Improving the Resilience of Transport Networks to Large-scale Failures

Juan Segovia, Pere Vilà, Eusebi Calle, and Jose L. Marzo
Institute of Informatics and Applications (IIiA), University of Girona, Spain
Email: {juan.segovia, pere.vila, eusebi.calle, joseluis.marzo}@udg.edu

Abstract—Telecommunication networks have to deal with fiber cuts, hardware malfunctioning and other failures on a daily basis, events which are usually treated as isolated and unrelated. Efficient methods have been developed for coping with such common failures and hence users rarely notice them. Although less frequently, there also arise cases of multiple failures with catastrophic consequences. Multiple failures can occur for many reasons, for example, natural disasters, epidemic outbreaks affecting software components, or intentional attacks. This article investigates new methods for lessening the impact of such failures in terms of the number of connections affected. Two heuristic-based link prioritization strategies for improving network resilience are proposed. One strategy is built upon the concept of betweenness centrality, while the second is based on what we call the observed link criticality. Both strategies are evaluated through simulation on a large synthetic topology that represents a GMPLS-based transport network. The provisioning of connections in a dynamic traffic scenario as well as the occurrence of large-scale failures are simulated for the evaluation.

Index Terms—Network resilience, Large-scale failures, Multiple failures, GMPLS, Link criticality.

I. INTRODUCTION

Today’s data transport networks are designed to withstand several types of failures, namely accidental or intentional fiber cuts, loss of switching capabilities caused by power outages, malfunctioning due to equipment aging, and even operator mistakes. This ability to maintain service continuity in the presence of failures owes to efficient recovery techniques incorporated in their design, as well as to diverse technologies that have been developed to that end. Several methods and techniques are reported in the literature for dealing with failures [1], [2]. The fundamental underlying idea is that of redundancy, whereby spare resources come into operation when the active one fails.

The majority of the approaches to network recovery assume that at any given time, only one failure is outstanding, which is known as the single-failure assumption [3]. However, networks are equally prone to multiple-failure events, that is, the concurrent failure of several communication elements. For instance, earthquakes, flooding and natural disasters have the potential to disrupt a large number of network elements simultaneously.

Although large-scale failure events may be relatively rare, that fact does not lessen the economic loss they cause, or the disruption the can bring onto thousands or even millions of users. Unfortunately, in such failure scenarios the redundancy-based recovery techniques that are effective under the single-failure assumption are not suitable anymore, simply because the cost of implementing massive redundancy for rarely occurring events is prohibitive [4].

Multiple failures has been studied in the context of complex networks, graph theory and epidemics for some time now, see for example [5], [6] and [7] and the references therein. However, in the context of the reliability of transport networks, which is our focus here, the number of reported research is fewer, much more recent and almost always concerned with multilayer networks, where several failures visible in an upper layer are all caused by exactly one failure at the physical layer.

In this article, we consider that a certain number of physical links which represent a large portion of the topology fail concurrently, and study how such large-scale failure affects the network’s resilience. The elements that fail do it randomly, without any constraint on locality. Our network scenario corresponds to a GMPLS-based transport network with dynamic traffic, where end-to-end connection is the unit of service. We propose and evaluate through simulations two strategies that can be used for improving resilience from the perspective of the number of connections that survive the failure.

In the next section, we review some recent instances of large-scale failures that gained world-wide notoriety. Section III presents basic concepts of network resilience and a review of the relevant literature. Our two proposed strategies for improving resilience is in Section IV, and the simulations carried out are described in Section V. Section VI presents the results and, finally, Section VII gives concluding remarks.

II. NETWORK VULNERABILITY TO LARGE-SCALE FAILURES

Most of the research in survivable optical networks assume that failures occur independently from one another, thus instances of failures such as fiber cuts and node malfunctioning are usually modeled as isolated and unrelated...
events. Furthermore, as multiple failures are considered possible but rare [8], the focus tends to be on single failures, and on single link failures in particular, with only a few studies tackling the design of networks capable of withstanding up to double link failures. Nonetheless, one specific form of multiple link failure that attracted much attention is that which results from damages to physical structures, such as ducts, that are shared by otherwise unrelated fiber links. The concept of Shared-Risk Link Groups [9] captures this situation and has been used extensively in network survivability.

However, several more disrupting failures can be found in the real world. These include the ones in which the malfunctioning cover a large geographical area, thus affecting several completely unrelated network elements simultaneously, where unrelated means different network operators, countries or users. Root causes of such large scale failures are typically natural disasters, but can also be virus or worms outbreaks as well as intentional attacks. One recent example is the 2006 earthquake in the Taiwan area. The damage it caused is detailed in [10]. Several submarine cables were broken, and the communication infrastructure of countries in the region suffered either complete interruption or serious disruption for several days. Although backup resources (multiple fiber cores installed together) were in place, and automatic restoring procedures were activated, the former proved useless as the earthquake affected them as well, and the latter caused even more trouble due to limitations in the management system that precluded it from fully handling the multilayer network, which ultimately forced human intervention to complete the repairing.

Hurricane Katrina is also a recent example of a natural disaster that had important consequences on the communication infrastructure of the affected area, which caused damages to telecommunication networks worth several billion dollars [11], [12]. Lastly, and out of the category of natural disasters, is the politically-motivated attack on web sites of Estonian government and businesses in 2007, which crippled the country’s network for days.

What all these examples have in common is the inability of the network to cope with pervasive failures, although they are quite capable of handling isolated cases of failure of links, nodes and other communication equipment that happens continually. However, such failures go unnoticed by users thanks to the recovery mechanisms put in place.

III. BASIC CONCEPTS OF NETWORK RESILIENCE

This section first gives an overview of basic protection schemes in transport networks, highlight their efficacy for dealing with single failures and their fundamental limitations to handle efficiently multiple failures. Then a review of network robustness metrics found in the literature is presented and their applicability to large-scale failures is discussed.

A. Resilience through Redundancy: Benefits and Limitations

Redundancy is key for improving reliability. On one hand, physical components (e.g., optical cross-connects) can be deployed in redundant configurations, so that spare components come into operation when a failure occurs. Likewise, specific spans (links) or segments can be protected by provisioning additional (e.g., redundant) path(s) so that traffic can be switched to such alternate path(s) when the protected element fails. Many recovery techniques have been proposed and several of them have gained wide acceptance in the industry. A summary of the ones more relevant to next-generation optical networks can be found in [13] and [1]. Two basic recovery schemes based on path protection are Dedicated Path Protection (DPP) and Shared Path Protection (SPP), devised essentially to protect against single failures.

Fig. 1 illustrates the basic operation of DPP, which can be implemented through any technology that provides path protection, for example SONET/SDH 1+1 (or 1:1) Automatic Protection Switching or MPLS Fast Reroute [14]. In this example, one (bidirectional) connection exists between nodes 1 and 9. With DPP, two (link- or node-) disjoint paths are exclusively assigned to the connection, one acting as the working path and the other as the backup path. Thus, it can survive any single (link or intermediate node) failure. Now let’s assume that links 2–3, 3–5 and 5–7 are geographically close to each other and that an event such as an earthquake affects them all so that their failure are concurrent in time. Although the network would continue being fully connected, DPP loses its efficacy because both paths are failed and, by design, dynamic recovery is not attempted. Note that the failed elements need not be geographically related; any failure that touches both paths will equally suffice. A possible solution is to assign more than two paths, say \( k \) disjoint paths. However, finding \( k \) such paths for arbitrary source-destination pairs is not always possible, as it depends on the topology and even on the routing strategy employed. Furthermore, even if there were, they might not comply with QoS constraints, for example on maximum hop count [15]. Note that in our example, we could not have three node-disjoint paths between nodes 1 and 9.

Nevertheless, DPP offers the fastest recovery and the best protection in single-failure scenarios. In fact, it works as expected even when there exist more than one concurrent failure network wide, for it operates at the connection level. The drawback is the total capacity required to support it, which is at least more than twice of what is necessary for unprotected connections. This situation can be alleviated by using SPP, which, in contrast to DPP, shares a single backup path among \( n > 1 \) separate connections, which can lead to substantial capacity savings. The sharing groups must be carefully set up, however, so that the working paths in each group are disjoint, a computationally complex problem especially in dynamic traffic scenarios [16]. If it is assumed that two or more working paths in the same set rarely fail at the same
service in the presence of faults [18]. The robustness of a network is a measure of its resilience, which can be appraised through a variety of approaches and metrics. One classical approach is through the graph-theoretical concept of connectivity, which determines the ability of a given topology to keep all its pair of nodes accessible via some path, as one or more nodes or links are removed. The level of disruption can also be studied by analyzing the flow variation in the network as a consequence of failures. Furthermore, the interest may be in evaluating the vulnerability to specific forms of failures, for example random failures versus attacks [19]. A more recent proposal is elasticity, which relates total throughput to node removal in complex networks [20].

Another dimension of the problem of assessing network robustness regards geographically correlated failures, which cause disruption to a large number of network elements (fiber ducts, regenerators, complete nodes, etc.) around a specific location. Correlated link failures caused by random line-cuts are studied in [21] and resilience metrics are proposed based on connectivity, more specifically, on all-terminal reliability and average two-terminal reliability. On the other hand, in [22] the focus is in identifying the most vulnerable areas of a given physical network, that is, the locations where large-scale failures would provoke a severe reduction of capacity and connectivity in the whole network.

C. Limitations of these metrics

The metrics just discussed, while clearly useful in the general case of topology analysis, show some limitations, however, when applied to data transport networks. This stem from the fact that they largely depend on topological features, thus disregarding traffic dynamics and operational constrains such as network load, heterogeneity in link capacity, and routing strategy. Of the metrics mentioned, only elasticity takes into account some of these aspects. Moreover, when pre-planned protection is the only mechanism considered, as we do here, network connectivity is only marginally useful. As we have already pointed out, it is quite possible that the topology remains connected after a multiple failure event, but even so the number of lost connections reaches unacceptable levels. Thus, instead of observing the state of the abstract topology, it might be better to wonder about the fate of the units of service of the transport network, i.e., connections. Such approach is also taken in [23], but there the elements under consideration are exclusively nodes which become partially or totally disabled as a consequence of failures described by an epidemic model.

In this article we propose using an alternate measure of robustness, namely, the number of connections that survive a large-scale failure or attack. This approach is appropriate for connection-oriented networks precisely because each connection embodies in its path the influence of the structural properties of the topology on the traffic flow, as well as the network operator’s policy on resource allocation, as implemented through routing.

Figure 1: Basic operation of DPP. A working path (solid line) and a backup path (dotted line) are provisioned for a connection between nodes 1 and 9.
IV. PROPOSED HEURISTICS FOR LINK PRIORITIZATION

Graph-theoretical studies on topology resilience usually focus on events of vertex removal, which translated to networking would mean complete node failure. However, more often than not, a network node fails only partially. In fact, the failure of one or more links attached to a node can be considered a partial node failure, altogether a much more frequent event. Therefore, from now on we will focus on link failure, which we assume as encompassing cable cuts as well as the malfunctioning of line cards, regenerators or any component necessary for a successful communication between two adjacent nodes, including software components running on the nodes. Naturally, the failure of all the links belonging to a node amounts to a full node failure.

Suppose that all the links in a network have equal probability of being hit by a certain failure, and that it is possible to make them invulnerable at a fixed cost per link. Suppose also that several links can be affected at once, and that a budget is available for shielding a limited number of them so as to reduce the total number of affected connections when such a large-scale failure event occurs. Which links should be part of this set of invulnerable links? What is the criterion for selecting them?

The combinatorial and non-deterministic nature of this problem make it difficult to offer a computationally simple and exact solution, and thus call for approximate solutions instead. In this section we propose two heuristic-based approaches to the problem. The first one takes advantage of the concept of betweenness centrality, which from now on we will identify as EDGEBC. The second is based on link usage statistics collected as part of the connection set-up phase, identified from now on as OLC for Observed Link Criticality.

In both cases, the idea is that they produce a prioritized list of links that we can choose from to satisfy the maximum number of links that are to become invulnerable. We proceed now to explain both approaches and highlight their strengths and limitations.

A. EDGEBC: The betweenness centrality approach

Betweenness centrality determines how often a node or link on a given network topology lies along the shortest path between all possible pair of nodes [24]. More formally, the edge betweenness centrality $B_e$, i.e., the betweenness centrality of the link $e$, is defined as follows:

$$B_e = \sum_{s,t \in V, s \neq t} \frac{\sigma(s, t|e)}{\sigma(s, t)}$$

where $V$ and $E$ are the set of nodes and the set of links, respectively, $\sigma(s, t)$ is the number of shortest paths that exist between nodes $s$ and $t$, and $\sigma(s, t|e)$ is the number of shortest paths between nodes $s$ and $t$ that use the link $e$, with $e \in E$. $B_e$ can be normalized so that a value close to 1 would mean that link $e$ is present in almost all the shortest paths in the network. Likewise, a value close to 0 would mean that its role as intermediary in the communication is marginal. Note that the above definition assumes the use of shortest paths, and thus it is sometimes called the Shortest-Path Betweenness Centrality. Although the cost function can vary, it is usually set to hop count.

Betweenness centrality has been used in network vulnerability studies to measure the impact of attacks that target those nodes which seem to play a bigger role as communication mediators in the topological sense, see for example [19] and the references therein. That approach is the converse of what we propose here, which is to explore proactive link protection measures against random failures.

Fig. 2 is a visual representation of the betweenness centrality of the links of the well-known COST266 reference topology\(^1\), which has 37 nodes and 57 undirected links. The higher the value of $B_e$, the thicker the line is. One can see that thick lines appear scattered on the topology, so that neither node position (periphery versus “core”) nor degree of connectivity warrant a high $B_e$.

Given that $B_e$ depends only on the topology, it can be computed just once as long as the topology remains unchanged. However, this very fact is also the source of its weakness, for it cannot fully take into account some fundamental aspects of an operational network. For instance, from the point of view of routing, the network topology suffers recurrent virtual and transient changes. There is a virtual link removal when the corresponding residual capacity reaches zero. Conversely, the link is re-inserted later on when the connections that use it are torn down. Therefore, the shortest path at any instant depends on the network state: one particular connection request might be assigned the ideal shortest path, but the next one might not. In contrast, the definition in Eq. 1

---

\(^1\)Available at http://sndlib.zib.de/
assumes unlimited capacity and thus immutable shortest paths. Consequently, for real-world data networks, $B_v$ can only give an approximate centrality. Further complications come from the variation in link capacity (not all links have the same capacity) and from the imbalances in the traffic matrix (the volume of communication between node pairs need not be the same). Though it would be feasible to recompute the betweenness centrality at each virtual topology change –its running time is in $O(|V||E| + |V|^2 \log |V|)$ [26]– it would not fully resolve the divergence between the real centrality and the estimation based on static data.

B. OLC: The Observed Link Criticality approach

This measure is based on the concept of criticality in minimum-interference routing [27]. The difference is that, instead of relying on an approximation based on static data, we can directly take advantage of dynamic information about resource usage that can be collected in the GMPLS control plane. Specifically, each link $e$ can have associated to it a counter $c_e$ for the number of connection paths that go through it, and that counter can be updated as connections are accepted and released. That way, the relative importance of $e$ is $M = \frac{c_e}{N}$, where $N$ is the number of active connections at a certain instant. From this, an estimation of the link importance can be obtained as a simple moving average of $M$:

$$I_e = \frac{M + M_{-1} + M_{-2} + \ldots + M_{-k-1}}{k} \quad (2)$$

where $k$ is a constant for the number of consecutive samples to use.

The disadvantage of this approach compared to $EDGEC$ is that the network must already be in operation, and preferably in a steady state, before it can be applied.

V. SIMULATION OF FAILURES FOR PERFORMANCE COMPARISON

In this section, we detail the steps carried out to compare through simulation the performance of $EDGEC$ and OLC in terms of their ability to minimize the number of affected connections when a large-scale failure occurs.

A. Simulation parameters

The topology used in this work is shown in Fig. 3. This is a synthetic topology that represents a large transport network consisting of 222 nodes and 371 links, and share structural properties with reference topologies found in the Survivable Network Design Library (SNDlib) [25]. The size differs significantly, however, as this topology is more than three times larger than the ones found in that repository. The main properties of this topology are shown in Table I. As it represents the physical topology of a transport network, the nodal degree range is 2 to 5, the dominant degree being 3, as can be seen in Fig 4. For simplicity, we assume that links are capable of carrying an arbitrary number of Label Switched Paths (LSPs) [28] as long as free capacity is available, and that all nodes support full wavelength conversion. To introduce a minimum degree of heterogeneity in capacity, links have either $C$ or $2C$ units of total capacity. Half of them belong to the first group and the rest to the second, where the membership to either set was decided on a random basis.

In order to simulate the provision of service in the network and the occurrence of large-scale failures, an event-driven simulator that reproduces the process of route selection in a path-oriented transport network was developed. The simulator handles the reception of connection requests between randomly-selected source and destination nodes, which arrive according to a Poisson process. As we are interested in a dynamic traffic scenario, the capacity allocated to an accepted connection, whose holding time is an exponentially distributed random variable, is released as soon as

<table>
<thead>
<tr>
<th>Property</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Number of nodes</td>
<td>222</td>
</tr>
<tr>
<td>Number of links</td>
<td>371</td>
</tr>
<tr>
<td>Network diameter</td>
<td>20 hops</td>
</tr>
<tr>
<td>Average shortest path</td>
<td>9.06 hops</td>
</tr>
<tr>
<td>Average nodal degree</td>
<td>3.3</td>
</tr>
</tbody>
</table>

Figure 3: The synthetic topology used in the simulations
the connection terminates. The aggregated traffic between any two pair of nodes is a fixed value or zero, meaning that either they do not communicate, or contribute the same amount of traffic as other pairs. This traffic matrix is randomly generated. Any demand whose source and destination are at four hops or less is disregarded (and not counted as rejected), i.e., we discard connections corresponding to “local traffic”. The capacity requested by connections is a uniformly distributed random variable in the range 1–10 units.

In accordance with the assumptions made in Section IV, a minimum-hop routing algorithm is used. Links that do not have enough residual capacity to satisfy the arriving demand are filtered out before the exploration begins. That is, the routing employs a Constrained Shortest Path First algorithm, where the constraint is the minimum capacity required per link.

To avoid creating unrealistically long paths, any request whose feasible path exceeds 24 hops is also rejected. Note that the average minimum path length in this topology is about 9 hops, while the diameter is 20 (see Table I). The blocking ratio is approximately 0.01 in all the experiments reported. For each accepted connection, one path from source to destination is created. As no protection is provided at the connection level, no additional path is created in addition to this working path.

B. Simulating a Large-scale Failure

Exactly one failure event is triggered during the simulation, whose time is chosen randomly once a stable state had been reached. In contrast, the extent of the failure and the size of the set of invulnerable links are user-provided input data, expressed as a percentage of the total number of links in the topology.

To emphasize that this work focuses on far-reaching failures, both in geographical coverage and size, from now on we refer to the extent of the failure as the infection level and, by analogy, to the percentage of invulnerable links as the immunization level.

The simulations were performed with infection levels 5, 10, and 20, and immunization levels 10, 20, and 30. Thus, one simulation run corresponds to a specific combination of: a) infection level, b) immunization level, and c) procedure for the selection of invulnerable links, which for simplicity is called immunization strategy from now on.

For comparison purposes, a procedure based on random selection of the links to be considered invulnerable was also added, so that the immunization strategies are three, as follows:

- **RANDOM**: failed links as well as invulnerable links are chosen randomly.
- **EDGE BC**: failed links are chosen randomly. Link immunization is based on their edge betweenness centrality.
- **OLC**: failed links are also chosen randomly. The immunization is based on average Observed Link Centrality.

This gives 27 cases in total. The values presented in Section VI are the average of 30 runs per case, each one processing a new demand set consisting of 95000 randomly-generated connection requests.

From each run, the following results are obtained, which constitute the figures of merit for comparing the performance of the immunization strategies:

1) The percentage of active connections affected by the failure.
2) The frequency distribution of path length of the affected connections.

A connection is considered affected if: a) its duration has not yet reached its declared lifetime, and b) at least one link included in its path was hit by the failure.

VI. SIMULATION RESULTS AND DISCUSSION

The objective of these simulations is to compare the effectiveness of the immunization strategies proposed. However, there is the question whether these strategies provide any improvement in resilience at all. To answer this question and put in perspective the value of the proposed strategies, we also simulated the zero immunization case. As can be seen in Fig. 5, the result is striking, since even when the infection level is minimal (5%), almost half of the connections (42%) active at the time the failure was triggered were affected. The percentage of affected connections continues to grow as the infection level increases, but a moderation is observed in its progression. Nearly all connections (>90%) are affected with 20% of infection. Thus, we consider that the infection scenarios worth exploring are between 5% and 20%.

Table II shows the distribution of the frequency of connection path length of one representative simulation run. For the reasons explained in Section V, the path length range is 5–24. Fig. 6 and Fig. 7 discriminate by path length the percentage of connections affected at infection levels 5 and 20, respectively. Each sub-figure presents the performance of one specific immunization strategy at immunization levels 10, 20, and 30.

It can be observed that RANDOM is essentially insensitive to the immunization level in both infection scenarios.
It is interesting to note in Fig. 6c that there exists a case in which the immunization level is six times the infection level, but even then the effect is negligible. This behavior is similar for all path lengths. Only for the longest paths in Fig. 6c does performance vary with respect to the immunization level, which is due to the fact that the number of connections of such long lengths is very small compared to the rest (see Table II).

In the rest of the cases, the behavior clearly depends on the level of infection and immunization. For instance, with 20% of infection (Fig. 7) and 10% of immunization, EDGEBBC and OLC offer similar results, outperforming RANDOM in that case as well as in almost all the others. However, when the immunization level is raised to 30, OLC is the one whose reaction is more visible, producing the lowest values for the number of affected connections. This effect is observed in the three infection scenarios.

Table III summarizes the performance of the three strategies. The column “% Aff. conn.” gives the percentage of connections affected by the failure. The remaining columns put connections into three groups based on their path lengths, and show what proportion of each group was adversely affected. The groups are as follows: a) short (5–8 hops), b) medium (9–18 hops), and c) long (19–24 hops). Each value is an average of the individual results in the range. Every combination of infection level, strategy and immunization level considered in this work has an entry in the table.

Fig. 8 shows graphically what happens from the perspective of connection path length when the infection level is 10 and the immunization level is 30. As can be seen, the difference between RANDOM and the other two is almost 20% for short paths. That difference jumps to around 30% for paths of medium length, and shrinks back to around 20% for long paths.

Additionally, the network’s two-terminal reliability obtained after the failure event is presented in Table IV. The values correspond to selected levels of immunization and infection when the strategy is EDGEBBC. We compute it as the ratio of the number of origin-destination pairs for which a path exists to the maximum possible number of paths. Thus, the closer this value to 1.0, the lower the network fragmentation is. As expected, our simulations confirm that this reliability measure is quite insensitive to the failure, for it remains very close to 1.0 in all cases, indicating almost full connectivity. That is, it does not reflect the degree of damage experienced by connections after the failure.

In summary, these results show the high sensitivity of a connection-oriented network to large-scale failures, because even a relatively small infection level (%5) causes disruption to almost half the connections in the studied scenario. Moreover, the RANDOM strategy, which implements a immunization without a specific criterion, shows...
TABLE IV.: Average two-terminal reliability after the failure event. Strategy: EDGEBC

<table>
<thead>
<tr>
<th>Immunization (%)</th>
<th>Infection 5%</th>
<th>Infection 10%</th>
</tr>
</thead>
<tbody>
<tr>
<td>10</td>
<td>0.9994</td>
<td>0.9973</td>
</tr>
<tr>
<td>20</td>
<td>0.9985</td>
<td>0.9970</td>
</tr>
</tbody>
</table>

that little or no benefit is obtained in terms of robustness by choosing links disregarding their role in the overall traffic flow.

With respect to the immunization strategies EDGEBC and OLC, results show that both are capable of minimizing the impact of these failures with the appropriate election of the immunization level. Of the two, we can see that OLC is the best performer, as with it the number of affected connections is lower and, at the same time, the number of surviving connections whose path lengths are medium and long is higher.

VII. CONCLUSION

In this article, the problem of improving the resilience of large transport networks to pervasive failures has been addressed. The scenario is a GMPLS-based network subjected to a pervasive multiple failure event, where several links fail concurrently in random locations, provoking the loss of all the end-to-end connections passing through them. The ultimate aim is to identify elements (e.g., links) to which extra network protection can be applied so that the impact of such failure events, in terms of the number of connections affected, is minimized.
Two new strategies of link prioritization have been presented, whereby a subset of links are made invulnerable to the proposed type of failure. The first strategy uses the well-known measure of betweenness centrality, while the second is based on a new concept called the Observed Link Criticality. Both have been evaluated through extensive simulations. For comparison purposes, a third approach based on random selection of links was also included in the study.

The obtained results highlight how easily a large-scale failure event can seriously disrupt the operation of a connection-oriented network. At the same time, it shows that robustness metrics such as two-terminal reliability are not appropriate to assess the state of the network from the point of view of its ability to provide service (connections). For example, even when the network is suffering a major service degradation, the average two-terminal reliability reports a very high degree of connectivity. Results also show that the two proposed strategies succeed in decreasing the number of affected connections. The one based on observed link criticality offers better overall robustness and, at the same time, preserves a higher number of connections of medium and long path lengths.

VIII. ACKNOWLEDGMENTS

This work is partially supported by Spanish Ministry of Science and Innovation project TEC 2009-10724 and by Generalitat de Catalunya research support program (SGR-1202).

REFERENCES


Juan Segovia is currently a PhD candidate at University of Girona, Spain. He received his bachelor’s degree in Computer Science from the National University of Asunció in 1994, and a MPM degree in 2000 from the same university.

He was a lecturer at the National University of Asunció, Paraguay, 1997-2005. He is currently a member of the Broadband Communications and Distributed Systems group, and his research interests include protection and restoration of GMPLS-based optical networks, and reliability against large-scale failures in complex networks.

Pere Vilà received his PhD in Computer Science from the University of Girona in 2004.

He is a lecturer in the Department of Computer Architecture and Technology at the University of Girona, and a member of the Broadband Communications and Distributed Systems research group. His current research interests are in the fields of network management, routing and protection, and interdomain mechanisms.

Dr. Vilà has co-authored several papers in journals and international conferences and worked on several funded research projects.

Eusebi Calle received his doctorate degree in Computer Science from the University of Girona (UdG) in 2004.

He is currently an associated professor at the UdG. Since 1998, he is a member of the research and teaching staff in the Broadband Communications and Distributed System Group, where he develops his research in GMPLS fault management, routing and network science.

Dr. Calle has co-authored several papers in international journals and international conferences. He is also member of different TPC, and part of the Institute of Informatics and Applications at the UdG.

Jose L. Marzo received his Ph.D. degree in Industrial Engineering in 1997 from the University of Girona, Spain. Currently, he is a Full Professor at the Department of Electronics, Informatics and Automatics at the same university.

He leads the research group Broadband Communications and Distributed Systems. His research interests are in the fields of management and performance evaluation of communication networks, network management based on intelligent agents, MPLS and GMPLS, and distributed simulation. From 1978 to 1991, he was with Telefónica de España.

Dr. Marzo is a member of the IEEE Communications Society. He has participated in technical program committees and chairing sessions of several international conferences. He serves in the editorial board of the International Journal of Communications Systems. He has co-authored several papers published in international journals and presented in leading international conferences.