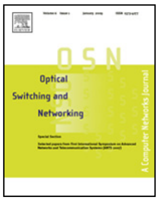
Optical Switching and Networking 8 (2011) 68–78

Contents lists available at ScienceDirect

Optical Switching and Networking

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



Multi-domain restoration with crankback in IP/MPLS networks

F. Xu [a], M. Peng [b], M. Esmaeili [a], N. Ghani [a,*], A. Rayes [c]

[a] *University of New Mexico, United States*
[b] *Wuhan University, China*
[c] *Cisco Systems, United States*

ARTICLE INFO

Article history:
Received 15 March 2010
Received in revised form 11 June 2010
Accepted 1 July 2010
Available online 14 July 2010

Keywords:
Network survivability
Multi-domain survivability
Restoration
Crankback signaling

ABSTRACT

Multi-domain network survivability is a key problem area and crankback signaling offers a very viable alternative for post-fault restoration. However, although some initial multi-domain crankback studies have been done, most have not considered post-fault recovery. Along these lines, this paper proposes a novel solution framework for joint intra/inter-domain crankback restoration in realistic MPLS/GMPLS network settings. Namely, dynamic link failure and intra-domain link-state routing information is coupled with the available inter-domain path/distance vector routing state to improve the recovery process. Mechanisms are also introduced to limit crankback overheads and delays. The performance of the proposed solution is then analyzed using simulation.

1. Introduction

Network survivability in IP-based *multi-protocol label switching* (MPLS) and optical *generalized MPLS* (GMPLS) networks is a very well-studied problem area. However, even though a wide range of pre-fault protection and post-fault restoration schemes have been proposed, most have assumed complete "network-wide" topology and resource visibility in the provisioning process. In general, this assumption is only valid in single "domain" settings, e.g., such as those controlled by a centralized provisioning entity and/or running distributed link-state routing protocols [1,2]. However, as user application demands continue to grow, there is a pressing need to extend service recovery across larger geographic ranges spanning multiple domains or *autonomous systems* (AS). In such settings, it is generally very difficult to have full "global" visibility across domains and inter-domain links, i.e., owing to obvious scalability and confidentiality limitations. Hence commensurate multi-domain recovery schemes must be designed to operate in a distributed, decentralized manner.

Now various survivability schemes have been proposed for handling inter-domain failures in IP and optical networks, nearly all of which focus on "pre-provisioned" protection [3–7]. (Note that most *intra-domain* failures are usually handled using existing domain-level recovery schemes.) For example, some designers have leveraged earlier SONET/SDH designs to implement "localized" dual/multi-homing interconnection [4] between border nodes in optical *dense wavelength division multiplexing* (DWDM) networks. Alternatively, others have developed more "globalized" protection schemes for multi-domain MPLS/GMPLS networks using sequential or parallel working/protection path computation [5–7]. In particular, some of these solutions have proposed hierarchical routing algorithms to compress and disseminate the inter-domain survivability states, i.e., path, link diversity [6,7]. This aggregated information is then used to compute and expand diverse paths across domains. However, even though these latter schemes deliver good blocking reduction, they pose notable concerns. Foremost, associated routing overheads are quite high owing to the larger dimensionality of the survivability-related state [6]. Moreover, many of these solutions will be difficult to realize in operational networks as carriers will prefer existing "inter-domain" distance/path

[*] Corresponding author. Tel.: +1 505 277 1475.
E-mail address: ghanin@yahoo.com (N. Ghani).

1573-4277/$ – see front matter © 2010 Elsevier B.V. All rights reserved.
doi:10.1016/j.osn.2010.07.001

vector protocols, e.g., *border gateway protocol* (BGP) variants. Now these protocols only provide next-hop domain and endpoint reachability state and do not support any link-state updates for *quality-of-service* (QoS) or survivability support [1]. Finally, most protection schemes have been primarily designed to handle single-fault (link) recovery, and hence may not be very effective against multiple failures.

In light of the above, there is a pressing need to develop alternate *restoration* schemes for multi-domain survivability. These solutions basically rely upon active post-fault crankback signaling [8] to search for new routes in reduced visibility settings. However, few studies have been done in this overall area. For example, most recent "per-domain" crankback schemes have only addressed *traffic engineering* (TE) setup for working routes [9–12]. Moreover, many of these crankback solutions pursue rather cumbersome "exhaustive" search strategies, yielding high signaling overheads. In response, the authors here have studied various improved multi-domain crankback strategies for optical DWDM [13,14], and IP/MPLS [15] networks. However, all of these contributions only treat working-mode operation. Hence there is significant scope to apply crankback strategies in more complex post-fault restoration settings. This is the focus herein.

Along these lines, this paper proposes a novel multi-domain crankback scheme for restoration in MPLS/GMPLS networks using the standard *resource reservation* (RSVP-TE) protocol [8]. Specifically, two levels of crankback are defined – intra- and inter-domain – and these are applied at the intermediate and end-to-end path levels. Furthermore, the solution addresses realistic settings where nodes have full internal domain visibility via link-state routing, e.g., *open shortest path first* (OSPF-TE), but limited "next-hop" inter-domain visibility, e.g., as per inter-area or inter-AS routing protocols such as hierarchical OSPF or BGP. Overall, this paper is organized as follows. Section 2 presents a survey of the latest work on multi-domain provisioning and survivability, including standards and research. Next, Section 3 details the enhanced intra/inter-domain crankback provisioning/restoration solution. Detailed performance analysis is then conducted in Section 4 and conclusions and future directions presented in Section 5.

2. Background

Multi-domain networking is a relatively well-studied topic area and a range of protocol standards have been evolved over the years, i.e., at the IP/MPLS and optical DWDM layers. In general, many of these standards also provide requisite capabilities for network survivability. For example, many IP routing protocols support varying degrees of inter-domain state exchange, e.g., next-hop/path vector exchange in *exterior gateway protocols* (EGP) and hierarchical link-state exchange in two-level OSPF-TE. Inter-domain routing is also supported by the *Optical Internetworking Forum* (OIF) as part of its *network-to-network interface* (NNI) standard [1]. Furthermore, the recent IETF *path computation element* (PCE) [3] framework has also formalized a new framework for multi-domain TE and survivability route computation. Specifically, this solution introduces domain computational entities to decouple path computation from setup signaling. At the inter-domain level, these PCE entities can interact in a distributed manner to resolve end-to-end routes using a specialized PCE-to-PCE protocol. Overall, the PCE framework supports two computation strategies to handle varying levels of "global" state, i.e., *per domain* and *PCE-based* [3,10]. The former computes paths in a "domain-to-domain" manner and is most germane for limited inter-domain visibility. Meanwhile the latter relies upon the head-end PCE to compute a *partial* or *loose* route to the destination ("skeleton path") and is better suited for increased inter-domain visibility. However, since blocking can occur at signaling setup, crankback extensions have also been defined for RSVP-TE to support re-tries on alternate routes [8]. Namely, several multi-domain crankback strategies have been outlined (local, intermediate, and source), but detailed algorithms are left to vendor implementation.

Meanwhile on the research side, a wide range of multi-domain networking studies have been done, see [1] and related references. Now with regards to distributed *multi-domain survivability* in particular, various protection strategies have been studied. For example, [4] proposes optical-layer domain interconnection strategies, e.g., dual, multi-homed, to protect working and protection paths traversing the same domain sequence. These solutions leverage legacy SONET/SDH and are quite robust to localized link failures. However, many of these "domain-to-domain" schemes are quite inefficient (costly) and highly susceptible to multiple failures at domain boundaries. Hence more advanced *distributed* multi-domain protection strategies have also been proposed for improved "domain diversity" between working/protection routes. For example [5] tables *sequential* and *parallel* strategies for working/protection route computation in MPLS networks. In particular, the sequential scheme first computes end-to-end working routes and then uses the returned paths to compute diverse protection routes. However, these schemes are shown to be less optimal (higher blocking) and also more susceptible to "trap" topology problems between domains.

Meanwhile, alternate parallel strategies implement more complex joint, i.e., *concurrent*, path pair computation. However, these schemes require added state to ensure non-overlapping routes across common domains. A means of achieving this is to use hierarchical routing to extract and propagate critical state information between domains. Namely, various graph topology abstraction schemes have been developed to condense domain resource and survivability (diversity) state. This information is then flooded to build "abstracted" global views for use in working/protection path pair computation. For example, [6] applies Surballe's path pair algorithm to provision dedicated protection recovery. Meanwhile [7] proposes novel shared inter-domain path and overlapped segment protection schemes using full mesh and virtual edge abstractions. Results here show good blocking reduction for several topologies. Nevertheless, many of these "survivability-aware" abstraction schemes generate