Computer Networks 53 (2009) 1530–1545

Contents lists available at ScienceDirect

Computer Networks

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

A novel path protection scheme for MPLS networks using multi-path routing

Sahel Alouneh [a,*], Anjali Agarwal [b], Abdeslam En-Nouaary [c]

[a] German-Jordanian University, Jordan
[b] Department of Electrical and Computer Engineering, Concordia University, 1515 St. Catherine West, Montreal, Canada H4G 2W1
[c] Institut National des Postes et Telecommunications (INPT) Madinat Al Irfane, Rabat, Morocco

ARTICLE INFO

Article history:
Received 17 April 2008
Received in revised form 17 November 2008
Accepted 3 February 2009
Available online 11 February 2009

Responsible Editor: G. Ventre

Keywords:
MPLS
Fault tolerance
Failure recovery
Path protection
Packet loss

ABSTRACT

Multi-protocol label switching (MPLS) is an evolving network technology that is used to provide traffic engineering (TE) and high speed networking. Internet service providers, which support MPLS technology, are increasingly demanded to provide high quality of service (QoS) guarantees. One of the aspects of QoS is fault tolerance. It is defined as the property of a system to continue operating in the event of failure of some of its parts. Fault tolerance techniques are very useful to maintain the survivability of the network by recovering from failure within acceptable delay and minimum packet loss while efficiently utilizing network resources.

In this paper, we propose a novel approach for fault tolerance in MPLS networks. Our approach uses a modified (k, n) *threshold sharing scheme* with multi-path routing. An IP packet entering MPLS network is partitioned into n MPLS packets, which are assigned to node/link disjoint LSPs across the MPLS network. Receiving MPLS packets from k out of n LSPs are sufficient to reconstruct the original IP packet. The approach introduces no packet loss and no recovery delay while requiring reasonable redundant bandwidth. In addition, it can easily handle single and multiple path failures.

1. Introduction

Multi-protocol label switching (MPLS) [1] is an evolving technology that improves routing performance and speed, and enables traffic engineering by providing significant flexibility in routing. It is also capable of providing controllable quality of service (QoS) by primarily prioritizing Internet traffic.

MPLS provides mechanisms in IP backbones for explicit routing using label switched paths (LSPs), encapsulating the IP packet in an MPLS packet. When IP packets enter a MPLS based network, label edge routers (LERs) assign them a label identifier based on classification of incoming packets and relating them to their forward equivalence class (FEC). Once this classification is complete and mapped, different packets are assigned to corresponding labeled switch paths (LSPs), where label switch routers (LSRs) place outgoing labels on the packets. In this basic procedure all packets which belong to a particular FEC follow the same path to the destination, without regards to the original IP packet header information. The constraint based label distribution protocol (CR-LDP) [2] or RSVP-TE [3], an extension of the resource reservation protocol, is used to distribute labels and bind them to LSPs. Fig. 1 shows a simple process for requesting and assigning labels in a MPLS network. Here, an IP packet with IP prefix value 47.1 enter-

[*] Corresponding author. Tel.: +1 5146929353.
E-mail addresses: sahel.alouneh@gju.edu.jo, sahel_a@yahoo.com (S. Alouneh), aagarwal@ece.concordia.ca (A. Agarwal), ennouaar@ece.concordia.ca (A. En-Nouaary).

1389-1286/$ - see front matter © 2009 Elsevier B.V. All rights reserved.
doi:10.1016/j.comnet.2009.02.001

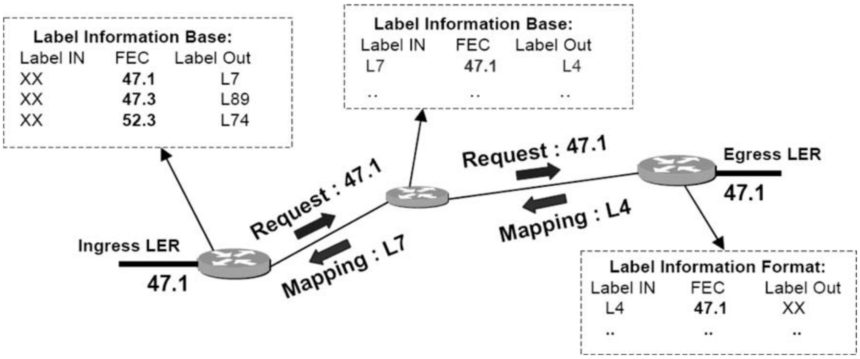

Fig. 1. MPLS single path label distribution.

ing the MPLS network is assigned labels L_7 and L_4 to setup an LSP used to forward the packet from the ingress router towards the egress router. Therefore, each LSR that receives a MPLS packet with *Label IN* value, after checking its FEC value, forwards the packet to the next router with *Label Out* value.

MPLS has many advantages for traffic engineering. It increases network scalability, simplifies network service integration, offers integrated recovery, and simplifies network management. However, MPLS is very vulnerable to failures because of its connection oriented architecture. Path restoration is provided mainly by rerouting the traffic around a node/link failure in a LSP, which introduces considerable recovery delays and may incur packet loss. Such vulnerabilities are much costly to time-critical communication [5] such as real-time applications, which tolerate a recovery time in the order of seconds down to 10's milliseconds. Therefore, service disruption due to a network failure or high traffic in the network may cause the customers significant loss of revenue during the network down time, which may lead to bad publicity for the service provider [4]. To prevent such bad consequences, routers and other system elements in MPLS networks should be resilient towards node or link failures. In other words, MPLS networks should implement efficient mechanisms for ensuring the continuity of operations in the event of failure anywhere in the network. This aspect is usually referred to as fault tolerance. It is defined as the property of a system to continue operating properly in the event of failure of some of its parts.

Over past years, several research works have been done to deal with fault tolerance in MPLS networks (for instance [5–14]). They can be classified into two categories, namely: pre-established protection techniques and dynamic protection techniques. In the former, a backup LSP is pre-established and configured at the beginning of the communication in order to reserve extra bandwidth for each working path. In the latter, no backup LSP is established in advance but after a failure occurs; hence, extra bandwidth is reserved upon the happening of failures. Pre-established path protection is the most suitable for restoration of MPLS networks in real-time due to fast restoration speed. The dynamic protection model, however, does not waste bandwidth but may not be suitable for time sensitive applications because of its large recovery time [5–7].

In addition, recovery schemes can be classified as either *link restoration* or *path restoration* according to the initialization locations of the rerouting process. In link restoration, the nodes adjacent to a failed link are responsible for rerouting all affected traffic demands. In contrast, in path restoration, the ingress node initiates the rerouting process irrespective of the location of the failure. When the reserved spare capacity can be shared among different backup paths, it is called shared path/link restoration. In general, path restoration requires less total spare capacity reservation than link restoration scheme [8].

Besides the above classification issue, protection techniques can be compared one to another based on parameters like bandwidth redundancy, type of failures handled, recovery time, and packet loss. The first parameter measures how much extra bandwidth is required by the protection scheme. The second parameter determines whether the protection technique recovers from single or multiple failures. The third parameter indicates how much time is required by the technique to reroute traffic after failure. Finally, the last parameter gives the percentage of packets lost due to failures. As pointed out later on, none of the existing fault tolerance schemes provides path protection without packet loss, recovery delay, and minimum redundant bandwidth. Therefore, there is still a need for new protection techniques that can optimize all of these factors.

In this paper, we present a novel approach for fault tolerance in MPLS networks using a modified (k, n) *threshold sharing scheme* with multi-path routing. An IP packet entering MPLS network is partitioned into n MPLS packets, which are assigned to n disjoint LSPs across the MPLS network. Receiving MPLS packets from k out of n LSPs is sufficient to reconstruct the original IP packet. The proposed approach has the following advantages. Firstly, it handles single failure as well as multiple failures. Secondly, it allows the reconstruction of the original packet without any loss of packets and a zero recovery delay. Thirdly, it requires a reasonable redundant bandwidth for full protection from failures. It is worth to note that in case the network topology does not offer n disjoint paths, the proposed approach should use n maximally disjoint paths. In this case, the reconstruction of the original packet might