Exploiting Excess Capacity, Part II: Differentiated Services Under Traffic Growth

Ferhat Dikbiyik, *Member, IEEE*, Massimo Tornatore, *Senior Member, IEEE*, and Biswanath Mukherjee, *Fellow, IEEE*

***Abstract*—Connections provisioned in a backbone network are usually protected. A "good" protection scheme can decrease the downtime experienced by a connection, which can reduce (or eliminate) penalties for the violation of the Service Level Agreement (SLA) between the network operator and its customer. Although "good" protection schemes can guarantee high availability to connections, they usually require high capacity (e.g., bandwidth). However, backbone networks usually have some excess capacity (EC) to accommodate traffic fluctuations and growth, and when there is enough EC, the high capacity requirement of protection schemes can be tolerated. However, under traffic growth, the network operator has to add more bandwidth to avoid capacity exhaustion, which increases upgrade costs. In this study, we show that, in case of connections supporting differentiated services, where connections' tolerable downtimes are diverse, efficient exploitation of EC can decrease both SLA violations and upgrade costs. We develop a novel EC management (ECM) approach that provides high-availability high-capacity protection schemes when EC is available, and reprovisions backup resources with multiple protection schemes so that SLAs are still respected, but network upgrade costs are kept under control. We formulate this problem as an integer linear program (ILP) and develop an efficient heuristic as the ILP is intractable for large problems. We present several alternatives of our ECM approach to show its compatibility with different protection-scheme combinations. Numerical examples are presented to illustrate how the proposed ECM technique finds a tradeoff between upgrade costs and penalties paid for SLA violations while reducing the total cost significantly.**

***Index Terms*—Excess capacity, network upgrade, reprovisioning, Service Level Agreement (SLA) violation, telecom network, traffic growth.**

I. Introduction

IS A protection scheme that provides high availability to connections (provisioned in a telecom network) always better? Surely, a high-availability protection scheme, which can decrease downtimes experienced by connections and therefore can reduce (or even eliminate) Service Level Agreement (SLA) violations, is highly desirable. However, providing such high availability usually requires high capacity (e.g., bandwidth) consumption and requires the network operator (NO) to upgrade the network by often adding bandwidth to avoid capacity exhaustion, especially under sustained traffic growth. Thus, in the context of a telecom network, providing the right level of protection to connections presents a tradeoff between SLA violations and upgrade costs.

A possible way to address such a tradeoff between SLA violation and upgrade cost consists in altering the connections' protection schemes based on the available amount of *excess capacity* (EC). In this study, we consider that backbone mesh networks typically have EC, i.e., the unused capacity which any operational network usually has to accommodate traffic fluctuations and to provision new connections. Connections can be provisioned by high-availability high-capacity protection schemes when the network has a large amount of EC and, when EC becomes low, they can be switched to low-availability low-capacity protection schemes.

In [1], we proposed an EC management scheme that improves network robustness in terms of various SLA specifications. Here, we extend our work with the consideration of service differentiation and upgrade costs because, in case of a network supporting differentiated services, the connections' tolerable downtimes may be different and the values of the tolerable downtimes may change in time. Thus, in this study, we investigate a new EC management scheme that exploits EC dynamically to decrease costs to the network operator in terms of both SLA violations and upgrade costs, while meeting the connections' diversified downtime requirements. Note that while services are traditionally differentiated from a quality-of-service (QoS) perspective (e.g., [2]), here we consider differentiation from protection perspective, where connections are provisioned by a certain protection scheme depending on their initial requirements (e.g., availability target) and switched to high- or low-availability protection schemes (by reprovisioning backup resources) depending on their changing tolerable downtimes and amount of EC available at a given time.

A. Related Work

Service differentiation in terms of reliability requirements of connections has been defined in [3] and [4], and several others have studied routing of connections considering differentiated reliability (DiR) [5]–[10] or availability [11], [12]. Some of these works (e.g., [5]–[8]) consider provisioning connections with a differentiated reliability guarantees against single-link failures, and some others consider the case where a network

Manuscript received March 26, 2013; revised January 29, 2014; accepted June 28, 2014; approved by IEEE/ACM TRANSACTIONS ON NETWORKING Editor A. Walid. Date of publication July 16, 2014; date of current version October 13, 2015. This work was supported by the Defense Threat Reduction Agency (DTRA) under Grant No. HDTRA1-08-10-BRCWMD. Preliminary versions of this work were presented at Photonics in Switching (PS), Monterey, CA, USA, July 25–28, 2010, and the IEEE International Conference on Advanced Networks and Telecommunications Systems (ANTS), Mumbai, India, December 16–18, 2010.

F. Dikbiyik was with the University of California, Davis, Davis, CA 95616 USA. He is now with the Department of Computer Engineering, Sakarya University, Sakarya 54187, Turkey (e-mail: fdikbiyik@sakarya.edu.tr).

M. Tornatore is with the University of California, Davis, Davis, CA 95616 USA, and also with the Politecnico di Milano, 20133 Milan, Italy (e-mail: tornator@elet.polimi.it).

B. Mukherjee is with the University of California, Davis, Davis, CA 95616 USA (e-mail: bmukherjee@ucdavis.edu).

Color versions of one or more of the figures in this paper are available online at http://ieeexplore.ieee.org.

Digital Object Identifier 10.1109/TNET.2014.2335252

link fails independently. For instance, [9] defines the concept of quality-of-protection (QoP), i.e., the probability of a connection to survive a failure under a specific protection, [10] considers different protection schemes for different IP services in an IP-over-WDM network, and [11] and [12] consider provisioning connections on the paths that satisfy their availability requirements. All these works focus on the initial reliability/availability requirements of connections. However, reliability/protection needs may change in time because connections' tolerable downtimes change due to failures, and the network operator should reactively respond to these changes.

There are some works that consider the changing needs of connections [13]–[16]. Reference [13] considers a low-availability low-capacity protection scheme, namely shared-path protection, such that, while admitting a new connection, the network operator recalculates SLA requirements of existing connections based on their remaining holding times and downtimes, and adjusts the sharing of backup resources to meet the new connection's SLA requirements. Other works [14]–[16] consider *backup reprovisioning* (e.g., [17]–[22]) to reoptimize backup resources because of network state changes (e.g., link failure). References [14] and [15] focus on ring networks, and [16] focuses on mesh networks, and they prioritize services by monitoring the downtime experienced by connections and reprovision backup resources to provide protection to connections that are close to violating (or have already violated) their SLA and left others unprotected. These studies consider to provide protection/no protection options (e.g., [16]) or low-availability low-capacity protection schemes (e.g., [13]) to get benefit of low resource consumption, while avoiding to violate connections' SLAs. However, we note that EC can be exploited to provide better protection to connections and to jointly address the connections' changing protection requirements and capacity exhaustion.

Exploiting EC has been investigated in some studies (e.g., [1], [23], and [24]), but it is a fairly unexplored field. Reference [23] proposes an EC management scheme to meet SLA requirements by employing a borrowing/lending bandwidth scheme. Reference [24] proposes to exploit EC by provisioning additional backup paths to increase availability. In general, EC is exploited to provide improved management of backup resources.

B. Our Contribution

In this study, we focus on protection schemes that guarantee 100% protection against single-link failures and provide different levels of availability to connections. Thus, we consider *different* protection schemes that we put in two categories: 1) high-availability (and high-capacity), and 2) low-availability (and low-capacity) protection schemes that provide different level of availability against multiple failures.

In the admission process, connections can enjoy high-availability protection if EC in the network is large. When the network state changes under traffic growth, the requirements of connections may also change depending on their downtime tolerances. Reprovisioning of backup resources can readjust the connections' availabilities (by altering their protection schemes), increase EC in the network, and avoid early upgrades. Thus, proper utilization of EC can play a very crucial role for service differentiation in terms of protection needs and for smooth capacity upgrade (i.e., balancing between SLA violations and upgrade costs).

In our work, for the first time, we consider to exploit EC to provide different levels of availability to support differentiated services with different protection schemes, while keeping the upgrade costs under control. Note that our approach is applicable to general mesh networks. However, we focus on optical wavelength-division multiplexing (WDM) networks as telecom backbone networks, and we assume that a connection requires a full wavelength channel.

This paper is organized as follows. In Section II, we survey different protection schemes to compare their effects on SLA violation and upgrade cost. We propose our EC management approach in Section III and alternative ECM schemes in Section IV. We evaluate our proposed schemes in Section V and conclude the study in Section VI.

II. Protection Schemes

In this study, we explore the opportunities to exploit the tradeoffs (i.e., high availability versus low bandwidth) of different protection schemes based on the connections' initial requirements and their changing tolerable downtimes after network failures. To explore these tradeoffs, we compare different protection schemes in terms of connection availability and capacity requirement. We consider three different protections: Dedicated Link Protection (DLP), where each link on a connection's primary path is protected by a dedicated path; $1 + N$ protection, where the primary path of a connection is protected by N link-disjoint backup paths; and Shared Path Protection (SPP), where a primary path is protected by a backup path and backup resources are shared among connections.

There are several studies [1], [25]–[28] that analyze and compare these protection schemes and can give information about the availability provided and their resource consumption. Numerical examples conducted on a US-wide network in [1] show that, for typical parameters, DLP can provide 0.99999 availability to connections, while $1+1$ provides 0.99998 availability, and SPP's availability varies between 0.999 and 0.9998, depending on amount of sharing. The same study also showed that the capacity required for DLP and $1 + 1$ are 3.3 and 2.5 times of the capacity required for SPP, on average. Reference [25] states similar numbers for resource consumption, e.g., capacity required for DLP and $1 + 1$ are 2.8 and 1.6 times of capacity requirement of SPP. Reference [26] evaluates that the average number of connections down when two simultaneous link failures occur for SPP is 1.39 times the down connections for $1 + 1$ (in a 15-node mesh network). The same study shows that capacity required for $1 + 1$ is 1.2 times higher than the capacity required for SPP. References [27] and [28] confirm that $1 + 1$ shows higher availability than SPP, and [28] also shows that availability increases for $1 + N$ with increasing N, and it decreases when sharing increases. Thus, we can classify DLP and $1 + N$ as high-capacity high-availability protections, and SPP as a low-availability low-capacity protection.

III. Excess Capacity Management (ECM)

The amount of EC in the network fluctuates, in the near form as the traffic fluctuates and in the longer term as network resources get close to be exhausted by traffic growth (EC decreases) or as new network resources get increased by

network upgrades (EC increases). EC can be exploited by admitting connections using high-availability protection schemes according to the amount of EC in the network and SLA requirements of connections. When a connection arrives, we consider DLP as the first choice to provide high-availability protection because DLP meets high service expectations better than $1+1$ and SPP.[1] If network resources are not enough to provide DLP to the connection, the next option is $1+1$. However, EC might not be enough to provide a high-availability protection to the connection request, then EC should be managed properly to accept the connection while the existing connections' different protection requirements are respected. In this scenario, our ECM scheme addresses the following questions.

1) If EC does not suffice to provide high-availability protection to the connection request, should the connection be protected by a *low-availability protection* scheme or should EC be increased by *reprovisioning* to provide high-availability protection to the connection request?
2) If reprovisioning is required, how can one *match existing connections' different protection needs and current EC* in the network?
3) After reprovisioning, if EC is not sufficient to provide protection to the connection, is an *early upgrade* of network capacity required?
4) If the connection is successfully established, is *proactive reprovisioning* still required to avoid capacity exhaustion?

Fig. 1 is a flowchart of the ECM, and details are as follows.

A. Low-Availability Protection or Reprovisioning

A low-availability protection scheme, e.g., SPP in our ECM approach, may provide sufficient availability to the connection to avoid SLA violations. An NO can determine if SPP meets the requested connection's availability requirement (A_t) by using an availability threshold $(A_{\rm th})$ (i.e., comparing the connection availability target to the average availability provided to the connections with SPP in the past). However, decision of $A_{\rm th}$ is not straightforward because availability provided by SPP depends on network load (e.g., amount of sharing) and network's state (e.g., downtimes experienced by connections) both change in time. Thus, $A_{\rm th}$ needs to be dynamic. For instance, the NO can update $A_{\rm th}$ periodically. The long-term average availability provided by SPP might be a reasonable choice for $A_{\rm th}$, but the amount of sharing and the network's state change with failures, traffic growth, and network upgrades. Thus, the most current values tend to better reflect the state of the process. An estimate that places more emphasis on the most recent data would therefore be more useful. Hence, we use an *exponentially weighted moving average*[2] (EWMA). The estimate $A_{\rm th}$ in period $(\tau+1)$ is given by

$$A_{\rm th}(\tau+1)=\begin{cases} A_{\rm th}(\tau)(1-\rho)+\overline{A}(\tau)\rho, & \text{if } \overline{A}(\tau)>0 \\ A_{\rm th}(\tau), & \text{if } \overline{A}(\tau)=0 \end{cases} \quad (1)$$

[1] $1+N$ (where $N>1$) can provide availability as high as DLP, but it might not be always feasible to find $1+N$ link-disjoint paths.

[2] A type of infinite impulse response filter that applies weighting factors that decrease exponentially (i.e., the weighting for each older datum point decreases exponentially, never reaching zero). This concept is commonly used for noise reduction in the process industries and round-trip-time estimation in TCP algorithms.

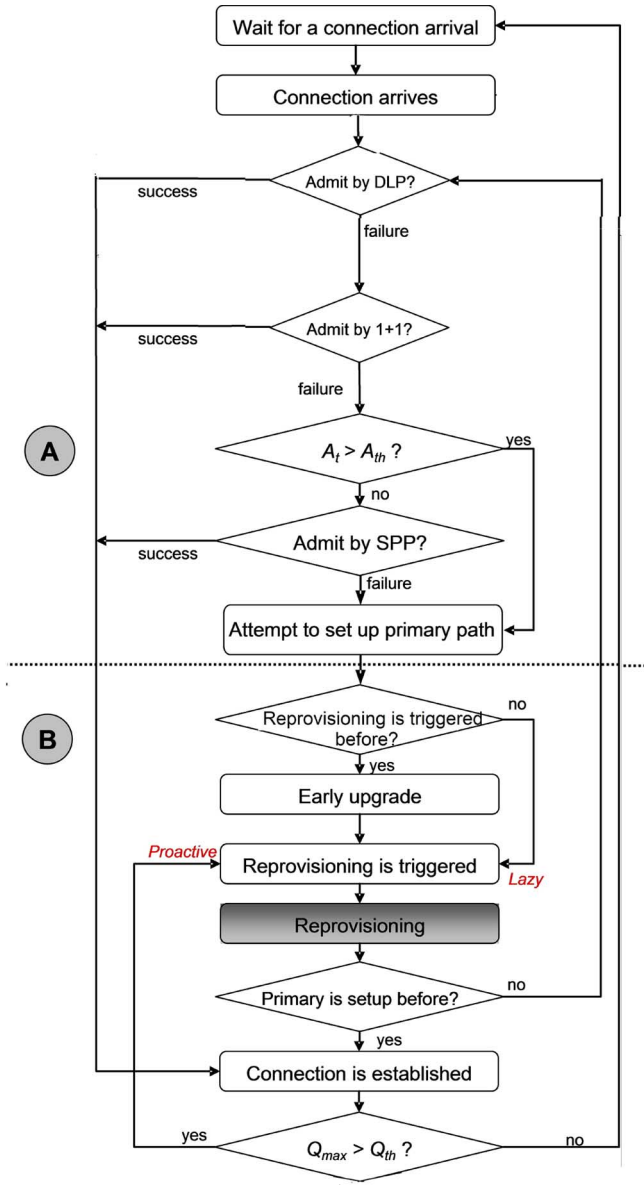


Fig. 1. Admission of a connection in ECM.

where ρ is a constant between 0 and 0.5, and $\overline{A}(\tau)$ is average availability provided by SPP in period τ. Numerical examples show that SLA violations decrease most when $\rho\approx 0.25$, they increase slightly when $\rho\to 0$ or $\rho\to 0.5$, and significantly when $\rho\geq 0.5$. Note that other types of $A_{\rm th}$ estimation methods such as average availability or a static threshold can be used. In our numerical examples, the performance of our ECM approach with different choices of $A_{\rm th}$ estimation methods are very close to each other. EWMA provides slightly better performance compared to other choices, and this is the reason why we chose it for our approach.

If current network resources are insufficient to admit the connection with any protection scheme or $A_t > A_{\rm th}$, the method tries to set up a primary path for the connection and then triggers backup reprovisioning (called lazy trigger) regardless of whether primary is set up or not. Note that if primary is already set up, the reprovisioning phase will return a backup path also for the new connection. If primary path could not have been

set up before reprovisioning because of lack of resources, ECM tries to provision the connection's primary and backup path(s) after reprovisioning.

B. Diffserv-Aware Backup Reprovisioning With Multiple Protection Schemes

Reprovisioning increases EC in the network so that future connections will have more opportunity to be established. However, while reprovisioning backup resources, connections' protection needs should be examined and satisfied with the amount of EC in the network. Connections may experience downtimes due to failures, and they may get close to violation of their SLAs. At this point, the protection scheme of such connections might not be good enough to protect them from initiating or increasing SLA violations for the rest of their holding times. Thus, these connections need to be switched to high-availability protection schemes.

On the other hand, there might be some other connections that can afford failures because they had not been experiencing much downtimes until the given time. Then, these connections can be provisioned by low-availability protection for their remaining holding time. Since switching these connections to low-availability protection by backup reprovisioning increases EC in the network, connections that need high-availability protection can preempt freed backup resources to switch to high-availability protection.

To determine connections' protection requirements at the time of reprovisioning, we use urgency level (UL) concept, which is introduced in [16], i.e., the higher the UL of a connection, the better protection it needs. In [16], UL is defined as a function of allowed number of failures (ANF), remaining holding time (RHT), and some penalty parameters for violating SLA. We modify the UL definition to capture the downtime tolerances of connections without dealing with all the input parameters introduced in [16]. ANF of connection t at a given time describes the risk of SLA violation and is defined as

$$\mathrm{ANF}_t = \left\lfloor \frac{(1-A_t)\times h_t - \mathrm{DT}_t}{\mathrm{MTTR}} \right\rfloor \tag{2}$$

where A_t is the target availability specified in SLA (e.g., 2–9s, 4–9s, etc.), h_t is holding time of connection t, DT_t is downtime of connection t, and MTTR is mean time to repair of a failure. When $\mathrm{ANF}=0$, a connection cannot afford any more failure. In this case, a connection needs better protection than the current one (i.e., UL is high), and RHT and UL are directly proportional since the less the time left to terminate the connection, the less risk the connection has. The UL of connection t at time of reprovisioning is given by

$$\mathrm{UL}_t = \begin{cases} \mathrm{RHT}_t/\mathrm{ANF}_t, & \text{if } \mathrm{ANF}_t > 0 \quad (3a) \\ \mathrm{RHT}_t, & \text{if } \mathrm{ANF}_t = 0 \quad (3b) \\ \mathrm{SDT}_t \times \mathrm{RHT}, & \text{if otherwise} \quad (3c) \end{cases}$$

where SDT_t, SLA downtime, is downtime after the connection t's SLA is violated, (3a) means that connection t can afford failure(s) and its UL is proportional to its remaining holding time and inversely proportional to how many more failures it can afford, (3b) shows that connection t cannot afford any failures and its UL depends on its RHT (RHT_t), and (3c) shows that connection t's SLA is already violated and urgency depends on how much SLA is violated and the remaining holding time of the connection.

1) Problem Formulation: The optimal backup reprovisioning where the objective is minimizing the total backup resources has been studied in several works (e.g., [17]) considering single protection scheme. Our objective is to provide the best possible protection to connections based on their ULs. We formulate and solve the problem into a mathematical model as an integer linear program (ILP) as follows.

- Given:
  - $G(V,E)$: Network topology, V is set of nodes, and E is set of links.
  - $T = \{t =< s_t, d_t >\}$: Set of existing connections, where s_t and d_t are source and destination of connection t, respectively.
  - Δ_{DLP}, Δ_{1+1}, and Δ_{SPP}: Positive integers for DLP, $(1+1)$, and SPP, respectively, used to form objective function and $\Delta_{\mathrm{DLP}} \gg \Delta_{1+1} \gg \Delta_{\mathrm{SPP}}$, to ensure that connections whose ULs are high are protected by high-availability connections.
  - F_{ij}: Number of free wavelengths on link (i,j).
  - R_{ij}^t: $R_{ij}^t = 1$, if primary path of connection t is routed through link (i,j), otherwise $R_{ij}^t = 0$.
- Binary variables:
  - K_t^{DLP}, $K_t^{(1+1)}$ or K_t^{SPP} is equal to 1, if t is protected by DLP, $(1+1)$, or SPP, respectively.
  - X_{ij}^t: $X_{ij}^t = 1$, if backup path of connection t is routed through link (i,j).
  - Y_{ij}^{tkl}: $Y_{ij}^{tkl} = 1$, if backup path of link (k,l) is routed through link (i,j) and $R_{kl}^t = 1$.
- Integer Variables:
  - B_{ij}: Number of backup wavelengths on link (i,j).
- Objective:

$$\min \sum_{t\in T} \mathrm{UL}_t \left(\frac{K_t^{\mathrm{DLP}}}{\Delta_{\mathrm{DLP}}} + \frac{K_t^{(1+1)}}{\Delta_{1+1}} + \frac{K_t^{\mathrm{SPP}}}{\Delta_{\mathrm{SPP}}} \right) + \epsilon \sum_{(i,j)\in E} B_{ij}. \tag{4}$$

- Constraints:
  - Flow conservation constraints:

$$\begin{aligned}
&\sum_{(i,s_t)\in E} X_{is_t}^t - \sum_{(s_t,j)\in E} X_{s_tj}^t = -(K_t^{(1+1)} + K_t^{\mathrm{SPP}}) && \forall t \in T \\
&\sum_{(i,d_t)\in E} X_{id_t}^t - \sum_{(d_t,j)\in E} X_{d_tj}^t = (K_t^{(1+1)} + K_t^{\mathrm{SPP}}) && \forall t \in T \\
&\sum_{(m,j)\in E} X_{mj}^t - \sum_{(m,k)\in E} X_{mk}^t = 0 && \forall t \in T, \forall m \in V, m \neq s_t, d_t
\end{aligned} \tag{5}$$

$$\sum_{(i,k)\in E} Y_{ik}^{tkl} - \sum_{(k,j)\in E} Y_{kj}^{tkl} = -(R_{kl}^t \wedge K_t^{\mathrm{DLP}}) \qquad \forall t \in T, (k,l) \in E$$

$$\sum_{(i,l)\in E} Y_{il}^{tkl} - \sum_{(l,j)\in E} Y_{lj}^{tkl} = (R_{kl}^t \wedge K_t^{\mathrm{DLP}}) \qquad \forall t \in T, (k,l) \in E$$

$$\sum_{(m,j)\in E} Y_{mj}^{tkl} - \sum_{(i,m)\in E} Y_{im}^{tkl} = 0 \qquad \forall m \in V, m \neq k, l \\ (k,l) \in E, t \in T. \tag{6}$$

— Protection constraints:

$$K_t^{\mathrm{DLP}} + K_t^{(1+1)} + K_t^{\mathrm{SPP}} = 1 \qquad \forall t \in T. \tag{7}$$

— Link-disjoint constraints:

$$R_{ij}^t + X_{ij}^t \leq 1 \qquad \forall (i,j) \in E, t \in T \tag{8}$$

$$Y_{ij}^{tij} = 0 \qquad \forall t \in T, (i,j) \in E. \tag{9}$$

— Capacity constraints[3]:

$$\sum_{t\in T} \sum_{(k,l)\in E} Y_{ij}^{tkl} + \sum_{t\in T} (X_{ij}^t \wedge K_t^{(1+1)}) \\ + \frac{1}{\mathrm{MAS}} \sum_{t\in T} (X_{ij}^t \wedge K_t^{\mathrm{SPP}}) \leq B_{ij} \qquad \forall (i,j) \in E \tag{10}$$

$$B_{ij} \leq Fij \qquad \forall (i,j) \in E. \tag{11}$$

The objective function (4) provides high-availability protection to those connections whose UL is high. The second term in the objective function is required to avoid long backup paths, where ϵ should be a small number to avoid compromising the primary objective (the first term in the objective function). In our examples, we see that ϵ should not exceed 10^{-5}. Flow-conservation constraints are set for both path and link protection in (5) and (6), respectively. Constraint in (7) is required to provide protection by one of the protection schemes to each connection. Equation (8) ensures that primary and backup paths are link-disjoint and (9) ensures that the backup path of a link does not go through itself. Equations (10) and (11) limit total backup resources on a link by free resources on the link, where MAS is maximum allowed sharing to limit sharing [17].

Reference [29] proves that spare capacity allocation problem with arc-flow formulation is NP-complete for both DPP and SPP. Considering that DLP is another version of DPP and we only provision backup resources (each link on primary path of a connection can be considered as a distinct subconnections), the backup reprovisioning problem for DLP is reducible to the DPP problem. If we assume that each connection request requires DPP (or SPP or DLP), our problem becomes the standard DPP (or SPP or DLP) optimization problem. Therefore, our problem is also an NP-complete problem since the DPP (or SPP or DLP) optimization problem is NP-complete.

2) Heuristic: Since ILP is not scalable and therefore intractable for large networks, we develop a heuristic for backup reprovisioning, shown in Algorithm 1. The heuristic first calculates ULs and sorts connections in descending order with respect to their ULs (the first connection in the sorted set is the connection that needs high-availability protection most urgently). Then, some UL thresholds have to be set such that connections whose ULs are above a threshold need urgent care (high-availability protection) and those whose ULs are below the threshold can tolerate possible failures, so a low-availability protection scheme would be sufficient for them. Hence, our approach uses two thresholds: $\mathrm{UL_H}$ and $\mathrm{UL_L}$, where connections whose ULs are more than $\mathrm{UL_H}$ are switched to DLP, those whose ULs are between $\mathrm{UL_H}$ and $\mathrm{UL_L}$ are switched to $1+1$, and the rest of the connections' backup resources are reprovisioned by using SPP. Low UL thresholds increase the portion of connections protected by high-availability protection schemes (which decreases SLA violations), but require high capacity and might cause unnecessary upgrades. High UL thresholds might prevent such upgrades, but may increase SLA violations. Thus, we propose a trial-and-error type of UL-threshold calculation. We use the concept of decile in descriptive statistics where we divide the set of sorted connections T into 10 equal-sized connection sets whose boundaries are marked with deciles, i.e., nine values that divide T. Our approach sets $\mathrm{UL_L}$ the first decile and $\mathrm{UL_H}$ the second decile (i.e., 10% of the connections will be protected by SPP, another 10% by $1+1$, and the rest by DLP) in the first round. If the reprovisioning is unsuccessful because of high resource requirements, then our approach tries higher decile values. The following equation shows which decile is set as UL threshold for each trial k, where $k = 1, \ldots, 9$:

$$\begin{cases} \mathrm{UL_H}(k) = \min(2k\text{th decile}, \max\limits_{t\in T} \mathrm{UL}_t) & \text{(12a)} \\ \mathrm{UL_L}(k) = k\text{th decile}. & \text{(12b)} \end{cases}$$

For $k = 9$, most of the connections are below $\mathrm{UL_L}$, and only a small portion (1/10) are above this threshold. If reprovisioning for $k = k_{\max}$ is unsuccessful, where $k_{\max} = 1, \ldots, 10$ and determines the maximum number of trials, an early upgrade (discussed below) is required since current network resources are not sufficient to provide different levels of services. After the upgrade, reprovisioning reinitiates with $k = 1$. Note that, while low $k_{\max}$ values may cause frequent early upgrades, but decrease SLA violations by providing high-availability protection schemes to the majority of connections, high $k_{\max}$ values decreases the upgrade costs.

A shortest-path algorithm (SPA) has computational complexity of $O(|E|+|V|\log|V|)$ for the given topology $G(V,E)$. It is performed for each link for *DLP*-reprovisioning and for each connection for $(1+1)$- and *SPP*-reprovisioning. Thus, the complexity of Algorithm 1 is $O(k_{\max} \times (|T_{\mathrm{DLP}}| \times P + |T_{1+1}| + |T_{\mathrm{SPP}}|) \times (|E| + |V|\log|V|))$, given that P is the average hop count of a connection's primary path, reprovisioned by DLP.

Note that switching backup resources from one protection to another requires reconfiguration of network resources, which can be easily handled in the GMPLS [30] control plane of today's state-of-the-art optical networks.

C. Early Upgrade

After reprovisioning, if EC is not enough to provide protection to the new connection, or reprovisioning is unsuccessful, then an early upgrade is required to avoid rejection. Different upgrade policies, trying to minimize blocking probability, exhaustion probability, or wavelength fill ratio, have been developed (e.g., [31]–[33]). Since our approach focuses on exploiting

[3] $\wedge$ operation in (6) and (10) is used to obtain a binary variable by using *and* operation. For instance, let A and B be binary variables, then $A \wedge B$ can be obtained by the following constraints: $A \wedge B \leq A$, $A \wedge B \leq B$, and $A \wedge B \geq A + B - 1$.

Algorithm 1: Backup Reprovisioning for ECM (DLP/(1 + 1)/SPP)

1: Create the connection set to be reprovisioned ($T_{\rm rp} = T$).
2: Calculate the ULs.
3: Sort connections in descending order with respect to their ULs and set trial number $k = 1$.
4: Set UL thresholds by (12a) and (12b).
5: Free backup resources.
6: Take first connection t from $T_{\rm rp}$.
7: Identify set of links which are on primary path of t. $p_t = \{n =< k, l >\}$ where k and l are ingress and egress nodes of link n.
8: **if** $\mathrm{UL}_t \geq \mathrm{UL}_{\rm H}$, **then**
9: Pick an unprotected link n from p_t.
10: Update link costs for each link e by $C(e) = 1 + W(e) - F(e)$, if $e \neq n$ and $F(e) > 0$, where $W(e)$ and $F(e)$ are total and free number of wavelength on link e. $C(e) = \infty$, otherwise.
11: Use SPA to compute backup path of link n.
12: **if** a finite-cost path is found, **then** provision backup path, **else** go to Step 23.
13: **if** all links on p_t are protected, **then** remove t from $T_{\rm rp}$ and go to Step 24, **else** go to Step 9.
14: **else if** $\mathrm{UL}_{\rm H} > \mathrm{UL}_t \geq \mathrm{UL}_{\rm L}$, **then**
15: Update link costs for each link e by $C(e) = 1 + W(e) - F(e)$, if $e \notin p_t$ and $F(e) > 0$. $C(e) = \infty$, otherwise.
16: Use SPA to compute backup path of t.
17: **if** a finite-cost path is found, **then** provision backup path, remove t from $T_{\rm rp}$, and go to Step 24, **else** go to Step 23.
18: **else if** $\mathrm{UL}_t < \mathrm{UL}_{\rm L}$, **then**
19: Update link costs for each link e by $C(e) = \varepsilon$, if existing backup wavelengths of link e can be shared and $e \notin p_t$. $C(e) = 1 + \varepsilon \times (W(e) - F(e))$, if $e \notin p_t$, existing backup wavelengths of link e cannot be shared, but $F(e) > 0$. $C(e) = \infty$, otherwise (ε is a small number, e.g., 10^{-4}).
20: Use SPA to compute backup path of t.
21: **if** a finite-cost path is found, **then** provision backup path, remove t from $T_{\rm rp}$, and go to Step 6, **else** go to Step 24.
22: **end if**
23: **if** $k < k_{\max}$, **then** increment k and go to Step 4, **else** upgrade the network resources and go to Step 3.
24: **if** $|T_{\rm rp}| = 0$, **then return** success, **else** go to Step 6.

EC under existence of an upgrade model rather than proposing an upgrade model, ECM is applicable to any upgrade model that periodically upgrades network resources. Note that the upgrade model should also be able to provide an early upgrade as an additional upgrade to the periodic one to provide protection to all connections after an unsuccessful backup reprovisioning.

Here, we consider an upgrade model that aims at maintaining the maximum primary-resource utilization (i.e., ratio between bandwidth consumed by primary paths on a link and the total bandwidth of that link) of links in a certain time period $(0, \tau)$ under a certain threshold, $R_{\rm th}$ (NOs usually want to keep primary-resource utilization low so that the network can handle traffic growth). This model does not consider the bandwidth used by backup paths because amount of backup resources used for a connection might change due to switching from one protection scheme to another. The additional bandwidth required for upgrade both in case of periodic upgrade and complementary early upgrade is as follows:

$$\begin{cases} \frac{P_{\max}(e)}{R_{\rm th}(e)} - W(e), & \text{if periodic upgrade} \\ \beta_\tau \times (\frac{P_{\max}(e)}{R_{\rm th}(e)} - W(e)), & \text{if early upgrade} \end{cases} \tag{13}$$

where $W(e)$ is total bandwidth of link e, $P_{\max}(e)$ is the maximum bandwidth used for primary paths on link e since the last upgrade of the network, and β_τ is required to determine how much bandwidth to add in period τ in advance in case of early upgrade. The NO can select different β_τ values depending on available upgrade budget in period τ. If the NO cannot afford early upgrade, β_τ is equal to 0. Since the NO would not want to reject any connection request, we assume that $\beta_\tau \neq 0$.

D. Proactive Reprovisioning

After the connection is established, ECM checks the maximum resource consumption ratio ($Q_{\max} = \max_{e \in E} Q(e)$), where $Q(e)$ is the resource consumption ratio on link e. If $Q_{\max}$ is greater than a certain threshold ($Q_{\rm th}$), it triggers reprovisioning. It is called *proactive* triggering because ECM does not have to wait for reprovisioning until a capacity exhaustion occurs. Reference [34] suggested to upgrade networks when resource consumption exceeds 60%, so we consider $Q_{\rm th} = 0.6$ to reprovision backup resources to free capacity.

IV. Alternative ECM Schemes

A. ECM With $1 + N$ and SPP

In this case, for a high-availability protection scheme, the NO can choose to use $1+N$ instead of DLP. In the admission phase, the NO tries to provision $1 + N$ protection, where N depends on the maximum link-disjoint backup paths for any node pair in the network. If resources are not sufficient or topology does not support $1+N$, ECM decrements N and repeats the process until $N = 1$, then it checks if the connection can be provisioned by a low-availability protection scheme. For backup reprovisioning phase, we consider a trial-and-error approach (for $N > 1$) since ECM cannot know *a priori* how many backup paths a connection can get. Backup reprovisioning heuristic can be obtained by replacing Steps 7–22 in Algorithm 1 by the steps shown in Algorithm 2. The new algorithm reprovisions backup resources of those connections whose ULs are higher than $\mathrm{UL}_{\rm L}$ by $1+N$, and lower ones by SPP. Determination of $\mathrm{UL}_{\rm L}$ again can be done by (12b). While reprovisioning by $1 + N$, Algorithm 2 starts from N and decrements the number of backup paths until reprovisioning by $1 + N$ is successful. Otherwise, it returns a failure for reprovisioning. SPA is run at most $N(N+1)/2$ times for each connection for $(1 + N)$-reprovisioning and once for

Algorithm 2: Backup Reprovisioning for ECM $(1+N/\text{SPP})$

Set $N_{\max} = N$.
if $\text{UL}_t \geq \text{UL}_\text{L}$, **then**
  Update link costs for each link e by $C(e) = 1 + W(e) - F(e)$, if $e \neq n$ and $F(e) > 0$, where $W(e)$ and $F(e)$ are total and free number of wavelength on link e. $C(e) = \infty$, otherwise.
  if N link-disjoint paths are available, **then** provision them, remove t from T_{rp}, and go to Step 6; **else** decrement N.
  if $N = 0$, **then** go to Step 24; **else** go to previous step.
else if $\text{UL}_t < \text{UL}_\text{L}$, **then**
  Repeat Steps 19–21 in Algorithm 1.
end if

SPP-reprovisioning. Therefore, the complexity of Algorithm 2 is $O(k_{\max} \times N(N+1)|T_{1+N}|/2 + |T_{\text{SPP}}|) \times (|E| + |V| \log |V|))$.

B. ECM With Single Protection

The NO might also decide to protect connections using a single protection scheme (to decrease control complexity). Thus, we propose two ECM approaches: ECM with $1+N$ and ECM with *SPP*. Fig. 2 shows the admission process for both approaches. The truncated part, Part (B') (below dashed line), is identical to Part (B) in Fig. 1; L-SPP and H-SPP are defined below.

1) ECM With $1+N$: Increasing N increases availability, but requires larger EC. Thus, our approach starts with an N value $N > 1$, when the amount of EC is large and the topology supports N number of link-disjoint paths. If providing N link-disjoint paths is not possible, ECM decrements N and tries again. The main difference between ECM with $1+N/\text{SPP}$ and ECM with $1+N$ is that ECM with $1+N$ never tries shared protection and directly calls backup reprovisioning.

This approach does not require a threshold like previous ECM approaches because it reprovisions connections by $1+N$ starting from highest possible N. Connections are sorted in descending order w.r.t. their ULs. Thus, connections that have high ULs have more of a chance to get a large number of backup paths. This heuristic is similar to Algorithm 2 excluding Steps 5 and 9–13 (i.e., there is no threshold and shared protection), and its complexity is $O(N(N+1)|T|/2 \times (|E| + |V| \log |V|))$.

2) ECM With SPP: Different levels of protection with SPP can be obtained by adjusting the amount of sharing, i.e., less sharing results in high availability, and vice versa. The typical cost assignments to provision backup resources for SPP (e.g., [35]) always tend to maximize sharing among backup resources, even in those network states where there is enough EC to provision the backup path on less-shared resources at the time of provisioning. However, increase in sharing among backup resources decreases the availability [1], [27]. Thus, a cost assignment that maximizes sharing might cause unnecessary availability reduction even if the network has a considerable amount of EC. In [36], we proposed a cost assignment that helps to exploit EC and increases availability by preferring less-shared or free resources to provision backup paths. We call SPP using cost assignment in [36] less-shared path protection (*L-SPP*), which can be used when the amount of EC is large. Reprovisioning connections by high-shared path protection (i.e., using typical cost assignment which encourages sharing), *H-SPP*, increases the availability. ECM with *SPP* exploits the different levels of protection provided by *L-SPP* and *H-SPP*. The admission process is shown in Fig. 2. Note that *L-SPP* is good for urgent connections ($\text{UL}_t \geq \text{UL}_\text{L}$) with its higher availability than *H-SPP* for backup reprovisioning. Backup reprovisioning heuristic can be obtained by replacing Steps 7–22 in Algorithm 1 by steps shown in Algorithm 3. Its complexity is $O(k_{\max} \times |T| \times (|E| + |V| \log |V|))$.

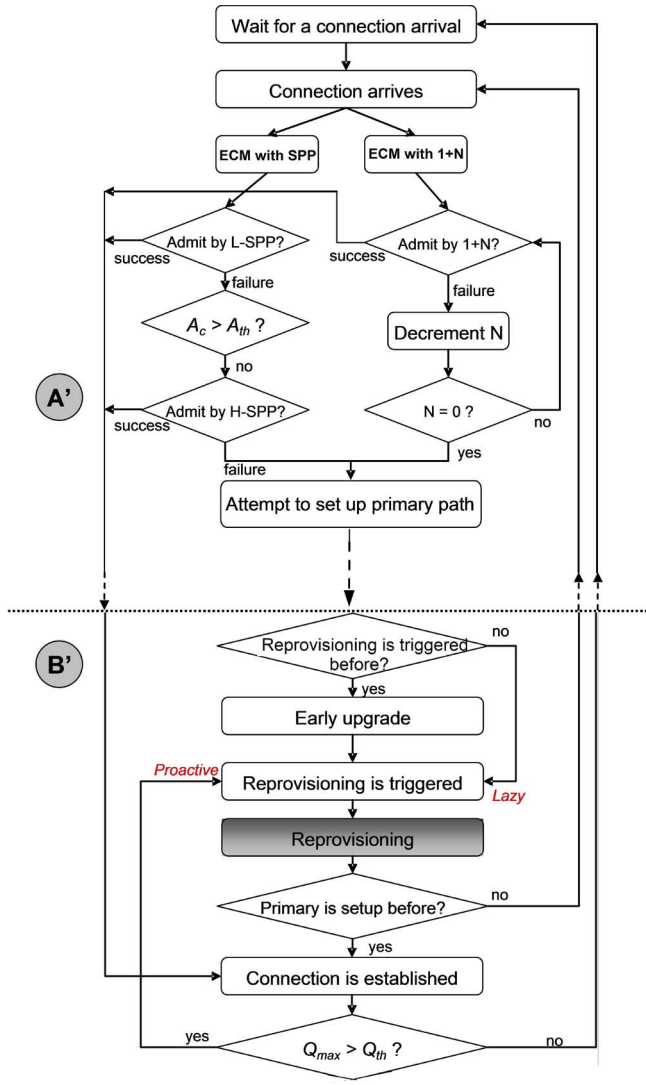


Fig. 2. Admission process in *single-protection* scenario.

V. Illustrative Numerical Examples

A. Example Settings

1) Topology: We study our proposed ECM approaches on the network shown in Fig. 3, a US-wide network with wavelength conversion (e.g., optical switches with O/E/O conversion). Initially, the network is empty (no connections are provisioned), and each link has 16 wavelengths in opposite directions. The

colors of nodes indicate the population (in millions) served by each node (adopted from [37]).

2) Traffic Model: We consider two traffic growth models: exponential and linear. Arrival rate (per day) of connections originating from node s and destined to node d during month m for exponential and linear traffic growth are as follows:

$$\lambda_{sd}(m) = \lambda_{sd}(0)(1 + \varphi_{sd}(1 - e^{-m/\eta})) \quad (14a)$$

$$\lambda_{sd}(m) = \lambda_{sd}(0)(1 + m/\eta) \quad (14b)$$

where $\lambda_{sd}(0)$ is the initial arrival rate between node pair (s, d), and φ_{sd} and η are constant parameters. We keep $\eta = 16$ [33] and determine different $\lambda_{sd}(0)$ and φ_{sd} parameters depending on the total population (q) served by all nodes, and population served by source (q_s) and destination (q_d) as follows:

$$\lambda_{sd}(0) = \left\lceil \left(\frac{q_s}{q_s + q_d}\right)\left(\frac{q_d}{q}\right)\left(\frac{q_s}{q}\right) \times 100 \right\rceil \lambda(0) \quad (15)$$

$$\varphi_{sd} = \left\lceil \left(\frac{q_s}{q_s + q_d}\right)\left(\frac{q_d}{q}\right)\left(\frac{q_s}{q}\right) \times 100 \right\rceil \varphi \quad (16)$$

where $\lambda(0)$ and φ denote the initial arrival rate of requests and constant to generate φ_{sd} values, respectively. For illustrations, we consider $\varphi = 5$ and a 5-year time interval. We conduct numerical examples for network loads varying between 20 and 400 Erlangs. We run our approaches 10 times for each $\lambda(0)$, and our results show the average.

Connections' availability requirements follow the distribution 0.9999: 0.9995: 0.999: 0.99: 0.95 = 1: 5: 15: 30: 50.

3) Upgrade Model: We assume R_{th} in our upgrade model is equal to 0.3, so the rest of the link capacity can be used for backup resources and to avoid capacity exhaustion.[4] We assume that $\beta_\tau = 0.5$. Note that this choice provides half of the actual upgrade requirement in advance and the rest will be provided at the end of the upgrade period. We consider 6-month upgrade periods.

4) Failure Model: We consider two failure models: fragile and robust. Links experience independent failures, and some links (called failure-prone links) are more prone to failures than others (rare-failure links), where each link falls in one of these two categories with equal probability. For each failure model and for each link category, mean time between failures (MTBF) is uniformly distributed between values shown in Table I. We consider that time to repair is exponentially distributed with mean of 12 h.

5) Cost Model: We define a cost model that captures SLA violation penalty and upgrade costs as follows:

$$\text{Total cost} = \alpha \times \sum_{t \in T_{\text{all}}} \text{SDT}_t + \zeta \times \sum_{e \in E} U(e) \quad (17)$$

where α is penalty per hour, T_{all} is the set of connections admitted, SDT_t is downtime of connection t after SLA is violated, ζ is cost of adding one wavelength to a fiber link (which usually requires a pair of optical transponders as CapEx), and $U(e)$ is number of added wavelengths to link e. The typical penalty per hour (α) values for SLA violation given by [16] varies from \$7200 to \$23 000, and [38] estimates the cost of a pair of 10 G transponders around \$5000. Thus, the typical value of ζ/α varies between 0.2 and 0.7. We consider the total cost at the end of 5 years while neglecting the inflation (as it affects both α and ζ).

[4]For instance, [25] suggests that the capacity required for backup resources can be 1.6 times the capacity required for primary resources for $1 + 1$.

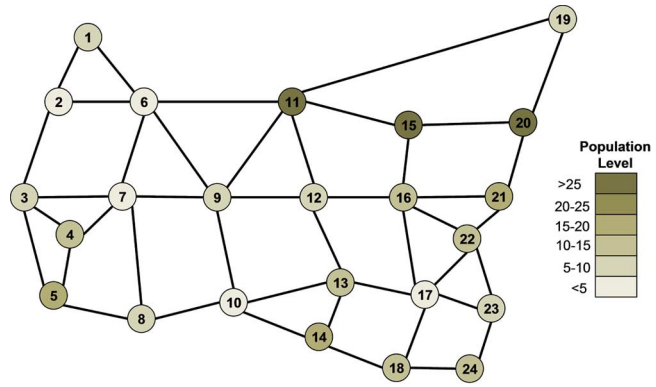


Fig. 3. US-wide network with population levels.

Algorithm 3: Backup Reprovisioning for ECM with *SPP*

if $\text{UL}_t \geq \text{UL}_{\text{L}}$, **then**
  Update link costs by for each link e by
  $C(e) = 1 + \varepsilon \times (W(e) - F(e))$, if existing backup wavelengths of link e can be shared and $e \notin p_t$.
  $C(e) = \varepsilon \times (W(e) - F(e))$, if $e \notin p_t$, existing backup wavelengths of link e cannot be shared, but $F(e) > 0$.
  $C(e) = \infty$, otherwise.
  Use SPA to find backup path of t.
  if a finite-cost path is found, **then** provision backup path and go to Step 6, **else** go to Step 24.
else if $\text{UL}_t < \text{UL}_{\text{L}}$, **then**
  Repeat Steps 19–21 in Algorithm 1.
end if

TABLE I
MTBF (HOURS) FOR FAILURE MODELS

Failure Model	Failure-prone links	Rare-failure links
Fragile	[200, 600]	[1000, 1600]
Robust	[2000, 6000]	[10000, 16000]

B. Comparison

We compare our ECM approach $(\text{DLP}/(1+1)/\text{SPP})$ to alternative ones $(1 + N/\text{SPP}, 1 + N$, and SPP), where $N = 2$ and $N = 1$ for $1 + N$, and with the following two traditional approaches (upgrade policy is also applied for them):

- $1+1$/No protection $((1+1)/\text{NP})$: Here, connections are provisioned by $1+1$. If $1+1$ is not available, they are provisioned without protection. In the reprovisioning phase, connections are sorted w.r.t. their ULs and reprovisioned by $1 + 1$, if it is feasible; else, they are unprotected.
- *Shared Path Protection (SPP)*: Now, connections are provisioned by SPP. For reprovisioning, connections are sorted w.r.t. their ULs and reprovisioned by SPP.

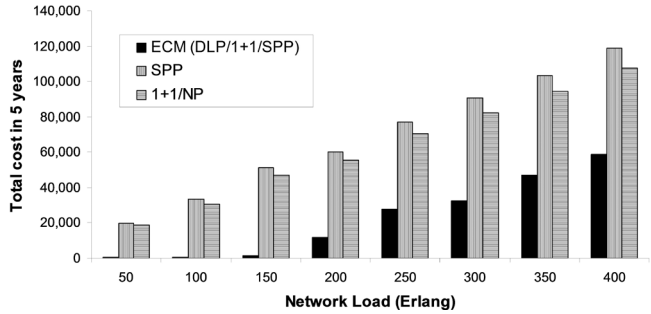


Fig. 4. Comparison of total cost in 5 years for fragile failure model and exponential traffic growth, when $\zeta/\alpha = 1/4$.

TABLE II
AVERAGE COST SAVINGS UNDER DIFFERENT FAILURE AND TRAFFIC GROWTH MODELS

	Average Cost Saving of ECM (DLP/(1+1)/SPP) compared to	
	1+1/NP	SPP
Fragile-Exponential	64.52%	67.56%
Fragile-Linear	68.15%	62.18%
Robust-Exponential	76.98%	54.56%
Robust-Linear	81.25%	51.95%

Fig. 4 compares ECM $(\mathrm{DLP}/(1+1)/\mathrm{SPP})$ to $1+1/\mathrm{NP}$ and SPP in terms of total cost in 5 years for fragile failure model and exponential traffic growth, when $\zeta/\alpha = 1/4$. Our ECM approach shows very low cost compared to traditional approaches because, in this scenario, due to unprotected connections in $1+1/\mathrm{NP}$ and high-backup resource sharing in SPP, traditional approaches show high SLA violations, while our approach decreases SLA violations significantly with high-availability protections and keeps upgrade costs under control by providing low-availability protections to some connections. Table II shows average cost savings over different network loads compared to $1+1/\mathrm{NP}$ and SPP for different failure and traffic growth models. Compared to $1+1/\mathrm{NP}$, cost savings are less for fragile failure profiles than the ones for robust failure profiles because SLA violations increase for ECM due to increase in backup-resource sharing and upgrade costs increase due to high-availability protection requirement. However, even for the fragile-exponential scenario, cost savings compared to $1+1/\mathrm{NP}$ are significant. Compared to SPP, cost savings are more for the fragile failure model than the savings for robust failure models because SPP suffers more due to sharing, while our approach uses high-availability protection schemes more than SPP in fragile models.

Fig. 5 shows average cost savings of ECM approaches compared to $1+1/\mathrm{NP}$ for different failure and traffic growth models, when $\zeta/\alpha = 1/4$. For all the scenarios, ECM with $\mathrm{DLP}/(1+1)/\mathrm{SPP}$ results in the lowest cost. Intuitively, for fragile failure model, SPP fails to handle frequent and simultaneous failures, and it fails more in exponential traffic growth model due to high backup-resource sharing. Thus, for fragile failure model under exponential traffic growth, SPP's low-capacity-requirement (low-upgrade-cost) advantage disappears

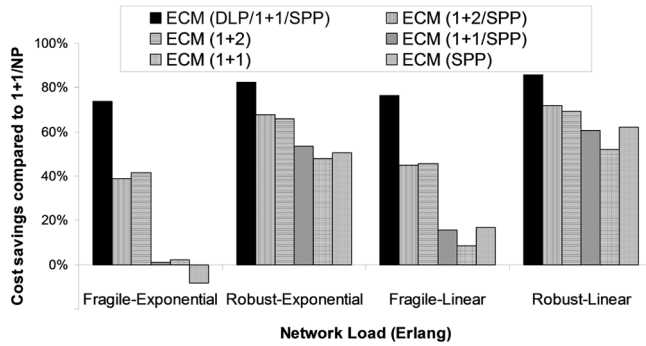


Fig. 5. Average cost savings of various ECM approaches compared to $1+1/\mathrm{NP}$ for $\zeta/\alpha = 1/4$.

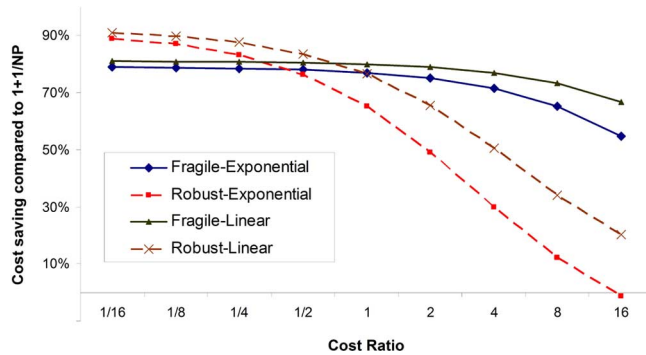


Fig. 6. Cost reduction with different ζ/α (traffic load = 200 Erlangs).

with rapid increase in SLA violation penalty. Fig. 5 validates this statement, where ECMs without SPP are less costly than their counterparts using SPP (e.g., ECM $(1+2/\mathrm{SPP})$ costs more than ECM $(1+2)$). However, when the traffic growth is linear, sharing decreases. Thus, SLA violation penalties decrease. Thus, for fragile failure model, ECMs using SPP become closer to ECMs without SPP. If the failure model is robust, SLA violation penalties due to sharing decrease significantly, thus ECMs using SPP become less costly than ECMs without SPP. ECM with $\mathrm{DLP}/(1+1)/\mathrm{SPP}$ exploits advantages of the three different protection schemes based on differentiated protection needs of connections, thus it shows lowest cost for any type of failure or traffic growth model.

1) Effect of Cost Model: The above comparisons are made for $\zeta/\alpha = 1/4$. Fig. 6 shows cost savings, which can be achieved by our approach, compared to $1+1/\mathrm{NP}$ for different ζ/α, when traffic load is 200 Erlangs. Our approach shows significant cost savings (more than 70%), especially for fragile failure model, for practical cost ratios depending on failure and traffic growth model. $1+1/\mathrm{NP}$ performs better if $\zeta/\alpha > 16$, which is an impractical value, for robust failure model and linear traffic growth.

2) Comparison to Pure ECM: In [1], we consider an ECM scheme with $\mathrm{DLP}/(1+1)/\mathrm{SLP}$ without considering the differentiated protection needs of connections. In that approach, connections enjoy high-availability protection when EC is high (regardless of their SLA requirements), and they are all reprovisioned by a low-availability protection scheme, when EC becomes low (regardless of their downtime tolerances at the time

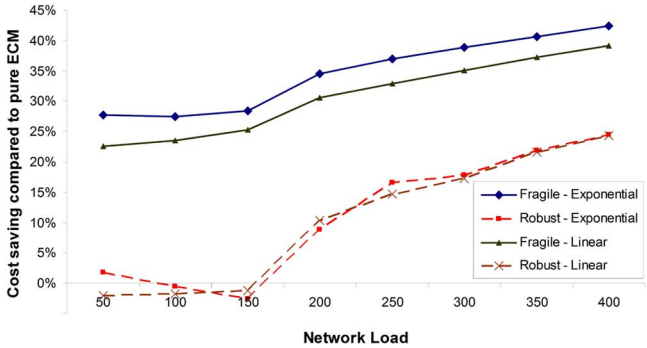


Fig. 7. Cost reduction compared to ECM without considering DiffServ ($\zeta/\alpha = 1/4$).

TABLE III
COST SAVINGS WITH ILP VERSUS HEURISTIC REPROVISIONING

Traffic Growth	Exponential		Linear	
Failure model	Fragile	Robust	Fragile	Robust
ILP	98.14%	99.52%	98.54%	99.65%
Heuristic	97.81%	99.40%	98.11%	98.57%

of reprovisioning). We compare our approach (*ECM for Differentiated Services*), ECM considering differentiated needs of connections with the approach we proposed in [1] (*pure ECM*). Fig. 7 shows cost reduction achieved by *ECM for Differentiated Services*. For fragile failure model, there is a significant cost reduction. For robust failure model, both approaches perform close to each other when the traffic load is low, but when traffic load increases, *ECM for Differentiated Services* shows less cost than *pure ECM*.

3) ILP Versus Heuristic: In Section III-B, we formulated the backup reprovisioning problem into an ILP and provided a heuristic. ILP reprovisions connections simultaneously to exploit EC to provide the connections with best possible protection scheme with link-capacity limitations. This helps to decrease SLA violations, but it might slightly increase upgrade costs. Our heuristic reprovisions connections one by one, which leads to the result that the higher the urgency level, the shorter is the backup path for the connection. Shorter backup paths also decrease SLA violations, but the heuristic does not solve the problem for all connections simultaneously as ILP does. Therefore, link capacity might be given to those connections that have high UL, so other connections might have to be provisioned on longer paths that slightly increase SLA violations. The cost savings compared to $1 + 1/\mathrm{NP}$, if ECM uses ILP versus heuristic for reprovisioing, are shown in Table III for network load 50 Erlangs (for larger network loads, ILP is intractable) and $\zeta/\alpha = 1/4$. The average execution time of reprovisioning for ILP takes days, while the heuristic solves the problem in minutes on today's standard desktop computing platforms. By using the proposed heuristic, results close to ILP can be achieved in a very short time.

C. Discussion on ECM Parameters

The parameters of our ECM approach (A_{th} for admission process, Δ and ϵ in the objective function of ILP, $k_{\max}$ in the heuristic, Q_{th} for proactive reprovisioning) may change ECM's performance. The extensive number of numerical examples to investigate the effects of these parameters are generated (omitted here due to space limitation), and the results are briefly discussed in related subsections in Section III. Thus, the main message of this work, i.e., significant cost reduction can be achieved with our ECM approach, remains the same. We also explored the effects of network connectivity. For well-connected topologies, since there is more opportunity to protect connections by DLP, SLA violations (so the total costs) can be reduced. For instance, COST239 European topology [39] (whose network connectivity is higher than the US topology in Fig. 3) decreases SLA violations more than US topology (around 6.5% on average), especially for high network loads. The quantitative results are omitted due to space limitations.

VI. CONCLUSION

In this paper, we proposed an EC management scheme for differentiated services under traffic growth to reduce SLA violations and upgrade costs paid by the network operator. We also proposed some alternative excess capacity management approaches. In our numerical examples, we compared the proposed schemes to some existing approaches to understand how they affect SLA violation penalty and upgrade costs under different traffic growth, failure, and cost models. Our approach significantly reduces the total cost of network operator compared to traditional approaches. We also showed that by considering differentiated protection needs of the connections, EC can be managed more efficiently, where additional cost savings are very significant.

REFERENCES

[1] F. Dikbiyik, L. Sahasrabuddhe, M. Tornatore, and B. Mukherjee, "Exploiting excess capacity to improve robustness of WDM mesh networks," *IEEE/ACM Trans. Netw.*, vol. 20, no. 1, pp. 114–124, Feb. 2012.
[2] E. Crawley, H. Sandick, R. Nair, and B. Rajagopalan, "A framework for QoS-based routing in the internet," Internet RFC 2386, 1998.
[3] N. Golmie, T. Ndousse, and D. Su, "A differentiated optical services model for WDM networks," *IEEE Commun. Mag.*, vol. 38, no. 2, pp. 68–73, Feb. 2000.
[4] A. Jukan and H. R. v. As, "Service-specific resource allocation in WDM networks with quality constraints," *IEEE J. Sel. Areas Commun.*, vol. 18, no. 10, pp. 2051–2061, Oct. 2000.
[5] A. Fumagalli and M. Tacca, "Differentiated reliability (DiR) in WDM rings without wavelength converters," in *Proc. IEEE ICC*, Helsinki, Finland, Jun. 2001, pp. 2887–2891.
[6] A. Fumagalli, M. Tacca, F. Unghváry, and A. Faragó, "Shared path protection with differentiated reliability," in *Proc. IEEE ICC*, New York, NY, Apr. 2002, pp. 2157–2161.
[7] C. Saradhi and C. Murthy, "Routing differentiated reliable connections in single-and multifiber WDM optical networks," in *Proc. OptiComm*, 2001, pp. 24–35.
[8] H. Luo, L. Li, and H. Yu, "Routing connections with differentiated reliability requirements in WDM mesh networks," *IEEE/ACM Trans. Netw.*, vol. 17, no. 1, pp. 253–266, Feb. 2009.
[9] O. Gerstel and G. Sasaki, "Quality of protection (QoP): a quantitative unifying paradigm to protection service grades," in *Proc. OptiComm*, 2001, pp. 12–23.
[10] C. Awad, B. Sanso, and A. Girard, "Diffserv for differentiated reliability in meshed IP/WDM networks," *Comput. Netw.*, vol. 52, no. 10, pp. 1988–2012, 2008.
[11] L. Song, J. Zhang, and B. Mukherjee, "Dynamic provisioning with availability guarantee for differentiated services in survivable mesh networks," *IEEE J. Sel. Areas Commun.*, vol. 25, no. 3, pp. 35–43, Apr. 2007.

[12] R. Lin, S. Wang, L. Li, and L. Guo, "A new network availability algorithm for WDM optical networks," in *Proc. Comput. Inf. Technol.*, Sep. 2005, pp. 480–484.
[13] D. Lucerna, M. Tornatore, B. Mukherjee, and A. Pattavina, "Trading availability among shared-protected dynamic connections in WDM networks," *Comput. Netw.*, vol. 56, no. 13, pp. 3150–3162, Sep. 2012.
[14] O. Gerstel and G. Sasaki, "A new protection paradigm for digital video distribution networks," in *Proc. IEEE ICC*, Istanbul, Turkey, Jun. 2006, pp. 2518–2523.
[15] O. Gerstel and G. Sasaki, "Meeting SLAs by design: A protection scheme with memory," in *Proc. OSA OFC*, Anaheim, CA, USA, Mar. 2007, pp. 1–3.
[16] M. Xia, M. Tornatore, C. U. Martel, and B. Mukherjee, "Service-centric provisioning in WDM backbone networks for the future internet," *J. Lightw. Technol.*, vol. 27, no. 12, pp. 1856–1865, Jun. 2009.
[17] L. Song, J. Zhang, and B. Mukherjee, "A comprehensive study on backup-bandwidth reprovisioning after network-state updates in survivable telecom mesh networks," *IEEE/ACM Trans. Netw.*, vol. 16, no. 6, pp. 1366–1377, Dec. 2008.
[18] E. Bouillet, J. Labourdette, R. Ramamurthy, and S. Chaudhuri, "Lightpath re-optimization in mesh optical networks," *IEEE/ACM Trans. Netw.*, vol. 13, no. 2, pp. 437–447, Apr. 2005.
[19] C. Assi, W. Huo, A. Shami, and N. Ghani, "On the benefits of lightpath reprovisioning in optical mesh networks," in *Proc. IEEE ICC*, Seoul, Korea, May 2005, pp. 1746–1750.
[20] W. Ni *et al.*, "An improved approach for online backup reprovisioning against double near-simultaneous link failures in survivable WDM mesh networks," in *Proc. IEEE GLOBECOM*, Washington, DC, USA, Nov. 2007, pp. 2304–2309.
[21] L. Guo, X. Wang, and L. Li, "Improving survivability for multi-link failures with reprovisioning in WDM mesh networks," *Photon. Netw. Commun.*, vol. 14, no. 3, pp. 265–271, Dec. 2007.
[22] X. Shao, L. Zhou, and Y. Wang, "Backup reprovisioning after shared risk link group (SRLG) failures in survivable WDM mesh networks," in *Proc. OSA OFC*, Anaheim, CA, USA, Mar. 2007, pp. 1–3.
[23] Y. Cheng and W. Zhuang, "Dynamic inter-SLA resource sharing in pathoriented differentiated services networks," *IEEE/ACM Trans. Netw.*, vol. 14, no. 3, pp. 657–670, Jun. 2006.
[24] M. Batayneh, S. Rai, S. Sarkar, and B. Mukherjee, "Efficient management of a telecom networks excess capacity: A traffic-engineering approach," in *Proc. ECOC*, Berlin, Germany, Sep. 2007, pp. 1–2.
[25] C. Mauz, "Unified ILP formulations of protection in mesh networks," in *Proc. ConTEL*, Zurich, Switzerland, Jun. 2003, pp. 737–741.
[26] S. Ramamurthy, L. Sahasrabuddhe, and B. Mukherjee, "Survivable WDM mesh networks," *J. Lightw. Technol.*, vol. 21, no. 4, pp. 870–883, Apr. 2003.
[27] L. Zhou, M. Held, and U. Sennhauser, "Connection availability analysis of shared backup path-protected mesh networks," *J. Lightw. Technol.*, vol. 25, no. 5, pp. 1111–1119, May 2007.
[28] D. Arci, G. Maier, A. Pattavina, D. Petecchi, and M. Tornatore, "Availability models for protection techniques in WDM networks," in *Proc. DRCN*, Oct. 2003, pp. 158–166.
[29] Y. Liu, D. Tipper, and P. Siripongwutikorn, "Approximating optimal spare capacity allocation by successive survivable routing," *IEEE/ACM Trans. Netw.*, vol. 13, no. 1, pp. 198–211, Feb. 2005.
[30] E. Mannie, "RFC 3945: Generalized multi-protocol label switching (GMPLS) architecture," Oct. 2004 [Online]. Available: http://www.ietf.org/rfc/rfc3945.txt
[31] M. Pioro and D. Medhi, *Routing, Flow, and Capacity Design in Communication and Computer Networks*. Amsterdam, The Netherlands: Elseiver, 2004.
[32] T. K. Nayak and K. N. Sivaranjan, "Dimensioning optical networks under traffic growth models," *IEEE/ACM Trans. Netw.*, vol. 11, no. 6, pp. 935–947, Dec. 2003.
[33] R. Roy, A. Nag, and B. Mukherjee, "Telecom mesh network upgrade to manage traffic growth," *IEEE/OSA J. Opt. Commun. Netw.*, vol. 2, no. 5, pp. 256–265, May 2010.
[34] M. D. Feuer *et al.*, "Simulations of a service velocity network employing regenerator site concentration," in *Proc. OSA NFOEC*, Los Angeles, CA, USA, 2012, pp. 1–3.
[35] G. Mohan, C. S. R. Murhty, and A. K. Somani, "Efficient algorithms for routing dependable connections in WDM optical networks," *IEEE/ACM Trans. Netw.*, vol. 9, no. 5, pp. 553–566, Oct. 2001.
[36] F. Dikbiyik, L. Sahasrabuddhe, and M. Tornatore, "Excess-capacity aware, shared-path protection with backup reprovisioning in telecom mesh networks," in *Proc. IEEE ANTS*, Mumbai, India, Dec. 2010, pp. 58–60.
[37] M. Batayneh, D. Schupke, M. Hoffman, A. Kristaedter, and B. Mukherjee, "On routing and transmission-range determination of multi-bit-rate signals over mixed-line-rate WDM networks for carrier ethernet," *IEEE/ACM Trans. Netw.*, vol. 19, no. 5, pp. 1304–1316, Oct. 2011.
[38] K. Christodoulopoulos, M. Angelou, D. Klonidis, P. Zakynthinos, E. Varvarigos, and I. Tomkos, "Value analysis methodology for flexible optical networks," in *Proc. OSA OFC*, Los Angeles, CA, USA, Mar. 2011, pp. 1–3.
[39] P. Batchelor *et al.*, "Study on the implementation of optical transparent transport networks in the European environment results of the research project COST 239," *Photon. Netw. Commun.*, vol. 2, no. 1, pp. 15–32, 2000.

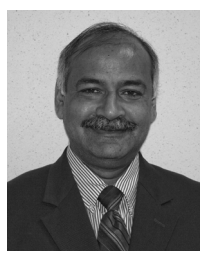
Ferhat Dikbiyik (S'10–M'14) received the B.S. degree in electrical and electronics engineering from Istanbul University, Istanbul, Turkey, in 2005, and the M.S. and Ph.D. degrees in electrical and computer engineering from the University of California, Davis, CA, USA, in 2009 and 2013, respectively.

He is an Assistant Professor with the Department of Computer Engineering, Sakarya University, Sakarya, Turkey. His research interests include design, development, and analysis of next-generation lightwave networks, especially excess capacity management, survivability against disasters, and network upgrade.

Massimo Tornatore (S'03–M'06–SM'13) received the Ph.D. degree in information engineering from the Politecnico di Milano, Milan, Italy, in 2006.

He is currently working as an Assistant Professor with the Department of Electronics, Information and Bioengineering, Politecnico di Milano. He also holds an appointment as an Adjunct Associate Professor with the Department of Computer Science, University of California, Davis, CA, USA, where he served as a Postdoctoral Researcher in 2008 and 2009. He is the author of more than 180 conference and journal papers, and his research interests include design, protection, and energy efficiency in optical core, metro, and access networks.

Dr. Tornatore is a co-recipient of six Best Paper awards from IEEE conferences.



Biswanath Mukherjee (S'82–M'84–SM'05–F'07) received the B.Tech. (Hons.) degree from the Indian Institute of Technology, Kharagpur, India, in 1980, and the Ph.D. degree from the University of Washington, Seattle, WA, USA, in 1987.

He is a Distinguished Professor with the University of California (UC), Davis, CA, USA, where he has been since 1987, and served as Chairman of the Department of Computer Science during 1997 to 2000. He served a 5-year term as a Founding Member of the Board of Directors of IPLocks, Inc., a Silicon Valley startup company and on the Technical Advisory Board of a number of startup companies in networking, most recently Teknovus (acquired by Broadcom), Intelligent Fiber Optic Systems, and LookAhead Decisions, Inc. He is author of the textbook *Optical WDM Networks* (Springer, 2006).

Prof. Mukherjee is Editor of Springer's Optical Networks Book Series. He serves or has served on the editorial boards of eight journals, most notably the IEEE/ACM TRANSACTIONS ON NETWORKING and *IEEE Network*. He served as Technical Program Co-Chair of the Optical Fiber Communications (OFC) Conference 2009, and General Co-Chair of OFC 2011. He served as the Technical Program Chair of the IEEE INFOCOM 1996 conference. He was Steering Committee Chair of the IEEE Advanced Networks and Telecommunications Systems (ANTS) Conference, and served as General Co-Chair of ANTS in 2007 and 2008. He is co-winner of the Optical Networking Symposium Best Paper awards at the IEEE GLOBECOM 2007 and 2008 conferences. He won the 2004 UC Davis Distinguished Graduate Mentoring Award and 2009 UC Davis College of Engineering Outstanding Senior Faculty Award.