Cross-Layer Approach to Survivable DWDM Network Design

Amir Askarian, *Student Member, IEEE,* Yuxiang Zhai, Suresh Subramaniam, *Senior Member, IEEE,* Yvan Pointurier, *Member, IEEE,* Maïté Brandt-Pearce, *Senior Member, IEEE*

***Abstract*—All-optical networks, in which the electrical regeneration bottlenecks are removed, are seen as the next-generation backbone networks. Any link failure in these high speed environments, if not dealt with promptly, is catastrophic and can cause the loss of gigabits of data. While techniques to improve the survivability of optical networks are now well-established, such is not the case with all-optical networks. In these environments, the absence of regeneration implies that physical impairments accumulate over long paths. So-called cross-layer techniques mitigate the physical impairments' impact on the network layer performance. In this work, we apply cross-layer techniques, previously successfully applied to the impairment-constrained routing and wavelength assignment problem [5], to the problem of improving the survivability of all-optical networks facing link failures. To the best of our knowledge, cross-layer survivability of all-optical networks has never been studied before. We present algorithms that improve the network survivability over non cross-layer algorithms by decreasing both the blocking probability and the vulnerability of the network to failures. Our mechanisms are evaluated with extensive simulations for a realistic regional-sized network. The cross-layer algorithms are computationally intensive, and to alleviate this issue we propose two new compound restoration algorithms as well as two novel Quality of Transmission aware protection schemes that exhibit low blocking probability and have moderate vulnerability ratio and time complexity.**

I. Introduction

The always increasing demand for high throughput transmission in the backbone of data networks has drawn attention to all-optical Dense Wavelength Division Multiplexing (DWDM) networks. In such ultra-high speed environments, the effect of a component failure becomes much more severe and survivability considerations can prevent significant service interruptions. But the design procedure in all-optical networks has particular challenges and, as shown in this paper, neglecting the physical layer issues can lead to unacceptable performance. This is mainly due to the removal of optical-electrical-optical (OEO) conversion, which is the main speed bottleneck but helps ameliorate signal quality. Consequently, the quality of the received signal can be below the accepted level for the receiver – thus causing the connection or call to be dropped [6]. We refer to this event as *Quality of Transmission* (QoT) or *physical* blocking. In this work, we measure QoT in terms of bit-error rates (BER), which could increase above an acceptable level (e.g., $BER = 10^{-9}$, a threshold value set by the network operator). Also, since all-optical wavelength conversion is not yet mature for commercial deployment, we assume no wavelength conversion in our study. In this case, a call may also be blocked due to unavailability of a wavelength-continuous path, or simply *wavelength* blocked.

Although the network survivability problem in DWDM networks has been extensively studied in the past [7], [8], [9], the physical layer has not been taken into account. Our studies show that in many cases the physical blocking can be the dominating component in the total blocking probability for a connection. These results call for a cross-layer approach in survivable network design. We show that cross-layer (or QoT-aware) designs can greatly increase the network performance in terms of lowering the blocking probability and vulnerability ratio (a metric we formally define later to quantify the survivability of the network to a random link failure).

There has been a significant amount of research on routing and wavelength assignments that consider physical impairments in DWDM networks [5], [10], [11], [12], [13], [14], [15], [16], [17], [18], [19], but network survivability has not been considered in these papers. The most closely related work to ours is [20], which investigated path protection Routing and Wavelength Assignment (RWA) algorithms considering transmission impairments with the goal of achieving maximum resource sharing, but it resorts to OEO placement in the network to achieve desired quality for the received signal. Our paper considers fully transparent networks and addresses this problem with a cross-layer approach, and also defines a metric to evaluate the vulnerability of the algorithms to a failure. To the best of our knowledge, routing and wavelength assignment algorithms that strive to improve the resilience of all-optical networks to link failures without sacrificing low call blocking probabilities are proposed and evaluated for the first time in this paper.

The main contributions of this paper are as follows. First we evaluate the performance of different existing survivability algorithms in all-optical networks with realistic physical layer impairments. Then we apply a cross-layer algorithm to protection and restoration schemes and show the considerable performance improvement they provide. To mitigate the high time complexity of the cross-layer algorithms, we also propose other simpler and yet powerful algorithms.

A. Askarian, Y. Zhai and S. Subramaniam were supported in part by NSF under grant CNS-0519911. Y. Pointurier and M. Brandt-Pearce were supported by NSF under grant CNS-0520060.

A. Askarian, Y. Zhai and S. Subramaniam are with the Department of Electrical and Computer Engineering, The George Washington university, Washington, DC 20052 USA (emails: amiran@gwu.edu, yzhai@gwu.edu, suresh@gwu.edu). Y. Pointurier is with Alcatel-Lucent Bell Labs, Nozay, France (email: yvan@ieee.org). M. Brandt-Pearce is with the Charles L. Brown Department of Electrical and Computer Engineering, University of Virginia, Charlottesville, VA (email: mb-p@virginia.edu).

Parts of this paper were presented in [1], [2], [3] and [4].

Survivability in DWDM networks can be achieved by protection or restoration, which in turn can be path-wise or link-wise; furthermore, protection algorithms can use either a shared protection path or a dedicated one [7]. We begin by looking at dedicated path protection (1+1). In dedicated path protection, every connection has two link-disjoint lightpaths to handle single-link failures, a *primary* path and a *backup* path. In networks with regeneration (such as SONET), both the primary and backup paths are simultaneously used, and the receiving node monitors each copy of the signal and uses the best one (lowest BER). This ensures quick traffic restoration in case one of the paths fails. However, in transparent DWDM networks that are transmission-impaired, keeping the backup path dark versus lighting it up has an impact on the QoT of other lightpaths in the network. Lighting up the backup path worsens the impairments for other lightpaths due to added crosstalk, and thus increases the blocking probability of lightpaths. On the other hand, keeping the backup path dark (until it is needed) can lead to increased traffic restoration times (due to additional needed signaling between transmitting and receiving nodes). Therefore, it is of interest to study the effect of lighting up the backup path on network performance. Besides blocking probability, we also study the impact of dark and lit backup paths on the vulnerability of connections to failures. A link protection approach in such environments is also evaluated. Path and wavelength provisioning for link protection schemes leads to long lightpaths for the connections. We show that link protection does not perform well in all-optical networks with physical layer impairments [3].

We also look at path and link restoration schemes. As expected, they exhibit better performance in terms of the blocking probability than their protection counterparts. An interesting result of our study shows that in realistic transmission-impaired DWDM networks, path restoration has a failure vulnerability close to that of path protection. This shows that a naive approach to reserve resources for failure recovery not only wastes the network resources and increases the blocking probability, but also cannot assure recovery from a failure any more than a simple restoration method that uses resources efficiently and has low blocking probability.

We use our previously proposed[1] cross-layer RWA algorithm called *Highest Q* or *HQ* [5] and apply it to both protection and restoration schemes. We will see that this cross-layer approach significantly improves the performance in terms of both blocking probability and failure vulnerability. The drawback of this algorithm is its high computational complexity; we propose two additional algorithms and two compound HQ-nonHQ algorithms that alleviate this issue.

The paper is organized as follows. In Section II we present the network model and assumptions for the physical layer, and define the metrics used for performance evaluation of the RWA algorithms. In Section III we look at the proposed cross-layer protection and restoration algorithms in DWDM networks. In Section IV we propose modifications to achieve high speed cross-layer algorithms for survivability in all-optical networks. In Section V we present simulation results and evaluation of the proposed algorithm performances. Finally we conclude the paper in Section VI.

[1]This algorithm was originally developed without considering survivability.

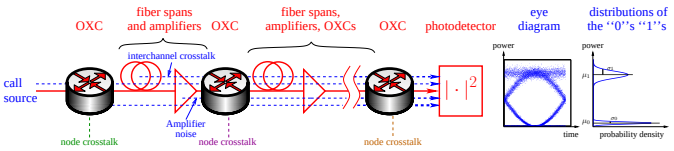

Fig. 1. Model of a transmission path used to compute the Q factor. Amplifiers inject ASE noise, interplay between channels in fiber spans cause nonlinear crosstalk, while leaks in the OXCs cause node crosstalk.

II. Network Model and Performance Metrics

A. Network Model

In this section, we present the model and assumptions for the physical layer used throughout the paper. This model was previously proposed by us in [15], [5], and we summarize it here for clarity and completeness.

We consider circuit-switched all-optical networks with no wavelength conversion. On a call arrival, either one or two new circuits are tentatively established depending on the RWA algorithm being used. The RWA algorithms are presented in Section III. Physically, a circuit corresponds to a *lightpath* [21], that is, the combination of a route (sequence of nodes called Optical Crossconnects or OXCs, separated by spans of fibers) and a channel (a wavelength). Note that by lightpath establishment we mean that the resources are reserved, whether the corresponding wavelength is lit or not. We assume that all links are bidirectional and carry exactly λ_{Total} wavelengths in each direction. Due to the absence of wavelength conversion, lightpaths must respect the *wavelength continuity constraint* and remain on the same wavelength end-to-end.

The physical components of a lightpath (see Fig. 1) are a transmitting laser, optical crossconnects, spans of fibers, and a receiver. We model amplifiers as non-saturating, and the receiver as a wideband optical filter (for demultiplexing purposes) and a photodetector followed by a narrow electrical filter. In this work, we do not assume that transmission at the physical layer is error-free: error-free transmission is a valid assumption only for small networks and large networks where signals are periodically regenerated electronically. In the context of regional or even metropolitan all-optical networks, the distances involved are so large that physical impairments are no longer negligible. We measure the QoT of a lightpath by its BER, which should remain below a threshold set by the network manager to ensure almost error-free data transmission.

To estimate BERs, we use the relation between BER and the so-called corresponding *Q factor* (an electrical signal-to-noise ratio) for on-off-keying modulation: $BER = \frac{1}{2}\mathrm{erfc}\left(Q/\sqrt{2}\right)$. The Q factor for a signal on a lightpath is given by, assuming Gaussian distributions for the ‘0’ and ‘1’ samples after photodetection [22]:

$$Q = \frac{\mu_1 - \mu_0}{\sigma_0 + \sigma_1} \tag{1}$$

where μ_0 and μ_1 are the means of the ‘0’ and ‘1’ samples, respectively, and σ_0 and σ_1 are their standard deviations.

Here, we account for four dominating impairments [23]: intersymbol interference (ISI), amplifier noise (ASE noise), interchannel nonlinear effects, also called nonlinear crosstalk, and optical leaks at the nodes, also called node crosstalk. A fifth impairment, polarization mode dispersion (PMD), is negligible at 10 Gbps but should be incorporated at faster data rates (40 Gbps/channel and more); we chose to ignore it in this work. Each of the four aforementioned effects can be accounted for in the Q factor as noise-like terms (variances), such that:

$$\sigma_1^2 = \sigma_i^2 + \sigma_n^2 + \sigma_{nl}^2 + \sigma_{nx}^2 \tag{2}$$

where σ_i^2, σ_n^2, σ_{nl}^2, σ_{nx}^2 are the variances due to ISI, ASE noise, nonlinear crosstalk, and node crosstalk, respectively.

ISI is caused by the interplay between fiber nonlinearity and dispersion characteristics, and ASE noise originates from the amplifier medium; therefore, for a given lightpath, ISI and ASE noise depend only on the lightpath's physical and topological properties (such as the number of spans of the lightpath, and their lengths). Fast techniques using precomputed tables exist in the literature to estimate σ_i and σ_n [24], [25]. Nonlinear crosstalk is the result of interplay between lit channels in fiber spans, while node crosstalk consists of leaks inside the nodes, whether it is at the demultiplexers (port crosstalk) or inside the switching fabric (fabric crosstalk). Demultiplexer crosstalk can in turn be either adjacent port crosstalk (the channels that interfere are adjacent in the optical spectrum) or non-adjacent port crosstalk. The intensity of fabric crosstalk and demultiplexer crosstalk vary according to the OXC implementation; however, non-adjacent crosstalk is always weaker than adjacent crosstalk. We presented a detailed model for node crosstalk in [15], which we reuse here. Contrary to ISI and ASE noise, nonlinear and node crosstalk depend on the network status: lighting more paths increases nonlinear interactions within fiber spans, thereby causing more nonlinear crosstalk, and increases the number of leaks in the OXCs, thereby causing more node crosstalk. Since crosstalks are network-status dependent effects, it is not possible to precompute their standard deviations σ_{nl} and σ_{nx}. However, it is possible to precompute the standard deviations for a single term of each kind of crosstalk [25], [26]; appropriate summation of these variances over the set of interfering lightpaths makes it possible to design fast QoT estimators, for which the only online computations consist in determining which lightpaths interfere, and summing their respective effects. Such estimators pave the way for the design of online QoT aware RWA algorithms, as shown in the next section.

B. Performance Metrics

We investigate RWA algorithm performance from two perspectives, blocking probability in the call admission process and vulnerability to a random failure during transmission. After taking the physical layer impairments into consideration, there are two types of blockings: wavelength blocking due to the unavailability of a continuous wavelength on the chosen path (wavelength continuity constraint not met) and QoT blocking due to the unsatisfactory Q factor of the path after network resources have been allocated to it (QoT constraint not met).

Since the purpose of survivability schemes is to prevent connections from breaking down because of failures, in addition to various types of blocking in the system, we are also interested in the network behavior when a random failure occurs. Single link failure is considered in this paper: at any time, at most one link failure is allowed in the entire network. In our link failure model, we consider that (single) link failure location and time of failure are randomly (uniformly) distributed over their respective domains.

We define the *Vulnerability Ratio* as a metric to describe the performance of our algorithms in the context of random single link failures. Vulnerability Ratio is defined as the probability that a randomly picked ongoing connection (at the time of failure) cannot be restored because of lightpath unavailability (in the case of restoration algorithms) or unacceptable QoT (for both protection and restoration algorithms), if a random link fails at a random point of time during the operation of the network. In order to compute the Vulnerability Ratio, we note that the vulnerability of a connection stays the same between network state changes (i.e., connection admissions and departures). Therefore, we can calculate the Vulnerability Ratio by averaging the vulnerability over all network states.

For a failure on link j in network state i, the probability that a random ongoing connection fails,

$$P_i^j = \frac{D_i^j}{T_i} \tag{3}$$

where D_i^j is the number of the connections that are dropped (due to unacceptable QoT or lightpath unavailability), and T_i is the total number of ongoing connections in state i. We denote by M the number of links, and by S the total number of network states during network evaluation. For each network state period, any of the links can fail with equal probability,[2] hence the following average over possible link failures:

$$P_i = \frac{1}{M}\sum_{j=1}^{M} P_i^j = \frac{1}{M}\sum_{j=1}^{M} \frac{D_i^j}{T_i} \tag{4}$$

Then, averaging over the entire network operation period, the Vulnerability Ratio is:

$$\mathcal{V} = \frac{1}{\sum_{i=1}^{S}\tau_i}\sum_{i=1}^{S} P_i\tau_i = \frac{1}{M}\frac{1}{\sum_{i=1}^{S}\tau_i}\sum_{i=1}^{S}\sum_{j=1}^{M}\frac{D_i^j\tau_i}{T_i} \tag{5}$$

where τ_i is the duration of state i.

III. Survivable RWA Algorithms

Traditional RWA algorithm design assumes a perfect physical layer, which leads to downgraded blocking probability performance when physical layer impairments are taken into consideration. These algorithms typically have low wavelength blocking probability but have high QoT blocking probability –

[2]We assume this in this paper. Other failure probability distributions can easily be incorporated if needed.

particularly when there are strong physical layer impairments – and hence an unsatisfactory total blocking probability. To deal with this situation, new QoT-aware RWA algorithms have been designed and their performances have been verified through extensive simulations. The idea behind QoT-aware RWA algorithms is to take physical layer impairments into consideration while choosing the wavelength and route for a connection request in the admission control process with the hope that this new connection does not significantly degrade the QoT performance of other ongoing connections.

We look at two non-QoT-aware RWA algorithms. In the first, a connection is routed according to the shortest path algorithm and the first (lowest index) available wavelength on that path (if any) is assigned to that connection. We refer to this method as *First Fit* or *FF* in short. In the second approach, for each working wavelength we try to find the shortest path (none may be available, due to wavelength unavailability somewhere along that path) and assign the shortest one among all to the connection. We refer to this approach as *Best Fit* or *BF*.

As a QoT-aware algorithm, we consider the *Highest Q Factor* algorithm (HQ) [5]. In HQ, a shortest path algorithm is run on each wavelength to find a candidate path on each wavelength. Then the end-to-end Q factor is calculated for all candidate paths and, among all the candidate paths, the path with the highest Q factor is chosen for the current connection. In our previous work [5], we have shown that this algorithm leads to low average BER and high fairness among connections with different path lengths.

A. Path Protection

In the context of dedicated path protection, three aforementioned RWA algorithms are considered here: shortest path routing with First-Fit wavelength assignment (FF), Best-Fit RWA (BF) and the Highest Q Factor RWA algorithm (HQ). These RWA algorithms using either a lit or dark backup path are investigated under dedicated path protection schemes using the same network topology and physical layer parameters.

First let us explain the connection admission procedure for the FF RWA. With the lit backup path protection scheme, the FF algorithm is run twice in order to compute two link-disjoint paths. If the wavelength continuity constraint cannot be met on either of the two paths, the connection is wavelength blocked. Otherwise, both paths are assumed to be lit up and QoT blocking verification starts (the wavelengths for the two lightpaths may be different). In this scheme, only one of the two paths of any ongoing connection needs to meet the BER threshold requirement for the receiving end to correctly receive the data. Thus, the interference brought into the network by the establishment of the two paths of the new connection request should be limited enough so that no connection in the network sees both its lightpaths disrupted (due to an unmet QoT constraint) at the same time. If both the primary and the backup path of any ongoing connection (or those of the new connection) do not meet the QoT constraint, then the requested connection is QoT-blocked. If the requested call is admitted, then both lightpaths are lit up.

In the dark backup path protection scheme, the wavelength blocking check is the same as with the lit backup path protection scheme; however, since the dark backup path protection scheme only lights up one path during the whole transmission period, the QoT verification phase differs. One of the paths (first shortest path) is assumed to be lit and the QoT constraint is checked for the primary path of every ongoing connection in the network, including the new connection itself. If all primary paths in the network meet the QoT constraint then the new connection is admitted; the path chosen to be lit is the primary path, while the other path (for which the QoT constraint is not checked) is the backup path. If the QoT constraint is violated, then the same procedure is repeated with the second shortest path of the incoming connection. If the QoT constraint cannot be met for both the first and the second shortest path, then QoT blocking occurs.

The procedure detailed above is similar in the case where the chosen RWA algorithm is BF or HQ instead of FF, except that the candidate paths for the roles of primary and backup path are not required to be the first and second shortest path, but are chosen according to the BF or HQ algorithms.

B. Path Restoration

Path restoration can be achieved in several ways. One approach is to use the shortest path routing and FF wavelength assignment scheme to set up a path for a requested connection, and to use the same to find the restoration path between the connection source and destination in case of link failure. We refer to this method as *FF-FF*[3] Path Restoration. To improve the performance of this method, we introduce a QoT-aware path restoration scheme, in which we use the HQ algorithm to find the path for the arrived connection and to restore a connection from a link failure. We refer to this approach as *HQ-HQ* Path Restoration. To have a fair comparison with the HQ algorithm that uses the shortest paths on all available wavelengths as the candidates to find the one with highest Q factor, we also look at the Shortest Path Best-Fit *(BF-BF)* path restoration method in which both for primary and restoration paths, the shortest path on every available wavelength is found and then the shortest among them is chosen for the connection.

Table I summarizes our path-wise algorithms, including the fast QoT-aware algorithms that will be introduced in Section IV.

C. Link Protection and Restoration

In link protection schemes, there is a need for an offline algorithm that finds a protection path for each link and reserves wavelengths along it, so that in case of link failure the protection path for that link is already known and the required wavelength is already reserved. The algorithm we use for link protection in this paper is derived from [27].[4] In that work, an algorithm is presented to find a 2-connected directed subgraph of the network graph. Let us call this directed subgraph

[3]In our terminology for path restoration schemes, the first acronym refers to the wavelength assignment algorithm to the primary route and the second refers to the restoration route. Routing algorithm is shortest path in both cases.

[4]To the best of our knowledge, this algorithm is the only one available in the literature that does not require wavelength conversion and is applicable to an arbitrary network topology.

TABLE I
PATH PROTECTION AND RESTORATION SCHEMES.

	Non-QoT-Aware	**QoT-Aware**	**Compound**
Protection Schemes	FF (Lit/Dark) Backup (Sec. III-A) BF (Lit/Dark) Backup (Sec. III-A)	HQ (Lit/Dark) Backup (Sec. III-A) SPALW (Lit/Dark) Backup (Sec. IV-B) MC (Lit/Dark) Backup (Sec. IV-B)	N/A
Restoration Schemes	FF-FF (Sec. III-B) BF-BF (Sec. III-B)	HQ-HQ (Sec. III-B)	HQ-FF (Sec. IV-A) HQ-BF (Sec. IV-A)

the *blue* digraph (directed graph). At the same time another subgraph, which we refer to as the *red* digraph, is generated that is exactly the same as to the blue digraph except that the edge directions are reversed. Half of the available wavelengths, say set Λ_1, are assigned to be used by primary paths on the blue digraph and by protection paths on the red digraph. The remaining set of wavelengths, say set Λ_2, are used to carry primary data on the red digraph and protection data on the blue digraph. Upon arrival, a connection can be routed on either of the two digraphs, using the wavelength set assigned for the primary data on that digraph. In this paper, we use the Shortest Path routing algorithm with First-Fit Wavelength assignment to find the primary path. In case of a link failure, those connections that were using that link on the blue digraph direction, which are using a wavelength in set Λ_1, would be routed on the backup path on the red digraph around that link. Since set Λ_1 was reserved for protection in the red digraph, it would be available for all those connections. The same approach would be followed to protect data on the other digraph.

The backup path for each link is static and can be found offline, hence in case of failure the backup path is already known around each link. In our approach, we assign the shortest path around each link (on the other digraph) for protecting a connection passing that link in each direction. Notice that all the connections on the failed link would follow the same backup path, therefore there is no need for demultiplexing and multiplexing these connections at either end of the failed link.

In the link restoration scheme we study here, arriving calls are routed according to the Shortest Path routing algorithm with First-Fit Wavelength assignment. In case of link failure, for each affected connection we find the shortest available path around that link on the same wavelength the connection is already using. It is obvious that different connections may need to use different restoration paths.

Clearly in both link and path restoration, there exists the possibility that a restoration path cannot be found due to wavelength unavailability. This contributes to the vulnerability ratio of the restoration algorithms and numerical results for it are presented later in the paper.

IV. FAST FAILURE-RECOVERY RWA ALGORITHMS

A. Compound Path Restoration Algorithms

As discussed in the previous section – and the simulation results in the next section support this fact – the HQ-HQ path restoration algorithm has a desirable performance in terms of both blocking probability and vulnerability ratio, but it is computationally intensive and can be slow for time sensitive applications such as streaming voice and video. To have a network with seamless connectivity even in the face of a failure, a high speed restoration algorithm is desirable. Toward this goal, we look at the combination of HQ connection setup and non-QoT-aware restoration schemes. The idea behind this approach is that some delay in connection setup phase can be acceptable, but when a failure happens, connections with time sensitive traffic should be restored as quickly as possible. For this reason we use the HQ algorithm in the call setup phase to gain low blocking probability, but for the restoration phase we use faster schemes.

In the first algorithm we look at, every arriving connection is routed based on the HQ method. In case of a failure, the restoration path for every affected connection is found according to the FF algorithm. We refer to this algorithm as HQ-FF. As opposed to the HQ-HQ method in which the restoration paths are also found according to the HQ algorithm, HQ-FF is expected to be considerably faster. Our simulation result in the next section supports this expectation. In the second approach, we establish the primary path according to the HQ algorithm, and for the restoration paths we use the BF approach. We refer to this algorithm as HQ-BF. The performances of these two proposed algorithms in terms of blocking probability and vulnerability ratio are discussed in Section V-D.

B. Path Protection Algorithms with Low Complexity

In order to avoid the computational complexity of the HQ algorithm even in the connection setup phase, for the applications that need rapid bandwidth provisioning, we first propose the idea of including information about the physical layer in link weights [28]. In this way, a simple shortest path algorithm can implicitly take into account the physical layer characteristics. We introduce the *Shortest Path with Adaptive Link Weights algorithm* (SPALW), a QoT-aware scheme that runs a shortest path algorithm on an adaptive link weight network. The link weights are chosen to represent the physical layer interferences. Three factors contribute to link weights: physical length of the link, wavelength availability of the link, and the number of established connections passing through the link's end nodes.

The physical length of the link accounts for the amplified spontaneous emission (ASE) noise from amplifiers. The longer the physical length is, the more the number of amplifiers are and the stronger the ASE noise is. We denote this factor by L.

Wavelength Availability is a parameter that accounts for the wavelength continuity constraint. In traditional routing techniques, links are weighted according to their length.

However, by assigning higher weights to links with fewer available wavelengths, connections tend to be routed on the links that have more available wavelengths, thereby increasing the chance to meet the wavelength continuity constraint. We define the Wavelength Availability Γ of a link as follows:

$$\Gamma = \frac{\lambda_{Used}}{\lambda_{Total} - \lambda_{Used}}.$$

Thus, when there are no used wavelengths on a link, $\lambda_{Used} = 0$ and $\Gamma = 0$. When all the wavelengths on a link are in use, $\lambda_{Used} = \lambda_{Total}$ and $\Gamma = \infty$.

In our physical layer model, we include impairments due to node crosstalk (optical leaks at the demultiplexers or within the switching fabric in nodes). In [15], three types of crosstalk were introduced, namely, switch port crosstalk, self crosstalk and neighbor crosstalk. Switch port crosstalk comes from the interaction between two connections that traverse the same node on the same wavelength. The other two types of crosstalk (adjacent crosstalk) are only possible if several connections using adjacent wavelengths traverse the same node; the more connections traversing a node, the higher the crosstalk impairments experienced by those calls. For this reason, we include in the link weights the number of established connections at the link's end nodes. We define the established connection quantity at the head node as Q_{Head} and at the tail node Q_{Tail}.

To make these three factors comparable and have the same relative influence on the link weights, three coefficients are defined. We call α the physical length coefficient, β the wavelength availability coefficient, and γ the established connection quantity coefficient. Overall, we define link weights as:

$$\begin{aligned} &Link\ Weight \\ &= \alpha L + \beta\Gamma + \gamma(Q_{Head} + Q_{Tail}) \\ &= \alpha L + \beta\frac{\lambda_{Used}}{\lambda_{Total} - \lambda_{Used}} + \gamma(Q_{Head} + Q_{Tail}) \end{aligned}$$

SPALW selects the path with the minimum weight using a shortest path algorithm in the weighted graph defined above, and assigns the first available wavelength to the connection.

We call our second RWA algorithm "Minimum Crosstalk" (MC). This algorithm is adopted from [15] and is adjusted here for protection purpose. Minimum Crosstalk (MC) is similar to HQ, with a different wavelength picking technique. MC runs a shortest path algorithm for each wavelength (with constant link weights equal to the physical link lengths) to find candidate routes. For each candidate route, the number of crosstalk components along the route is calculated. Since the two types of crosstalk we consider have different leak ratios, we use two coefficients to differentiate their influences. For each route candidate, the crosstalk intensity (CI) on wavelength j is defined as:

$$CI_j = \sum_{i=1}^{N_r} \eta N_i^s + \delta N_i^a,$$

where N_r is the number of nodes on the considered route and wavelength j, N_i^s is the number of connections on the same wavelength at node i, N_i^a is the number of connections on adjacent wavelengths at node i, η is the switch port crosstalk ratio, and δ the adjacent wavelength crosstalk ratio. Among all the candidate routes, the MC algorithm chooses the route with the minimum crosstalk intensity: $CI = \min_j\{CI_j\}$.

It should be noted that the low complexity protection algorithms proposed here only improve the speed in the connection setup phase. In case of a failure, switching impacted connections to their protection paths takes the same time as in path protection algorithms presented earlier (for lit backup or dark backup schemes, respectively).

TABLE II
PHYSICAL PARAMETERS FOR THE SIMULATED NETWORK.

Description	Value
Span length	70 km
Signal peak power	2 mW
Bit duration	100 ps (10 Gbps)
Pulse shape	NRZ
Fabric crosstalk	-40 dB
Adj. port crosstalk	-30 dB
Non adj. port crosstalk	-60 dB
Adj. Wavelength crosstalk	-25 dB
Fiber loss	0.2 dB/km
Nonlinear coefficient	2.2 (W km)$^{-1}$
Linear dispersion	17 ps/nm/km
Dispersion compensation	100% post-DC
ASE noise factor	2
Receiver electrical bandwidth	7 GHz
Number of wavelengths	8
Minimum Q factor	6

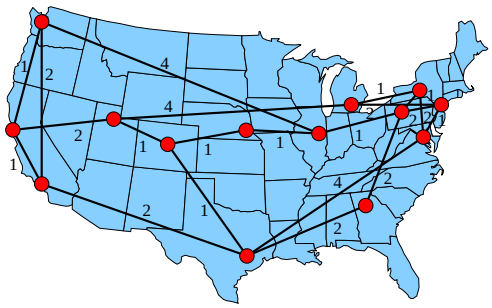

Fig. 2. **Topology used in the simulations.** We used a downscaled version of the NSF net topology (14 nodes, 21 bidirectional links) to perform our simulations. The link weights on the figure correspond to the number of 70 km long fiber spans.

V. SIMULATION RESULTS

A. Simulation Model

To evaluate our algorithms, we use the NSF topology depicted in Fig. 2, as an example of a mesh topology. We downscale the NSF topology (originally a continental-size network) by a factor of 10, resulting in a regional-size network. Continental-size networks require intermediate electrical regeneration: indeed, even considering ISI and noise only and ignoring network state-dependent impairments (nonlinear and node crosstalks), it is not possible to transmit signals over more than roughly 1000 km with standard techniques[5] while achieving adequate QoT ($BER < 10^{-9}$, corresponding to a Q factor of 6) [5]. The regional network we consider, on

[5]Note that link distances longer than 1000 km are achievable using optimized long-haul link design and components.

the contrary, exhibits milder impairments that are low enough to guarantee that, at low loads (and hence when no or low crosstalk occurs), any node is reachable from any other node while maintaining adequate QoT. At higher loads, interchannel and node crosstalks become disruptive but their effects are mitigated by QoT-aware RWA algorithms such as HQ, as shown below. For simplicity, we modified the NSF topology such that each link consists of an integer number of 70-km fiber spans.

The physical parameters for the simulated network are summarized in Table II; the values used are typical for modeling next-generation regional-size all-optical networks. The high attenuation for non-adjacent port crosstalk we used essentially means that we ignored it; indeed, in practice, the main leaks at the demultiplexers come from adjacent wavelength channels. The typical value for switch port crosstalk ratio and adjacent wavelength crosstalk ratio are -30dB and -25dB, therefore the parameters of the MC algorithm are $\eta = 10^{-30dB/10} = 0.001$ and $\delta = 10^{-25dB/10} = 0.0032$. We used $\alpha = 1$, $\beta = 100$, and $\gamma = 2$ in SPALW. Calls are assumed to arrive according to a Poisson process and have exponentially distributed holding times with unit mean. The results for each simulation run are averaged over 5000 connection arrivals. The source and destination nodes of a connection are randomly (uniformly) selected. The network load is thus the total arrival rate of calls to the network.

B. Performance Evaluation: Blocking

First we look at the path and link protection schemes. The wavelength blocking probability, which is only due to unavailability of wavelength and does not take into account the quality of the received signal, is shown in Fig. 3. One noticeable observation here is that the link protection scheme has much lower wavelength blocking probability than path protection schemes. This can be explained as follows. In path protection schemes, for each requested connection a working path and a link-disjoint backup path are reserved. This means that considering all shortest paths between all source-destination pairs in the network, only half of the wavelengths are available to set up a working path. But in the link protection scheme we consider here, on each digraph half of the wavelength set is available for the working path, and in case no free wavelength is found, the connection would search on the working wavelength set on the other digraph (notice that considering any of the two digraphs alone, the network is still fully connected). Intuitively speaking, in the link protection scheme a larger number of wavelengths are available to an arriving connection. This is achieved at the cost of longer paths and, as we will see next, has negative result on the quality of the received signal and induces a high vulnerability to failure.

One other observation is the lower wavelength blocking of the lit backup scheme in all RWA algorithms. The reason is that in lit backup schemes (as we will see in Fig. 4) more connections are blocked due to the low quality of their received signals, therefore more free wavelengths are available for the new arrivals. In this graph, we also see that the wavelength blocking probabilities of BF and HQ path protection algorithms are in the same range and all are lower than that of FF schemes. This is due to the fact that BF and HQ search for the shortest path on *all* available wavelengths but FF finds the shortest path, then tries to find an available wavelength on that path.

Next we look at the total blocking probability[6] of protection schemes, depicted in Fig. 4. Considering the lower offered load values, the lit backup protection scheme has much worse performance than the dark backup one. This is due to the increased interference caused by lighting up the backup paths, and consequently deteriorating the quality of newly arriving connections. The lower blocking probability of the dark backup scheme can be weighted against its slower traffic restoration compared to the lit backup scenario.[7] We can also see that while the link protection scheme has a better wavelength blocking probability, it exhibits much higher blocking probability when we take QoT into account. This is due to the fact that in this scenario the route of a connection is to be found in one or the other of the two digraphs, therefore it may not be the shortest path. Increasing the path length leads to more noise and crosstalk in more intermediate nodes and finally lower quality of the signal at the receiver.

In this graph, we also consider the cross-layer (or QoT-aware) path protection algorithm HQ, and as we can see, it significantly improves the performance of both lit and dark backup scheme. We also see that the HQ lit backup algorithm even outperforms the FF dark backup scheme. Best-Fit dark backup algorithm also shows very good performance which is the consequence of combining the low wavelength blocking of the BF algorithm and good performance of the dark backup scheme. At higher loads, all algorithms become wavelength-blocking limited, and there is little that QoT-aware algorithms, including HQ, can do to improve performance.

The wavelength blocking probability of the restoration algorithms are shown in Fig. 5. The FF-FF path restoration and link restoration have the same blocking probability because they behave the same way in the call setup phase. This graph shows that BF wavelength assignment leads to much lower wavelength blocking than FF (notice that regarding wavelength availability, BF and HQ have the same performance). But as for the total blocking probability, which includes QoT-blocking, we see from Fig. 6 that the BF scheme is much less advantageous. It can be seen that the proposed HQ-HQ path restoration algorithm strongly outperforms other algorithms in the presence of physical layer impairments, which supports the idea of using cross layer approaches in all-optical network design. This advantage comes at a cost of increased time complexity, which is discussed later in the paper.

C. Performance Evaluation: Vulnerability

We now look at the vulnerability ratio as an indication of the capability of these algorithms to recover from a failure. Recall that the vulnerability ratio is the probability that a random

[6]Note that P(blocking) = P(wavelength blocking) + [1 – P(wavelength blocking)] P(QoT blocking). Thus, the total blocking probability is *not* the sum of the wavelength and QoT blocking probabilities.

[7]Restoration time analysis is out of the scope of this paper.

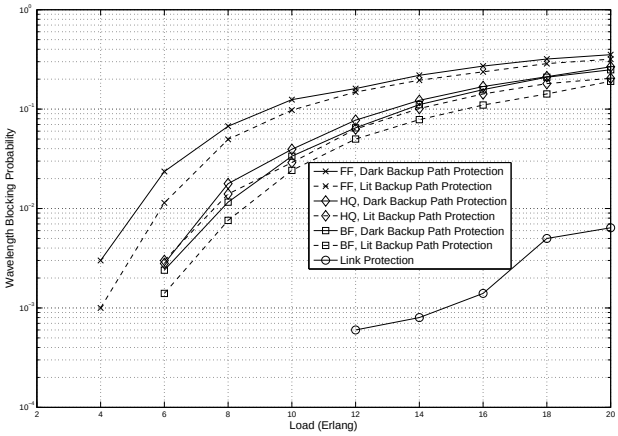

Fig. 3. Wavelength blocking probability vs. traffic load for protection algorithms.

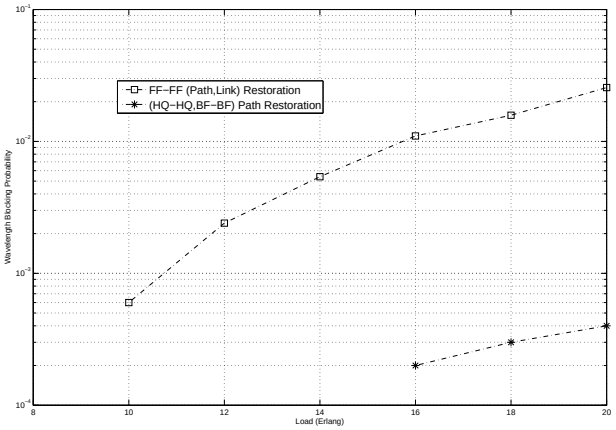

Fig. 5. Wavelength blocking probability vs. traffic load for restoration algorithms.

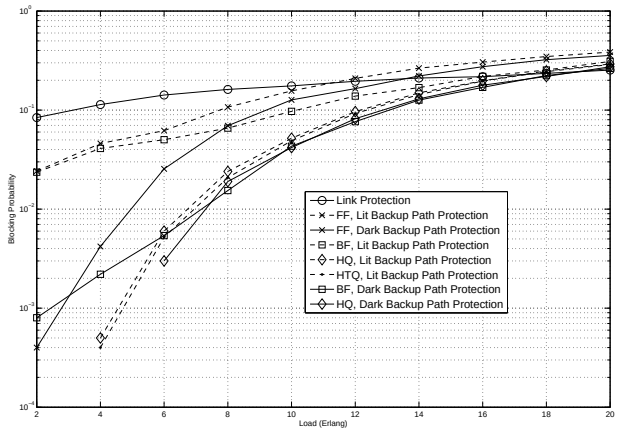

Fig. 4. Total blocking probability vs. traffic load for protection algorithms.

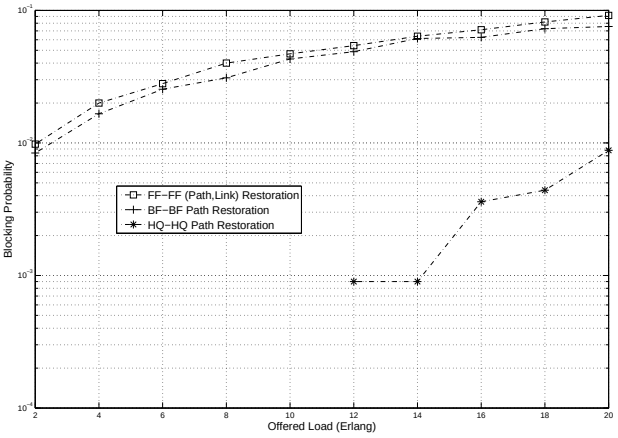

Fig. 6. Total blocking probability vs. traffic load for restoration algorithms.

ongoing connection (at the time of failure) cannot be restored due to unacceptable QoT (or even unavailability of lightpath in the case of restoration), if a random link fails at a random point of time during the operation of the network.

First we look at the vulnerability ratio of protection schemes, shown in Fig. 7. When connections affected by a failure start using their backup paths, the backup paths for a fraction of these connections may not have adequate QoT (the only reason why a connection would not be restored in the lit backup path case) or they may even influence other lightpaths (in the case of dark backup path protection and link protection).

In the low offered load range (below 10 Erlangs), we see that the link protection scheme has the highest vulnerability. This is again due to the long primary paths used in this scheme, which makes them highly exposed to the interference caused by lighting up the backup path for the failed link. In this load range, we see that again the HQ algorithm improves the performance due to its capability of providing higher Q factor margin for each connection in the setup phase by carefully spreading wavelengths out over the network. When a random link failure happens, although interference may increase due to the protection scheme, the path signal quality represented by its Q factor could still remain above the required threshold, though decreased. From another perspective, HQ improves the vulnerability ratio over FF by a larger margin for the lit backup scheme than for the dark backup scheme. This is because in the lit backup scheme, HQ knows the backup path's signal quality, so that it can take measures to alleviate its interference with others. In the dark backup scheme, the backup path is lit only when a failure happens and it is impossible for HQ to predict the interference that the dark backup paths are going to introduce when they are lit. Moreover, we see that the BF algorithm provides no improvement over the FF algorithm, due to the fact that the non-QoT aware BF RWA is not able to intelligently spread out the connections over the network, as opposed to HQ. This shows that cross-layer algorithms are capable of reducing the vulnerability more than just through a more efficient wavelength assignment.

We see from Fig. 7 that as the offered load to the net-

work increases toward 9 Erlangs and there are more ongoing connections spread out over the entire network, the HQ algorithm cannot improve the performance by finding better paths because there is too much interference on all candidate paths. Indeed, at higher offered loads, HQ has a negative impact. This phenomenon can be explained by the fact that HQ, by providing lower blocking probability, admits more connections into the network, which in turn greatly increases the vulnerability of the network to a failure, and since there are already too many connections spread all over the network, HQ cannot be of much help in the recovery phase. The same argument explains the higher vulnerability of BF compared to FF as the load increases. In general, in these load ranges, the network does not have a good performance in terms of both blocking probability and vulnerability ratio and the network operators should avoid these operating regions.

The vulnerability ratio for restoration algorithms is plotted in Fig. 8. One interesting observation here is that even the non-QoT-aware path restoration algorithms have vulnerability ratios at the same level as the dark backup path protection, and significantly lower than the lit backup protection schemes (either QoT-aware or non-QoT-aware ones; see Fig. 7). In theory we can argue that by reserving some resources for protection, we may encounter higher blocking probability but the network can be guaranteed to recover from failure. But we see that in fact where the physical layer has impairments, this argument is not true and a naive approach to resource reservation would even increase the vulnerability of the network to failure. In the same way, we can see that link restoration has lower vulnerability compared to link protection.

These results also show that adding QoT awareness to the path restoration scheme by using HQ for initial call setup and finding the restoration path, in other words using HQ-HQ path restoration, further decreases the vulnerability ratio of the network significantly. It is obvious that the restoration algorithms may not be able to recover the affected connections from a failure due to the unavailability of wavelengths. The probability of such an event, called the "wavelength vulnerability ratio", is shown in Fig. 9. Note that this probability is zero for the protection algorithms (because backup wavelengths are *reserved* at the time of call setup) and is included in the computation of the vulnerability ratio shown in Fig. 8 for the restoration algorithms.

D. Performance of the High Speed Algorithms

So far we have seen the advantages of HQ in protection and restoration schemes in terms of both blocking probability and vulnerability ratio. As was discussed earlier, the drawback of HQ is its high computation time. Next we look at the performance of the proposed high speed algorithms.

Fig. 10 shows the blocking probability for the high speed algorithms proposed in Section IV. We see that the HQ-FF and HQ-BF as well as HQ-HQ path restoration algorithms enjoy a very low blocking probability. Note that these three algorithms behave exactly the same way in the call setup phase, therefore they have the same blocking probability. Also we observe that SPALW and MC both have lower blocking

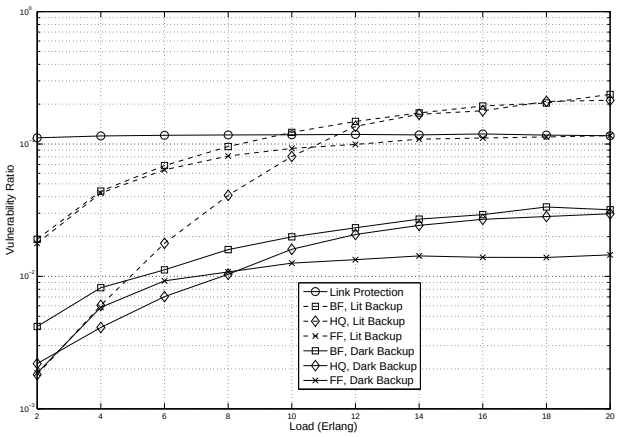

Fig. 7. Vulnerability ratio vs. traffic load for protection algorithms.

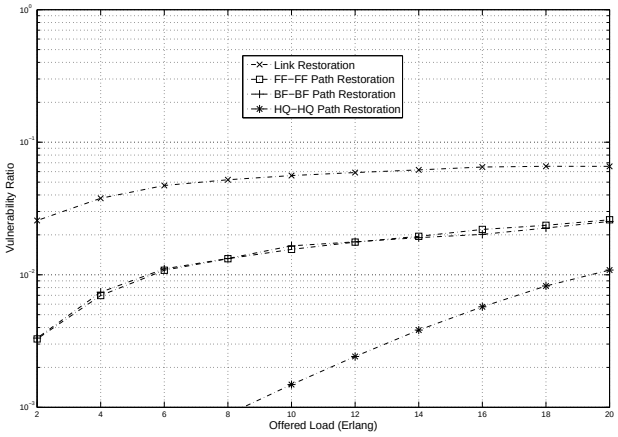

Fig. 8. Vulnerability ratio vs. traffic load for restoration algorithms.

probability than FF path protection schemes (see Fig. 4) and in the higher traffic load region, their performance is similar to the HQ path protection schemes (in dark or lit back up cases, respectively; the curve for the dark backup case is repeated here for comparison).

Looking at the vulnerability ratio in Fig. 11, we see that the HQ-BF and HQ-FF path restoration algorithms, SPALW, MC dark backup path protection algorithms perform in the same range and have vulnerability ratios close to that of the HQ dark backup scheme, while lit back up path protection algorithms are more vulnerable to a failure.

Fig. 12 shows the processing time[8] for the restoration algorithms. Here we can see the high time complexity of HQ-HQ path restoration, and that the compound algorithms

[8]The processing time here is the total simulation time. As was mentioned earlier, in order to measure the vulnerability ratio, any time the network state changes (either a connection arrival or departure occurs) we fail all the links in the network one by one and compute the number of ongoing connections that cannot be restored, and then average over all link failures. Thus, this measured time is only for comparing the time complexity of the algorithms to one another, and does not directly measure call setup times of each algorithm. The simulation is run on an unloaded general purpose computer.

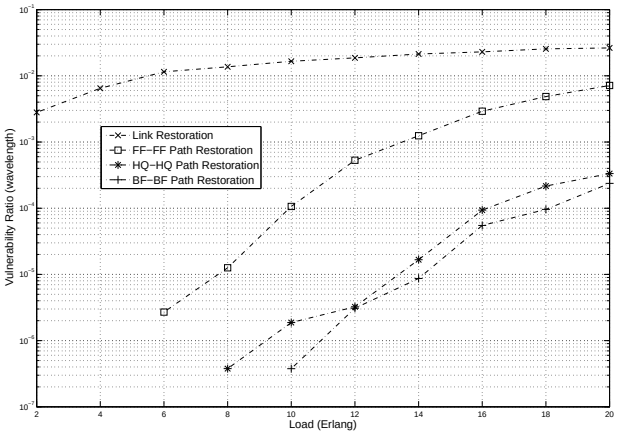

Fig. 9. Wavelength vulnerability ratio vs. traffic load for restoration algorithms.

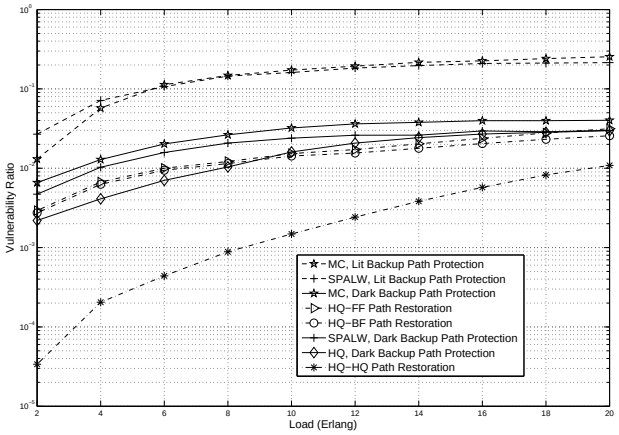

Fig. 11. Vulnerability ratio vs. traffic load for high speed algorithms.

produce significant improvements and are almost as fast as non-QoT-aware algorithms. Fig. 13 shows the processing time for the protection schemes. Here also we see the improvements in time complexity caused by the SPALW and MC algorithms compared to the HQ path protection. These results show the performance trade offs between these algorithms and, depending on the particular application, how the right one should be chosen.

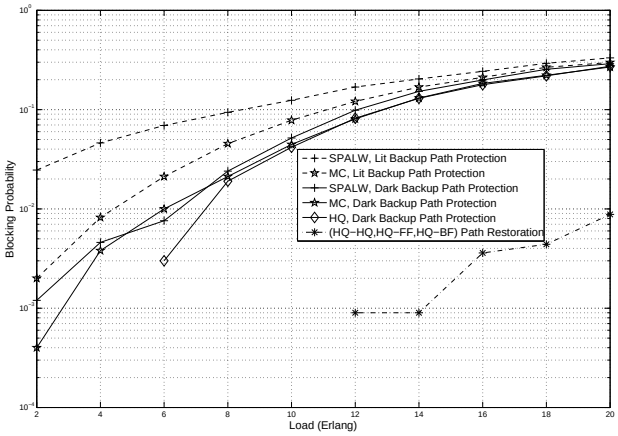

Fig. 10. Blocking probability vs. traffic load for high speed algorithms.

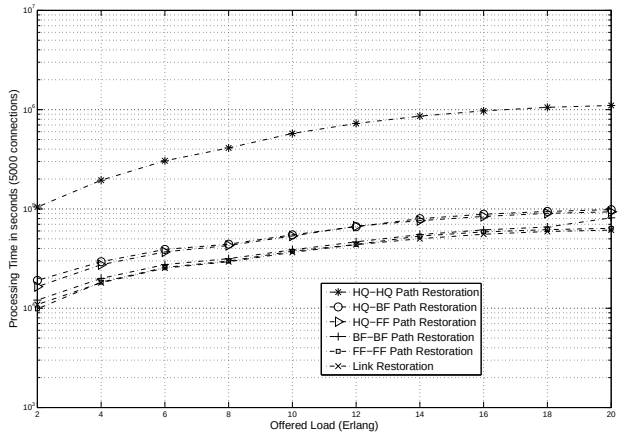

Fig. 12. Time complexity vs. traffic load for restoration algorithms.

VI. Conclusions

In this work, the problem of survivable all-optical network design has been addressed from a new viewpoint – namely, the consideration of physical layer impairments – that raised some questions on the validity of the traditional approaches in next generation all-optical networks. We saw some unexpected results, such as similar vulnerability ratios for path *protection* and *restoration* schemes, which stem from neglecting the physical layer impacts on the performance of higher level algorithms. The new cross-layer algorithms proposed in this work significantly mitigate the physical layer impairment effects on network survivability.

The QoT-aware algorithms, if not designed deliberately, can be computationally intensive. This issue was also addressed in this work and compound QoT-aware setup/non-QoT-aware restoration algorithms, and two simpler yet powerful QoT-aware path protection algorithms were proposed.

Our work can be extended to include other schemes, such as shared path protection. The optimization framework in this case should consider the physical layer characteristics in order to lead to algorithms with good performance in all-optical networks. Time complexity analysis for restoration algorithms that considers the necessary signaling delays is also a topic for future study.

References

[1] Y. Zhai, Y. Pointurier, S. Subramaniam, and M. Brandt-Pearce, "QoS-aware RWA algorithms for path-protected networks," in *Proceedings of the IEEE/OSA Optical Fiber Conference (OFC)*, Anaheim, CA, USA, Mar. 2007.

[2] ——, "Performance of dedicated path protection in transmission-impaired DWDM networks," in *Proceedings of the IEEE International Conference on Communications (ICC)*, Glasgow, Scotland, Jun. 2007.

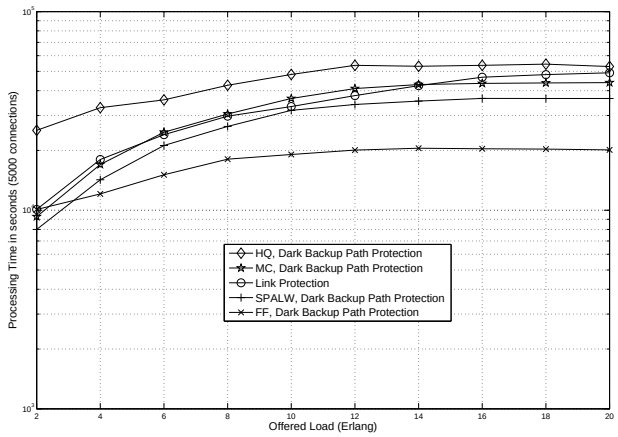

Fig. 13. Time complexity vs. traffic load for protection algorithms.

[3] A. Askarian, Y. Zhai, S. Subramaniam, Y. Pointurier, and M. Brandt-Pearce, "Protection and restoration from link failure in DWDM networks: A cross-layer study," in *Proceedings of the IEEE International Conference on Communications (ICC)*, Beijing, China, May 2008.

[4] ——, "QoT-aware RWA algorithms for fast failure recovery in all-optical networks," in *Proceedings of the IEEE/OSA Optical Fiber Conference (OFC)*, San Diego, CA, USA, Feb. 2008.

[5] Y. Pointurier, M. Brandt-Pearce, S. Subramaniam, and B. Xu, "Cross-layer adaptive routing and wavelength assignment in all-optical networks," *IEEE Journal on Selected Areas in Communications*, vol. 26, no. 6, pp. 32–44, Aug. 2008.

[6] J. Strand, A. Chiu, and R. Tkach, "Issues for routing in the optical layer," *IEEE Commun. Mag.*, vol. 39, no. 2, pp. 81–87, Feb. 2001.

[7] D. Zhou and S. Subramaniam, "Survivability in optical networks," *IEEE Network Magazine*, vol. 14, no. 6, Nov./Dec. 2000.

[8] S. Ramamurthy and B. Mukherjee, "Survivable WDM mesh networks, part I – protection," in *Proceedings of the IEEE Conference on Computer Communications (INFOCOM)*, 1999, pp. 744–751.

[9] ——, "Survivable WDM mesh networks, part II – restoration,," in *Proceedings of the IEEE International Conference on Communications (ICC)*, 1999, pp. 2023–2030.

[10] B. Ramamurthy, D. Datta, H. Feng, J. Heritage, and B. Mukherjee, "Impact of transmission impairments on the teletraffic performance of wavelength-routed optical networks," *J. Lightw. Technol.*, vol. 17, no. 10, pp. 1713–1723, Oct. 1999.

[11] J. Martins-Filho, C. Bastos-Filho, E. Arantes, S. Oliveira, L. Coelho, J. de Oliveira, R. Dante, E. Fontana, and F. Nunes, "Novel routing algorithm for transparent optical networks based on noise figure and amplifier saturation," in *Proceedings of the IEEE International Microwave and Optoelectronics Conference (IMOC)*, vol. 2, 2003, pp. 919–923.

[12] D. Penninckx and C. Perret, "New physical analysis of 10-Gb/s transparent optical networks," *IEEE Photon. Technol. Lett.*, vol. 15, no. 5, pp. 778–780, May 2003.

[13] A. Jukan and G. Franzl, "Path selection methods with multiple constraints in service-guaranteed WDM networks," *IEEE/ACM Trans. Netw.*, vol. 12, no. 1, pp. 59–72, Feb. 2004.

[14] J. He and M. Brandt-Pearce, "RWA using wavelength ordering for crosstalk limited networks," in *Proceedings of the IEEE/OSA Optical Fiber Conference (OFC)*, Anaheim, CA, USA, Mar 2006.

[15] T. Deng, S. Subramaniam, and J. Xu, "Crosstalk-aware wavelength assignment in dynamic wavelength-routed optical networks," in *Proceedings of the IEEE International Conference on Broadband Networks (Broadnets)*, Oct 2004, pp. 140–149.

[16] J. He and M. Brandt-Pearce, "Dynamic wavelength assignment using wavelength spectrum separation for crosstalk limited networks," in *Proceedings of the IEEE International Conference on Broadband Networks (Broadnets)*, San Jose, CA, USA, 2006.

[17] Y. Huang, J. Heritage, and B. Mukherjee, "Connection provisioning with transmission impairment consideration in optical WDM networks with high-speed channels," *J. Lightw. Technol.*, vol. 23, no. 3, pp. 982–993, Mar. 2005.

[18] I. Tomkos, S. Sygletos, A. Tzanakaki, and G. Markidis, "Impairment constraint based routing in mesh optical networks," in *Proceedings of the IEEE/OSA Optical Fiber Conference (OFC)*, Anaheim, CA, USA, Mar. 2007.

[19] N. Zulkifli and K. Guild, "Moving toward upgradeable all-optical networks through impairment-aware RWA algorithms," in *Proceedings of the IEEE/OSA Optical Fiber Conference (OFC)*, Anaheim, CA, USA, Mar. 2007.

[20] X. Yang, L. Shen, and B. Ramamurthy, "Survivable lightpath provisioning in WDM mesh networks under shared path protection and signal quality constraints," *J. Lightw. Technol.*, vol. 23, no. 4, pp. 1556–1567, Apr. 2005.

[21] I. Chlamtac, A. Ganz, and G. Karmi, "Lightpath communications: a novel approach to high bandwidth optical WANs," *IEEE Trans. Commun.*, vol. 40, no. 7, pp. 1171–1182, Jul. 1992.

[22] G. Agrawal, *Fiber-Optic Communications Systems*. John Wiley & Sons, Inc., 2002.

[23] B. Mukherjee, "WDM optical communication networks: Progress and challenges," *IEEE J. Sel. Areas Commun.*, vol. 18, no. 10, pp. 1810–1824, Oct. 2000.

[24] B. Xu and M. Brandt-Pearce, "Analysis of noise amplification by a CW pump signal due to fiber nonlinearity," *IEEE Photon. Technol. Lett.*, vol. 16, no. 4, pp. 1062–1064, Apr. 2004.

[25] Y. Pointurier and M. Brandt-Pearce, "Study of crosstalk enhancement by fiber nonlinearity in all-optical networks using perturbation theory," *J. Lightw. Technol.*, pp. 4074–4083, December 2005.

[26] B. Xu and M. Brandt-Pearce, "Comparison of FWM- and XPM-induced crosstalk using the Volterra Series Transfer Function method," *J. Lightw. Technol.*, vol. 21, no. 1, pp. 40–53, Jan. 2003.

[27] M. Medard, R. A. Barry, S. G. Finn, W. He, and S. Lumetta, "Generalized loop-back recovery in optical mesh networks," *IEEE/ACM Trans. Netw.*, vol. 10, no. 1, pp. 153–164, Feb. 2002.

[28] T. Deng and S. Subramaniam, "Adaptive QoS routing in dynamic wavelength-routed optical networks," in *Proceedings of the IEEE International Conference on Broadband Networks (Broadnets)*, Oct 2005, pp. 184–193.