Review on Fault Tolerance Strategies in MPLS Network

Ravi Yadav  
M.Tech. student in Shekawati  
College of Engineering Dundlod  
Rajasthan

Mrs. Laxmi Prasanna  
Asst. Prof. in Shekawati  
College of Engineering  
Dundlod Rajasthan

Anil Vadhwa  
Asst. Prof. in RPS  
College of Engineering  
Mohindergarh Haryana

Abstract

In order to provide reliable services MPLS network uses set of procedures (fault detection, fault notification and fault recovery) which provide appropriate protection to the traffic carried in active LSP (Label Switching Path). When fault occur in active LSP, the recovery scheme must re-direct the affected traffic to the recovery path which bypass the fault. The two basic recovery mechanism defined by IETF used to re-direct affected traffic is rerouting and protection switching. In protection switching number of faults can be handled simultaneously in the active and recovery path and is faster as compared to rerouting switching. On the other hand, rerouting switching can utilize resources in an efficient way but is slower than protection switching. In this paper we present a survey of various fault recovery schemes, initially we start reviewing some approaches of protection switching then we discuss the characteristics of some rerouting approaches. Finally the review recovery mechanisms are classified according to the set of characteristics considered relevant.

Keywords

Switching, LSP, MPLS, AP, FIS, POR.

1. Introduction

With the needs of real-time, high priority, and mission critical application services, network reliability and survivability have become important issues in Internet. When a network failure occurs by the excessive Internet traffic, the recovery mechanism by the current IP may take a long time from a few seconds to several minutes, which may result in a large amount of packet loss. This amount of packet loss causes a serious problem of service and network performance degradation. This is also unacceptable for many ISPs (Internet Service Provide) to provide highly reliable services. They may want to use network resources more efficiently, minimize the recovery time, and maximize network reliability and survivability or service availability.

The IETF has proposed MPLS (Multi Protocol Label Switching) technology as a solution for the explosive Internet traffic [27]. To provide network survivability in MPLS network, an LSP (Label Switching Path) can be protected from a network fault. MPLS-based protection LSP is a logical LSP, which makes traffic travel through it as the same service quality regardless of any failures. The protection LSP has two types of path, the one is a active path that carries traffic in a normal situation, and the other is a backup path that is used when a fault occurs.

In order to carry the same labeled traffic in MPLS network, an LSP should be established beforehand, and then rapidly forwards the traffic by high-speed label swapping method. To protect an LSP in MPLS, the protection LSP establishes the active path and backup path at its setup time. When a network failure occurs, MPLS may perform recovery action faster than the best-effort IP network only by switching working traffic onto the backup path. The IETF defined two recovery models that are protection switching and rerouting model. A network service provider must apply different recovery schemes according to the QoS characteristics of the carried traffic flow (service class), satisfying service-level agreements and simultaneously consuming minimum resources. This has spurred the proposal of a huge number of recovery schemes that offer dependability by fault tolerance.

2. Protection switching

The protection switching mechanism pre-established a recovery path (before the fault detection) for each active path (AP). When an AP fails the affected traffic is switched to the pre-established RP. Recovery can also be local or global and resource or path oriented.

2.1 Local Recovery

The local protection is performed in a distributed manner and its main aim is to protect against any neighboring link or node failure. In order to protect the entire active MPLS path, the local protection mechanisms require substantial recovery path computation and management task. When fault occur the traffic on the working path is switched over to the recovery path in the MPLS based local protection mechanism. The nearest upstream label switch router is responsible for the recovery path selection and switching when it uses local recovery according to [28].

If a fault occur and immediate upstream is unable to recover may be because it not a point of repair (POR) or it is POR but unsuccessful in its effort, then it sends a fault indication signal (FIS) to its immediate node, where a new effort (of local) recovery take place, we conceive it as local recovery.
mechanism (even if the node that successfully recover the AP coincides with the head-end node).

### 2.1.1 Resource Oriented

If a recovery mechanism is focuses to protect the node and/or link then it is said to be resource oriented. Local recovery with protection switching and resource (link and/or LSR) oriented recovery is provided by various schemes including [12, 17, 22].

P. Pan et al. [22], gives two Fast Reroute (FRR) schemes define RSVP-TE extension to establish backup label switch path (LSP) tunnels for local repair of LSP tunnels. If failure occurs, this scheme enables the re-direction of traffic onto backup LSP tunnels in 10s of milliseconds. The one-to-one method creates detour LSP for each protected LSP at each potential point of local repair. The facility method creates a bypass tunnel to protect a potential failure point. Facility protection will only be relevant to protected LSP with guaranteed bandwidth, as not all paths that use a resource must be protected in the same way.

Mellah and Mohamed [12], proposed a scheme (protects only link faults) which also uses bypass tunnel but in this no RSVP-TE extension is required and proposed scheme protect all the LSP that use the protected links but scheme is restricted within per-platform label space.

In the approach of Hundessa and Pascual [14] uses tagging and buffering techniques to overcome the packet disorder problem. 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 help 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.

Another scheme proposed by Kang and Reed [17], dedicated to protection uses bypass tunnels with bandwidth guarantee in MPLS networks. It uses p-cycles (pre-configured cycles). Before any fault occurs p-cycles [30] pre configure the entire network capacity in cycles that allows not only recovery of fault but also links connecting any two non-adjacent nodes in the “p-cycle” (straddling links) which contributes significantly for the p-cycle efficiency.

### 2.1.2 Path Oriented

When a recovery mechanism tries to recover a particular active path (AP) then it is said to be path oriented [28].

In the approach of Ho and Mouftah [13] 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 failure in a protected segment, the corresponding PSL switches the affected traffic to the corresponding pre-established backup path. After the affected traffic is around the faulty segment of the failed LSP, the PML redirects the affected traffic back to the failure-free segment of the failed LSP. The fault-tolerant idea of the approach of Ho and Mouftah [14] is not novel, which is fully based on the local recovery (Sharma et al., 2003) to protect the affected traffic. The contribution of this approach is on the capacity allocation for the backup paths.

In the approach of Haskin and Krishnan [11] a backward backup path is pre-establishes for each active LSP. There are two backup paths for an active LSP. The route of the backward backup path is reverse with the route of the corresponding primary LSP. When a failure is detected in an active LSP, new incoming packets are carried by the disjoint backup path. As for the in-transit packets, they are sent back to the ingress LSR using the backward backup path. When the ingress LSR receives the in-transit packets, it further redirects the packets to the disjoint backup path. This approach introduces the packet disorder problem, such that new incoming packets are earlier than the in-transit packets to be carried by the disjoint backup path.

Two methods proposed in [22]. The one-to-one method creates a detour path (protection path) for each protected LSP for each potential point of local repair. While the facility method creates a bypass tunnel to protect a potential failure point; by taking the advantage of MPLS label stacking, the bypass tunnel can protect a set of LSPs that have similar backup constraints.

The one-to-one method requires a huge number of recovery paths. In order to reduce the number of recovery path, path merging is implemented whenever possible, while facility backup is available only for protected LSPs possible with guaranteed bandwidth.

In the recovery scheme of [18] Kodialam and Lakshman’s for a new LSP request, both the primary and backup path is determined on-line and simultaneously. If the bandwidth requested for primary and backup path is not satisfied, then the request is rejected. The proposed scheme needs the prior knowledge of bandwidth used by the primary and backup path in each link, and also the knowledge of free bandwidth in each link, this is called Partial Information (PI) model (according to the author). Proposed scheme deals with single link failure, but can be extended to manage single node failure as well.

Xu et al. [8] proposed a refined ILP model and a dynamic programming heuristic for a novel shared segment protection approach called Protection Using Multiple Segments (PROMISE) that combines the best of link and Path protection schemes. PROMISE allows for overlapping active segments AS’s (and BS’s) and exploits bandwidth sharing not only among the BS’s for different active paths, but also among those for the same active path.
The first major contribution Xu et al. [8] is an Link-Labeling scheme which enables us to develop an ILP model that determine the optimal partition of a given active path into AS’s and find corresponding BS’s. ILP model can also be used to obtain an optimal solution for a medium-to large network. The second contribution is fast dynamic programming based heuristic for PROMISE that has polynomial time complexity and this heuristic obtain near-optimal set of AS’s and their BS’s for a given active path.

### 2.2 Global recovery

The global protection is executed in a centralized manner and its main aim is to protect against any node or link failure on the entire path or the segment of path. In case of global protection, the path switch LSR (PSL) switches the traffic from the failed working path to the recovery path. However, the PSL is not generally next to the point of failure. In order to switch the affected traffic to recovery path, the fault notification should be propagated to PSL. When the failure on the working path is modified the traffic may be switched over to the working path [28]. Recovery schemes based on global recovery is shown below.

In [18, 19] three information scenario are described, the first is no information scenario in which only the reserved and residual (free) bandwidth is known for each link. The second information scenario permits the best sharing need large amount of information which prevent it to be used in practical situations and the third is partial information scenario is fairly modest in terms of amount of information to be maintained. These algorithms only consider single link failure, but can easily be entered to handle single node failures as well.

In [18, 19] both algorithm explain how to share the backup path bandwidth. In the no information case sharing of bandwidth is not possible while in complete information case only inter-demand sharing is possible and in partial information case some inter-demand i.e. not full sharing is allowed. The active and backup are selected by using linear programming models and are computed at ingress node for both no information and partial case, but in actual reservation it can reserve the actual amount of protection bandwidth in each line provided that the backup path is signaled , carrying the complete path of the corresponding protected active path.

Yetginer and Karasan [9] consider off-line computation of disjoint active and recovery path. They first compute maximum number of paths for each demand. They propose four different approaches for selecting active and recovery paths, the first two methods handle active and recovery path design separately. A traffic uncertainty model is developed in order to evaluate performances of these four approaches based on their robustness with respect to changing traffic pattern. They show that by carefully distributing the traffic load over network resources the joint design approaches in carrying additional traffic resulting from traffic uncertainty. This scheme appears to be hardly implementable for non-trivial sized networks (in any four approaches) because it requires solving complex integer linear programming problems. Even though the off-line characteristic may lessen this constraint, for medium or bigger networks this approach seems unwise.

Wei et al. [29] presented a novel approach to alleviate restoration of LSP in the MPLS network. The proposed approach establishes bypass tunnels rather than backup paths, because the bypass tunnels are established to backup up all protected LSPs, not for one particular protected LSP. In order to know what links are necessary between LSRi and LSRj, the Max-Flow Min-Cut theorem is adopted to find the necessary links through which all paths between LSRi and LSRj must pass. The shortest augmenting path algorithm is then adopted to establish the backup path. The main purpose of the shortest augmenting path algorithm is to find all paths passing through all links in a min-cut. [29] also compares the pre-established bypass tunnel (PBT) algorithm and the PBT algorithm with disjoint bypass tunnels (PBT-D). The approach has less in rerouting and can allow more affected LSPs to reroute traffic than RSVP and efficient Pre-Qualify.

Huang et al. [3] presented a scheme for minimizing the delay of notification messages when fault is detected. This scheme proposes a reserve notification tree (RNT) structure for efficient and fast distribution of fault notification messages. A faster Hello protocol for fault detection and a lightweight transport protocol for handling notification messages are also proposed in this scheme. However, the approach of Huang et al. [3] has the packet loss problem since it does not reroute the packets currently carried in the failed LSP (the in-transit packets). In [5] propose several additional objects for the Resource Reservation Protocol (RSVP) extension allowing the establishment of explicitly routed label switched paths using RSVP as signaling protocol that enables timely node failure detection. The authors also show that the RNT can be implemented in any layer.

#### 2.2.1 Load distribution

Xiaoming et al. [31] propose an adaptive load balancing scheme based on the real-time measurement, which is able to hold integrity per flow while minimizing congestion. This approach focuses on load balancing among multiple parallel Label Switched Paths (LSPs) in Multi-protocol Label Switching (MPLS) networks. The goal of the ingress node is to distribute the traffic across the LSPs so that the loads are balanced and congestion is thus minimized. The traffic to be balanced by the ingress node is the aggregated flows that share the same destination. The introduction of CAC function guarantees the QoS of flows already into LSPs.

Dana et al. [1] proposes a scheme in which pre-assigned LSPs is used for recovery, when fault occurs. In this faulty traffic is distributed by using case-based reasoning (CBR) to the pre-assigned LSPs. CBR is a method to find out the amount of traffic forwarded on each pre-assigned LSP based on past experiences. The pre-assigned LSPs and the percentage of traffic splitting are calculated Online based on desired QoS.
LSR assigns one of other ingress LSRs as its backup. When the recovery path of an LSP, the ingress LSR (I-LSR) performs two primary tasks after the failure is detected in the LSP, and selects the best recovery path. To achieve this, it uses a path selection algorithm to select the optimal path from the available backup paths. The path selection is based on several criteria, such as the cost, availability, and reliability of the path. Once the best recovery path is selected, the I-LSR initiates the process of label stacking, where it appends a new label to the packet, indicating the new path to the destination. Simultaneously, it also modifies the path lookup table at the ingress to reflect the new path. This process ensures that the packets are redirected to the new path without any loss of data.

3.1 Establish-on demand

In the approach of Ahn et al. [10], each LSR has one or more candidate protection merging LSRs (candidate PMLs). The candidate PMLs of an LSR indicate the LSRs located on the downstream direction of the LSR. While an LSP is established, each LSR on the LSP also finds the information about its candidate PMLs. Once detecting a failure in an LSP, the LSR that detects the failure first calculates all the costs of the possible recovery paths from it to each of its candidate PMLs. Then, the LSR selects the recovery path with the least cost. Next, the constraint-based label distribution protocol (CR-LDP) is used to explicitly establish the route of the best recovery path. However, [10] incurs a nontrivial recovery time for finding the least-cost recovery path.

In the approach of Agarwal and Deshmukh [2] each ingress LSR assigns one of other ingress LSRs as its backup. When failure occurs in ingress LSR, the failed ingress LSR is unable to execute label switching to forward the packets of source host. In such case, the source host will send the faulty packets to the assigned backup ingress LSR. The backup ingress LSR forwards the packets along itself corresponding LSP using label stacking. When the packets arrive at the egress LSR of the corresponding LSP, the egress LSR strips off the stacking labels of the packets and forwards them to the destination host using normal IP routing. But the approach is not applicable to the intermediate or egress LSR failure.

Hong et al. [6] propose a LSP rerouting scheme that dynamically aligns the restoration scope (RS) in MPLS network. Because this scheme dynamically adjusts the restoration scope depending on the fault and congested location and the overall network status. In this scheme, each iteration searches an optimal alternative path from the PSL to the working path egress LSR. In order to minimize the recovery time, the scheme begins to look for such a path on a subset of the LSRs, where the tentative PSL is the LSR closest to the failure and the PML is always the egress LSR. This subset (delimiting the range of recovery) is successively enlarged whenever a recovery path is not found. Every time a subset is extended, a process called hierarchical restoration, a new PSL is used (the next upstream LSRs in the working path). This procedure, if unsuccessful, is repeated until the PSL is the ingress node.

These schemes are very efficient on resource utilization, which is partially explained by the rerouting model. In [6], the number of iterations required defines the speed of recovery (as the total number of operations increases, each successive iteration is harder to solve). However, as the authors [6] pointed out, using too small recovery ranges may result in ignoring the available bandwidth.

3.2 Pre- Qualified

Pre-qualified protection type which just establishes a new recovery path without path selection time by specifying a recovery path before the occurrence of a fault, namely at protection LSP setup time. Since it does not reserve resources for recovery path beforehand and is able to reduce the recovery path selection time in the occurrence of a fault, the total recovery time of the latter is smaller than that of the former [27].

Park et al. [21] proposed a pre-qualified mechanism for MPLS networks named dynamic path protection, in order to quickly recover node or link failures. When fault occurs in the LSP, a recovery path is selected among the existing active paths that start or transit there and with the same destination (if there are more than paths to choose from, the paper proposes some ranking criteria). If later a fault occurs in the previously selected recovery path, the same procedure is followed again. This scheme is fast as it avoids signaling a new path, and needs simple routing table changes. In case, if no such paths can be found, the LSR must create a new path (from itself up
to the original destination). The author claimed in [20] that this scheme does not require signaling protocol extensions.

Yoon et al. [27], proposed a pre-qualified recovery mechanism. When a LSR detects a failure between it and its next LSR, the corresponding pre-qualified recovery path is actually established. The bandwidth resource is also reserved for the pre-qualified recovery path. Since the route of the recovery path is pre-determined, the approach of Yoon et al. [26] does not take actions to find the recovery route after the failure. However, during normal time, this approach incurs the route calculation overhead.

Jenn-Wei et al. [15] presented an efficient approach for enhancing the fault-tolerant performance in MPLS network. The proposed approach utilizes failure-free working LSPs (the active 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. To minimize the influence of the affected traffic on failure-free working LSPs, the proposed approach applies the solution of minimum cost flow to determine the amount of affected traffic to be transmitted by each failure-free LSP. They also propose a permission token scheme and piggyback method to solve the packet disorder and loss problems.

References


