Capacity versus Robustness: A Tradeoff for Link Restoration in Mesh Networks*

Steven S. Lumetta  
U. of Illinois at Urbana-Champaign  
ECE Department  
Coordinated Science Laboratory  
lumetta@uiuc.edu

Muriel Médard  
Massachusetts Institute of Tech.  
EECS Department  
Lab. for Info. and Decision Systems  
medard@mit.edu

Yung-Ching Tseng  
U. of Illinois at Urbana-Champaign  
ECE Department  
Coordinated Science Laboratory  
ytseng@uiuc.edu

Abstract

Link recovery in high-speed four-fiber networks can be achieved using dynamic searches, covers of rings, or generalized loopback. We present a method to provide link recovery for all links in a network without using all links for backup traffic transmission. The method extends generalized loopback to operate on a subgraph of the full backup graph. The backup capacity on such links can then be used to carry unprotected traffic, i.e., traffic that is not recovered in case of a failure, while primary fibers on the links retain failure protection. Although all primary fibers remain fully robust to single-link failures, reserving links for unprotected traffic does reduce a network's ability to recover from multiple failures. We explore the tradeoff between capacity and robustness to two-link failures for several typical high-speed optical fiber networks, comparing the properties of three link-restoration algorithms based on generalized loopback with the properties of covers of rings. Our results demonstrate robustness comparable or superior to that available with covers of rings while providing an additional unprotected traffic capacity of roughly 20% of the network's primary capacity.

Keywords: optical communication, optical fiber communication, wavelength division multiplexing, network reliability, robustness, metropolitan area networks, wide area networks

*This material is based in part upon work supported by grant MDA972-99-1-0005 from the Defense Advanced Research Projects Agency. The content of the information does not necessarily reflect the position or the policy of that organization.
1 Introduction

As the communications infrastructure grows in size and importance, the reliability of high-speed backbone networks becomes imperative to maintain. At the same time, the topologies of high-speed networks become increasingly complex and dynamic. New additions to existing networks occur at a fast pace to sustain rapidly growing and increasingly fluid communication demands. The constant admission of new entrants to the high-speed networking arena leads to interconnections of large networks. This increasingly complex and dynamic nature, as well as the growing diversity of ownership, gives rise to four important goals for the design of reliable high-speed networks: generality, scalability, distribution, and speed. First, the rise in complexity necessitates recovery algorithms capable of operating on a diverse set of network topologies, not just rings or simple derivatives of rings. In defining generality, we target an arbitrary two-connected mesh topology. Second, the rapid pace of change and aggregation implies that recovery schemes must be easily scalable: local changes should not require global coordination. Unlike networks of the past, no single entity operates the entire high-speed infrastructure. Reliability must therefore be provided through distributed operations rather than through the actions of a unique, centralized manager. Finally, the high data rates in modern and future networks—on the order of several Gb/s in an optical network—exacerbate the severity of service disruptions, requiring that restoration of service be very rapid, at least as fast as the 60 milliseconds required in SONET self-healing rings (SHR's). Progress towards these four goals must contend with the goal of network management to provision capacity in a cost-efficient manner. As the same physical infrastructure carries both primary service and backup traffic, the benefits of obtaining more capacity for primary service exacts a price in terms of robustness.

This paper describes a recovery scheme which meets the four goals stated above and, using this scheme, investigates tradeoffs between capacity provisioning and reliability. We construct simple measures of robustness to aid in this evaluation. We present results in the area of link recovery and comment on the applicability of our approach to node recovery. We also compare our results with alternative approaches to link recovery from the literature. We evaluate those approaches with
respect to the design goals given above and compare their performance according to our measures of robustness.

We organize the paper as follows. The next section begins with a discussion of background material, then surveys related work in the field of recovery for link failures. In Section 3, we outline our approach to recovery, which is derived from [22]. Section 4 presents our robustness measures and introduces several algorithms for comparison. We present results and commentary for several representative networks in Section 5. Finally, in Section 6, we provide conclusions and directions for future work.

2 Background

One of the most common failure modes for all-optical networks is the failure of links. Links can fail in many ways, ranging from amplifier failure to power outages to wayward backhoes. Generally, the failure of a link entails the failure of all fibers traversing that link, and algorithms for recovery must not assume that some part of the link remains intact.

Two main approaches exist for recovery from a link failure: path protection and link restoration [6, 11, 28]. Link restoration replaces a failed link by selecting a backup route between the end nodes of the link. Path protection entails end-to-end replacement of a path between a source and destination. Hence, path protection requires knowledge of the whole path and selection of an alternate path. The two techniques are complementary and can co-exist in a same network. We focus on link restoration, however, as it is better suited to distributed restoration.

Methods commonly employed for link restoration in high-speed networks can be classified as either dynamic or preplanned. The two types offer a tradeoff between adaptive use of backup (or “spare”) capacity and speed of restoration [4, 21]. Dynamic restoration typically involves a search for a free path using backup capacity [17] through broadcasting of help messages [5, 12, 13, 20, 21, 33]. The performance of several algorithms is given in [1, 5]. Overheads due to message passing and software processing render dynamic processing slow. For dynamic link restoration using SONET digital cross-connect systems, a two second restoration time is a common
goal [12, 13, 21, 24, 33, 35]. Thus, our goal of speed comparable to SONET SHR's is not met.

Preplanned methods typically offer a speed advantage over dynamic systems. For optical networks, opto-mechanical add-drop multiplexers [24, 27] yield recovery in a few milliseconds and acousto-optical switches [7, 34] in a few microseconds. Despite these superior restoration speeds, preplanned methods suffer from poorer capacity utilization than dynamic systems. Dynamic methods make use of real-time availability of backup capacity, whereas preplanned methods require that capacity to be allocated permanently, requiring a backup capacity equal to the maximum primary capacity through any link.

For preplanned link restoration, the main approaches are through the use of rings and, more recently, through generalized loopback in mesh networks [22]. The most direct approach is to design the network in term of rings [16, 23, 32] or partially using rings [3, 14]. Such architectures allow distributed recovery from link failures. However, rings are not necessary to construct survivable networks; mesh-based topologies can also provide redundancy [25]. Ring-based architectures may be more expensive than meshes [3], and as nodes are added, or networks are interconnected, ring-based structure may cease to be maintained, thus limiting the scalability of the approach. Even if we constrain ourselves to always use ring-based architectures, such architectures may not be easily scalable as the network grows [31, 32], making mesh-based architectures a more promising candidate for future networks.

Before discussing recovery strategies for mesh networks, we must first consider the structure of the underlying physical network. Typically, links in both ring and mesh networks contain multiples of either two or four fibers. In a four-fiber system, one pair of fibers carries primary traffic in each direction, and the second pair is typically used for protection. As full fibers are available in each direction, WDM traffic is recovered by switching an entire primary fiber onto a secondary fiber. In contrast, each fiber in a two-fiber system must carry both primary and secondary (protection) traffic to allow bidirectional communication along the links. With a WDM system, this effect can be accomplished logically by partitioning wavelengths, either according to the direction of primary traffic on a link or according to whether a wavelength carries primary or secondary traffic.
The latter approach requires wavelength conversion for recovery but supports arbitrary routing of traffic for each primary wavelength. Given these alternatives, the choice between two- and four-fiber systems is usually orthogonal to the choice of recovery strategy. We assume a four-fiber system in the remainder of the paper.

One approach to supporting recovery in mesh topologies involves the selection of rings within a mesh network and the use of distributed, ring-based algorithms to effect recovery on each ring. For example, a set of rings can be chosen such that every node falls on one or more rings and every link falls on at most one ring, as in [29, 30]; such a set is called a node cover. Link restoration is effected on each ring in the same manner as in a traditional SHR, by routing the backup traffic around the ring in the opposite direction to the primary traffic. In general, a node cover does not cover all links, however, and can not easily recover traffic on uncovered links. Primary routing is thus restricted to covered links, and uncovered links can only be used to carry unprotected traffic, i.e., traffic that may not be restored if the link carrying it fails.

In order to allow every link to carry protected traffic, every link must be covered by a ring. A set of rings chosen such that every link falls on at least one ring is called a ring cover and is considered in [14]. Ring covers suffer from capacity drawbacks in that each ring requires physical capacity: a link covered by two rings requires eight fibers; a link covered by four rings requires sixteen. Alternatively, the logical fibers can be physically routed through four physical fibers, but only at the cost of significant network management overhead. Minimizing the amount of fiber required to obtain redundancy using a ring cover is equivalent to finding the minimum cycle cover of a graph, an NP-hard problem [26]. For existing networks, recovery based on ring covers must choose between generality and speed. As small changes to a network can result in major restructuring of ring covers, the technique also lacks scalability.

A recent extension to ring covers, known as p-cycles [15], takes advantage of the fact that a ring can be used to protect all of its chords (links spanning the ring) as well as links on the ring itself. Finding optimal solutions, we believe, remains NP-hard, although good approximations for the purposes of network design are fairly easy when the granularity of protection is a small
fraction of link capacity. The approach also addresses a more general problem than that discussed in this paper, in which primary capacity may vary from link to link and electro-optical conversion is (implicitly) assumed for each hop. For all-optical networks, p-cycles must strike a balance between minimizing path length and minimizing spare capacity. In existing networks, the problems suffered by ring covers remain: optimal solutions typically require additional fiber, and the entire network may be reconfigured in response to a minor extension.

An alternative to ring covers, intended to overcome the difficulty of finding good covers, is to cover every link in a network with exactly two rings [9]. A set of rings that meets this requirement is called a double cycle cover [19]. For planar graphs, double cycle covers can be found in polynomial-time; for non-planar graphs, it is conjectured that double cycle covers exist, and they are typically found quickly in practice for network graphs. However, if a link or node is added to a network, the structure of the cover can change significantly, implying a potential need for global reconfiguration in response to local network extensions and limiting the scalability of the technique. From a practical viewpoint, double cycle covers also require four-fiber physical networks, as the relationship between the rings significantly complicates wavelength partitioning for a two-fiber system.

Another approach to link restoration on mesh networks, known as generalized loopback, was presented in [22]. The principle behind generalized loopback is to select a digraph, called the primary, such that the conjugate digraph, called the secondary, can be used to carry backup traffic for any link failure in the primary. Construction of a primary involves selection of a single direction for each link in the network. Loopback then occurs along the secondary in a manner akin to loopback in a SONET bi-directional line-switched ring (BLSR). Figure 1 demonstrates generalized loopback for a simple network. In the figure, only two fibers per link are shown—one primary fiber and its corresponding secondary fiber. When the link \([U, V]\) fails, traffic from the primary digraph floods onto the secondary digraph starting at \(U\). The secondary digraph carries this backup traffic from one endpoint of the failed node to the other endpoint, possibly along multiple paths. When traffic reaches \(V\) (along the first successful path), it is again placed on the primary fiber, as though
no failure had occurred. Unnecessary backup paths are subsequently torn down. The fact that multiple paths may exist for restoration plays a key role in the next section, where we consider the effect of reclaiming some arcs (fibers) from secondary digraphs to carry additional traffic.

Logically, one can view a four-fiber mesh network using generalized loopback as a set of four digraphs: two primaries and two secondaries. Each fiber in the network is represented by a single arc and is associated with a single digraph. The primaries are conjugates, allowing traffic to cross any link in any direction, and each secondary is the conjugate of its primary. These digraphs serve solely to define recovery and have no impact on the selection of routes. An end-to-end path crosses freely between the two primaries. For each link, the path is associated with a particular primary, and failure of that link is recovered through the corresponding secondary. However, this association has meaning only on a link by link basis.

Recall our four goals for reliable networks: generality, scalability, distribution, and speed. Generalized loopback can be applied to arbitrary link-redundant networks, i.e., networks whose associated graphs are two-edge redundant, and thus supports very general topologies. If a new link is added, recovery for the new link can be provided without changing the recovery mechanism for the old portion of the network, allowing network scalability. Recovery is performed by using loopback and by broadcasting backup traffic, which requires only operations distributed among the network switches. Finally, if backup routes are preplanned, recovery can occur very quickly.

Table 1 draws a comparison, according to our criteria, among the main link recovery approaches discussed. The last row of the table, labeled “route freedom,” indicates whether or not all primary fibers in the network can be used to carry protected traffic. Dynamic restoration of failed links provides fairly efficient protection, but only at the cost of recovery speed. Ring-based techniques generally suffer from scalability problems: as a network grows, small localized changes can require global network reconfigurations to support recovery. Generalized loopback is the only technique that uses a fast, distributed algorithm to provide recovery on arbitrary two-edge redundant mesh topologies in a way that restricts neither the selection of routes nor the growth of the network.
<table>
<thead>
<tr>
<th></th>
<th>dynamic restoration</th>
<th>ring-based techniques</th>
<th>generalized loopback</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>node cover</td>
<td>ring cover</td>
<td>double cycle cover</td>
</tr>
<tr>
<td>generality</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>scalability</td>
<td>✓</td>
<td>x</td>
<td>x</td>
</tr>
<tr>
<td>distribution</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>speed</td>
<td>x</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>route freedom</td>
<td>✓</td>
<td>x</td>
<td>✓</td>
</tr>
</tbody>
</table>

Table 1: Comparison among restoration algorithms for link failures. Ring covers can trade speed for generality.

In this paper, we examine restoration approaches that allow efficient use of backup capacity and explore the relationship between the use of that capacity and a network's robustness to failures. We limit our investigation to the problem of efficient use of existing networks, setting issues of network planning aside. In efficiency terms, dynamic restoration and generalized loopback are nearly equivalent: each seeks to find an alternative path for a failed link. Dynamic restoration uses signaling for further efficiency, whereas generalized loopback provides dedicated backup fibers for speed. Ring-based approaches require as many fibers for backup as they provide for protected traffic, and are always less-efficient than path-based schemes [14]. Node covers allow some secondary fibers in a network to be reclaimed for unprotected traffic, but only by disallowing protection of the primary fibers over the reclaimed links. Double cycle covers are the most promising alternative to generalized loopback in terms of the stated goals, but still require the full replication of primary capacity inherent to ring-based solutions. As we demonstrate in the next section, generalized loopback allows efficient use of backup capacity while retaining full protection for primary traffic on every link in the network. It fully exploits an existing network's capacity without restricting its ability to withstand failures.

In Section 4, we probe deeper into the question of robustness, examining the cost of using
backup capacity for additional traffic in terms of a network's ability to recover from multiple failures. The tradeoff between capacity and robustness takes form in this investigation.

3 Capacity-Efficient Recovery

In this section, we consider the use of generalized loopback to provide recovery in a capacity-efficient manner for four-fiber networks. We address the goal of achieving link recovery in a capacity-efficient manner through the construction of backup digraphs that support failure recovery for every link without using all secondary fibers in a network. In other words, a subset of the secondary fibers carry unprotected traffic, and while all backup traffic is carried on secondary fibers, secondary fibers do not only carry backup traffic, but also unprotected working traffic. The links for which unprotected traffic is carried on secondary fibers are termed non-critical links. The following definitions help to clarify the discussion:

Protected capacity: the aggregate capacity of bidirectional links in a network that can be guaranteed to be restored should they fail singly.

Unprotected capacity: the aggregate capacity of bidirectional links in a network that cannot be guaranteed to be restored should they fail singly.

Backup capacity: the aggregate capacity of bidirectional links in a network that must be reserved (or released on short notice) to allow recovery of failed protected links.

Non-critical link: a link whose associated arcs can be removed from the secondary digraphs without affecting the ability of generalized loopback to restore any failed link.

Valid backup digraph: a sub-digraph of a network digraph that strongly connects all nodes in the network.

Minimal backup digraph: a backup digraph with the minimum number of arcs possible to allow recovery from all one-link failures.

Figure 2 illustrates the identification of non-critical links for recovery from single-link failures with generalized loopback. The network is the same as in Figure 1, except for the addition of
the link \([X, Y]\). If any link fails in Figure 2, loopback traffic traverses the secondary digraph. In particular, we can establish a backup route in the secondary digraph between the endpoints of any arc in the primary digraph. Thus, the extra link is a non-critical link. On that link, instead of reserving the secondary fibers for backup traffic, we can use those fibers to carry unprotected traffic while still protecting the primary traffic.

The approach we have illustrated generalizes to any link-redundant network. As generalized loopback works on any two-edge redundant graph, we can perform loopback by using only the links on any link-redundant subnetwork. In contrast to the original generalized loopback concept described in [22] and illustrated in Figure 1, some secondary fibers are not used for any secondary digraph. Thus a minimal backup digraph uses only the minimum number of links necessary to provide a link-redundant network that includes all nodes in a network.

Note that many networks, by virtue of the assignment of primary and backup capacities, have some amount of unprotected capacity [1]. Thus, unprotected capacity already exists and is available for use in networks. Non-critical traffic can be assigned to such unprotected capacity.

We explore the number of non-critical links in five sample networks. For three of these networks, we are able to find Hamiltonian cycles that allow complete backup with one link per node. For the other two, we find minimal backup graphs with one more edge than the number of nodes. Figures 3 through 7 show minimal backup graphs for these networks. The figures for the first three networks also show the directions chosen for our measurements of robustness, as described later. The New Jersey LATA network shown in Figure 3 has been simulated previously [1, 5, 14, 35] and provides a good case study for metropolitan area networks. The second network, shown in Figure 4, is a model of the ARPANET. The third network, the LATA Interconnect, or LATA 'X', in Figure 5, was considered in [1], and provides an example of a nationwide network.
4 Measures and Methodology

Intuitively, use of a network’s unprotected capacity must adversely impact the network’s ability to recover from failures. The method used to identify non-critical network links ensures that a reduced backup digraph is adequate for generalized loopback to guarantee full recovery from single link or node failures. However, removing these non-critical links increases typical backup path lengths, leading to increased jitter and associated problems. Use of unprotected capacity also reduces the likelihood of recovery from multiple failures. To understand this tradeoff, we use three sample networks—NJ LATA, ARPANET, and LATA ‘X’—to investigate the impact of utilizing unprotected capacity on both path lengths and on recovery from multiple failures. This section defines the measures through which we explore the tradeoff between capacity and robustness, then outlines our measurement techniques for several approaches to restoration.

As a measure of path length, we report the longest backup path required for any primary arc. We also report three measures of recovery from two-link failures. A two-link failure consists of two independent link failures in a network graph. The second failure occurs long enough after the first to allow normal recovery to complete but before any physical repair can be accomplished. None of the fibers in a failed network link remain usable; all primary and backup arcs through that link are broken. With generalized loopback, restoration occurs independently on each of the two backup digraphs, but the use of backup arcs complementary to the primary arcs renders the subproblems of recovery on each digraph fully equivalent.

The first recovery measure, robustness, is the percentage of all two-link failures from which a network successfully recovers, restoring both failed links simultaneously through the intact portion of the backup digraph. Robustness represents a global notion of a network’s ability to recover. The second and third recovery measures, which we term reliability, capture a more local notion: the reliability of individual arcs in the primary digraph. Both measures are defined as the worst-case, over all links \([U, V]\), of the percentage of other links that, should they fail, do not prevent recovery of link \([U, V]\). First-failure reliability represents the reliability measure when \([U, V]\) fails first.
and second-failure reliability represents the reliability measure when $[U, V]$ fails second. Two measures are necessary to capture the effect of time ordering on the failures. Recovery of the first failed link occurs before recovery of the second, and the backup path for the first link may occupy links necessary to restoration of the second. First-failure reliability is thus usually at least as high as second-failure reliability.

We apply these four measures to four approaches to link restoration: double cycle cover, preplanned shortest paths, dynamic shortest paths, and two-path search. Double cycle cover provides an alternative to generalized loopback, but does not admit exploitation of non-critical links for unprotected capacity. Finding a good double cycle cover can be a difficult problem; we chose to use a cover from [8] for ARPANET and to use a cover drawn from a planar embedding for NJ LATA. A double cycle cover restores two failed links if and only if the links do not reside on the same cycle. Robustness can be calculated by counting the number of link pairs that meet this criterion, and reliability is a simple function of the number of links in the longest cycle. As restoration with double cycle cover is both static and symmetric, time ordering plays no role in reliability.

Preplanned shortest paths, the simplest form of generalized loopback, redirects traffic from a failed primary arc back along a precalculated shortest path through the backup digraph. When several shortest paths exist for an arc, one path is selected at random in advance. Restoration paths are static, but arc dependencies are not symmetric; a link that fails before another may prevent successful restoration of the second link. First-failure reliability depends only on the number of links used by a backup path, and is only a function of the longest backup path. Robustness requires both that neither failed link fall on the backup path of the other and that the backup paths for the two failed arcs share no links. Second-failure reliability depends on similar conditions. The second failed arc is certainly restored when the robustness conditions are met, but can also be restored when the second failed link lies on the backup path of the first but does not use the first for backup. In this case, we assume that the network recognizes its inability to restore the first failed link and chooses to recover the second rather than occupying the backup digraph with the first link's traffic.
Restoration with dynamic shortest paths applies flooding to adapt to the presence of backup traffic from previous link failures and represents the full form of generalized loopback. Traffic from a failed primary arc spreads out across the backup digraph until a backup path is found. The effect of recovery from single link failures is exactly the same as with preplanned paths, thus first-failure reliability is also the same. The dynamic approach improves robustness, however, by successfully restoring some second link failures when a first failed link lies on the second link's preferred backup path. Provided that the second link does not lie on the backup path for the first, as severed backup paths are not restored dynamically, two failed links can be recovered whenever a backup path for the second primary arc can be found in the backup digraph using neither failed link nor any arc from the first backup path. With regard to second-failure reliability, we again assume that the network reuses backup arcs from a severed first link backup path to restore primary arcs from a second link. Second-failure reliability is otherwise specified by the stated robustness conditions.

The last approach to restoration, two-path search, replans the backup path for a first failure to recover from and to allow recovery of a second failure. When two arc-disjoint paths exist in the remaining backup digraph, the network routes traffic from the two failed primary arcs across two such paths. Robustness to a two-link failure is equivalent to the existence of such paths, and in terms of robustness, two-path search is optimal for a given digraph. If no such paths exist, the network gives priority to the first failed arc, then tries to recover the second arc if recovering the first arc proves impossible. Disjoint paths can be precomputed or discovered dynamically for our sample networks, but the problem is in general NP-complete [10]. The attempt to recover a first failure's severed backup path improves first-failure reliability relative to that of dynamic shortest paths. For the same reason, second-failure reliability can be lower than that of dynamic shortest paths, but the improvement due to remapping of the first backup path to make way for a second opposes this effect.

The four approaches to restoration represent a range of adaptivity and difficulty in implementation, from the completely static and straightforward double cycle cover to the fully dynamic and
NP-complete two-path search. In the next section, we examine the impact of these approaches on recovery for three sample networks.

5 Results

This section presents the results of the investigation. Many of the measurements present data based on the number of links removed from the backup digraph. The order in which such links were removed was chosen to maximize the robustness of the resulting digraph with dynamic shortest paths (generalized loopback), which has some minor implications for accuracy of the data. The impact of these choices is highlighted in the discussion.

Figure 8 shows how backup path length varies with the number of non-critical links used to carry unprotected traffic. For each of the three networks, path lengths remain relatively stable until nearly all non-critical links have been removed from the backup digraph, at which point backup paths must traverse nearly all remaining links. The bump in the NJ LATA line at 1 link comes from fixing the direction of the primary arc through a link when adding it to the backup digraph. Figure 9 illustrates the effect. One direction of the central link allows a backup of length \( N \), whereas the opposite direction requires a backup of length \( N + 1 \). By fixing the direction as shown to optimize robustness, we force an increase in backup path length for the primary arc associated with the link.

5.1 NJ LATA

Consider the NJ LATA network shown in Figure 3. We construct a double cycle cover for this network by transforming the graph into planar form and making each face and the outer perimeter into a cycle. The longest cycle thus formed consists of five links, and the cover provides robustness of 79% and reliability of 82%.

We also select an orientation of edges on the minimal backup digraph and select directions and an ordering for the addition of non-critical edges into the backup digraph, as shown in the figure. A given backup digraph can be used to back up either primary arc within a non-critical.
link. For graphs with unprotected capacity, we measure all combinations of directions and report the measurements for the best choice. Measured values of robustness and reliability for dynamic shortest paths, the approach typically employed with generalized loopback restoration, appear in Figure 10. The horizontal axis in the graph gives the number of non-critical links extracted for unprotected capacity, ranging from 0 to 11 for this network. For each measure, a solid line indicates values superior to those obtained with the double cycle cover, while a dotted line indicates inferior values.

Notably, we are able to use four links of unprotected capacity while retaining robustness and reliability equal to or better than that provided by a double cycle cover. These four links represent a 17% increase in the traffic capacity of the network. For equivalent or better robustness, we can utilize as many as six links, or 26% more.

The knees in the curves near the right side of the figure are also interesting. The first non-critical edge added to the minimal backup graph produces a topology of two double-homed rings, allowing links in each ring to be recovered independently and significantly increasing both robustness and reliability. Adding another two non-critical links to bring unprotected capacity down to 8 links transforms the topology into three rings sharing one node between each pair of rings.

5.2 ARPANET

We next consider the ARPANET network shown in Figure 4, for which we use a double cycle cover provided by [8]. The network is non-planar, and the cover uses one 14-link cycle, giving robustness of 60% and reliability of 58%. Measured values of robustness and reliability for dynamic shortest paths appear in Figure 11. Solid and dotted lines again indicate the relationship between the values obtained with dynamic shortest paths and the values obtained with a double cycle cover.

The dynamic shortest path approach to restoration in the case of ARPANET cannot provide the same level of second-failure reliability; however, it provides higher first-failure reliability and higher robustness out to six non-critical links used for unprotected capacity, resulting in a traffic capacity increase of 19%.
As with NJ LATA, the addition of two non-critical links to the minimum backup graph provides independent paths for many backups and results in a large robustness increase. A third non-critical link is necessary to increase first-failure reliability, which is limited by a single primary arc that must be backed up on the Hamiltonian cycle with only two added non-critical edges.

5.3 LATA 'X'

No double cycle covers of LATA 'X' are known to us, and the graph is non-planar, precluding a simple construction. Measured values of robustness and reliability for dynamic shortest paths appear in Figure 11. Unlike previous figures, the line styles do not provide a visual comparison with rings.

5.4 Loopback Approaches

Figures 13 through 15 show robustness for the three approaches based on generalized loopback as a function of unprotected capacity. Figures 16 through 18 compare first-failure reliability for the same three approaches. Finally, Figures 19 through 21 show second-failure reliability. Notice that the use of two-path search—an NP-complete problem [10]—does very little to improve either the robustness or the reliability of the networks. Recall that two-path search can result in lower second-failure reliability that other approaches because it gives priority to the first-failure when full restoration is impossible. This effect occurs twice in the figures, at 10 links in Figure 20 and at 15 links in Figure 21.

5.5 Discussion

A close examination of the figures reveals several minor anomalies: increases in reliability as additional links are claimed for unprotected capacity, and even minor increases in robustness in certain cases. These anomalies occur for two reasons: first, our focus in selecting edges and directions was to improve robustness, potentially at the cost of reliability; second, adding a non-critical link to the backup digraph fixes its direction and potentially co-locates backup paths for
other arcs on shared links, reducing robustness.

In terms of accuracy, the results for both preplanned shortest paths and two-path search suffer slightly from the ordering of non-critical link removal in terms robustness for dynamic shortest paths. However, given the set of arcs to be used in the digraph, the data reflect the optimal choice of primary directions for each algorithm rather than the optimum for dynamic shortest paths. As the choice of directions has substantially greater impact on robustness and reliability than the order of edges to be removed, we feel that the numbers reported convey an accurate relationship between the algorithms. Neither choice has any relevance to double cycle covers.

6 Conclusions and Future Directions

We have presented a new method for providing link recovery in mesh networks. Our method allows for rapid recovery, easy extensibility when new links are added, and distributed operation. Moreover, we can assign the capacity in secondary fibers, which are generally reserved to provide backup capacity in case of failure, to carry unprotected traffic. This reassignment of capacity allows for more efficient use of capacity in networks. The other main approach to providing rapid link failure recovery in mesh networks is through networks of rings. We compared our method with one type of cycle cover approach and showed that algorithms based upon our new method for link failure recovery afford significant advantages in terms of spare capacity. However, these gains in spare capacity for unprotected traffic do not come without drawbacks. Even though for primary traffic a single failure on any link is recoverable, robustness and reliability measures for failures of two links are adversely affected.

Several directions of future work spring from our results. One of them is the consideration of node failures. Loopback for node failure recovery is possible using generalized loopback [22], but is difficult with ring covers. The node-redundant minimal backup digraphs presented earlier are thus capable of full recovery from single node failures, but the distinct requirements on traffic rerouting for such failures may affect robustness differently than for link failures. We expect that the tradeoff is similar to that found for two-link failures, however. Another direction of future
work is the examination of guaranteed recovery for multiple link faults [2] for stronger robustness requirements.

Looking further afield, there are many possibilities in further expanding the options of generalized loopback. For instance, we may consider the case where the secondary and primary graphs are not conjugates of one another. We may also investigate the fact that, while having strongly connected secondary digraphs is sufficient for loopback recovery for link failures, it is not clear that it is necessary. Having secondary digraphs composed of several unconnected strongly connected components would limit the number of hops required for recovery. The number of hops may also be directly addressed by placing hop limits, as is done for other schemes. In this paper, we considered the effect of spare capacity on hop count in the backup paths. Finally, we may also consider the application of secondary graphs to provide not only link and node recovery, but also end-to-end path restoration. Since path restoration can offer advantages in terms of capacity [18, 28], such an approach may be used to improve further the use of existing networks.

References


Figure 1: Link restoration using generalized loopback.

Figure 2: Generalized loopback on a reduced backup digraph.

Figure 3: The New Jersey LATA network.

Figure 4: The ARPANET network.
Figure 5: The LATA 'X' network.

Figure 6: The COST239 network.

Figure 7: The National network.
Figure 8: Maximum backup path lengths for three networks.

Figure 9: Longer backup path due to link inclusion.

Figure 10: Robustness and reliability using dynamic shortest paths for NJ LATA. Solid lines are superior to a double cycle cover; dashed lines are inferior.

Figure 11: Robustness and reliability using dynamic shortest paths for ARPANET. Solid lines are superior to a double cycle cover; dashed lines are inferior.
Figure 12: Robustness and reliability using dynamic shortest paths for LATA ‘X’. No double cycle cover was available for comparison.

Figure 13: Robustness of the NJ LATA network for three approaches to link restoration.

Figure 14: Robustness of the ARPANET network for three approaches to link restoration.

Figure 15: Robustness of the LATA ‘X’ network for three approaches to link restoration.
Figure 16: First-failure reliability of the NJ LATA network for three approaches to link restoration.

Figure 17: First-failure reliability of the ARPANET network for three approaches to link restoration.

Figure 18: First-failure reliability of the LATA ‘X’ network for three approaches to link restoration.

Figure 19: Second-failure reliability of the NJ LATA network for three approaches to link restoration.
Figure 20: Second-failure reliability of the ARPANET network for three approaches to link restoration.

Figure 21: Second-failure reliability of the LATA 'X' network for three approaches to link restoration.