Optical Switching and Networking 14 (2014) 149–163

Contents lists available at ScienceDirect

Optical Switching and Networking

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

Resilient arcs and node disjointness in diverse routing ☆

Teresa Gomes [a,b,*], Mateusz Żotkiewicz [c]

[a] *Department of Electrical and Computer Engineering, University of Coimbra, 3030-290 Coimbra, Portugal*
[b] *INESC Coimbra, Rua Antero de Quental 199, 3000-033 Coimbra, Portugal*
[c] *Institute of Telecommunications, Warsaw University of Technology, Nowowiejska 15/19, 00-665 Warszawa, Poland*

ARTICLE INFO

Article history:
Received 23 December 2013
Received in revised form
25 May 2014
Accepted 30 May 2014
Available online 6 June 2014

Keywords:
Routing
Protection
Disjoint paths

ABSTRACT

In multi-layer networks protection can be provided at multiple layers. Hence some links at an upper layer may be *resilient* because they are protected at a lower layer. We will designate as *resilient arc* at a given layer, an arc which has some form of protection at an underlaying layer. When path diversity is used at an upper layer, and resilient arcs are taken into account, it may not be necessary for the considered paths to be fully disjoint.

We solve a problem of finding the shortest node-disjoint pair of paths that can share resilient arcs. It is assumed that a network consists of a set of nodes and a set of arcs. Moreover, a number of available arcs are resilient. Our goal is to find the shortest pair of paths such that they share only those nodes that are incident to shared resilient arcs. Moreover, we assume that the resulting paths cannot contain loops, and costs of shared resilient arcs are counted only once towards the objective function.

In the paper we present two novel algorithms solving the above problem, and two supporting algorithms that are utilized as subroutines. We implement the proposed algorithms and compare them to an MIP approach.

1. Introduction and motivation

The deployment of broad-band services has increased the bandwidth demand of telecommunication networks. Satisfying this demand has been made possible by optical networks, which carry a huge amount of traffic. A single link failure in an optical network can have a significant impact in the carried traffic. Because many critical infrastructures depend on the correct and continuous operation of telecommunication networks, these networks must be resilient [2].

Path diversity is a form of protection that consists in routing a traffic demand, between two specific node pairs, using a set of paths. The survivability of traffic flows, in single links (or node) failure scenarios, can be 100% guaranteed by a pair of link-disjoint (or node-disjoint) paths [3]. In multi-layer networks protection can be made at multiple layers. Hence some links at an upper layer may be *resilient* because they are protected at a lower layer. We will designate as *resilient arc* at a given layer, an arc which has some form of protection at an underlaying layer. When path diversity is used at an upper layer, and resilient arcs are taken into account, it may not be necessary for the considered paths to be fully disjoint.

In [4] the Partial Disjoint Path algorithm is proposed to avoid protection duplications in a multi-layer scenario. It is a two step approach: first it calculates the AP (active path or working path or primary path), and then in it seeks to

☆ The idea was originally presented at RNDM 2013 – 5th International Workshop on Reliable Networks Design and Modeling, co-located with ICUMT 2013 Congress (September 10–12, 2013, Almaty, KZ) under title "Finding the shortest node-disjoint pair of paths that are allowed to share resilient arcs" [1].

* Corresponding author at: Department of Electrical and Computer Engineering, University of Coimbra, 3030-290 Coimbra, Portugal.

E-mail addresses: teresa@deec.uc.pt (T. Gomes), mzotkiew@tele.pw.edu.pl (M. Żotkiewicz).

http://dx.doi.org/10.1016/j.osn.2014.05.022
1573-4277/© 2014 Elsevier B.V. All rights reserved.

obtain the shortest BP (backup path or secondary path) which is disjoint with AP only in the unreliable links. The resulting paths are designated failure-disjoint paths because they do not share any risk of failure (assuming nodes do not fail) because they only share resilient arcs. Although this approach allows for sharing of resilient links (counted only once) between the AP and BP, it does not calculate, among all such path pairs, the one of minimal total (additive) cost. Hence the approach of [4] may require more network resources than would have been strictly necessary. This problem is solved in [5], where a polynomial time algorithm for finding failure-disjoint paths of min-sum cost is proposed.

Node disjointness implies link disjointness, so using node disjoint path pairs (or sets of paths) results in higher network availability. Considering there exist resilient arcs in the network layer, where a node disjoint path pair is to be calculated, it may be advantageous from the point of bandwidth usage or cost to admit paths that share those arcs. This implies that the node disjointness restriction, at the end nodes of shared resilient arcs, would have to be relaxed. These resilient arcs may for instance represent interconnections of two sub-networks of a single operator using a third party network. Also, in a Multi-Protocol Label Switching Transport Profile (MPLS-TP) network, resilient arcs may represent (protected) tunnels at the Wavelength Division Multiplexing (WDM) layer. Real-world communication networks are generally made up of different layers, for example, a SONET/SDH layer over an optical network layer. A link of the SONET/SDH layer can be considered as a demand that should be routed through a path in the optical layer. If this path is protected against failures, then the link is reliable. Otherwise the link can fail and hence requires some protection against failures at the SONET/SDH layer. This leads to two kinds of arcs: perfectly reliable arcs that do not fail, and unreliable arcs that can fail [6,3]. This kind of problem is consider for instance in [7], where the authors replace the optical protection with the protection in higher layers for some links. Another example are Free Space Optics (FSO) networks [8] facilitated with fiber connections for some vital routes. In this case, the technology used for fiber links makes them much more resilient to failures than the other links that are built on FSO [9].

In the context described above a new problem arises, which is the calculation of a pair of paths, from node *s* to node *t*, such that they are node-disjoint, except possibly at the end nodes of shared resilient arcs. Moreover, the returned pair of paths cannot contain loops. In this work a formal, mathematical description of the problem of calculating the shortest node-disjoint pair of paths that are allowed to share resilient arcs is proposed and two novel algorithms are introduced for solving it.

As for general requirements that have to be met in practice by such algorithms consider a Multi-Protocol Label Switching (MPLS) context. In the Generalized Multi-Protocol Label Switching (GMPLS) architecture a Path Computation Element (PCE) [10] is a computational unit that calculates routes as requested by a Path Computation Client (PCC). A PCE can be implemented in any system; embedded in a network element or a network management system, or implemented as a separate server dedicated to path computations [11]. The route calculation made by a PCE can be made in a centralized or distributed manner [10]. A centralized PCE usually has good processing capabilities, and it may have a response time in the order of a few seconds, answering to requests from the network management system. In a distributed model the PCE, which may be embedded in a network element, should be able to provide a rapid response, although it may have limited calculation power and memory resources. For end-to-end protection in GMPLS networks, considering that information about resilient links is distributed, the PCE should be capable of calculating failure-disjoint path pairs, to avoid protection duplications. This shows the importance of developing efficient algorithms[1] for determining failure-disjoint paths.

The paper is organized as follows. In Section 2 we present a short literature review on resilient routing. In Section 3 we present a formal, mathematical description of the problem. This is followed by a description of related failure-disjoint problems in Section 4. Problems described there at first sight may look similar to our problem. In Section 5 supporting algorithms are presented. They are utilized as subroutines in the core algorithms solving our problem presented in Section 6. Numerical results are presented in Section 7. The paper ends with conclusions in Section 8.

2. Literature review of resilient routing issues

In [12] network challenges are defined as adverse events causing faults that may result in service failures. Network service providers seek to ensure their networks' survivability, so that when a fault occurs its impact is strongly mitigated and in many cases not even perceived by the users. To attain this objective, two main recovery options are available: protection and restoration. In the first case, backup resources are reserved in advance, before any fault occurs. In the second case, after detecting a fault a solution to recover the affected connection is searched for, and the necessary resources are then allocated to restore the affected services. Protection has higher cost, but strict recovery time, and is the preferred solution at the optical layer [13]. Restoration is more bandwidth efficient than protection, as it makes better use of network resources. However, the efficiency is at the expense of longer recovery times, and hence should only be used for services which can tolerate some disruption resulting in worse quality of service.

Regarding the scope, the recovery can be global, local, or segment oriented [6]. When global path protection is utilized, the AP is utilized in normal network operation conditions. When a fault occurs (due to a node or link failure) a fault indication signal (FIS) is generated by the node closest to the failed element and is sent towards the head end of the path. Once the head end of the failed AP receives the FIS, it will switch the traffic to the BP. When

[1] This work was in fact motivated by a R&D Project under contract with PT Inovação.