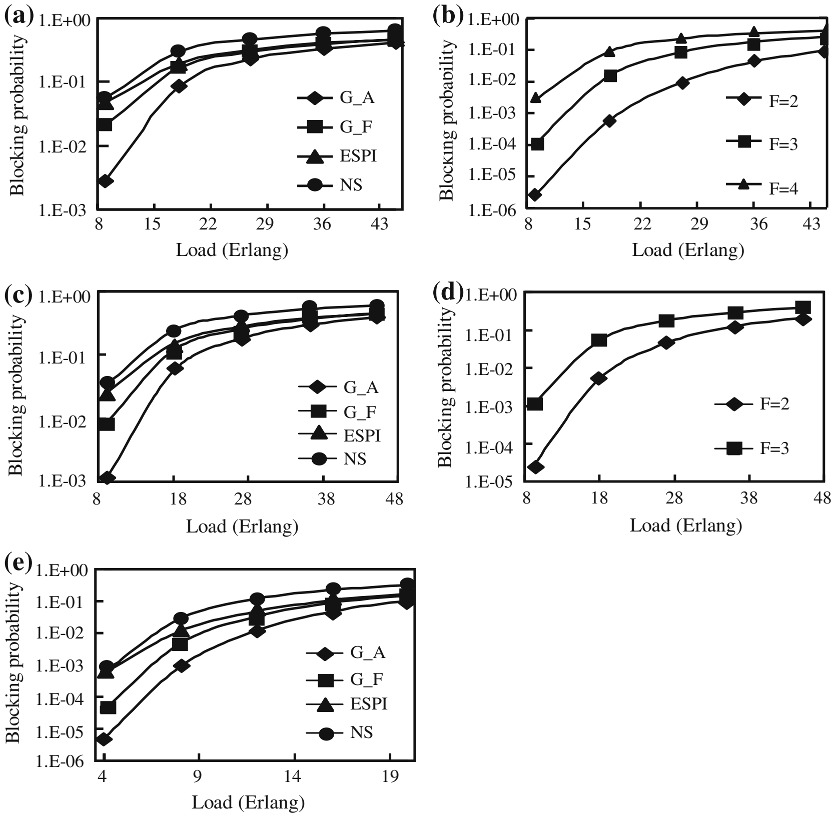


Fig. 3 (**a**) Blocking probability in Topology A. (**b**) Blocking probability in Topology A using G_A algorithm. (**c**) Blocking probability in Topology B. (**d**) Blocking probability in Topology B using G_A algorithm. (**e**) Blocking probability in Topology C

will be rejected. In network blocking comparison, the link capacity is set to be finite. A request is blocked if either the working or the backup paths cannot be found for the connection or the link resource required by the working and the backup paths is unavailable. To investigate the total bandwidth consumption increase in different F-failure cases, we define Bandwidth Increase Ratio (BIR) as:

$$BIR = \frac{TBC(F=i) - TBC(F=1)}{TBC(F=1)} \quad (i = 2, 3, 4) \tag{12}$$

TBC is Total Bandwidth Consumption (TBC) for protection against F (*F = 1, 2, 3, 4*) link failure.

Figure 2a, d, and g show the total bandwidth consumed in the sample networks using different algorithms. Greedy algorithm with alternate routing scheme (G_A) has the least bandwidth consumption. Alternate routing is more superior in saving bandwidth than fixed routing. The difference between G_A and G_F algorithms depends on the number of alternate routes. From the comparison, our algorithms (G_A and G_F) provide the most sharing of backup bandwidth and G_A algorithm saves more total bandwidth ($F=2$, 12%; $F=3$, 17%; $F=4$, 22%) than the ESPI algorithm and saves 32% compared to the total bandwidth consumed using NS algorithm. Figure 2b and e show the total bandwidth consumption for G_A algorithm to protect against different number of link failures. Figure 2c, f and h give the total bandwidth increment for G_A algorithm. When traffic increases, the sharing efficiency is improved and thus, the total bandwidth increase is reduced. To protect against multiple-link failures, network bandwidth increases drastically with the number of faults ($F=2$, 70%; $F=3$, 146%; $F=4$, 230%).

Figure 3 shows the blocking probabilities of the sample networks employing different algorithms. Figure 3a, c, and e show that our algorithms (G_A and G_F) have less blocking probability than other algorithms. Figure 3b and d show that the blocking probability of G_A algorithm is improved with the increase in the number of faults. Simulation results (Figs. 2, 3) show that our algorithms (G_A and G_F) save more bandwidth than other algorithms and have less blocking probability.

4 Conclusion

In this article, we present a joint working and protection path selection scheme and a greedy algorithm to reserve backup bandwidth for protection against multiple-link ($F>2$) failure under dynamic traffic. Our schemes maximize sharing of backup bandwidth and exhibit a fast online computation time. Simulation shows that our algorithms save more total bandwidth consumption ($F=2$, 12%; $F=3$, 17%; $F=4$, 22%) than the ESPI algorithm and save 32% of the total bandwidth consumption using NS algorithm. Our algorithms achieve superior performance both in total bandwidth consumption and blocking probability than other algorithms for protection against multiple-link failures.

References

[1] Ramamurthy, S., Sahasrabuddhe, L., Mukherjee, B.: Survivable WDM mesh networks. IEEE/OSA J. Lightwave Technol. **21**(4), 870–883 (2003)

[2] Xin, C., Ye, Y., Dixit, S., Qiao, C.: A joint working and protection path selection approach in WDM optical networks, Proc. of IEEE GLOBECOM '01, San Antonio, TX, USA, Nov, vol. 4, pp. 2165–2168 (2001)

[3] Zhang, J., Zhu, K., Mukherjee, B.: A comprehensive study on backup reprovisioning to remedy the effect of multiple-link failures in WDM mesh networks. Proc. of IEEE ICC'04, Paris, France, vol. 3, pp. 1654–1658. June (2004)

[4] Frederick, M.T., Datta, P., Somani, A.K.: Evaluating dual-failure restorability in mesh-restorable WDM optical networks. Proc. of ICCCN 2004, Chicago, IL, USA, Oct. 2004, pp. 309–314 (2004)

[5] He, W., Somani, A. K.: Path based protection for surviving double-link failures in mesh restorable optical networks, Proc. of IEEE GLOBECOM'03, San Francisco, CA, USA, Dec. 2003, pp. 2558–2563 (2003)

[6] Choi, H., Suresh, S., Choi, H.: On double-link failure recovery in WDM optical networks, Proc. of IEEE INFOCOM'02, New York, YN, USA, June 2002, vol. 2, pp. 808–816 (2002)

[7] Doucette, J., Grover, W.D.: Capacity design studies of span-restorable mesh transport networks with shared-risk link group (SRLG) effects, Proc. of SPIE Opticomm'02, Boston, MA, US, July/August 2002, vol. 4787, pp. 25–38 (2002)

[8] Clouqueur, M., Grover, W.D.: Mesh-restorable network with complete dual failure restorability and with selectively enhanced dual-failure restorability properties, Proc. of SPIE OptiComm'02, Boston, MA, USA, July/Aug, vol. 4874, pp. 1–12 (2002)

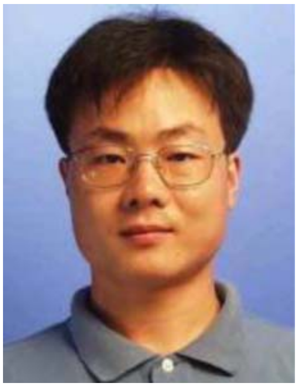
[9] Banerjee, G., Sidhu D.: Label switched path restoration under two random failures, Proc. of IEEE GLOBECOM'01, San Antonio, Tx, USA, Nov. 2001, vol. 1, pp. 30–34 (2001)

[10] Cheng X.F., Lu, C., Zhong, W.D., Chai, T.Y., Shao, X.: Adaptive resource reservation for survivable optical network, Proc. of OECC'04, Yokohama, Japan, July, pp. 772–773 (2004)

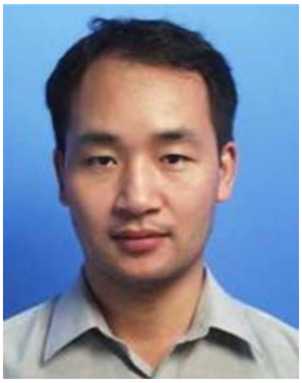
[11] Kodianalm M., Lakshman T.V.: Dynamic routing of bandwidth guaranteed tunnels with restoration, Proc. of IEEE, INFOCOM'00, Tel Aviv, Israel, March, pp. 902–910 (2000)

Author Biograpies

Xiaofei Cheng (chengxf@i2r.a-star.edu.sg) received his MS degree in optical engineering from Nanjing University of Science and Technology, Nanjing China, in 1999, and the Ph.D. degree in electromagnetic field and microwave technology from Beijing University of Posts and Telecommunications, Beijing, China, in 2002. Since 2002, he has been with the Department of Network Technology in the Institute for Infocomm Research (I^2R) in Singapore. His research interests include high-speed optical transmission technologies and IP over WDM optical networking.



Xu Shao (shaoxu@i2r.a-star.edu.sg) received the Ph.D. degree in Communication and Information System from Beijing University of Posts and Telecommunications, Beijing, China, in 2002, and the M.S. degree and B.S. degree from the Xidian University, Xi'an, China, in 1999 and 1996, respectively. In 1999, he worked as an engineer in Huawei Technologies Ltd., Shenzhen, China. Currently he works as senior research fellow in Institute for Infocomm Research in Singapore. His research interests include optical and wireless networking, signal processing, and embedded system development.



Yixin Wang (wangyx@i2r.a-star.edu.sg) received the B.E. degree in electronic engineering from Zhejiang University, China, in 1989, and the Ph.D. degree in electromagnetic theory & microwave technology from Beijing Institute of Technology, China, in 1999. From 1989 to 1996, he was with Nanjing Research Institute of Electronic Technology, China, where he was a director of the Opto-electronic system to radar lab. From 1999 to 2000, he was with the Zhongxing Telecom Ltd., China, where he was a Chief Engineer & Project Manager of optical network division. From November 2000 to October 2002, he was a research fellow in Nanyang Technological University, Singapore. Currently, he is a research scientist of the Institute for Infocomm Research, Singapore.