Vulnerability Modelling for Periodical Flexgrid Network Planning

M. Ruiz* and L. Velasco

Optical Communications Group (GCO), Universitat Politècnica de Catalunya (UPC), Barcelona, Spain

**e-mail: mruiz@ac.upc.edu*

ABSTRACT

Dynamic flexgrid optical networks are being developed to operate under highly changing traffic scenarios. Planning such optical networks is fully dependent on the traffic characteristics whereas the constant traffic evolution needs of continuous network planning actions to adapt to new scenarios. Therefore, networks need to be periodically re-planned to consider features such as survivability degree to be reached during its operation. Since traffic changes could lead to the violation of some of these requirements, they can trigger network upgrading process. In this work, we introduce network vulnerability modelling with the aim of providing statistical models to be used as vulnerability predictors in periodical network planning problems.

Keywords: network vulnerability, dynamic flexgrid networks, statistical modelling.

1. INTRODUCTION

Future flexgrid-based optical networks need to be designed to operate in dynamic traffic scenarios. Dynamicity in the network is coped by means of a control plane allowing automatic connections set-up and tear down. Significant research and standardisation effort has assisted in defining control plane architectures and protocols to automate connection provisioning. Starting from a distributed paradigm, control plane have lately moved towards a centralised one led by the development of the software-defined network (SDN) concept with the introduction of OpenFlow [1].

Due to the constant increase and evolution of Internet traffic, optical networks must be periodically re-designed (in response to predicted traffic changes) in order to keep committed service requirements for the next period [2]. In dynamic networks, network planning entails enormous complexity as a consequence of including probabilistic distributions or even hardly predictable patterns into mathematical programming formulations. In our previous work, we introduced a method facilitating the design of flexgrid-based optical networks under dynamic traffic operation by means of statistical traffic models easily usable in network design algorithms running mathematical programming formulations [3].

Among the requirements commonly considered in optical network design, survivability is a prominent topic. To ensure such survivability, periodical network planning must deal with a proper dimensioning of spare capacity needed in case of failures, as well as a topology design maximizing network robustness [4]. Moreover, an on-line recovery mechanism must be implemented and applied each time a failure impacts the network to restore the affected traffic. Recently, a dynamic restoration algorithm based on bulk path computation has been proven as a fast and effective procedure to restore optical connections (lightpaths) affected by a link failure [5].

It is worth mentioning that significant traffic changes in terms of volume or distribution could lead to saturate part of the network capacity resources affecting the effectiveness of the restoration algorithm to find alternative routes in case of failure. In this scenario of continuous traffic evolution, it is crucial to anticipate the network survivability degradation, *i.e*., to predict *network vulnerabilities*. By means of a model predicting such vulnerability, a network upgrading step can be triggered when the expected vulnerability reaches a given threshold.

In this paper, we introduce the use of statistical models of vulnerability prediction to be used in periodical network planning with the aim of upgrading an existing network and keeping network survivability along traffic evolution. Hereafter, the vulnerability is defined as the probability that a lightpath affected by a link failure cannot be recovered by the dynamic restoration mechanism. In the following we first present a flow chart illustrating the process of periodical network planning for a dynamical network operation. Then, a numerical study on vulnerability using reference topologies from real operators is provided. The objective of this study is to detect which network characteristics are more tightly related with vulnerability, being this the seed of a further modelling contribution targeting at finding accurate vulnerability prediction models.

2. PERIODICAL NETWORK PLANNING FLOW CHART

Figure 1 shows the periodical network planning flow chart considered in this work, where the following list of elements involved in the process is assumed:

- A dynamic optical network automatized by means of a control plane and a software-defined network (SDN)-based controller. Although not detailed in the figure, the SDN controller includes several functional elements such as an active stateful Path Computation Element (PCE).

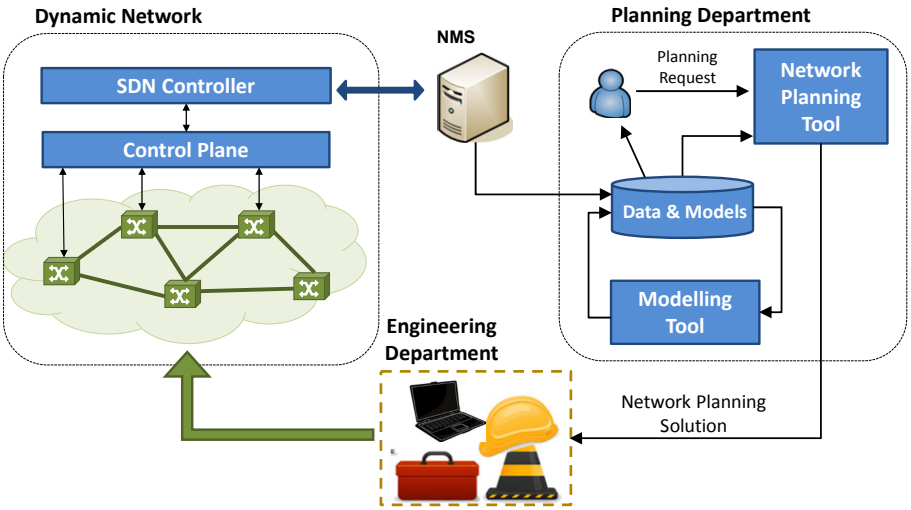

Figure 1. Periodical network planning flow chart.

- The Network Management System (NMS) managing the core network, implementing fault, configuration, administration, performance, and security (FCAPS) functions.
- A Planning Department administrating the planning process, *i.e.*, analyzing the network performance and finding bottlenecks, receiving potential clients' needs, evaluating network planning upgrades, *etc*.
- An Engineering Department, performing actions related to equipment installation and set-up.
- A Planning Tool in charge of computing solutions for each planning step. Several sub-problems related to network reconfiguration, planning, and dimensioning, among others, need to be solved.
- A Modelling Tool in charge of generating network models from the data obtained from real operation. Using statistical modelling and machine learning techniques, a set of models for selected variables (*e.g*. network vulnerability) are continuously improved to increase the accuracy of future predictions.
- A Data & Models database, containing the statistical models and reference parameters to be used for analytical purposes and as inputs for the planning tool when a planning problem needs to be solved.

We consider that a network planning step begins when the planning department detects from the available data and models that a planning step can improve the performance of the current network, *e.g*. the vulnerability at some part of the network is reaching the maximum permitted threshold. Without entering into details, optimization problems available in the planning tool belong to one of the next two classes:

- *Network reconfiguration problems* consisting in reconfiguring the existing network resources without purchasing and installing new flexgrid equipment. Among others, some of the possible actions that could form a solution of this reconfiguration phase are, (*i*) modifying the physical intra-connectivity at central stations, (*ii*) moving physical devices, *e.g*., transponders, from one location to another in a different part of the network, and (*iii*) activating already purchased and installed network resources not yet in operation.
- *Network upgrading problems* involving several network planning and dimensioning sub-problems, such as enlarging the network with new capacity resources or extending the network towards non-covered areas. The overall objective is to find solutions meeting new traffic requirements while minimizing the total cost including purchasing, installing and configuring new equipment.

Once a solution is accepted by operators at the planning department, the changes to be done in the network are sent to the engineering department, which, in turn, organizes and schedules the set of processes that will physically implement the solution in the network. When the changes are implemented and tested, then the network can start operating with the new set of resources. Note that these network changes have a clear impact on the performance of dynamic algorithms dealing with routing and restoration. Moreover, recall that a planning step is triggered as a consequence of a detected traffic change. Therefore, for these very reasons, the statistical models used for planning must be re-fitted and adapted to the new in-operation scenario. This continuous model fitting allows strengthening the potential of models for predicting unknown situations and training the system for new future planning steps.

3. NUMERICAL STUDY ON NETWORK VULNERABILITY

The behavior of a dynamic network subject to link failures has been emulated by means of an ad-hoc OMNeT++ event-driven simulator. The simulator mainly runs two online algorithms: a) a dynamic RSA algorithm for provisioning lightpaths for incoming requests and b) a dynamic restoration algorithm based on bulk path

computation [5] to recover all optical connections affected by a link failure. As previously anticipated, sometimes the restoration is not complete and, hence, some of the lightpaths must be rejected due to the lack of free spectrum resources when searching for a new route skipping the failed link. For this reason, we define the *restorability* of a network as the percentage of traffic that can be restored after the event of a link failure. Therefore, vulnerability is measured in terms of restorability.

Three reference topologies were used to obtain large datasets, namely, the 12-node Deustche Telekom (DT), the 22-node British Telecom (BT), and the 30-node Telefonica (TEL) topologies. Two types of requests were randomly generated: *intra-domain* and *inter-domain*. An intra-domain request consists in a node pair source-destination randomly chosen among all network nodes with identical probability. On the other hand, an inter-domain request is defined by a randomly chosen source node (as for intra-domain requests) and a randomly selected destination among the reduced set of nodes connecting to other domains (named as inter-connection nodes). New connection arrivals are generated following a Poisson process, whereas holding connection times fit the exponential distribution. Moreover, we assume that each incoming connection requests a bit rate equal to 40, 100, or 400 Gb/s with probability 0.66, 0.26, and 0.08, respectively. By combining different proportion of intra and inter-domain requests, we generated traffic according to three different traffic profiles (TPs): 100% intra-domain (TP-100), 50%-50% intra and inter-domain (TP-50), and 100% inter-domain (TP-0).

For each of the topologies and TPs, we exhaustively studied the impact of each link on the overall network restorability in a scenario of high vulnerability. Specifically, we consider that the maximum allowed vulnerability is met when restoration is close to 99%. For the network load causing such vulnerability, an exhaustive simulation is run generating random failures at only one of the links at each time. After the failure event is processed, the restoration algorithm is executed, the resultant restorability is stored, and the link is activated again. The process is repeated until ensuring that each of the links has received a large amount of failures (more than 100). Note that the time between consecutive failures is enough large to ensure that none of the connections existing when a failure occurs are still set up when the next failure comes.

With the data obtained from the experiment above, the vulnerability of the network is analyzed for each of the network links separately. Thus, we aim at finding the relationship between the characteristics of the link and its associated restorability. In the ongoing analysis, we firstly focus on the impact of the amount of traffic carried in the link before the failure event and, afterwards, the correlations between few topology-dependent variables and restorability is evaluated.

A priori, one could state that the higher the traffic carried in a link, the higher the probability that the restoration algorithm rejects part of the traffic and, consequently, the higher the vulnerability. However, this assumption cannot be confirmed when observing Fig. 2, where the restorability is depicted as a function of the network load. In view of the figures, it is worth noting that the lowest restorability values are not observed for those higher loads. Especially interesting is the case of TEL, where poor restorability (91% – 92%) is observed for very low loaded links (around 10%). Aiming at complementing these results, Fig. 3 depicts the specific case of the DT topology where network links with the lowest restorability and highest load are highlighted with colored thick lines. As can be observed, most vulnerable links (with restorability<99%) do not coincide with highest loaded links, and hence, we should conclude that additional information is needed if an accurate restorability prediction model is desired.

Figure 4 depicts the restorability as a function of three topology-dependent variables. The *algebraic connectivity* and the *average hop path length* are topology variables related with network robustness and connectivity (see [3] and [4] for further details). Since we look for link variables instead of topology variables, both variables are computed for the network after removing such link, thus obtaining different values for each of the links. Moreover, the *hub connectivity* is a link variable created to illustrate the centrality of those links incident with an inter-connection node (being > 0 in this case and 0 when link is not incident with inter-connection nodes). Curves depict the trend of the correlation between variables, where a remarkable slope indicates a strong correlation, whereas a soft and horizontal trend denotes that the variable does not provide usable information to predict the restorability. In light of the results, several conclusions can be obtained. First, we can see that the algebraic connectivity has a strong positive correlation with restorability when the traffic is uniformly distributed (TP-100), losing its prediction strength when inter-domain traffic increases and connection requests are asymmetrically distributed along the network. A similar behavior is observed for the average hop path length but with a remarkable difference: correlation is not monotonic with respect to that variable, being positively or negatively correlated depending on the range. This leads us to consider the use of non-linear interactions among topology-dependent variables which should be deeply investigated in order to find those combinations more useful for statistical modelling. Finally, we observe that the hub connectivity explains better the restorability when the inter-domain traffic increases. In view of this, we conclude that the traffic distribution is a crucial factor to determine which variables are significant in order to predict the restorability.

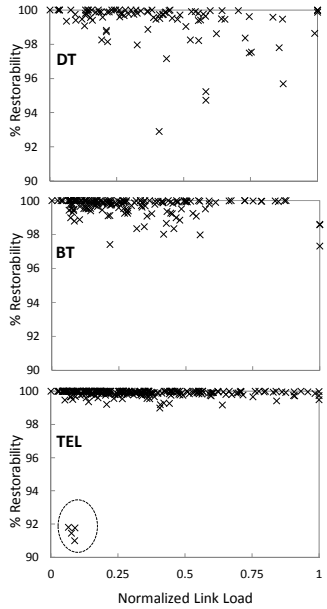

Figure 2. Restorability vs. link load.

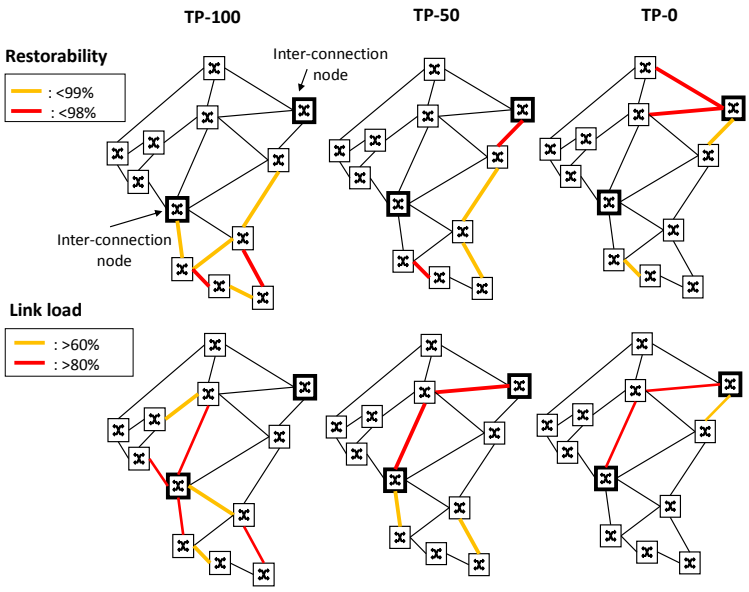

Figure 3. Links with highest load and highest vulnerability in DT topology.

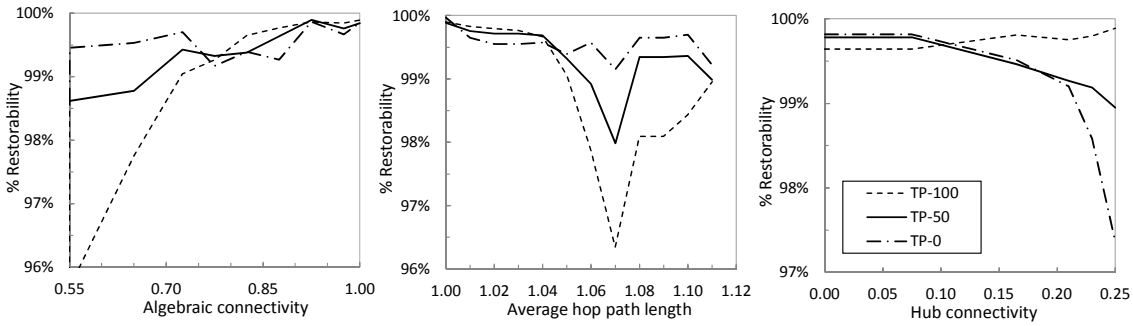

Figure 4. Correlation between restorability and selected topology dependent variables.

4. CONCLUDING REMARKS

An approach to the network vulnerability modelling for adaptive periodical network planning has been proposed. A numerical study has been presented to illustrate the correlation between some network characteristics and vulnerability. In view of the results, we concluded that a vulnerability model should contain not only variables related with the link resource usage but also with topology-dependent variables. However, the significance of all these variables is strongly dependent on the traffic the network must deal with. Therefore, the proposed evolutionary modelling process must consider the addition or removal of model variables to better adapt to traffic evolution.

ACKNOWLEDGEMENTS

The research leading to these results has received funding from the European Community's Seventh Framework Programme FP7/2007-2013 under grant agreement n° 317999 IDEALIST project. Moreover, it was supported by the Spanish science ministry through the TEC2011-27310 ELASTIC project. The authors want to thank MSc. Noemí Germen for his very valuable contribution to this work.

REFERENCES

[1] L. Velasco *et al*., "In-operation network planning," *IEEE Communications Magazine*, vol. 52, pp. 52-60, 2014.
[2] M. Ruiz *et al*., "Planning fixed to flexgrid gradual migration: Drivers and open issues," *IEEE Communications Magazine*, vol. 52, pp. 70-76, 2014.
[3] M. Ruiz, L. Velasco, J. Comellas, and G. Junyent, "A traffic intensity model for flexgrid optical network planning under dynamic traffic operation," in *Proc. IEEE/OSA Optical Fiber Communication Conference (OFC)*, 2013.
[4] W. Liu, H. Sirisena, K. Pawlikowski, and A. McInnes, "Utility of algebraic connectivity metric in topology design of survivable networks," in *Proc. DRCN*, 2009.
[5] A. Castro, L. Velasco, J. Comellas, and G. Junyent, "On the benefits of multi-path recovery in flexgrid optical networks," accepted in *Springer Photonic Network Communications*, 2014.
[6] L. Velasco, A. Castro, M. Ruiz, and G. Junyent, "Solving routing and spectrum allocation related optimization problems: From off-line to in-operation flexgrid network planning," [Invited Paper] *Journal of Lightwave Technology (JLT)*, 2014.