Optics Communications 381 (2016) 327–335

Contents lists available at ScienceDirect

Optics Communications

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

Protecting core networks with dual-homing: A study on enhanced network availability, resource efficiency, and energy-savings

Sandu Abeywickrama [a], Marija Furdek [b], Paolo Monti [b], Lena Wosinska [b], Elaine Wong [a,*]

[a] Dept. of Electrical and Electronic Engineering, The University of Melbourne, VIC 3010, Australia
[b] KTH Royal Institute of Technology, Optical Networks Laboratory, Dept. of Communications Systems, ICT School, Kista, Sweden

ARTICLE INFO

Article history:
Received 26 March 2016
Received in revised form
29 June 2016
Accepted 1 July 2016
Available online 23 July 2016

Keywords:
Dual-homing
Energy-efficiency
Network protection
Routing and wavelength assignment
Survivability

ABSTRACT

Core network survivability affects the reliability performance of telecommunication networks and remains one of the most important network design considerations. This paper critically examines the benefits arising from utilizing dual-homing in the optical access networks to provide resource-efficient protection against link and node failures in the optical core segment. Four novel, heuristic-based RWA algorithms that provide dedicated path protection in networks with dual-homing are proposed and studied. These algorithms protect against different failure scenarios (i.e. single link or node failures) and are implemented with different optimization objectives (i.e., minimization of wavelength usage and path length). Results obtained through simulations and comparison with baseline architectures indicate that exploiting dual-homed architecture in the access segment can bring significant improvements in terms of core network resource usage, connection availability, and power consumption.

1. Introduction

Recent analysis has shown that global Internet traffic will grow 3.2 fold from 2014 to 2019, at a compound annual growth rate of 26% [1]. To meet the growing bandwidth demand of next generation Internet, Wavelength Division Multiplexed (WDM) telecommunication networks which can support very high aggregate data rates through wavelength and packet statistical multiplexing, are being deployed in the metro/core and access segments. The access network, either in a point-to-point or point-to multipoint topology, spans tens of kilometers and connects users directly to a Central Office (CO) where traffic is aggregated and separated. In comparison, the long-haul metro/core network comprises metro/core nodes that are interconnected in a mesh topology. Due to the extremely high data rates supported, even a short network service downtime in the core/metro network caused by fiber cuts or component failures can result in the loss of a huge amount of data. It is therefore critical to implement a resilient network with very low network outage times in order to minimize data and revenue losses. Approaches for ensuring core network survivability typically rely on the presence of physically-disjoint backup resources which support the traffic from the working paths affected by a failure. Backup resources can be reserved end-to-end in advance during connection set up time, which is the basic principle of protection. In dedicated path protection (DPP), the resources used for protection along a backup path (which must be link-disjoint with the working path) are reserved for a specific demand and cannot be shared amongst different connections. Alternatively, backup resources can be dynamically provisioned end-to-end after a failure occurs, in the approach known as restoration [2–4].

In the access segment, one method to ensure connectivity between the access and the metro/core segment in the presence of failures is to use dual-homing [5]. Specifically, in a dual-homed optical access network, a Local Exchange (LE) is connected to two different Metro/Core (M/C) nodes, protecting the access segment against feeder fiber and/or M/C node failures. Dual-homing is illustrated in Fig. 1, where two dual-homed LEs and a core network comprising a number of M/C nodes are interconnected by an optical circuit-switched wavelength layer. The example shown in Fig. 1 is the architectural option envisaged by the FP7 project DISCUS [6], and also the architecture considered in this work. Typically, the M/C node physically closest to an LE is assigned as its primary home and is used under normal operating conditions. The second closest M/C node is typically assigned as the secondary home and is used when a failure disables the feeder fiber or the primary home. In Fig. 1, the primary homes of the source and

* Corresponding author.
E-mail address: ewon@unimelb.edu.au (E. Wong).

http://dx.doi.org/10.1016/j.optcom.2016.07.003
0030-4018/© 2016 Elsevier B.V. All rights reserved.

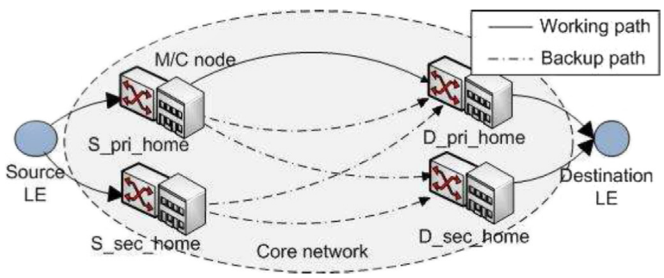

Fig. 1. Core network architecture with dual-homed Local Exchanges (LEs) showing different possible working/backup path options through the core.

destination LEs are denoted as *S_pri_home* and *D_pri_home*, respectively, while *S_sec_home* and *D_sec_home* denote their secondary homes. As can be observed, dual-homing increases LE accessibility and allows for greater flexibility in establishing working and backup paths through the core network by differently combining the usage of primary and secondary homes of the source and the destination LEs. Dual-homing through 1+1 protection mechanism was reported in [7] to protect long-reach passive optical networks. In 1+1 protection, downstream data is replicated at both the primary and secondary M/C nodes with the dedicated secondary M/C node remaining active throughout to monitor for failures. Traffic is required to be replicated through the core. While 1+1 protection yields the fastest possible fault recovery time, the cost from having to reserve extra capacity to carry the duplicated backup traffic is high. In [8], a 1:1 protection scheme was proposed instead, removing the need to duplicate data in the core. Upon failure detection, the 1:1 protection mechanism switches traffic through to the secondary M/C node, restoring services in the access while also re-routing traffic through the core. In [9], the 1:1 protection was further extended to N:1 protection, whereby a common secondary M/C node is shared by multiple primary M/C nodes, providing further cost savings. Field trials and demonstrations of dual-homed protection have been reported in commercial Gigabit PONs [10], automated virtual local area networks (VLANs) [11], and 10G-EPONs [12].

Dual-homing can be beneficial not only to protect the access segment of the network from the feeder and primary home failures, but also to provide resilience against failures in the core segment in a more resource efficient way than if only primary homes are considered as possible sources and destinations of working and backup paths. In recent years, many dual-homing based solutions have been proposed to enhance WDM core mesh network survivability [13–16]. In [13], an integrated dual-homing and core network protection to handle a single link failure by considering a dual-homed IP-over-WDM architecture was implemented. In [14], the authors proposed a coordinated protection scheme for dual-homed-based IP-over-WDM networks in which enterprises/users connect to IP routers of different service providers. Their approach considered the presence of dual-homing only at the source node of each communication request. The aim was to establish a working and a backup path between any of the two homes at the source side and the single home at the destination side, with the objective of minimizing the total, i.e. working plus backup, path lengths. The authors extended their work to consider dual-homing at both source and destination LEs, providing two pairs of paths to ensure connections between all combinations of homes, i.e. connections between both (primary and secondary) source homes and both (primary and secondary) destination homes [15]. The authors considered a generalized failure scenario in which independent failures can occur in the access network at the source side, the access network at the destination side, as well as the optical core network, and presented a wavelength cost analysis for the proposed coordinated solution. In [16], a scalable scheme for partial multicast protection based on a dual-homing architecture was presented. Their work investigated the use of dual-homing to protect against fiber failures in one-to-many communication without making any changes to the routing algorithm in the core network. In [15] and [16], the authors assume full-wavelength conversion capability at each core node.

In [17], we carried out a preliminary study to investigate the benefits of utilizing dual-homing at both the source and the destination LEs while protecting demands against different types of failure scenarios in the core network segment. Specifically, we investigated the survivable Routing and Wavelength Assignment (RWA) problem with dual-homing with the aim to protect against *single link failures* in the core segment. In our proposed dedicated path protection with dual-homing scheme, the backup route can be set up between *any of the two homes of the sources and destination LEs*. Due to greater LE accessibility and higher number of alternative choices for protection paths, our proposed approach has been shown to significantly reduce the average path length and the number of used wavelengths [17]. In addition, our solution was also able to obtain higher connection availability in a country-wide Irish network when compared to the baseline approach without dual-homing.

In this work, we extend our initial investigation that achieves single link failure protection to *also provide protection against a single link or an intermediate node failure*. Note that an intermediate node is defined as an M/C node that is neither the source or the destination node of the considered lightpath. For each of the considered failure scenarios, we propose two heuristic algorithms to solve the RWA problem with DPP with two different objectives: (i) minimizing the number of used wavelengths; or (ii) minimizing the total path length. Minimizing the number of wavelengths and path lengths reduces resource usage which in turn reduces network operation costs.

Our proposed approach differs from previous dual-homing based survivable approaches in that we focus on establishing a *single path pair*, i.e. one working path and one backup path, from/to either primary or secondary home of the source and destination LEs to protect against either single link or single intermediate M/C node failure. This is unlike previous work, whereby two pairs of working and backup paths exist to connect both source homes (primary and secondary) to both destination homes (primary and secondary). Further, our approach considers a fully transparent network with no wavelength conversion capabilities and ensures *wavelength continuity in all established lightpaths*.

Our work also differs from previous investigations in that we consider the potential energy-savings in exploiting dual-homing in the access network to provide core network protection. Network energy efficiency is becoming a crucial parameter in operating communication networks. The worldwide electricity consumption of telecommunication networks was estimated to be 350 TW h in 2012 (nearly 2% of the worldwide electricity consumption), with an average annual growth rate of 10% from 2007 [18]. As such, the energy consumption and thus increased operating cost arising from implementing backup resources in protecting the network cannot be ignored and must therefore be minimized. Compared to conventional DPP solutions where primary and backup paths can only be established between primary and secondary homes, respectively, our initial study in [17] indicated that our approach yields reduced lightpath length and fewer used wavelengths. In this work, we quantify the improvement in resource usage through these reductions and translate them into energy-savings in the core network. We also present a