Shared protection for time slotted optical networks

Abdelilah Maach, Gregor v. Bochmann, Hussein Mouftah
School of Information Technology & Engineering, University of Ottawa Canada
amaach@site.uottawa.ca, bochmann@site.uottawa.ca, mouftah@site.uottawa.ca

Abstract

Shared protection aims to provide the same level of protection, against failure, as the dedicated one while using less network resources. In this paper we present the issue of survivability in a time slotted optical networks deploying DWDM. To guarantee the recovery, sufficient resource needs to be available at the setup time of the protection. However it is possible to optimize the protection capacity. Indeed the primary traffic is composed of a set of flows, which may be going through different paths. Therefore a protection could be found using just enough resources by sharing the backup among many flows. We propose here a technique to identify and provision the protection using the minimum necessary resources. We prove through simulation results that this shared mesh protection scheme can significantly reduce the required network protection capacity.

1. Introduction

With the progress and development being achieved in dense wavelength division multiplexing (DWDM) optical networks, with their enormous bandwidth, seem to offer the best solutions for meeting the growing demand for telecommunication services. However this huge capacity makes such a network very vulnerable to any failure in the network components. Failures may result in a large disruption in the network traffic and data steams. Therefore network survivability enhancement is a necessity.

Most of the works in the literature have focused on wavelength routed networks where the major concern is the restoration or the protection of an already established lightpath [1]. In this context both protection based and restoration based schemes have been proposed. In protection based optical networks, dedicated protection such as redundant resources are established to cope with failures [2,3]. This is very similar to the techniques used in conventional networks where at the moment of establishment, the path/link is protected by another path/link.

A network protection against failure of some network component provides a backup for every flow established [4]. However this technique is resource consuming and the network may fail in finding a backup for every path. Another alternative is 1:N or M:N path protection [5], which is very useful when the backup paths are shared risk group disjoint from the primary paths. Consequently the protection cannot use the links used by the primary paths. Such a constraint may limit the restoration capacity of the network. Indeed a traffic going from a source to a destination may use many flows going through different paths and may share many links. Excluding these links may limit the protection. One needs to manage the risk rather than avoid it.

In this paper we propose an algorithm that identifies, for every primary traffic (composed of a set of flows), another backup (also composed of a set of flows) for protection. The goal of the algorithm is to achieve the same level of protection provided by a dedicated protection while using the resources more efficiently. This algorithm relies on the fact that the primary traffic may be composed of many flows going through different physical paths. Therefore the protection could be achieved more efficiently and cost effectively by provisioning a backup and sharing it among these flows. The protection technique we propose is performed in three steps: computation of the optimal backup capacity, identification of the potential capacity that could be used by the protection on every link, and backup provisioning.

Our proposed scheme could be deployed in the context of multiple flow networks in general. However, in this paper we consider the specific case of protection for all-optical mesh networks by using both wavelength routing and time division multiplexing. This architecture consists of flows of slotted bursts being established between end nodes. A flow may be

composed of many time slots, which we call in this paper a flow unit.

In this work we are interested in the protection against a single component failure, assuming that the event of failure is very rare and independent.

The rest of this paper is organized as follows. Section 2 presents the network architecture and the details of our proposed protection scheme. The performance analysis of the proposed technique is presented in Section 3. Section 4 concludes the paper

2. Shared protection scheme

In wavelength routed networks, when a source has traffic to send to a destination, a lightpath is established. However, the source may not have enough traffic to fill the whole bandwidth available in a lightpath. That leads to some bandwidth waste and low resource utilization. To avoid this problem, [6,7] propose another alternative that consists of dividing the bandwidth of a wavelength into many small channels by using time division multiplexing. Every wavelength is divided into time slots with fixed duration. Every time slot is switched from source to destination following its assigned switched path.

Traffic-based protection is a scheme where the whole information crossing the network from a source to a destination needs to be protected. The traffic involves many flows carrying each a different number of flow units. In the following algorithm we propose to protect the primary traffic against a single failure, using just enough resources. If the flows composing the traffic are shared risk group disjoint, then a single link failure cannot affect more than one flow. Therefore a backup with as much capacity as the largest flow of the traffic is enough to protect the traffic. However, practically these flows could be sharing many links making it difficult to protect them separately. The algorithm analyses the shared risk to determine the capacity required for the traffic protection. In our protection scheme we allow the backup to share links with the primary traffic.

In this algorithm we use the following definitions:

-N is the number of nodes in the network.

-Eij an edge from the node Ni to the node Nj

-Tsd is traffic being carried from Ns to Nd.

-PTsd the protection (backup) of the traffic Tsd

-$Fsd^{(i)}$ is a flow numbered i carrying flow units from the source Ns to the destination Nj.

-Capacity($Fsd^{(i)}$) is the number of flow units being carried by a flow $Fsd^{(i)}$.

-PRsd,ij the protection required for the link Eij for the given traffic Tsd.

-PAsd,ij the protection available on link Eij for the given Traffic Tsd.

-NSij the number of flow units available in link Eij

-PNSsd,ij the number of flow units that could be used by the protection on link Eij

At the time of establishing traffic flows from a source to a destination, the protection is also identified and resources are reserved for that purpose. This protection scheme is carried out in three phases:

a- Identification of the protection capacity required for the backup of Tsd from the source s to the destination d. The traffic Tsd is composed of k flows.

1-for $(1 \le i \le N)$ and $(1 \le j \le N)$, PRsd,ij = 0;

2-for all flows that compose the traffic Tsd ($Fsd^{(h)}$ with $1 \le h \le k$)

for $(1 \le i \le N)$ and $(1 \le j \le N)$ if Eij is crossed by $Fsd^{(h)}$ then PRsd,ij = PRsd,ij + capacity ($Fsd^{(h)}$).

3- Psd = Max $(1 \le i \le N, 1 \le j \le N)$ (PRsd,ij)

For a given traffic Tsd, Psd is the number of flow units required to protect the traffic against a single failure. The Psd represents the highest risk; it is also the maximum number of flow units of the traffic, riding the same physical link.

If PTsd is the backup protection of the working flow Fsd then PTsd should carry, at least, Psd flow units in order to provide protection of a working connection with guaranteed recovery of similar grade of service.

b- The identification of the resources that could be used for the protection: the protection on the primary traffic may share some links. However, one needs to make sure that in case of a link failure, there is enough bandwidth on the other protection flows to restore the traffic affected. If PNSsd,ij is the number of flow units that could be used by the protection then it should respect the two following constraints:

- The total flow units available: indeed the capacity of a link is limited. The link could also be used by other flows belonging to other traffics. This constraint could be expressed as follows: For $(1 \le i \le N)$ and $(1 \le j \le N)$ $PNSsd,ij \le NSij$

- The shared risk constraint: in order to balance the protection over the links and avoid sending too much traffic on a single link (from the primary and backup traffic), one needs to control the backup flows. This could be expressed as follows.

For $(1 \le i \le N)$ and $(1 \le j \le N)$, $PNSsd,ij \le Psd - PRsd,ij$;

PNSsd,ij is the maximum number of flow units that could be used by the backup on link Eij. That is For $(1 \le i \le N)$ and $(1 \le j \le N)$, PNSsd,ij = min (NSij , Psd - PRsd,ij).

c- Protection provisioning: The backup PTsd could be considered as new traffic requiring Psd flow units

from the source s to the destination d. The resource allocation module is therefore engaged to reserve the required number of flow units.

Lemma: If the shared protection scheme described above is deployed in a network then it is possible to recover from any single link failure.

Proof: Let us consider a failure in link Eij.

Let Tsd be the traffic going from s to d with some flow units riding Eij (Tsd has exactly PRsd,ij flow units going on Eij). If Tsd is protected with PTsd backup using a shared flow protection scheme then PTsd is carrying Psd flow units.

The protection shares the links with the primary traffic. It may have some flow units riding Eij. Let A be the number of flow units belonging to the protection and going on the link Eij. We know that A + PRsdij is less or equal to Psd. That means that PFsd must have at least PRsd,ij flow units crossing other links. Therefore in case of Eij failure, the PRsd,ij flow units could be switched over the protection on the other links (the protection available on other links could accommodate at least PRsd,ij flow units).

3. Simulation results and analysis

We studied the performance of the proposed scheme by means of simulations, considering the NSFNET topology with 14 nodes. The traffic is uniformly distributed across the network.. The number of connections is varied to study the impact of the load. The source and the destination are chosen randomly and uniformly among the network nodes. In the simulation, more than one flow may be used to carry the flow units, we used k-Dijkstra algorithm to identify the k shortest paths (we use 4 paths in this simulation) between a source and a destination.

The goal of the simulation experiment is to study the performance of our proposed protection scheme used in time slotted optical network (TSON) as compared to the same protection in wavelength routed optical network (WRO).

We are first interested in investigating the protection efficiency (the ratio of the required back-up capacity over the capacity of the primary traffic).

In order to analyze the impact of the routing strategy on the performance of shared protection, we use two schemes to distribute the flows units over the k shortest flows; in the first one, which we call shortest-paths-first scheme (SPFS), we start by filling up the shortest flows first. In the second one, which we call diversity-first scheme (DFS), we distribute the flow units over all the k shortest paths in order to have the maximum diversity possible.

Figure 1 shows the protection efficiency versus the traffic load for SPFS routing strategy. As the traffic load increases, the charts show that shared protection uses less resource than WRO. Nevertheless when the traffic is light the backup use almost the same amount of bandwidth. As the traffic gets higher the requests carry more flow units and need more than one flow creating more opportunities for shared protection to save bandwidth. For wavelength routed protection the requests use the whole wavelength to carry the traffic and therefore the whole wavelength should be protected. Thus the protection requires almost 100% of the primary traffic. When the traffic gets higher there is more chance to fill more than one wavelength and consequently some bandwidth saving could be achieved.

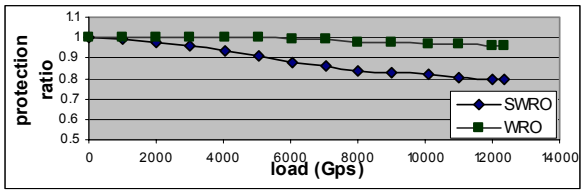

Figure 1. Protection efficiency for SPFS

Figure 2 illustrates the impact of a routing strategy on the protection efficiency. In deed when the DFS routing strategy is used, the traffic of a request is sent over many different flows. This gives more chance to our proposed scheme to optimize the shared backup. When the traffic is light the efficiency is very high. However when the traffic increases the number of path between a source and a destination becomes limited and the diversity decreases.

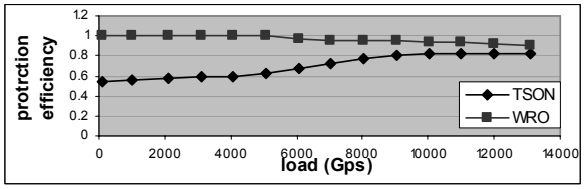

Figure 2. Protection efficiency for DFS

In the previous simulation, we investigated only the bandwidth needed for the backup without any reservation. However if some resources are effectively used for the backup then both future primary traffic and their protection may suffer shortage in resources leading to some blocking for some requests or their backups. One of the metrics we investigate in the second simulation is the blocking ratio, which reflects the percentage of traffic that must be discarded due to shortage in resources

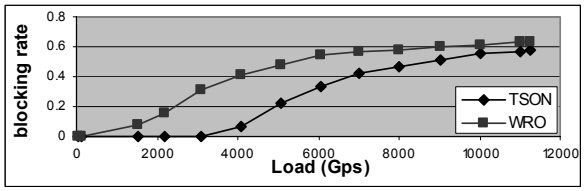

Figure 3. Blocking rate for DFS

Figure 3 shows the blocking ratio versus the traffic load. As the traffic load increases, the charts show that TSON accommodates more traffic than WRO technique. In addition, TSON maintains a zero blocking ratio; while WRO blocked more than 10% of the traffic. When the load gets lighter, the blocking rate is very high (more than 60%); TSON is performing slightly better than wavelength routing technique. This is resulting from the excessive use of resources by the primary and backup.

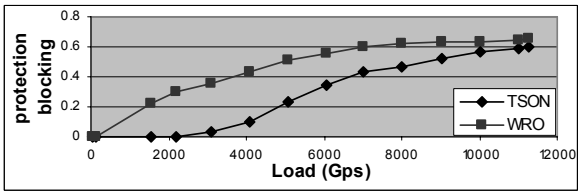

Figure 4. Protection blocking rate for DFS

Besides the primary traffic, resources also should be allocated and reserved for the backup. Figure 4 shows the blocking rate for the protection. This reflects the percentage of protection traffic that must be discarded due to shortage in resources. The trend of the curves is very similar to the blocking rate for the primary traffic. Indeed for the resource allocation module the primary and backup are considered equally. And hence the backup suffers the same blocking ratio as the primary traffic. Nevertheless the protection blocking is a little bit higher than that of primary traffic because the protection is observing more constraints than the primary traffic.

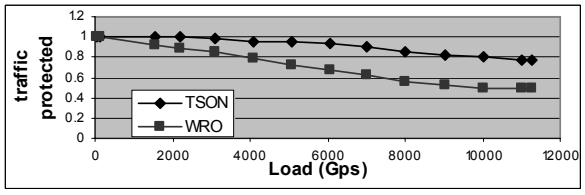

Figure 5. Ratio of the traffic protected for DFS

When the protection fails to find enough resources for a backup, a part of primary traffic is left without protection. Figure 5 shows the ratio of traffic protected. For light traffic the TSON protect 100% of the traffic whereas WRON drop some protections early. This is because with TSON the blocking rate is very low. Besides that the protection requires only a small capacity for the backup. The RWO requires 100% of the primary traffic. Therefore both primary and backup traffic will suffer some blocking. When the traffic gets heavier, both WRO and TSON fail to protect the whole primary connections. However, as the traffic gets higher the gap between the two techniques gets larger.

4. Conclusion

In this paper, we proposed a new shared protection scheme that aims to use the bandwidth more efficiently while providing the same level of protection as a dedicated protection. For a given traffic from a source to a destination, the different flows are analyzed and the optimal shared protection is identified. The simulation proves that this protection scheme combined with slotted optical network is resource efficient.

Further work is needed to deal with the multi-failure where more than one link or more than one node is down.

5. References

[1] E. Modiano and A. Narula-Tam, "Survivable routing of logical topologies in WDM networks," Proceeding of IEEE INFOCOM, Apr. 2001, pp. 348-357.

[2] G. Maier, S De Patre, A. Pattavina, and M. Martinelli, "Optical network survivability: protection techniques in the WDM layer," Photonic Networks Communications, Feb. 2002, pp 251 – 269

[3] G. Mohan and A.K. Somani, ``Routing Dependable Connections with Specified Failure Restoration Guarantees in WDM Networks," in Proceding of IEEE INFOCOM, Vol. 3, Mar. 2000, pp 1761-1770.

[4] Ramamurthy, S.; Mukherjee, B "Survivable WDM mesh networks. II. Restoration," ICC '99 Vol 3, Jun 1999, pp. 2023 – 2030

[5] Dexiang John Xu; Wei Yen; Ho, E "Proposal of a new protection mechanism for ATM PON interface" ICC'01, Vol. 7, Jun 2001, pp. 2160 – 2165.

[6] Liew. S.Y, Chao. H.J.; "On slotted WDM switching in bufferless all-optical networks" High Performance Interconnects, 2003, Aug. 2003, pp 96 -101

[7] Ramamirtham. J, Turner. J.; "Time sliced optical burst switching," Proceeding of IEEE INFOCOM, Vol 3(30) March/April 2003, pp 2030 – 2038