

# Resilient network dimensioning for optical grid/clouds using relocation

(Invited Paper)

Chris Develder\*, Jens Buysse\*, Marc De Leenheer\*, Brigitte Jaumard†, and Bart Dhoedt\*

\* Dept. of Information Technology – IBCN, Ghent University – IBBT, Ghent, Belgium

† CSE Dpt, Concordia University, Montreal (Qc) Canada

Email: chris.develder@intec.ugent.be

**Abstract**—In this paper we address the problem of dimensioning infrastructure, comprising both network and server resources, for large-scale decentralized distributed systems such as grids or clouds. We will provide an overview of our work in this area, and in particular focus on how to design the resulting grid/cloud to be resilient against network link and/or server site failures. To this end, we will exploit relocation: under failure conditions, a request may be sent to an alternate destination than the one under failure-free conditions. We will provide a comprehensive overview of related work in this area, and focus in some detail on our own most recent work. The latter comprises a case study where traffic has a known origin, but we assume a degree of freedom as to where its end up being processed, which is typically the case for e.g., grid applications of the bag-of-tasks (BoT) type or for providing cloud services. In particular, we will provide in this paper a new integer linear programming (ILP) formulation to solve the resilient grid/cloud dimensioning problem using failure-dependent backup routes. Our algorithm will simultaneously decide on server and network capacity. We find that in the anycast routing problem we address, the benefit of using failure-dependent (FD) rerouting is limited compared to failure-independent (FID) backup routing. We confirm our earlier findings in terms of network capacity savings achieved by relocation compared to not exploiting relocation (order of 6–10% in the current case studies).

## I. INTRODUCTION

Easy access to powerful, and often distributed, hardware and software resources has been of key importance for science (e.g., the groundbreaking EGEE project [1]) as well as business (e.g., the hosting facilities offered by Amazon.com). As the resource offerings continue to grow and are also coming in reach of non-professional users, we are witnessing the emergence of a wide variety of novel applications also targeting this audience. A common observation in all these domains is the increasing reliance on networking, and hence a distributed infrastructure as sketched in Fig. 1.

The resulting grid/cloud infrastructure implies the need for efficient interworking of networking, storage and computing resources. Whereas grids mainly originated from scientific/academic needs — i.e., so-called e-Science applications, including high performance computing (HPC) — clouds manifest themselves in more commercially oriented applications (as opposed to the publicly funded research oriented grids), which often involve loosely coupled tasks, and are typically interactive [3]. In terms of infrastructure, they typically run in large data centers (as opposed to HPC infrastructures for

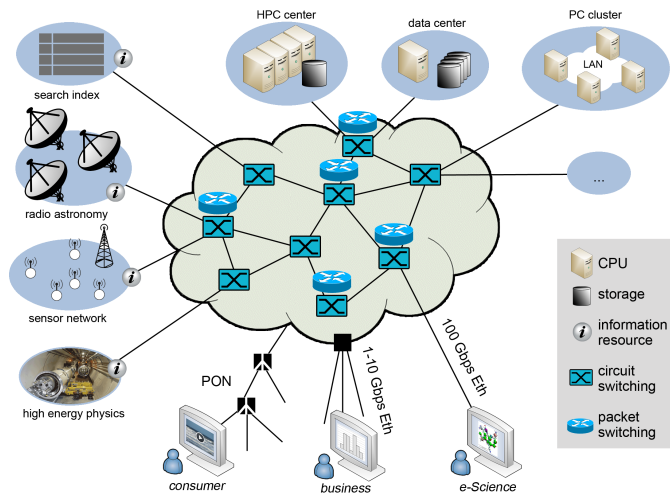


Fig. 1. Various types of users can tap into a resource rich optical grid/cloud environment, offering infrastructural resources (storage, computation and connectivity) and information (e.g., experimental data). Optical technology provides the high bandwidth connectivity to facilitate advanced application scenarios. (Reproduced from [2].)

many grid applications). It is clear that, given the increased popularity of such infrastructure, reliability is a prime concern. In the considered grid/cloud applications, this applies to both the network and IT resources for storage and computation. Whereas various approaches have been defined in each of these domains (network vs. IT) separately, their interdependency needs to be kept in mind to successfully deploy resilient grids/clouds.

In this paper, we particularly focus on jointly optimizing network and data center server capacities in a dimensioning study. Hereby, on the network part, we focus on the backbone network, which we assume to be an optical circuit-switched WDM network. Indeed, given their low latency and high capacity characteristics, optical technologies are a prime choice to support grids/clouds [2]. To deal with potential network failures, various network resilience strategies for WDM networks have been devised [4]. A well-known classical path protection scheme protects a primary path from source to destination by a link-disjoint backup path which is used in case of a failing link (this link diversity guarantees that the primary and

backup paths will never fail simultaneously for any single link failure). In a grid/cloud-like scenario however, we proposed the idea of exploiting relocation [5], which is possible due to the anycast routing principle. Since a grid/cloud user generally does not care about the exact location where his workload is being processed, it could be better to relocate the request to another resource (different from the one chosen under failure-free conditions).

The main contributions of this paper are: (i) a adjustment and extension of our previously proposed column-generation based model [6] for resilient grid/cloud dimensioning with failure-independent backup routing, in particular to also cover the case of 1:N server protection; (ii) a new model to solve the resilient grid/cloud dimensioning problem with failure-dependent backup routing; and (iii) a comprehensive discussion of both failure-dependent and failure-independent rerouting schemes in a fairly large EU-network topology, outlining the differences between them as well as the effects of relocating on both network and server resource capacity requirements. In the next section, we show the relation of these contributions to current state-of-the-art in research.

## II. RELATED WORK

The current paper addresses anycast in optical circuit-switched (OCS) WDM networks. The anycast routing problem in such OCS WDM networks amounts to the anycast routing and wavelength protection (ARWA), finding routes for each anycast request while e.g., minimizing the total number of wavelengths used, and/or the load on the links [7]. In [8], that *offline* problem for a given set of static traffic is solved in three subsequent phases: (i) destination decision, (ii) path routing, and (iii) wavelength assignment. This phased approach is shown to be outperformed by a heuristic algorithm (based on simulated annealing and genetic algorithms) in [9]. A generalized static *offline* RWA problem, comprising not only anycast, but also unicast and multicast requests, is described in [10], where heuristic algorithms are proposed to solve it. A similar problem is addressed in [11], but the author considers the joint routing of both unicast and anycast connections, and proposes a heuristic solution based on Langrangean relaxation. (Note that [11] also briefly touches on the associated *online* routing problem. Heuristic solutions to online anycast routing in WDM networks are also studied in [12], which proposes to vary the number of candidate anycast sites over time, according to time-varying load, and highlights the impact of physical layer impairments.)

Whereas the above mentioned works addressed the anycast routing problem in WDM networks to find working paths from source to one of the candidate anycast destinations, the authors of [13] extended the problem to also find backup paths. Also, they considered grooming: traffic granularity is supposed to be sub-wavelength and hence at intermediate nodes, traffic flows are re-combined to fill the wavelength channels most efficiently. They solved the *online* routing problem using an algorithm based on an auxiliary graph model, which finds working and backup routes for a single incoming anycast

request. The *offline* problem, which we will focus on, is addressed in [14], which considers the optimization of both working and shared backup paths of anycast and unicast demands jointly. The authors consider protection against single link failures and apply shared path protection.

Note that the above works address the network dimensions (i.e., wavelengths) only. However, we are interested in grid/cloud scenarios, and hence also want to consider server resources (for storage and computation). *Online* routing approaches taking into account both network and server constraints for such a scenario are presented in e.g., [15]. (Note that we consider a set of independent grid/cloud tasks/requests, each to be executed individually at one particular data center; for e.g., online scheduling of multiple interdependent tasks, see e.g., [16]).

In the current paper, we are addressing the *offline* dimensioning problem, as first tackled in [17]. In that work, we proposed a phased approach to determining both network and server dimensions for an optical grid scenario, without considering resiliency. A similar problem, but assuming mobile users, was addressed in [18] to find server locations and amount of servers for the case of mobile thin client computing.

A problem setting very close to the one studied by us below is presented in [19]: given a capacitated network, including servers, determine the placement of content, as well as primary and backup routing of requests for that content, with a given maximum number of replicas per content item. Thus, the main differences between our work and [19] (which only studies rather small scale problems) boil down to: (i) The candidate destination of an anycast (content) request in [19] is limited to a subset of all available data center locations, whereas we do not consider such limitation (although our model is fairly straightforward to extend by adding constraints); (ii) To protect against failures, [19] enforces relocation, whereas in our default model it is optional (but enforcing is straightforward); (iii) The focus in [19] is on minimizing used network resources, where server capacity is only indirectly controlled by limiting the number of replicas per content item rather than minimizing/limiting the server capacity.

## III. RESILIENT OPTICAL GRIDS/CLOUDS PROBLEM STATEMENT

For the sake of completeness, we formally recall the problem statement that we will address [6]:

### Given

- *Topology* comprising the source sites where traffic originates, data center sites that are the (candidate) destinations, as well as the optical network interconnecting them;
- *Demand* stating the amount of traffic originating at each of the source sites (where a unit demand implies 1 unit of network capacity, i.e., 1 wavelength, and 1 unit of server capacity); and
- *Survivability requirements* specifying the failures that should be protected against,

### Find

- $K$  destination locations, chosen out of the given candidate data center sites, where server infrastructure should be provided;
- Destination sites and routes to follow for all traffic, originating with given intensity at the various source sites (where each destination should be one of the  $K$  data center locations);
- Network and server capacity to provide on each of the links and data center sites;

**Such that** the latter resource capacity (server and network resources) is minimized.

To achieve the latter objective, we allow sharing capacity (wavelengths, servers) for the backup of connections whose primary resources do not fail simultaneously. Similarly, at each server site, we install the minimum capacity required to cope with each one of the considered failure scenarios (as well as the failure-free case, obviously). Thus, we allow reclaiming of server and network resources for backup purposes, if they are no longer used as primary under failure conditions.

We express the *survivability requirement* through the concept of a shared risk link group (SRLG): a set of resources (links) that may fail jointly, because of shared dependencies (e.g., fibre ducts [20]). Links in our model either are optical network links, or represent the connection to the data center. Thus, also server failures are modeled as failures of links, implying that through the SRLG concept we can model both network and server failures.

The ILP models below jointly determine the network and server capacities, as well as routes to follow for the anycast traffic. We assume WDM networks and consider the following network model, illustrated in Fig. 2:

- $G = (V, L)$ , directed graph representing an optical grid/cloud, where  $V$  is the node set and  $L$  is the set of (directed) links, where every link has the same unlimited transport capacity.
- $V = V_{\text{SRC}} \cup V_{\text{NET}} \cup V_{\text{DST}}$ , the set of all nodes indexed by  $v$ , comprising pure OXCs ( $V_{\text{NET}}$ ), data center sites  $V_{\text{DST}}$  (with  $|V_{\text{DST}}| = K$ ), and explicitly modeled sources  $V_{\text{SRC}}$ .
- $L = L_{\text{SRC}} \cup L_{\text{NET}} \cup L_{\text{DST}}$ , the set comprising all directed network links, indexed by  $\ell$ , again split into the core network links  $L_{\text{NET}}$  interconnecting OXCs, and the modeled access links  $L_{\text{SRC}}$  from job sources and those towards the data center sites  $L_{\text{DST}}$ .
- $\Delta_v$  The number of unit demand requests, originating from a source node  $v \in V_{\text{SRC}}$ .
- $S$  The set of SRLGs, where an individual  $s \in S$  is a set of links that can simultaneously fail. Note that the empty set ( $\emptyset$ ) will denote the failure free case.

We also will use the following notations:

- $\text{IN}(v)$  represents the set of incoming links of  $v \in V$ .
- $\text{OUT}(v)$  represents the set of outgoing links of  $v \in V$ .

#### A. Failure-independent (FID) path rerouting with relocation

Our previous work [6] considered a single backup path for each unit connection, i.e., we adopted a shared path protection

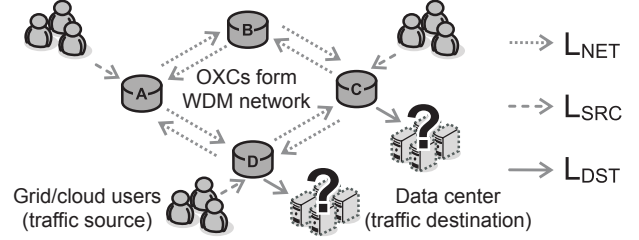


Fig. 2. Network model of the input data: (i) network links and nodes (OXCs labeled A-D), (ii) source nodes where traffic originates (represented here as users), and (iii) candidate data center sites.

concept. Thus, for a given demand unit the alternate path (possibly to a different destination) under any failure condition affecting the primary path was always the same. This is generally known as failure-independent (FID) restoration [20], [21], which previously also has been described as state-independent restoration [22], [23].

In previous work [6], [24], we proposed a column generation based solution for the dimensioning problem in this FID case. The results in the current work are based on the models proposed in [6]. Due to space constraints, we here simply point out our modifications to that model, which pertain to (i) an extension to cater for 1:N server protection, and (ii) adjusted constraints in the pricing problem (PP).

The extension (i) results in a change in the restricted master problem (RMP). To determine the number of servers to install (whose amount is expressed as  $w_\ell$  for  $\ell \in L_{\text{DST}}$ ), we will introduce a factor  $\rho_\ell$  to account for 1:N server protection. The latter requires that per  $N$  servers, 1 extra is added for protection, i.e., we need  $1+1/N$  times the total server capacity that is required to satisfy demand:

- $\rho_\ell$  Constant, which will be  $1 + 1/N$  for 1:N server protection for links  $\ell \in L_{\text{DST}}$ , and 1 in any other case (i.e., for network links  $\ell \in L_{\text{NET}}$ , or in case of no server protection for  $\ell \in L_{\text{DST}}$ ).

With this definition, equation (4) of [6] becomes:

$$w_\ell \geq \rho_\ell \cdot \left( \sum_{c \in C} \pi_{cls}^W \cdot z_c + \sum_{c \in C} \pi_{cls}^B \cdot z_c \right) \quad \forall s \in S, \forall \ell \notin s \quad (1)$$

The pricing problem (PP) adjustment (ii) concerns the fact that therein  $\pi_{\ell s}^W$  is defined to be 1 if both (a) the working path crosses link  $\ell$ , and (b) this working path remains unaffected by failure of SRLG  $s$ . Equation (10) of [6] does express only (a), and fails to capture the part (b). Therefore, constraint (10) of [6] should be replaced with the following, where  $p_\ell^W$  is a binary that equals 1 iff the working path crosses link  $\ell$ :

$$\left. \begin{aligned} \pi_{\ell s}^W &\geq p_\ell^W - a_s^W \\ \pi_{\ell s}^W &\leq p_\ell^W \\ \pi_{\ell s}^W &\leq 1 - a_s^W \end{aligned} \right\} \quad \forall s \in S, \forall \ell \notin s \quad (2)$$

Constraint (2) hence enforces that  $\pi_{\ell s}^W \equiv p_\ell^W \wedge \neg a_s^W$ . We also note that [6] lacked an upper bounding constraint for  $a_s^W$ .

The latter binary variable equals 1 iff (b) holds, translating to the logical relation  $a_s^W \equiv \bigvee_{\ell' \in s} p_{\ell'}^W$ , and (12) of [6] should be:

$$\left. \begin{aligned} M \cdot a_s^W &\geq \sum_{\ell' \in s} p_{\ell'}^W \\ a_s^W &\leq \sum_{\ell' \in s} p_{\ell'}^W \end{aligned} \right\} \forall s \in S, \text{ with } M = |s| \quad (3)$$

### B. Failure-dependent (FD) path rerouting with relocation

The alternative we will consider here is that of failure-dependent (FD), aka state-dependent, rerouting. To study the FD case, we make use of a fairly straightforward ILP as sketched below. Since we did not observe scalability issues in studying fairly large problems (see Section IV), we did not resort to column generation as in the FID case [6]. Note that the ILP for the FD case below assumes that the  $K$  best candidate destination locations have been chosen. This can be realized through a simple ILP model as described in [17].

In addition to the constants  $\rho_\ell$  as defined before in Section III-B, we define the following ILP variables:

- $p_{vls}$  The number of unit demands originating from  $v \in V_{\text{SRC}}$  that are crossing link  $\ell \in L$  under failure of  $s \in S$  ( $s = \emptyset$  represents the failure free case).
- $w_\ell$  The capacity to provide on link  $\ell \in L$ . For network links  $\ell \in L_{\text{NET}}$ , this amounts to the number of wavelengths. For data center links  $\ell \in L_{\text{DST}}$  this will represent the number of nodes  $v \in V_{\text{SRC}}$ .

The objective is given in (4): we minimize the amount of network resources (wavelengths  $w_\ell$ ) and the amount of server resources, which in our model is conveniently represented as the capacity on server links. We introduce a factor  $\alpha$  that expresses the cost ratio of the server capacity corresponding to a workload filling a single wavelength with data, compared to the cost of a single wavelength on a single link.

$$\min \left( \sum_{\ell \in L_{\text{NET}}} w_\ell + \alpha \cdot \sum_{\ell \in L_{\text{DST}}} w_\ell \right) \quad (4)$$

The first set of constraints constitute the demand constraints which dictate where traffic originates (5)–(6) and ends (7), as well as the traditional flow conservation constraint in intermediate network nodes (8). These constraints have to hold  $\forall v \in V_{\text{SRC}}, \forall s \in S$ :

$$p_{v\ell's} = \Delta_v \quad \text{where } \{\ell'\} = \text{OUT}(v) \quad (5)$$

$$p_{vls} = 0 \quad \forall \ell \in L_{\text{SRC}} \setminus \text{OUT}(v) \quad (6)$$

$$\sum_{\ell \in L_{\text{DST}}} p_{vls} = \Delta_v \quad (7)$$

$$\sum_{\ell \in \text{IN}(v')} p_{vls} = \sum_{\ell \in \text{OUT}(v')} p_{vls} \quad \forall v' \in L_{\text{NET}} \quad (8)$$

The next constraint (9) expresses that traffic cannot cross affected links for each respective failure scenario:

$$p_{vls} = 0 \quad \forall v \in V_{\text{SRC}}, \forall s \in S, \forall \ell \in s \quad (9)$$

The final constraint amounts to counting the capacity required for each link (or data center):

$$w_\ell \geq \rho_\ell \cdot \sum_{v \in V_{\text{SRC}}} p_{vls} \quad \forall v \in V_{\text{SRC}}, \forall s \in S, \forall \ell \in L_{\text{NET}} \cup L_{\text{DST}} \quad (10)$$

The aforementioned equations cover the case of failure-dependent rerouting, exploiting relocation (if it is beneficial). To obtain resource dimensions for the non-relocation case, we need to enforce that for all failure cases the same data center is chosen as in the failure free case. This implies  $\forall v \in V_{\text{SRC}}, \forall s \in S \setminus \{s'\}, s' = \emptyset, \forall \ell \in L_{\text{DST}}$ :

$$p_{vls} = p_{vls'} \quad (11)$$

As a final remark, note that the model defined by (4)–(10) amounts to optional relocation, i.e., an alternate destination site will only be chosen if that leads to lower overall costs as per the objective. In case we want to enforce relocation under failure conditions (as in [19], we can add the following constraint<sup>1</sup>,  $\forall v \in V_{\text{SRC}}, \forall \ell \in L_{\text{DST}}, s' = \emptyset$ :

$$(p_{vls'} = 0) \vee \left( \sum_{s \in S \setminus \{s'\}} p_{vls} = 0 \right) \quad (12)$$

## IV. CASE STUDY

Our case study to assess the impact of relocation under failure-dependent backup routing used the same test network of [6], i.e., a European network topology composed of 28 nodes and 41 bidirectional links. We compared the following cases for failure-dependent backup rerouting:

- *FD, 1L, NoReloc*: Protect against single link failures only, without relocating, i.e., using model (4)–(11).
- *FD, 1L, Reloc*: Protect against single link failures only, exploiting relocation, i.e., using model (4)–(10).
- *FD, 1LSN, NoReloc*: Protect against single failures of either links or data center servers (using 1:N protection for servers), without relocating, i.e., using model (4)–(11).
- *FD, 1LS, Reloc*: Protect against single failures of either links or data center servers, exploiting relocation, i.e., using model (4)–(10). To ensure relocation is optional (meaning that server failures can also be protected by adding backup servers at the primary location), we foresee 2 parallel server links between each data center node and its corresponding OXC (thus  $L_{\text{DST}}$  contains twice as much elements as for the other cases).

The settings for the SRLG set  $S$  and the link capacity factors  $\rho_\ell$  in the various failure scenarios are summarized in Table I.

In our results, we consider the case of  $K = 3$  server sites, where we did not fix the locations a priori (as opposed to [25]). As pointed out previously, we use the server location ILP of [17] to choose them, based on the demand. For the latter, we varied the total number of unit demands ( $D = \sum \Delta_v$ ) between

<sup>1</sup>Note that a constraint of the form  $(a = 0) \vee (b = 0)$  can be easily modeled as linear constraints. Let  $A, B$  be binary variables, so that  $A \equiv (a = 0)$  and  $B \equiv (b = 0)$ . Then the  $\vee$  constraint becomes  $A + B \geq 1$ .

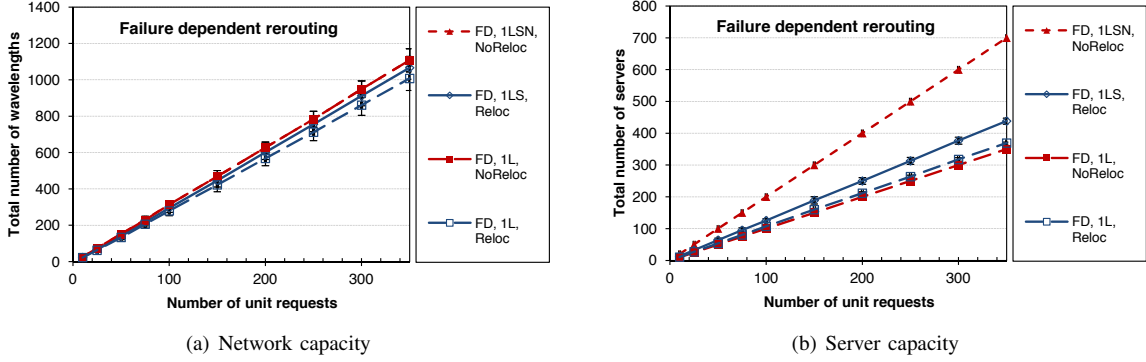


Fig. 3. The resource capacity required in the EU network for  $\alpha = 1$ ,  $K = 3$ , in case of *failure dependent* (FD) rerouting, using  $N = 1$  for the  $1 : N$  server protection in the NoReloc 1LSN case. Error bars (which are largely hidden behind data point markers) indicate 90% confidence intervals derived from the 10 random instances per data point. Note that the network capacity is exactly the same for both NoReloc cases.

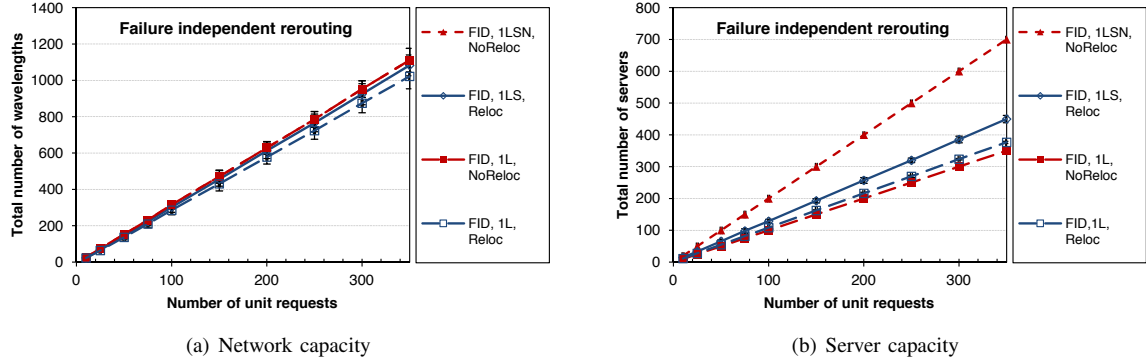


Fig. 4. The resource capacity required in the EU network for  $\alpha = 1$ ,  $K = 3$ , in case of *failure independent* (FID) rerouting, using  $N = 1$  for the  $1 : N$  server protection in the NoReloc 1LSN case. Error bars (which are largely hidden behind data point markers) indicate 90% confidence intervals derived from 10 random instances per data point. Note that the network capacity is exactly the same for both NoReloc cases.

Table I  
MODEL SETTINGS FOR THE CONSIDERED FAILURE SCENARIOS.

Acronym	ILP model settings
1L	$S = \{\{\ell, \ell'\} \mid \ell, \ell' \in L_{\text{NET}}, \ell \text{ is the reverse of } \ell'\} \triangleq S_{1L}$ $\rho_\ell = 1, \forall \ell \in L$
1LS	$S = S_{1L} \cup \{\{\ell\} \mid \ell \in L_{\text{DST}}\}$ $\rho_\ell = 1, \forall \ell \in L$
1LSN	$S = S_{1L}$ $\rho_\ell = 1 + 1/N$ if $\ell \in L_{\text{DST}}$ , else 1

10 and 350. For each  $D$ , we created 10 random instances. The measures plotted below are averages over those 10 random instances per demand case. We set the relative server cost parameter  $\alpha = 1$ .

Let us first look at the results for failure dependent rerouting (FD), as per our new model of Section III-B. In the case of protecting against *single link failures* (1L), we note the clear advantage of exploiting relocation on network capacity: we observe a reduction of required number of wavelengths in the order of 10.7% (average over all  $D \in [10, 350]$  cases; in line with our earlier findings for the failure-independent rerouting case [6]). The price we pay for this reduced network capacity, is a slight increase in required server capacity (order of +6.4%, again averaged over our  $D \in [10, 350]$  cases; with lower values

for higher demand). With our assumed wavelength/server unit cost ratio of  $\alpha = 1$ , and the dominant network resources (cf. scale difference between Fig. 3(a) and (b)), there is indeed a net advantage to exploiting relocation. For the case of protection against both *single link or single server failures* (1LS / 1LSN), the advantage continues to hold. We observe in this case a reduction in total wavelength capacity in the order of 6% (avg. over all  $D \in [10, 350]$ ). The relocation case (*Reloc 1LS*) obviously requires additional server capacity compared to the *NoReloc 1L* case, but considerably less than adding 1:1 server protection: server capacity reduction achieved by *Reloc 1LS* compared to *NoReloc 1LSN* amounts to around 36.5% (avg. over all  $D \in [10, 350]$ ). Thus, the server cost to realize protection against link or server failures exploiting relocation is of the same order as 1:3 server protection without relocation (but still with a clear reduction of network resources).

Coming now to the difference between failure dependent (FD) and failure independent (FID) rerouting, we see that the discussion above continues to hold for the FID case. Indeed, comparing the respective cases (in terms of exploiting relocation and server/link protection scenario) for FID versus FD, we see that obviously FID never outperforms FD. Yet, deviations, i.e.,  $FID/FD - 1$ , are quite limited: below 1% for the *NoReloc* cases, and around 2% for the *Reloc* cases (a

difference well below the 90% confidence interval bounds, cf. Fig. 3 and Fig. 4.) Thus, in the considered case of anycast routing, both with and without exploiting relocation, the advantage of having backup routes tailored to the particular failure case (i.e., FD instead of FID) is limited. This is in line with similar conclusions comparing FD vs. FID rerouting in cases of simple unicast traffic [20], [23].

## V. CONCLUSION

We have presented in this paper, and its predecessor [6], scalable methods to dimension both the network and data center capacities in an optical grid/cloud context to satisfy a given (static) set of requests for data center infrastructure (server capacity) and network connectivity to reach it. We particularly stress the importance of recognizing the freedom to choose the exact location of those data centers and the ones that are chosen to fulfill a particular request. This can be exploited in the form of so-called relocation to protect not just against network link, but also data center server failures: requests can be relocated to alternate data centers in case of failures. Exploiting relocation brings benefits in terms of required network capacity (reductions of over 10% in our case study), and comes at an additional server capacity cost (compared to failure-free conditions) well below that of 1:1 server protection. In our case study, failure-dependent (FD) rerouting, where backup routes (and server locations) may be chosen differently for different failure cases, does not bring significant benefits compared to failure-independent (FID) routing with a single backup path and destination for all failure cases. Our ILP models (which in the FID case are based on column generation) prove to be quite scalable, given our case study on a large EU network with up to 350 requests.

## ACKNOWLEDGMENT

Work described in this paper was partly funded by the European Commission through the 7th ICT-Framework Programme (FP7) project Geysers (grant FP7-ICT-248657) and by Ghent University through GOA Optical Grids (grant 01G01506). Results were obtained using the Stevin Supercomputer Infrastructure at Ghent University. J. Buysse was funded through a Ph.D. grant from the agency for Innovation by Science and Technology (IWT). M. De Leenheer and C. Develder (in part) were supported as post-doctoral fellows of the Research Foundation Flanders (FWO-VI.).

## REFERENCES

- [1] F. Gagliardi, B. Jones, F. Grey, M.-E. Bégin, and M. Heikkurinen, "Building an infrastructure for scientific grid computing: status and goals of the EGEE project," *Philos. Transact. A Math Phys. Eng. Sci.*, vol. 363, no. 1833, pp. 1729–1742, Aug. 2005.
- [2] C. Develder, M. De Leenheer, B. Dhoedt, M. Pickavet, D. Colle, F. De Turck, and P. Demeester, "Optical networks for grid and cloud computing applications," *Proc. IEEE*, vol. 100, no. 4, Apr. 2012.
- [3] I. Foster, Y. Zhao, I. Raicu, and S. Lu, "Cloud computing and grid computing 360-degree compared," in *Proc. Grid Computing Environments Workshop (GCE 2008)*, Austin, TX, USA, 16 Nov. 2008, pp. 1–10.
- [4] S. Ramamurthy and B. Mukherjee, "Survivable WDM mesh networks, part I – protection," in *Proc. 18th IEEE Conf. Computer Commun. (INFOCOM 1999)*, vol. 2, San Francisco, CA, USA, 29 Mar. – 2 Apr. 1999, pp. 744–751.

- [5] J. Buysse, M. De Leenheer, B. Dhoedt, and C. Develder, "Providing resiliency for optical grids by exploiting relocation: A dimensioning study based on ILP," *Comput. Commun.*, vol. 34, no. 12, pp. 1389–1398, Aug. 2011.
- [6] C. Develder, J. Buysse, A. Shaikh, B. Jaumard, M. De Leenheer, and B. Dhoedt, "Survivable optical grid dimensioning: anycast routing with server and network failure protection," in *Proc. IEEE Int. Conf. Commun. (ICC 2011)*, Kyoto, Japan, 5–9 Jun. 2011.
- [7] M. Tang, W. Jia, H. Wang, and J. Wang, "Routing and wavelength assignment for anycast in WDM networks," in *Proc. 3rd Int. Conf. Wireless and Optical Commun. (WOC 2003)*, Banff, Canada, 14–16 Jul. 2003, pp. 301–306.
- [8] D.-R. Din, "Anycast routing and wavelength assignment problem on WDM network," *IEICE Trans. Commun.*, vol. EE88-B, no. 10, pp. 3941–3951, Oct. 2005.
- [9] —, "A hybrid method for solving ARWA problem on WDM networks," *Comput. Commun.*, vol. 30, pp. 385–395, Jan. 2007.
- [10] E. Hyytiä, "Heuristic algorithms for the generalized routing and wavelength assignment problem," in *Proc. 17th Nordic Teletraffic Seminar (NTS-17)*, Fornebu, Norway, 25–27 Aug. 2004, pp. 373–386.
- [11] K. Walkowiak, "Anycasting in connection-oriented computer networks: Models, algorithms and results," *J. Appl. Math. Comput. Sci.*, vol. 20, no. 1, pp. 207–220, Mar. 2010.
- [12] K. Bhaskaran, J. Triay, and V. M. Vokkarane, "Dynamic anycast routing and wavelength assignment in WDM networks using ant colony optimization," in *Proc. IEEE Int. Conf. Commun. (ICC 2011)*, Kyoto, Japan, 5–9 Jun. 2011.
- [13] Q. She, X. Huang, Q. Zhang, Y. Zhu, and J. Jue, "Survivable traffic grooming for anycasting in WDM mesh networks," in *Proc. IEEE Global Telecommun. Conf. (GLOBECOM 2007)*, Washington D.C., USA, 26–30 Nov. 2007, pp. 2253–2257.
- [14] K. Walkowiak and J. Rak, "Shared backup path protection for anycast and unicast flows using the node-link notation," in *Proc. IEEE Int. Conf. Commun. (ICC 2011)*, Kyoto, Japan, 5–9 Jun. 2011.
- [15] T. Stevens, M. De Leenheer, C. Develder, B. Dhoedt, K. Christodouloulopoulos, P. Kokkinos, and E. Varvarigos, "Multi-cost job routing and scheduling in grid networks," *Futur. Gener. Comp. Syst.*, vol. 25, no. 8, pp. 912–925, Sep. 2009.
- [16] X. Liu, C. Qiao, W. Wei, X. Yu, T. Wang, W. Hu, W. Guo, and M.-Y. Wu, "Task scheduling and lightpath establishment in optical grids," *IEEE J. Lightwave Technol.*, vol. 27, no. 12, pp. 1796–1805, Jun. 2009.
- [17] C. Develder, B. Mukherjee, B. Dhoedt, and P. Demeester, "On dimensioning optical grids and the impact of scheduling," *Photonic Netw. Commun.*, vol. 17, no. 3, pp. 255–265, Jun. 2009.
- [18] L. Deboosere, P. Simoens, J. De Wachter, B. Vankeirsbilck, F. De Turck, B. Dhoedt, and P. Demeester, "Grid design for mobile thin client computing," *Futur. Gener. Comp. Syst.*, vol. 27, no. 6, pp. 681–693, Jun. 2011.
- [19] M. Habib, M. Tornatore, M. De Leenheer, F. Dikbiyik, and B. Mukherjee, "A disaster-resilient multi-content optical datacenter network architecture," in *Proc. 13th Int. Conf. Transparent Optical Netw. (ICTON 2011)*, Stockholm, Sweden, 26–30 Jun. 2011, pp. 1–4.
- [20] H. Zang, C. Ou, and B. Mukherjee, "Path-protection routing and wavelength assignment (RWA) in WDM mesh networks under duct-layer constraints," *IEEE/ACM Trans. Netw.*, vol. 11, no. 2, pp. 248–258, Apr. 2003.
- [21] 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.
- [22] Y. Xiong and L. G. Mason, "Restoration strategies and spare capacity requirements in self-healing ATM networks," *IEEE/ACM Trans. Netw.*, vol. 7, no. 1, pp. 98–110, Feb. 1999.
- [23] Y. Xiong and L. Mason, "Comparison of two path restoration schemes in self-healing networks," *Comput. Netw.*, vol. 38, no. 5, pp. 663–674, Apr. 2002.
- [24] A. Shaikh, J. Buysse, B. Jaumard, and C. Develder, "Anycast routing for survivable optical grids: scalable solution methods and the impact of relocation," *IEEE/OSA J. Opt. Commun. Netw.*, vol. 3, no. 9, pp. 767–779, Sep. 2011.
- [25] B. Jaumard, J. Buysse, A. Shaikh, M. De Leenheer, and C. Develder, "Column generation for dimensioning resilient optical grid networks with relocation," in *Proc. IEEE Global Telecommun. Conf. (GLOBECOM 2010)*, Miami, FL, USA, 6–10 Dec. 2010, pp. 1–6.