Computer Networks 53 (2009) 2537–2551

Contents lists available at ScienceDirect

Computer Networks

journal homepage: www.elsevier.com/locate/comnet

# Heuristic algorithms for designing self-repairing protection trees in mesh networks

Shahram Shah-Heydari [a,*], Oliver Yang [b]

[a] University of Ontario Institute of Technology, Oshawa, Ontario, Canada L1H 7K4
[b] University of Ottawa, School of Information Technology and Engineering, Ottawa, Ontario, Canada K1N 6N5

ARTICLE INFO

*Article history:*
Received 23 July 2008
Received in revised form 10 February 2009
Accepted 12 May 2009
Available online 31 May 2009

Responsible Editor: J. Sole-Pareta

*Keywords:*
Network protection
Shared backup trees
Mesh network restoration

ABSTRACT

Protection trees have been used in the past for restoring multicast and unicast traffic in networks in various failure scenarios. In this paper we focus on shared self-repairing trees for link protection in unicast mesh networks. Shared protection trees have been proposed as a relatively simple approach that is easy to reconfigure and could provide sub-second restoration times with sub-optimal redundancy requirement. The self-repairing nature of this class of protection trees may make them an attractive option for cases where dynamic changes in network topology or demand may occur. In this paper, we present heuristic algorithms to design a self-repairing protection tree for a given network. We study the restorability performance of shared trees and examine the limitations of such schemes in specific topologies, such as cases where long node chains exist. Using extensive simulations with thousands of randomly generated network graphs. We compare redundancy and average backup path length of shared protection trees with optimal tree designs and non-tree designs. We also apply our algorithms to the problem of designing the protection tree in a pre-designed fixed-capacity network, and study the performance of shared protection trees in this scenario under different network loads and link utilization levels.



## 1. Introduction

### 1.1. Background

Network failure recovery has been an important subject of research in the field of network design and service reliability for more than two decades. The large volume of traffic (data, voice, video on demand, etc.) carried by backbone networks draws special attention to the issue of network recovery and protection against node and link failures, because interruption of such huge traffic flow (and, consequently, the offered user services) could cripple businesses and cost millions of dollars. Fast restoration of traffic after failure is essential, whether the failure is caused by a fiber cut, node failure or higher layer service point failure. At the physical layer ring-shaped designs for optical backbone networks, e.g. SONET UPSR and BLSR rings [1] are used commonly. However more recently, particular attention has been paid to mesh networks, by which we refer to networks in which at least one node is connected to three or more other nodes. Mesh networks in particular address the scalability issues of ring-based architectures, because in mesh networks links and nodes can be added or upgraded solely based on traffic demand without imposing a certain physical topology.

Failure recovery schemes in mesh networks are generally categorized as Path restoration schemes and Link protection schemes [2]. In path restoration schemes, failed connections are restored individually by their source nodes through new end-to-end routes. In link protection schemes, an alternative local path between the end nodes of the failed link is found through the network, and all connections on the failed link are switched in bundle to the local detour. The term link is used in a broad sense here; it could refer to a multi-fiber span, a single fiber, a single

* Corresponding author. Tel.: +1 905 721 8668.
*E-mail address:* shahram@ieee.org (S. Shah-Heydari).

1389-1286/$ - see front matter © 2009 Elsevier B.V. All rights reserved.
doi:10.1016/j.comnet.2009.05.009

wavelength on a fiber, or even a higher layer logical connection. As such, different wavelengths on a fiber may be re-routed on different paths. Path and link protection schemes could use dedicated spare capacity for each backup path, or share the spare capacity on each link among all backup paths that traverse it.

In general, link protection could potentially provide faster recovery service than path restoration because there is no need to inform the source node of each individual connection, or to re-compute the end-to-end path from the source node. This factor could become even more important in backbone networks where each fiber might carry thousands of connections between different source-destination pairs. On the other hand, studies have shown that end-to-end path restoration could provide more capacity efficiency and reduce the required redundancy in the network [3]. In practice, link protection schemes are preferable for quick restoration of physical layer communication in backbone networks, while path restorations can be deployed at the internetworking layer of the network.

### 1.2. Related work

We focus our attention on those studies that are more relevant to the subject of this paper, namely the design of tree-based link protection schemes. Therefore, this review does not cover huge amount of prior research on path restoration algorithms. Specifically, we briefly review mesh survivable design techniques, ring and cycle-based techniques, and then discuss applications of unicast trees in network service restoration and dynamic reconfiguration.

Research on mesh survivability schemes has been conducted for about two decades by now. At first, such research efforts focused on using network digital cross-connects to re-route the connections of a failed link over $k$ shortest-paths either from the source node or between the end nodes of the failed link. Distributed protocols such as the SelfHealing Network (SHN) [4] have been proposed to eliminate the need to maintain a central link-state database. Such approaches allowed sharing of spare capacities for backup paths of different links, essentially assuming that the probability of two concurrent link failures was low. The problem of optimizing backup paths to minimize redundancy (often referred as Spare Capacity Assignment – SCA) has been formulated as an Integer Linear Programming (ILP) in several studies under different constraints [5–9]. For the SCA problem it is assumed that the network topology and the working capacity of each link are known, and then the shared spare capacity is optimized by finding the best backup paths for each unit of working capacity. SCA optimization formulations are NP-complete and thus difficult to solve except for small networks. However, such optimal solutions are often used as yardsticks for evaluating the performance of equivalent heuristic methods.

More recent proposals have employed cycle-based protection in which backup paths for network links are arranged on one or more graph cycles [10–13]. This approach would provide certain advantages, such as easier migration from ring-based SONET to a mesh network, as well as faster restoration speed if the cycles are pre-connected. The equivalent SCA design problem for protection cycles has been formulated as an ILP with cycle enumeration (pre-processing a list of potential cycle candidates) [14]. This formulation adds a new constraint to the unrestricted optimal mesh survivable design; that the backup paths should be selected from links on a pre-selected group of cycles. As a result, the redundancy requirement of a cycle-based design tend be higher than the optimal mesh design. The ILP approach to cycle design is also NP-Complete, with exponential computational times reported in [14]. Heuristic design algorithms were proposed in [15,16] to reduce computational times by limiting the number of cycle candidates at the cost of higher redundancy.

The high computational complexity of designing optimal mesh and cycle protection schemes has generated some interest in alternatives with less computational complexity and with simpler manageability; i.e. the ability to reconfigure, scale, maintain and regionalize network wide protection scheme with ease while still providing sub-second restoration speed with sub-optimal redundancy requirements. Network trees provide an alternative option for pre-planning backup paths with reasonable computational complexity. Trees are local by nature and changes on one branch have limited impact on other branches and higher layers in the hierarchy. This fact also provides simpler handling of multiple-link failure or node failures with tree-based protection schemes. A number of telecommunication protocols for constructing spanning trees already exists in various layers of today's networks and can be modified for construction of protection trees. Network state information and databases for tree-based algorithms have already been developed and deployed in the networks. It is easy to grow, modify, add branches or repair a spanning tree using common protocols currently deployed in the mesh networks. Furthermore when static vs. re-configurable networks are being considered, shared protection trees can be managed in a self-repairing manner, where a disconnected node can reconnect itself to the protection structure using primarily local state information and without the need to re-compute the complete set of backup paths for each link. Such computation can be done in advance and stored in the node so that no routing computation would be necessary after failure. On the other hand, it is expected that shared-capacity unicast protection trees in general may require more network redundancy than an equivalent shared-capacity optimal mesh or cycle-based designs. One reason is that a tree provides one backup path for each link while a cycle could provide two backup paths (clockwise and counterclockwise) for each non-cycle link and thus more sharing of spare capacity is possible [12].

Spanning trees have been used widely for routing and protection of traffic in telecommunication networks, for instance, for maintaining connectivity between bridges that connect subnets [17], and in ATM multicast path restoration [18,19], where node or edge-disjoint spanning trees could be used for providing the main and backup routes for multicast traffic from source to sink nodes. Core-based shared tree [20] has also been used for shared protection of multicast traffic. Multicast networks primarily use span-