The Journal of Systems and Software 83 (2010) 609–620

Contents lists available at ScienceDirect

The Journal of Systems and Software

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

Redirection based recovery for MPLS network systems

Jenn-Wei Lin *, Huang-Yu Liu

Dept. of Computer Science and Information Engineering, Fu Jen Catholic University, Taiwan, ROC

ARTICLE INFO

Article history:
Received 2 January 2009
Received in revised form 29 October 2009
Accepted 30 October 2009
Available online 5 November 2009

Keywords:
MPLS
Fault tolerance
Label switched path
Affected traffic
Minimum cost flow

ABSTRACT

To provide a reliable backbone network, fault tolerance should be considered in the network design. For a multiprotocol label switching (MPLS) based backbone network, the fault-tolerant issue focuses on how to protect the traffic of a label switched paths (LSP) against node and link failures. In IETF, two well-known recovery mechanisms (protection switching and rerouting) have been proposed. To further enhance the fault-tolerant performance of the two recovery mechanisms, the proposed approach utilizes the failure-free LSPs to transmit the traffic of the failed LSP (the affected traffic). To avoid affecting the original traffic of each failure-free LSP, the proposed approach applies the solution of the minimum cost flow to determine the amount of affected traffic to be transmitted by each failure-free LSP. For transmitting the affected traffic along a failure-free working LSP, IP tunneling technique is used. We also propose a permission token scheme to solve the packet disorder problem. Finally, simulation experiments are performed to show the effectiveness of the proposed approach.

© 2009 Elsevier Inc. All rights reserved.

1. Introduction

With rapid growth of Internet and increase in real-time and multimedia applications, hop-by-hop packet forwarding is insufficient to support the data transmission. The IETF has proposed multiprotocol label switching (MPLS) as a new forwarding technology for meeting the requirement of explosive traffic. In addition to fast forwarding, fault tolerance is also an important issue in the network design. If an Internet service provider (ISP) adopts the MPLS technology to design its backbone network, a fault-tolerant mechanism is also necessary to protect the traffic of a label switched path (LSP) against node and link failures. The LSP is a transmission path in the MPLS network. A lot of research work (Huang et al., 2002; Haskin and Krishnan, 2000; Hundessa and Pascual, 2001; Ho and Mouftah, 2004; Yoon et al., 2001; Ahn et al., 2002; Agarwal and Deshmukh, 2002) has been studied the fault-tolerant issue of the MPLS network. The main ideas of these work are derived from the two IETF recovery mechanisms: *protection switching and rerouting* (Sharma et al., 2003). The protection switching mechanism pre-establishes a backup path for each working LSP. When an LSP fails, the carried traffic in this LSP is switched to a pre-established backup path of the LSP. However, if there is also a node (link) failure in the pre-established backup path, this recovery mechanism cannot work successfully. For the rerouting mechanism, the backup path is dynamically found. There is non-trivial overhead for finding of the backup path. In addition, the rerouting mechanism may also fail if it cannot find a suitable backup path.

In this paper, we propose an efficient approach for enhancing the fault-tolerant performance of the protection switching and rerouting recovery mechanisms. If a failed LSP cannot be recovered successfully using anyone of the above two recovery mechanisms, the proposed approach is initiated to perform the recovery of the failed LSP again. The proposed approach utilizes failure-free working LSPs (the working LSPs without suffering from failures) to carry the traffic of the failed LSP (the affected traffic). For transmitting the affected traffic along a failure-free working LSP, IP tunneling technique is used to encapsulate each packet of the affected traffic to be with the forwarding equivalence class (FEC) type of the LSP. With IP tunneling technique, it is not required to perform additional label assignment. However, in the above protection switching and rerouting recovery mechanisms, extra labels are assigned for each backup path to transmit the affected traffic. The proposed approach can avoid performing the complicated label assignment task (Applegate and Thorup, 2003). To minimize the influence of the affected traffic on failure-free working LSPs, the proposed approach transfers the problem of affected traffic distribution to the problem of minimum cost flow. We also propose a permission token scheme to solve the packet disorder problem. Finally, we perform simulation experiments to show the performance and overhead of the proposed approach.

The rest of this paper is organized as follows. Section 2 gives background knowledge. Section 3 proposes our fault-tolerant approach. Section 4 compares the proposed approach with previous approaches. Finally, concluding remarks are made in Section 5.

* Corresponding author.
E-mail address: jwlin@csie.fju.edu.tw (J.-W. Lin).

0164-1212/$ - see front matter © 2009 Elsevier Inc. All rights reserved.
doi:10.1016/j.jss.2009.10.043

2. Background

2.1. Network model

The network model referred to this paper is shown in Fig. 1, which consists of an MPLS backbone network, two IP based access networks, and an OAM (operations, administration, and management) center. In the MPLS backbone network, a number of label switched paths (LSP) are established in advance. Each LSP consists of an ingress label switching router (ingress LSR), one or more intermediate label switching routers (intermediate LSRs), and an egress label switching router (egress LSR). The establishment of an LSP can be accomplished using label distribution protocol (LDP) (Andersson, 2007). This dedicated protocol is developed by IETF for assigning labels to an LSP. With the label assignment, an LSP is responsible for carrying the packets with a particular forwarding equivalence class (FEC) type (header). The FEC represents an aggregation of packets which are treated using the same transmission manner. For a packet, the FEC of this packet is determined by some fields of its header, such as the source and/or destination addresses.

As shown in Fig. 1, there are also many components in the MPLS network system. Generally, an OAM center is equipped within a network system for managing the operations, verifying the performance, and monitoring the statuses of all the components. In (Cavendish et al., 2004), authors have described the OAM of MPLS network system in more details.

2.2. Failure assumption and detection

Although a whole MPLS network system includes an MPLS backbone network, two IP based access networks and an OAM center (see Fig. 1), we mainly studies the fault-tolerance issue of MPLS backbone network. Failures are assumed to occur in the MPLS backbone network only. The failure detection is based on a well-known *Hello* mechanism. In this mechanism, a Hello message is periodically sent between each two neighbor LSRs. After a period of time, if each LSR on an LSP does not receive a Hello message from one of its neighbor LSRs, a *failure indication signal* (FIS) message is sent to report the failure detection. Next, the proposed approach is initiated to perform the recovery of the failed LSP.

2.3. Related work

All existing MPLS fault-tolerant approaches are based on the two IETF recovery models: protection switching and rerouting (Sharma et al., 2003). The backup path in the two recovery models is either pre-established or dynamically found.

The approaches of Huang et al. (2002), Haskin and Krishnan (2000), Hundessa and Pascual (2001) and Ho and Mouftah (2004) are based on the protection switching mechanism. In the approach of Huang et al. (2002), each working LSP has a disjoint backup path between the ingress LSR and egress LSR. The backup path is pre-established, and it does not share any intermediate LSRs with the corresponding primary LSP. When detecting one or more failure in a working LSP, the FIS message is sent back to the ingress LSR of the failed LSP. Upon receiving the FIS message, the ingress LSR reroutes the incoming packets through the disjoint backup path. However, the approach of Huang et al. (2002) has the packet loss problem since it does not reroute the packets currently carried in the failed LSP (the in-transit packets).

To solve the packet loss problem, the approach of Haskin and Krishnan (2000) additionally pre-establishes a backward backup path for each working LSP. There are two backup paths for a working LSP. The route of the backward backup path is reverse with the route of the corresponding primary LSP. When a failure is detected in a working LSP, new incoming packets are carried by the disjoint backup path. As for the in-transit packets, they are sent back to the ingress LS using the backward backup path. When the ingress LSR receives the in-transit packets, it further redirects the packets to the disjoint backup path. Although the approach of Haskin and Krishnan (2000) can solve the packet loss problem, it may additionally introduce the packet disorder problem, such that new incoming packets are earlier than the in-transit packets to be carried by the disjoint backup path.

To overcome the packet disorder problem, the approach of Hundessa and Pascual (2001) uses tagging and buffering techniques to improve the approach of Haskin and Krishnan (2000). The tagging technique is used to make each path switch LSR (PSL) on the failed LSP know its last received packet before the failure. The buffering technique is used to make each PSL actively store the incoming packets after the failure. By the assistance of the above two techniques, the in-transit packets and new incoming packets can be carried by the disjoint and backward backup paths under an in-order manner.

Unlike the above protection switching based approaches, the approach of Ho and Mouftah (2004) pre-establishes several backup paths for each working LSP. In this approach, a working LSP is first subdivided into several protected segments. Each protected segment forms a protection domain, which has a PSL and a PML (path merge LSR). In a protection domain, each backup path is pre-established and disjoint with its protected segment. Once detecting a

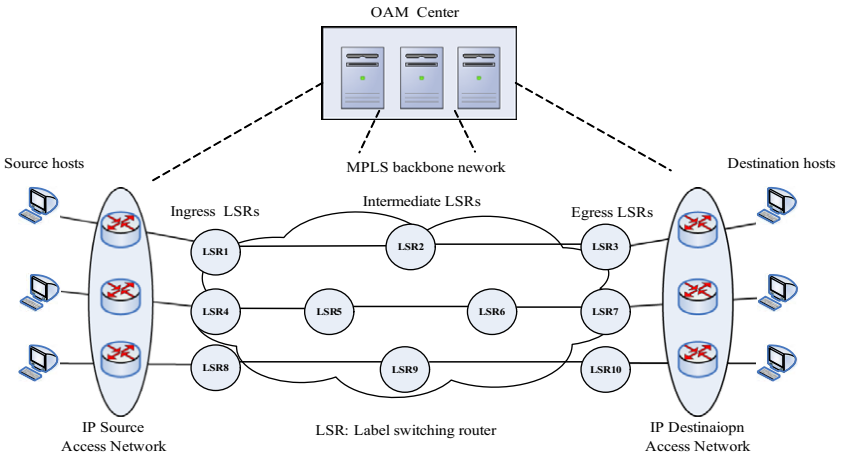

Fig. 1. MPLS network model.

Download English Version:

https://daneshyari.com/en/article/461973

Download Persian Version:

https://daneshyari.com/article/461973

Daneshyari.com