Recovery schemes for different distributed connection management in generalized multi-protocol label switching networks

Can Wang (王 璨) and Yuefeng Ji (纪越峰)

Optical Communication Center, Beijing University of Posts and Telecommunications, Beijing 100876

Received August 14, 2006

As the wavelength division multiplexing (WDM) technology matures and the demands for bandwidth increase, survivability becomes more and more important in generalized multi-protocol label switching (GMPLS) controlled intelligent optical networks (IONs). There are great interests to study the performance of restorability under one certain connection management strategy. And studies in the problem of providing recovery from link failures under two different resource reservation schemes, forward reservation protocols (FRPs) and backward reservation protocols (BRPs), are presented. They are examined from the point of view of connection blocking probability, restorability and average recovery time. The two different connection management schemes and the survey of different recovery schemes are first presented. The performance of these recovery strategies is analyzed and compared both through theoretical analysis and simulation results. The main stressed idea is that using BRPs gives the best performance in terms of restorability and blocking probability in restorable GMPLS networks.

OCIS codes: 060.2330, 060.4250, 060.4510.

Survivability in generalized multi-protocol label switching (GMPLS) controlled intelligent optical networks (IONs) becomes more and more important as the wavelength division multiplexing (WDM) technology matures and the demands for bandwidth increase. ION survivability solution has many requirements, including low blocking rate, fast recovery and high restorability. The challenge lies in the fact that these requirements always contradict each other in a single recovery scheme. The Internet Engineering Task Force (IETF) proposed a series of GMPLS-based recovery schemes to provide different tradeoffs between the requirements[1]. There are great interests in developing optimal algorithms and protocol extensions for these recovery schemes in order to mine the best performance possible from them[2−4]. In this paper, we not only study the performance differences between different recovery schemes, but also compare the performance between different connection management strategies. From our theoretical analysis and simulation result, we can see that using backward reservation protocols (BRPs) gives best performance in restorability.

The forward reservation with dropping works as follows[5]. When the source node wishes to establish a connection, the source node finds the pre-computed route to the destination node and composes a reservation (RESV) packet with AvailSet to record the wavelength status. This message is then routed to the destination hop by hop and reserves free wavelengths along the path.

While at the source node, local node looks for the information about the free wavelengths to the next hop from link resource management (LRM) module. Then it locks all free wavelengths along the path and updates the AvailSet to the next hop.

Each intermediate node will remove currently unavailable wavelengths from this list according to its local link information and reserve all residual wavelengths on the list. Once the destination node receives the RESV packet and the final list is not empty, a wavelength will be selected to make the actual connections on the optical switches, and other temporarily locked wavelengths will be unlocked during this backward configuration process.

Forward reservation protocols (FRPs) tend to temporarily lock many resources that they will not use. To overcome the disadvantage of this over-reservation behavior, BRPs use a destination-initiated reservation scheme. BRPs send a probe (PROB) packet toward the destination to collect the wavelength availability information. With this information, the destination will be able to choose one suitable wavelength and then send an acknowledgement (ACK) packet to setup the light path along the backward path.

The GMPLS recovery terminology currently being standardized by IETF has explicitly defined protection as the paradigm whereby one or more dedicated protection label switching path (LSP)/span(s) is/are fully established to protect one or more working LSP/span(s), while LSP/span restoration as the paradigm whereby the complete establishment of the restoration LSP/span occurs only after a failure of the working LSP/span, and requires some additional signaling[6]. Restoration can be further divided into four categories according to whether restoration path calculation, restoration resource reservation and restoration channel assignment functions are performed before or after failure respectively[1]. The five forms of recovery mechanisms are illustrated in Table 1[7]. In Table 1, "resource" means backup path, not the same with meaning FRPs and BRPs (that means wavelength along the path).

In protection schemes, the network operator creates dedicated backup resources for protected traffic. However, in restoration schemes, the network operator establishes new connections or activates backup resources for displaced traffic when a fault occurs. Restorations 1 and 2 both reserve backup path resources before the fault occurs. We call them pre-planning restoration. Restorations 3 and 4 do not reserve backup path before the fault

Table 1. Five Forms of GMPLS Recovery Schemes

Category	Functions			
	Calculate Path	Reserve Resource	Assign Channel	Configure Cross-Connection
Protection	Before	Before	Before	Before
Restoration 1	Before	Before	Before	After
Restoration 2	Before	Before	After	After
Restoration 3	Before	After	After	After
Restoration 4	After	After	After	After

occurs. We call them dynamic restoration. As protection mode must finish cross-connection before fault occurs, so we call it pre-configuration restoration. The more network operation is finished before the fault, the higher the pre-configuration level is. The share ability of backup resource could be affected according to the different pre-configuration level and results in differences in the recovery time and restorability.

Blocking probability is composed of routing block and setup block. Routing block results from no free wavelength in the fibers. Setup block results from different reasons: first, if all wavelengths are used to transmit data and there is no free wavelength in the fiber; second, if it is restoration 2, that is FRPs, one possible case is once all free wavelengths are locked by some connection request, even some particular wavelength is still not assigned, but all the wavelength cannot be used for other connection requests.

A connection request can be set up successfully only if both the working path and the backup set up successfully. In our simulation, we call a connection request a "session". So the block probability is expressed as

$$\text{block\_rate} = 1 - \frac{\text{success\_session}}{\text{total\_session}} = \frac{\text{setup\_block} + \text{routing\_block}}{\text{total\_session}}. \quad (1)$$

Apparently, there are redundant path resources in restoration 1/2. As a result, the block probability is bigger than restoration 3/4. Because protection strategy cannot share backup resources, the block probability is the biggest of all.

Additionally, all free wavelengths in FRPs are locked forward, this gives the bigger block probability results than BRPs. The shorter the interval time of connection request, the more notable this advantage is.

The recovery time[7] is service interruption time which from the time the fault occurs to success to use backup path to transmit data information. It is generally composed of two main parts: fault management time, T_{mana}, which includes failure detection, localization and notification time, and failure recovery time T_{reco}. Failure recovery time must include the time for the source node to switch the traffic from the failed working path to the backup path T_{swit}, and might include recovery route computation time T_{comp}, recovery route setup time T_{setup}, depending on the selected recovery scheme. Recovery route setup time might consist of recovery channel allocation time T_{alloc}, and optical cross connection (OXC) configuration time T_{conf}, depending on the selected recovery scheme. Their relationship is illustrated in Fig. 1[7].

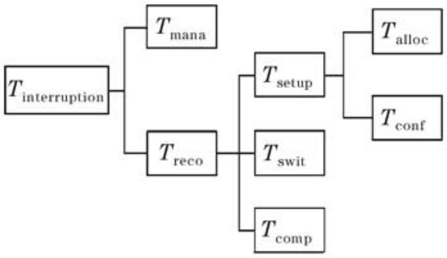

Fig. 1. Possible components of service interruption time.

For restoration 4, since all three network opterations mentioned above are not performed before failure, the service interruption time after a failure occurs will be

$$T_{\text{interruption}} = T_{\text{mana}} + T_{\text{swit}} + T_{\text{comp}} + T_{\text{alloc}} + T_{\text{conf}}.$$

For restorations 2 and 3, since recovery route has been pre-computed before failure, the service interruption time after failure occurs will be

$$T_{\text{interruption}} = T_{\text{mana}} + T_{\text{swit}} + T_{\text{alloc}} + T_{\text{conf}}.$$

For restoration 1, since both the processes of recovery route computation and channel allocation have been performed before failure, then the service interruption time will be

$$T_{\text{interruption}} = T_{\text{mana}} + T_{\text{swit}} + T_{\text{conf}}.$$

For protection scheme, since all three network operations are performed before failure, then the service interruption time will be expressed as

$$T_{\text{interruption}} = T_{\text{mana}} + T_{\text{swit}}. \quad (2)$$

From the analysis above, it is easy to see that the relation of service interruption time of the five forms of recovery mechanisms is

$$\text{restoration 4} > \text{restoration 3}$$
$$= \text{restoration 2} > \text{restoration 1} > \text{protection}.$$

The restorability is the ratio of the successfully recovered sessions to the total number of affected sessions. It is computed in this case by taking the ratio of the number of successfully restored connections to the total number of failed connections. As the FRP is a kind of greedy method in resources reservation, it is not hard to get the result that using FRPs gets worse performance in restorability than BRPs. Moreover, we can also get the simple fact that the more the backup resource, the greater the restorability is.

We simulated the behavior of path recovery schemes discussed above using NS2 tools. Specifically, the recovery schemes to be compared are

path-based restoration 3/4 under FRP,
path-based restoration 3/4 under BRP,
path-based restoration 1/2 under FRP,
path-based restoration 1/2 under BRP,
path-based protection under FRP,
path-based protection under BRP,
non-protection under FRP,
non-protection under BRP.

In order to compare the performance of path recovery schemes under different connection management strategies discussed above, we simulated two large-scale backbone network topologies over a range of offered loads: NSFNET (Fig. 2(a)) and COST239 (Fig. 2(b)). Suppose there is wavelength consistency in light path and the links between nodes are bidirectional. Each bidirectional link is composed of 8 wavelengths. Each wavelength supports 2.5 Gb/s. In the NSFNET topology, there are 19 nodes with an average degree of 3.368. In the COST239 topology, there are 11 nodes with an average degree of 4.727. We assume that no switches in either network are capable of wavelength conversion. We ran all simulation for 2000000 s, which is around 23 days. We also assume one fiber down at 25300 s (7.28 hours) and up one day later. Each algorithm is compared with a total number of 1000 connection requests, with each request requires one unit of bandwidth.

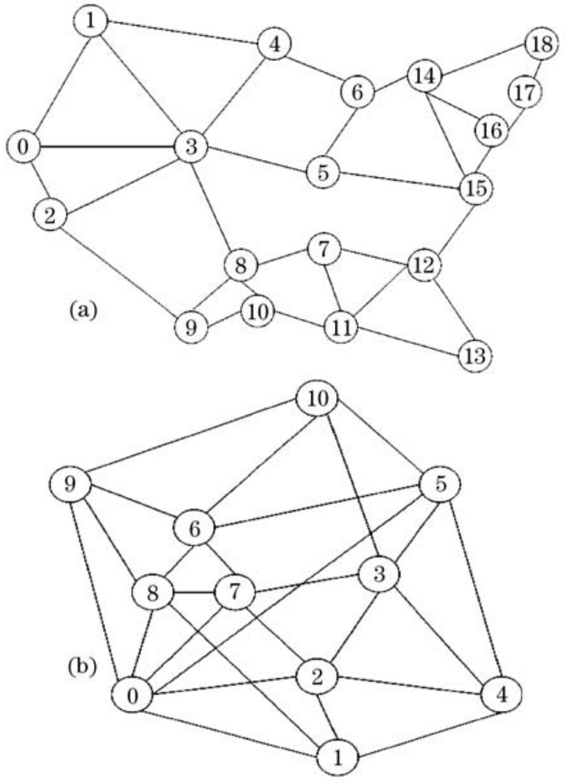

Fig. 2. (a) NSFNET and (b) COST239 network topologies.

We use traffic generator we made on NS2 platform to generate Poisson stream of connection requests. All connections were protected using the same path recovery scheme (under different connection management schemes) in each simulation process. The traffic holding time was exponentially distributed with a mean value of 360000 s which is 100 hours. The intervals of traffic are 1, 0.5, 0.2 and 0.1 hour, that is to say, the traffic arrive rates are 1, 2, 5 and 10 requests/hour. So the network loads are 100, 200, 500 and 1000 elangs. We assume the delay for routes computing/label assigning is 0.1 ms. The configure delay of OXC is 7 ms.

Figures 3 and 4 are the simulation results associated with path-based failure under different connection management strategies for COST239 and NSFNET respectively.

The new connection blocking probabilities are illustrated in Fig. 3(a) and Fig. 4(a). From the results above, we can see the blocking probability for protection strategy is the highest of all, even at 100 elangs, the blocking probability is still very high. It results from the redundant backup resources in the process of working path setup even it is not influenced by the failure. The blocking probability of restoration 1 is lower than protection strategy but higher than restoration 4. This is because protection strategy cannot share backup resources. Restoration 4 is almost the same as

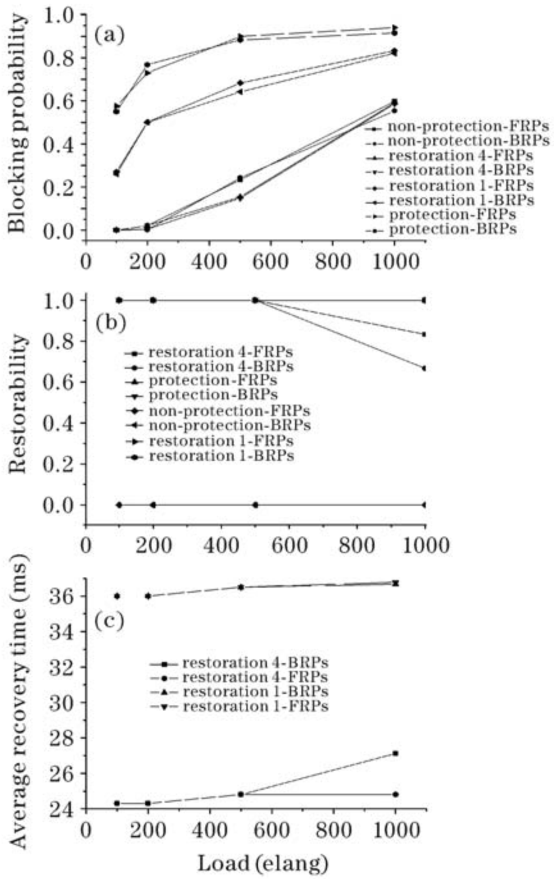

Fig. 3. Performance of path recovery under different connection management strategies in COST239 network. (a) Connection blocking probability versus load; (b) restorability versus load; (c) average recovery time versus load.

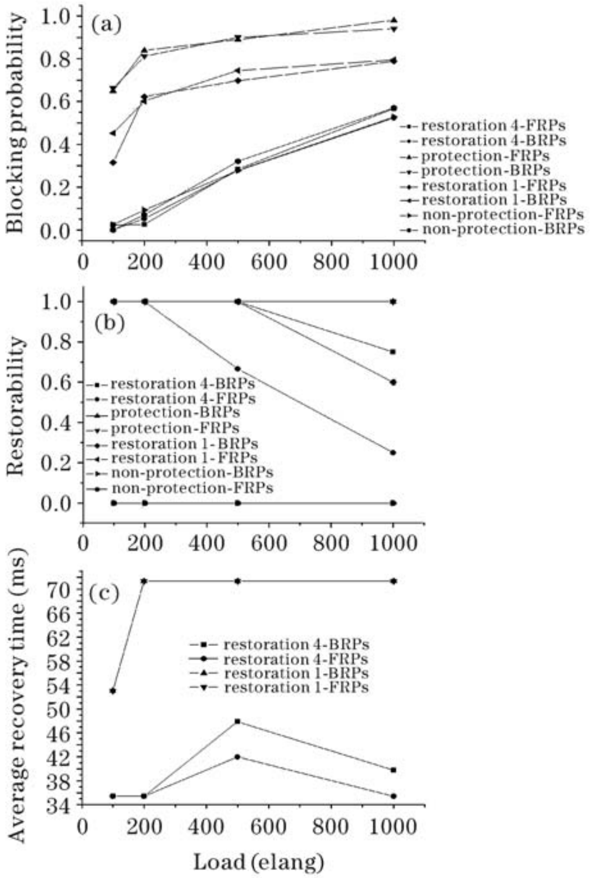

Fig. 4. Performance of path recovery under different connection management strategies in NSFNET network. (a) Connection blocking probability versus load; (b) restorability versus load; (c) average recovery time versus load.

non-protection strategy, for there is no backup path resource before network failure. It begins to compute backup route only after the failure occurs.

But we find that the performance of BRPs and FRPs for COST239 network is almost the same, this is because our interval of traffic arriving (0.1—1 hour) is much longer than the routing setup time (about 20—30 ms). So the majority block session is routing block, which results from the long traffic duration (360000 s). If we only consider the setup blocking probability, the performance of BRP is better than FRP. And if we reduce the interval time of traffic arriving, the advantage of BRPs to FRPs is more significant. On the other hand, in NSFNET network, we get a surprising result that for restoration 4, while the traffic load is over 500 elangs, the blocking probability performance of FRPs is better than BRPs. It is because the restorability of FRPs is much lower than BRPs and gives rise to more routing block than BRPs, but the setup blocking probability of FRPs is still worse than BRPs.

The restorabilities for COST239 and NSFNET network are shown in Fig. 3(b) and Fig. 4(b) respectively. Because protection strategy reserves sufficient backup resource before the failure occurs, it can guarantee 100% restorability. Non-protection scheme cannot recover from network failure, so the restorability is 0%. In COST239 network, restoration 1 also can achieve 100% restorability, but in NSFNET network it cannot do. It is due to the topology. The connectivity of COST239 is better than NSFNET, so it can compute backup resources easilier and activate backup path with less resource confliction. With the increasing of network load, the restorability of restoration 4 decreases rapidly for the reason that available resources decrease which results in the decrease of available restore path.

We illustrate the average recovery time in both networks in Fig. 3(c) and Fig. 4(c). Apparently, the recovery time of restoration 4 is much longer than restoration 1.

We find that while the load grows heavier than 500 elangs, the average recovery time under BRPs in both the two networks is longer than FRPs. This is because there is higher restorability in BRPs while in heavy traffic load. In other words, when the load is heavy, the restorable path is long, so it needs longer recovery time.

In conclusion, the performance of recovery schemes for different distributed connection management protocols is studied. The theoretical analysis and simulation results proved that the BRPs are better than FRPs in terms of blocking probability in GMPLS controlled ION. We discussed why the performance of these recovery schemes differs under various connection management protocols. From theoretical analysis and simulation result, we can find it is more efficiency to use BRPs in restorable networks. Our simulation result also showed the tradeoff between restorability and connection blocking probability. The higher the pre-configuration level, the greater restorability the recovery scheme is at the expense of a greater rejection rate for new connections. Protection is so ineffective that there are very few implementations in practical. Restoration 4 is most resource effective, but the restorability deteriorates while the network load is heavy. So restoration 1 is more preferable in practice. It is a good tradeoff between restorability and resource efficiency.

This work was jointly supported by the National Science Fund for Distinguished Young Scholars (No. 60325104), the National Natural Science Foundation of China (No. 60572021), and the SRFDP of MOE (No. 20040013001). C. Wang's e-mail address is abc830108@gmail.com, and Y. Ji's e-mail address is jyf@bupt.edu.cn.

References

1. E. Mannie, *Generalized multi-protocol label switching architecture* http://bgp.potaroo.net/ietf/idref/draft-ietf-ccamp-gmpls-architecture.
2. M. Kodialam and T. V. Lakshman, in *Proceedings of IEEE INFORCOM 2000* 902 (2000).
3. G. Li, D. Wang, C. Kolmanek, and R. Doverspike, in *Proceedings of IEEE INFORCOM 2002* 140 (2002).
4. C. V. Saradhi, N. C. Kong, and M. Gurusamy, in *Proceedings of MILCOM 2004* 1331 (2004).
5. X. Yuan, R. Melhem, and R. Gupta, Proc. IEEE **HPCA3,** 38 (1997).
6. E. Mannie, *Recovery (protection and restoration) terminology for generalized multi-protocol label switching (GMPLS)* http://www.potaroo.net/ietf/idref/draft-ietf-ccamp-gmpls-recovery-terminology.
7. L. Lei, J. Zhao, and Y. Ji, in *Proceedings of ICCT 2003* 647 (2003).