A New Protection Paradigm for Digital Video Distribution Networks

Ornan Gerstel
Advanced Technology, CRBU
Cisco Systems
San Jose, USA
ori@ieee.org

Galen Sasaki
Department of Electrical Engineering
University of Hawaii
Honolulu, USA
galens@hawaii.edu

Abstract—A protection scheme is proposed that can be applied to video distribution networks. Instead of fully protecting affected High Definition TV connections it provides reduced bandwidth that suffices for Standard Definition TV. Two versions of this scheme are studied: when working and protection bandwidth are separate, and when working bandwidth may be "victimized" (interrupted). An analysis is given to determine when such a scheme is economical.

Keywords-optical networks; wavelength division multiplexing; digital video distribution networks; protection.

I. INTRODUCTION

Traditional telecom networks are based on an "all or nothing" approach to service protection – services are either fully protected against failures or they are not protected at all. Several attempts have been made (e.g., [1]) to provide differentiated protection using priorities, allowing reduction in network bandwidth; however, such alternatives have failed to provide any protection guarantees. As a result it is hard to imagine how they will be used for real service definitions.

Renewed interest in novel protection schemes is fuelled by the huge growth of bandwidth required for delivery of digital video services – mainly Video on Demand (or VoD). While the bandwidth needs for VoD are much more significant than for most other applications, the price point must be low. Therefore it is important to optimize the use of bandwidth even if it means lower availability. Video providers have even considered using unprotected traffic across both sides of the ring, so that in the event of a failure, half the bandwidth is lost and the surviving half can only accommodate 50% of the peak traffic. This approach works well as long as failures do not coincide with peak viewing hours, but it falls short if the two overlap.

Recently we have reported several new approaches to this problem. In [2], motivated by the notion of Quality of Protection (QoP), we have defined a continuum of services, from unprotected to fully protected services, where the level of service is defined by its probability to survive a failure. Thus, for the first time, intermediate services can be defined with consistent semantics. We also defined a deterministic version of this QoP approach, in which, upon a failure, a service is guaranteed a surviving bandwidth but at a prescribed fraction of the bandwidth under normal circumstances.

We have also reported a new framework for definition of services and protection, based on a risk management approach [3]. This is a holistic economic approach to protection that looks at the ultimate service provider goal – the profit from services over time after subtracting the cost of the network. More protection implies higher network costs but also higher service charges.

The current paper combines ideas from [2] and [3] and puts them in a realistic context of video distribution networks. Such networks are built around the world today with huge investment and one of the questions service providers grapple with is the need to protect them against failures. The traditional 99.999% availability benchmark is challenged as it is clear that the required bandwidth for video cannot be cost effectively satisfied with traditional SONET/SDH technologies. Indeed, many of these networks are built using packet (typically Metro Ethernet) over DWDM technology. Such a network is depicted in Fig. 1. It is a DWDM ring network for distribution of video traffic between a head-end (where the video server resides) and distribution nodes, which connect to the customer distribution networks -- such as the HFC or DSL plant.

Since packet networks have much more flexibility in deciding how to drop packets, it is now possible to reduce bandwidth for video streams that are impacted by failures. Specifically for video, the application also allows for at least one level of reduced bandwidth that is still valuable to customers: standard definition TV (SDTV). The bandwidth required for SDTV is about 20% of the bandwidth required for high definition TV (HDTV). It should be noted that this ratio is sensitive to the video encoding scheme and other factors and thus varies from service provider to service provider.

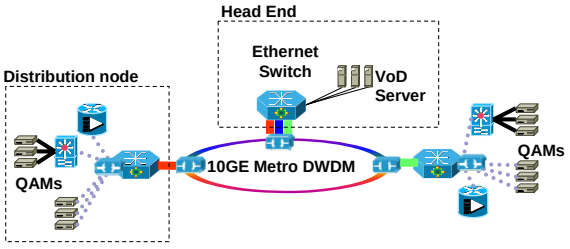


Figure 1. Video distribution network.

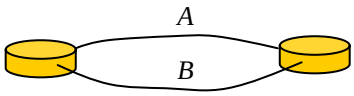


Figure 2. Two parallel fiber-links connecting two nodes.

In Section II, we describe the protection strategy. Section III considers a hubbed ring network, and Section IV discusses economic considerations. Some implementation issues are addressed in Section V. Final comments are given in Section VI.

II. Problem Definition

Consider a DWDM ring network for distribution of video traffic between a head-end node and distribution nodes, such as depicted in Fig. 1. Assume that the required protection bandwidth for a service is a fraction r of the working bandwidth. For example, consider the case when the distribution is for HDTV. If $r = 0$ then an HDTV connection has no protection, if $r = 1$ then an HDTV connection has full protected. The value $r = 0.2$ would model the case when the protection bandwidth is reduced to supporting SDTV.

There are two protection scenarios we consider. The first is when the bandwidth is partitioned into working and protection bandwidths. We refer to this as *partitioned bandwidth protection*. Existing protection schemes operate this way, e.g., SONET BLSR. The deterministic version of the QoP approach in [2] is also this way.

The second scenario is when working connections that were not directly affected by the failure may be pre-empted (or "victimized") to support protected traffic. We refer to this as *victimized bandwidth protection*. Such a method has only been considered in the context of low-priority traffic (such as "extra traffic" in SONET), which proved to be of little value since most users will not settle for a service which has only a negative guarantee: to completely fail whenever a failure occurs in the network. By contrast, the scheme we are proposing will not cause any service to completely fail and will allow several connections to partially recover by reducing the bandwidth on a single connection.

A. Point-To-Point System

To illustrate the two scenarios, we consider a simple point-to-point case shown in Fig. 2, where a head-end node and a single distribution node are connected by two parallel DWDM fiber-optic links. There are W wavelengths per link, each supporting the same bandwidth b.

We assume the distribution node requires an amount B of working traffic from the head-end. For simplicity, we assume that the working traffic between the head-end and distribution node may be split arbitrarily among multiple wavelengths. This is a reasonable assumption if individual connections use a small portion of the bandwidth in a wavelength.

Under the partitioned bandwidth scenario, the wavelengths are partitioned into working traffic and protection bandwidth. Let us assume that the bandwidth in each wavelength is divided into separate working and protection bandwidths. In particular, $\frac{1}{r+1}b$ bandwidth is working bandwidth, and $\frac{r}{r+1}b$ bandwidth is protection bandwidth. Each wavelength has enough protection bandwidth for the working traffic of a faulty wavelength because its protection bandwidth is a fraction r of the working bandwidth. Note that the fiber-links protect each other.

Note that each wavelength can carry $\frac{1}{r+1}b$ working traffic and there are W wavelengths in two fiber-links. Then the number of required wavelengths is

$$W = \left\lceil \left(\frac{r+1}{b} B \right) / 2 \right\rceil. \quad (1)$$

Now we turn to consider victimized bandwidth protection. We assume that under normal conditions, all the bandwidth of wavelengths is used for working traffic. When a fault occurs, the working traffic on the failed wavelengths are rerouted to protection bandwidth on surviving wavelengths (at bandwidth rate $r \cdot b$), which is freed up by victimizing other working traffic on surviving wavelengths.

Note that a surviving wavelength has bandwidth rate b, so when it is victimized, it can host $\lfloor 1/r \rfloor$ protection traffics. Also note that if a wavelength is victimized, its working traffic is discontinued, and its protection traffic must be carried. It is assumed that the victimized wavelength will carry its own protection traffic. Therefore, a victimized wavelength can carry the protection traffic of at most $\lfloor 1/r \rfloor - 1$ other (failed) wavelengths.

In order for this protection to make sense, we will assume $r \le 0.5$. Then a victimized wavelength has enough bandwidth to carry the protection traffic of at least one other (failed) wavelength. Under the assumption, note that the each fiber-link has sufficient protection bandwidth to protect the working traffic of the other fiber-link.

Therefore, the number of required wavelengths W is equal to the minimum needed just for working traffic, or:

$$W = \left\lceil \left(\frac{B}{b} \right) / 2 \right\rceil. \quad (2)$$

Note that this value of W is the minimum possible even if the working traffic were unprotected. Thus, victimized bandwidth protection is the most efficient in utilizing wavelengths.

Comparing (1) and (2), victimized bandwidth protection requires less bandwidth by a fraction r. But the availability of a working wavelength may be smaller because it can be victimized even though it has not failed.

This work was supported in part by the Cisco University Research Program. It appeared in the Proc. ICC 2007 Istanbul, June 2006.

TABLE I. COMPARISON FOR THE POINT-TO-POINT SYSTEM

	Partitioned bandwidth	**Victimized bandwidth**
Number of wavelengths per fiber-link	$\left\lceil (r+1)\left(\frac{B}{b}\right)/2 \right\rceil$	$\left\lceil \left(\frac{B}{b}\right)/2 \right\rceil$
Fraction of time p^* at reduced bandwidth	$p^* = p$	$p \le p^* \le 2p$

We will compute the availability using the following simplified model. We consider the availability over a finite time window. Each fiber-link fails for a fraction p of the time, and the links do not fail simultaneously.

For partitioned bandwidth protection, a connection will be at the reduced protection bandwidth whenever it experiences a fault. Therefore, it is at the reduced protection bandwidth for a fraction p of the time. For the case of victimized bandwidth protection, a connection could be at the reduced protection bandwidth whenever it experiences a fault or it is victimized. The fraction of time it experiences a fault is p. The fraction of time it is victimized may be up to p. Therefore, it is at a reduced protection bandwidth for a fraction p^* of the time, where $p \le p^* \le 2p$. Table I summarizes the results.

If we want a better estimate on p^*, we need to specify how wavelengths are victimized. In a fiber-link, each wavelength can protect $\lfloor 1/r \rfloor - 1$ wavelengths from the other fiber-link. Then, when a fault occurs in a fiber-link, the minimum number of wavelengths that will be victimize is

$$\left\lceil \frac{W}{\lfloor 1/r \rfloor - 1} \right\rceil.$$

Which of the wavelengths are victimized depend on the protection implementation. If we assume that each wavelength is equally likely to be victimized then the fraction of time a wavelength is victimized is

$$p \cdot \left(\left\lceil \frac{W}{\lfloor 1/r \rfloor - 1} \right\rceil / W \right).$$

For large W, this is approximately $p \cdot \frac{1}{\lfloor 1/r \rfloor - 1}$. Then p^* is approximately $p \cdot \left(\frac{1}{\lfloor 1/r \rfloor - 1} + 1 \right)$.

III. HUBBED RING NETWORK

We can extend the results of the point-to-point system of Fig. 2 to a network, and in particular a hubbed DWDM bidirectional ring network shown in Fig. 3. Such a network models a typical DWDM video distribution ring as in Fig. 1.

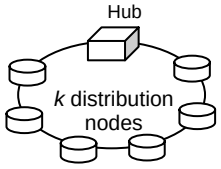


Figure 3. DWDM hubbed ring network.

The hub is the head-end (server) node, and the other nodes are distribution nodes. Let k denote the number of distribution nodes.

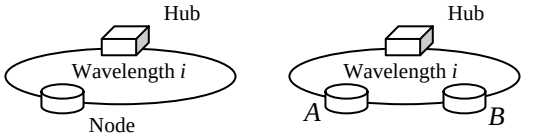
Again, we assume W wavelengths, and each wavelength carries b bandwidth. We assume each distribution node requires an amount B of working traffic from the hub. For simplicity, we assume that the working traffic between the hub and any distribution node may be split arbitrarily among multiple wavelengths.

We consider two scenarios: partitioned and victimized protection bandwidth.

A. Partitioned Bandwidth Protection

We describe an implementation of partitioned bandwidth protection. In the implementation, there are two configurations of a wavelength. The first configuration is when a wavelength i is dedicated to connecting a single node to the hub, as shown in Fig. 4(a). There are two transponders each at the node and hub. The wavelength connects the node to the hub on both sides of the ring. If there is a failure then one side will survive, and protect the failed side.

The bandwidth of wavelength i is divided into working and protection bandwidth. In particular, on both sides of the ring a fraction $\frac{1}{r+1}$ of the wavelength is working bandwidth, and a fraction $\frac{r}{r+1}$ of the wavelength is protection bandwidth. Note that the protection bandwidth is a fraction r of the working bandwidth. Then if one side of the ring fails, the other side has enough bandwidth to protect it. We refer to this wavelength configuration as the *one-node configuration*. Note that this configuration can carry $\frac{2b}{r+1}$ working traffic between the hub and node.



(a) One-node configuration (b) Multi-node configuration

Figure 4. Wavelength configurations.

The second configuration is when a wavelength i is dedicated to connecting multiple nodes to the hub. Fig. 4(b) shows the configuration when there are two nodes. There are two transponders at each of the nodes and hub. The bandwidth of the wavelength is divided among the nodes. A node's bandwidth is divided further into working and protection bandwidth, where the amount of protection bandwidth is sufficient to protect the working traffic.

As an example, consider node A in Fig. 4(b). Suppose it has bandwidth c in wavelength i around the ring (node B will also have bandwidth in wavelength i dedicated to it). The amount of node A's working bandwidth is $\frac{c}{r+1}$, and the amount of its protection bandwidth is $c\frac{r}{r+1}$. Note that it has enough bandwidth to protect its working traffic. Also note that the bandwidth can carry $\frac{2c}{r+1}$ of working traffic between the hub and node. We refer to this wavelength configuration as the *multi-node configuration*.

We now describe how traffic is divided into wavelengths, and how the wavelengths are configured. First, each node has assigned to it $\left\lfloor B/\left(\frac{2b}{r+1}\right)\right\rfloor$ wavelengths that are in the one-node configuration. These wavelengths can carry

$$\left(\frac{2b}{r+1}\right)\left\lfloor B/\left(\frac{2b}{r+1}\right)\right\rfloor$$

working traffic between the node and hub. Note that there is

$$R = B - \left(\frac{2b}{r+1}\right)\left\lfloor B/\left(\frac{2b}{r+1}\right)\right\rfloor$$

amount of working traffic that are not yet assigned to wavelengths for the node. We refer to R as the residual working traffic for the node.

The residual working traffic of the nodes will be assigned to the remaining wavelengths. Also assigned is the protection bandwidth for this working traffic. Thus, the total working and protection bandwidth for the residual traffic is $R(1+r)$.

Nodes assigned to a wavelength are in the multi-node configuration for the wavelength. The assignment is as follows.

We pick an unused wavelength and sequentially assign nodes to it until the residual traffic of the nodes (and their protection bandwidth) fill the wavelength. Note that there may be insufficient bandwidth for all the residual traffic of the last node to be assigned. Then the remaining traffic is assigned to another unused wavelength, and we continue assigning nodes to the wavelength. We continue in this way until all the residual traffic of nodes are assigned to wavelengths. Note that all wavelengths are completely filled except possibly one.

Since the total working traffic is $k \cdot B$ and each wavelength can carry $\frac{2b}{r+1}$ working traffic, the number of wavelengths is

$$\left\lceil kB/\left(\frac{2b}{r+1}\right)\right\rceil = \lceil (r+1)kB/2b \rceil$$

We can also calculate the number of transponders. Note that each node has two transponders in each of its wavelengths. If a distribution node's residual traffic R is zero then it is only in one-node configuration wavelengths. If $R > 0$ then it is in one or two multi-node configuration wavelengths. It will be in two multi-node configurations if it were the last node to be assigned to a wavelength and it still had some remaining residual traffic to be assigned to a second wavelength. Thus, the total number of wavelengths a distribution node is assigned to is at most

$$\left\lceil B/\left(\frac{2b}{r+1}\right)\right\rceil + 1 = \lceil (r+1)B/2b \rceil + 1,$$

and the total number of transponders is at most

$$2(\lceil (r+1)B/2b \rceil + 1).$$

Since there are k distribution nodes, the total number of transponders at distribution nodes is at most

$$2k \cdot (\lceil (r+1)B/2b \rceil + 1). \quad (3)$$

The number of transponders at the hub is twice the number of wavelengths. Since the number of wavelengths is $\lceil (r+1)kB/2b \rceil$, the total number of transponders is

$$2\lceil (r+1)kB/2b \rceil \ . \quad (4)$$

By combining (3) and (4), the total number of transponders is

$$2k \cdot (\lceil (r+1)B/2b \rceil + 1) + 2\lceil (r+1)kB/2b \rceil. \quad (5)$$

To simplify Expression (5), assume that B is very large. Then the expression is approximately $2kB(1+r)/b$.

B. Victimized Bandwidth Protection

Now we turn to victimized bandwidth protection. As in the point-to-point system, we assume $r \le 0.5$. Then a victimized wavelength on one side of the ring can protect the traffic in the wavelength on the other side of the ring.

We can use similar arguments used for the partitioned bandwidth protection to determine the number of wavelengths and transponders for the victimized bandwidth protection. We

have one-node and multi-node configurations for wavelengths but where the entire wavelength is used for working traffic.

The number of wavelengths is $\lceil kB/2b \rceil$, and the number of transponders is $2k \cdot (\lceil B/2b \rceil + 1) + 2\lceil kB/2b \rceil$. Again, we can simplify the last expression by assuming B is very large. Then the expression is approximately $2kB/b$.

C. Discussion

Table II summarizes the number of wavelengths and transponders for partitioned and victimized bandwidth protection. Our analysis shows that victimized bandwidth leads to smaller number of wavelengths and transponders. But the availability of working traffic will be smaller because wavelengths are victimized even though they are not directly along the fault.

We should note that reduced bandwidth protection for mesh networks was studied recently in [4]. Simulations were used to show that reduced bandwidth protection can lead to lower network cost and better performance than full protection. However, the study focused only on partitioned bandwidth protection (i.e., the deterministic QoP of [2]), and did not provide formulas for network cost as a function of r.

IV. Economic Considerations

Victimized bandwidth protection is cost effective. As shown in Sections I and II, it requires the same number of wavelengths as unprotected bandwidth. So it is a viable alternative if working traffic can be interrupted (victimized) even when it is not on a fault.

However, often in practice, working traffic that is not on a fault cannot be disturbed. This is the case with partitioned bandwidth protection. This protection scheme leads to network cost (wavelengths and transponders) that is dependent on r. For the point-to-point system and hubbed ring network in Sections II and III, the cost can be approximated by a linear function of r. This section discusses the economic considerations that determine the appropriate value of r for partitioned bandwidth protection. For simplicity, we assume that the network cost is a linear function of the bandwidth, namely $C(1+r)$, for some constant C. Note that when $r = 0$ (unprotected), the cost C is for the working bandwidth. When $r = 1$ (fully protected), the cost is $2C$, which is twice the cost of the working bandwidth.

TABLE II. Comparison for the Hubbed Ring Network

	Partitioned bandwidth	**Victimized bandwidth**
Number of wavelengths	$\lceil kB(1+r)/2b \rceil$	$\lceil kB/2b \rceil$
Approximate number of transponders if B is large	$2kB(1+r)/b$	$2kB/b$

Note that if we were to optimize network cost then we would always choose $r = 0$, unprotected service. But in many cases, unprotected traffic is not an ideal service. For example, if the network provided HDTV video services for live sporting events such as the Super Bowl, a fault on an unprotected service could have a dramatic negative effect on customer satisfaction and revenues. Thus, there is a penalty associated with each value of r. For example, the penalty may be due to lost customers or a rebate that the provider may offer in compensation for the failure.

We represent this penalty as a function $P(r)$. Note that when $r = 1$ then the services are completely protected and there is no penalty, i.e., $P(1) = 0$. When $r = 0$ then the services are unprotected and we would expect some high penalty, possibly of infinite value. We assume that P is a non-increasing function. Later at the end of this section, we provide an example of a penalty function.

We can combine the network cost and the revenue penalty to give a combined cost: $F(r) = C(1+r) + P(r)$.

A relevant design problem is to find a value of r that minimizes F. This value defines the optimal service for the network. This problem is equivalent to finding a value r that minimizes $f(r) = Cr + P(r)$. Note that $f(0) = P(0)$, and $f(1) = C$.

Observation. A service with reduced protection bandwidth r (e.g., $r = 0.2$ for SDTV) is viable if:

$Cr + P(r) < \min\{ C, P(0) \}$.

The above observation implies that before defining a service with reduced bandwidth r, one should understand how the shape of the penalty function P affects the feasibility of the service. If P is a concave function then F is a concave function and is minimized when $r = 0$ (unprotected) or $r = 1$ (full protection). Thus, a reduced bandwidth scheme does not make sense for this case.

If P is a convex function then F is a convex function and the optimal value for r may lie between 0 and 1, i.e., values for r when reduced protection bandwidth makes sense. If P (and F) are differentiable then we can determine the optimal value of r by using the derivative of F with respect to r. In particular, F is minimized when $dF/dr = 0$, which is equivalent to $dP(r)/dr = C$. Obviously, a reduced bandwidth r makes sense if it satisfies $dP(r)/dr = C$.

Other cases to consider are: (*a*) P dominates the function F (i.e., penalties are very high) or (*b*) P is negligible to F (i.e., penalties are negligible). In the first case the optimal solution is $r = 1$, which is full protection; and in the second case the optimal solution is $r = 0$, which is no protection.

The following is an example of a penalty function.

A. Example: Rebate for a Video on Demand Outage

Suppose the network supports services which are connections of a few hours, e.g., video on demand or pay-per-view (Super Bowl, championship boxing, World Cup soccer). Each connection will give the network revenue D, which is its price to the user. The price is independent of the amount of

protection bandwidth. Let N_1 denote the expected total number of connections over the lifetime of the network.

If a fault occurs then the affected connections will have reduced bandwidth, and in particular a fraction *r* of their normal bandwidth. When a connection is affected, the network will compensate the user for his dissatisfaction with a rebate *R*(*r*). The rebate should be high enough so that the user will continue to be a customer. We assume that the rebate decreases with increasing *r* because connection service improves. For example, consider HDTV connections. When *r* = 1 (full protection), there should be no rebate because service is never interrupted. When *r* = 0.2 (SDTV protection), the user gets continued service but at a lower quality. So the user could get his money back, i.e., *R*(0.2) = *D*. When *r* = 0 (no protection), the service is completely interrupted, and to satisfy the user, *R*(0) could be many multiples of *D*.

Let N_2 denote the expected total number of connections that are affected by failures over the lifetime of the network. which can be high in a fault prone network. The total net revenue over the lifetime of the network is $N_1 D - N_2 R(r)$. We can define a penalty function from this, which is the lost net revenue $P(r) = N_2 R(r)$.

Note that if *R*(1) = 0, *R*(0.2) = *D*, and *R*(1) is many multiples of *D* then the function *R*(r) is convex. Then *P*(*r*) is convex. Also, note that the reduced protection bandwidth *r* = 0.2 is viable if

$$C \cdot (0.2) + N_1 \cdot R(0.2) < \min\{C, N_1 \cdot R(0)\}.$$

V. Implementation

In this section, we discuss implementation issues, specifically as the scheme pertains to HDTV distribution from video servers to the HFC or DSL plant (the part of the network depicted in Fig. 1). The main challenge stems from the need to change from HDTV to SDTV format as part of the protection process. There are three approaches for solving this problem:

- Transmit both HDTV and SDTV signals during normal operation.
- Encoding scheme that allows extracting an SDTV signal from an HDTV stream.
- Coordinate the protection process with the video server, to change the signal format.

The first approach relies on the fact that most channels are transmitted in both formats over the network to accommodate customers with different service agreements. Switching to protection requires that the network is aware of which HDTV channel corresponds to which SDTV channel. This information can be provisioned into the nodes during connection setup. Note that this requires control at the packet level – most likely by assigning a different MPLS connection or VLAN ID to different channels.

The second approach calls for an encoding scheme that encodes some basic lower definition video stream in separate packets and builds on this information to construct a high-definition video using additional packets, e.g., hierarchical or layered coding [5]. Then it is possible to assign higher priority to packets that carry the low-definition data to ensure they survive an outage. During a protection event, high-definition packets may be dropped and the surviving packets will allow constructing a low-definition stream at the minimum. Note that the encoding schemes must allow for the reconstruction of the video stream based on low-definition frames only or a combination of low-definition packets and some high-definition packets.

The third approach requires the transport layer – most likely Ethernet switches that are used in hub offices to aggregate video streams for video servers into wavelengths – will have to signal to the video server via some form of a backward defect indicator (BDI), that specific data flows have failed, causing the transmission of the equivalent SDTV stream from the video server.

VI. Conclusions

We propose reduced bandwidth protection for Video Distribution Networks to lower network costs while providing reasonable protection. We describe the cost and penalty structure when this paradigm makes sense. We also describe a reduced bandwidth protection strategy that "victimizes" working connections for their bandwidth, to be used as protection bandwidth for failed connections. The scheme does not require any protection bandwidth and is thus very attractive from a cost perspective. Finally we touch upon implementation issues involving the switch from HDTV to SDTV and back. We conclude that such a protection scheme will require additional functionality at the packet layer – not just the optical layer.

Acknowledgment

The authors are grateful for the insightful comments of the reviewers.

References

[1] N. Golmie, T.D. Ndousse, and D.H. Su, "A differentiated optical service for WDM networks," IEEE Comm. Magazine, vol. 14, pp. 68-73, February 2000.

[2] O. Gerstel and G. Sasaki, "Quality of protection (QoP): a quantitative unifying paradigm to protection service grades," Optical Networks Magazine, vol. 3, May 2002, pp. 40-49.

[3] N. Bambos, S. Gitzenis, A. Miura, O. Gerstel, and L. Paraschis, "A service risk-management approach to capacity protection in optical networks," *IEEE LANMAN*, (San Francisco Bay Area, 2004), pp. 69- 74.

[4] J. Fang, M. Sivakumar, A. Somani, and K. Sivalingam, "On partial protection on groomed optical WDM networks," *Proc. 2005 Conference on Dependable Systems and Networks* (*DSN '05*), (Yokohama, 2005), pp. 228-237.

[5] T. Chiang and D. Anastossiou, "Hierarchical Coding of Digital Television," IEEE Communications Magazine, vol. 32, pp. 38-45, May 1994.