Comparison Studies on Path Recovery Schemes in MPLS Network

Veneta P. Aleksieva[1]

***Abstract* – In this paper are discussed the problems in the existing MPLS/Multi Protocol Label Switching/ recovery mechanisms. The simulation-based experiment studies and compares the performance of existing MPLS recovery models, based on the system of parameters. It uses three criteria of the comparison.**

***Keywords* – MPLS recovery mechanisms, MPLS network**

I. INTRODUCTION

Internet is currently requiring a means for providing different users with different service levels. Traffic with high requirements for example delay, jitter and bandwidth has to be treated with a certain priority, while the traditional best effort services are still available. Many types of multimedia such as video conference or voice conference have become more important and have been widely used nowadays. Generally network operators aim to provide the fastest, most stable and the best protection mechanism that can be provided at a resource consumed.

Diffserv enables network traffic to be classified into different priority levels and then applies different scheduling and queuing mechanisms at the nodes according to the priority level [1].

The ToS field in the IP header is used to mark a packet and then is used as an indication of how the packet is forwarded.

MPLS is used as a traffic engineering tool to direct traffic in a network in a more efficient way then original IP shortest path routing. Path in the network can be reserved for traffic that is sensitive, and links and router that are more secure and not known to fail can be used for this kind of traffic. If MPLS is used, it sets up LSPs /Label Switched Paths/ along links with available resources, this ensures that bandwidth is always available for a particular flow to avoid congestion [2].

Most of the techniques used for recovery in MPLS are already available at other network layers. It seems that it is not necessary to implement these mechanisms again in another layer, but the main reason is: MPLS operates between layer 2 and layer 3 in the OSI model. This gives us now possibilities in network recovery with new functionality. MPLS is designed to work with many different network technologies and has its own mechanisms for recovery, independent of other layer mechanisms. Here they are faster and non-visible into higher layers.

[1]Veneta P. Aleksieva is with the Department of Computer Science and Engineering, Technical University of Varna, str.”Studentska ”1, 9010 Varna, Bulgaria, e-mail: ven7066@abv.bg

A number of recovery schemes for MPLS have been proposed in recent years and most of the current schemes focus only on wire network and rarely there are solutions for multiple failures recovery in dynamic topologies based on wireless. The main goal of path recovery schemes is to minimize time of service disruption, which depends on the time to detect failure, time to notify, time to compute backup and time to switch traffic to the new one. MPLS recovery must have the ability to ensure recovery from a link or node failure with minimal disruption to the data traffic. Often the limit of 50 ms is considered because this has been set as the longest acceptable disruption to voice traffic and is used as a limit for recovery time in SONET/SDH networks.

In this approach is presented comparison of some MPLS recovery technique and their advantages and disadvantages.

II. NETWORK RECOVERY OF STATIC AND DYNAMIC MPLS NETWORK

Actually, to fully provide QoS in the network there also needs to be a guarantee for what happens with traffic in the case if congestion is caused by link or node failures:

First, the network must be able to detect the failure.

Then the nodes that detect this failure must send a message to the certain nodes in the network of the failure. Which nodes will be notified about the failure depends on used recovery technique.

Next, the backup path must be computed.

Finally, a node must send traffic on the backup path instead the previous path.

MPLS recovery provides different levels of service, based on their service requirements. It should give the flexibility to select the recovery mechanism, choose the granularity at which traffic is protected and choose the specific types of traffic that are protected in order to give operations more control over that tradeoff. [3]

If a failure occurs in a network there must be a way to detect this so that the recovery operation can start. But failure detection depends on the type of failure and may be done by the failing node, at a node adjacent to the failure or at a configured point of repair in the network. MPLS recovery techniques are 2 main types [4,5]:

- **Protection Switching** – This is pre-establishing a recovery path based on network routing policies and requirements of the traffic.
- **Rerouting** – This is establishing new paths or path segments on demand for restoring traffic after the failure.

Both have advantages and disadvantages, which are shown in Table 1 and Table 2.

TABLE I
COMPARISON OF MPLS RECOVERY MODELS

Recovery model	Protection Switching		Rerouting	
Recovery Path Setup	Before fault		After fault	
Restoration of service	Lacks efficient use of network resources as the recovery path is setup		Optimizing the recovery path	
	Fast restoration of resources		Slower restoration of resources	
Reservation of resources	Before a failure occurs		Does not reserve any resources in the network, but they may not be available at the time of recovery path	
Recovery path type	1+1	1:1, 1:n, m:n	Pre computed	Established on demand
Recovery time	fourth	third	fastest	Second fast
Resource utilization optimization	first	second	third	fourth
Comparison with non MPLS based recovery mechanism	Like lower layer recovery		Like rerouting at the network (IP) layer	

In the table below is presented different comparison:

TABLE II
COMPARISON OF MPLS RECOVERY MODELS

Restoration and repair method	Resource requirement	Speed of repair	Packet loss	Length of protection path
Dynamic Local Repair	No	Slow	Minimum	Might not be theSP available
Dynamic Global Repair	No	Slow+ FIS	High	Path is shortest available
Fast rerouting local	Yes, if not shared	Fast	Minimum	May not be the optimal
Fast rerouting global	Yes, if not shared	Fast, depends of FIS	High	Better than fast rerouting global

There are two techniques to set-up recovery path in MPLS[6], but in both the recovery path is set up from the PSL /Path Switch Label Switch Router/ to the PML /Path Marge Label Switch Router/, but in different ways put the labels:

1. **Splicing** – the PSL change its forwarding table when the recovery path shall be used to forward packets on the recovery path instead of the failed working path. A new outgoing interface and a new label are used by the PSL to forward packets on the recovery path.

2. **Stacking** – the PSL also update its forwarding table to use a new outgoing label and a new outgoing interface for the affected LSP, but the new label for the recovery path is pushed on top of the label that would have been used for the failed working path. The next LSR /Label Switch Router/ in the recovery path pops the label stack revealing the old working path label before it forwards the packet to the PML, which doesn't know about the failure because it has the same label as a packet from the working path. Actually, this technique works if PML uses global label space and PSL has to know the label it would have used on the working path for PML.

Each of these techniques has advantages and disadvantages and it is one significant requirement for traffic management to support QoS guaranteed tunnels, according to link or node failure or topology changes. There are some proposed models for MPLS recovery, which is presented follow.

All models can protect a working path end-to-end in one MPLS domain, but there is no protection for node failures on the ingress or egress LSR. This will be a problem if it must recover the paths cross multiple MPLS domains.

In this research is used Network Simulator version 2 [7] for MPLS. With this tool are compared seven models:

1. **Makam's model** [8] – This is global recovery with protection switching, because it builds a global recovery path between the ingress and egress routers. This model has proposals for both a pre setup (protection switched) recovery path and a dynamically established (rerouted) recovery path. When a failure is detected anywhere along the working path, a fault indication signal /FIS/ is used to travel information about the occurrence of the failure to the PSL. Then the PSL is responsible for switching traffic over to the recovery path. The traffic will be sent down the failed working path until this FIS has been received by the PSL. This will result in dropped packages at the LSR that is upstream of the failure, as this node does not have any forwarding information for these packages since the downstream node is not reachable. If the failure is situated far away from the point of repair and the transmission rate is high, the number of packets dropped can be very high.

2. **Huang's model** [9] –This model develops a notification tree in a global or segment protected environment using 1:1 protection. The reverse notification tree is a point to multipoint tree rooted at the PML along which a FIS can be sent to the PSLs affected by a failure. In a case of global protection, the node that detects the failure has to communicate from the point of failure to the PSL upstream in the working path. As LSP are setup unidirectional there has to be information of how the FIS shall be sent upstream.

3. **Haskin's model** [10]- The idea of reverse backup is to reverse traffic at the point of failure in the working path, back to the PSL (ingress LSP). As soon as a LSR detects a failure on the working path, it redirects the incoming traffic on to an alternative LSP that is setup in the reverse direction of the working path. When the reversed traffic reaches the PSL, it forwards this traffic on to a global protection path. Both the reverse path and the global protection path are pre reserved. When a failure is detected, the traffic will be switched onto an alternative path by protection switching directly. In this model

both 1:1 protection and 1:N protection can be achieved. But this model has one disadvantage- until the PSL receives any of the reversed traffic, packages will be forwarded on the broken working path. When the PSL receives traffic from the reversed path, it will start to forward incoming traffic onto the global backup path. For a short period the incoming traffic will be mixed with the reversed traffic as it is forwarded on the recovery path.

4. **Hundessa's model** [11]- When a failure is detected by a LSR, the packets that would have been forwarded on the failed path are returned to the PSL via a reversed backup path as in Haskin's model. But when the first packet, acting as a FIS arrives in the reverse direction at an upstream LSR, that LSR tags the next packet, it sends out on the working path. The next packets it receives, which belong to the same working path, are buffered. The last packet that an LSR sends out on the broken working path is tagged by setting a bit in the EXP field in the MPLS header.

5. **Fast reroute** - End-to-end recovery paths needs to be pre-setup for each link or node in the working path. In extensions to the RSVP-TE protocol are defined to establish an LSP with end-to-end fast reroute backup tunnels. Two techniques are described in this method - the one-to-one backup model and the facility backup model.[12] Here is used one-to-one backup model.

6. **Sa-Ngiamsak's model** [13] – This recovery technique focus on multiple point of failure which may frequently occur on such dynamic network. Its name is Modified Flexible MPLS Signaling (MFMS). If multiple mobile nodes failed, the FMS may become malfunction or can not find a feasible recovery path. This work in five phases: LSP setup, Failure detection, Failure recovery, Ingress coordination and LSP Refresh and Recovery abort. In the simulation of this model it is accepted fixed transmission rate among mobile network nodes.

7. **Nagarajan's model** [14]- This model is created for recovery in dynamic network topologies. It uses new flexible signalling protocol for LSP rerouting in dynamic network environments. The signalling protocol recovers from node and link failures reactively, taking a local approach to LSP reestablishment.

III. Results of MPLS Recovery Models Comparison

The performance of the different MPLS recovery models is evaluated through simulations. In this research is used Network Simulator version 2.26 [7] for MPLS. The network topology and settings used in the following simulations are the same for all simulated cases. The propagation delay between two nodes is set to 1ms and the bandwidth is set to 100Mbps. Each simulated model is setup to use end-to-end recovery, so the models can recover from a single link break anywhere on the working path. The models can also recover from node failures anywhere on the working path, apart from the ingress or egress LSR. The hello mechanism is used for failure detection. The mechanism is activated for all nodes that have a RSVP-TE agent attached and start time it set to 0.01s. The hello interval is set to 5ms and the multiplier set for the failure detection interval is set to 3.5ms. So a failure check will be performed in 15ms intervals. For each simulation it is wrote data for how many packets that are dropped when the link breaks. As the settings for the hello mechanism are set to the same values for all simulations, the packet dropped during the failure detection interval is the same in all simulations.

The results are presented below. There are used 3 criteria of comparison for the network recovery models:

1. **The packet loss during the recovery operations-** The fig.1 shows the number of dropped packages for each model. It is not presented, but the number of dropped packets decreases when the failure occurs closer to the egress LSR, because the backup path to setup becomes shorter.

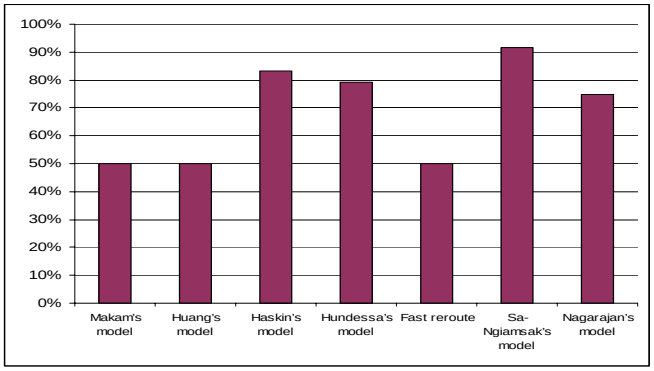

Fig. 1. Dropped packets

2. **The service disruption time** - The fig.2 shows the service disruption time, measured from the last packet that was sent over the link before it breaks is received by egress node, until the first package that is using the backup path is received by this node.

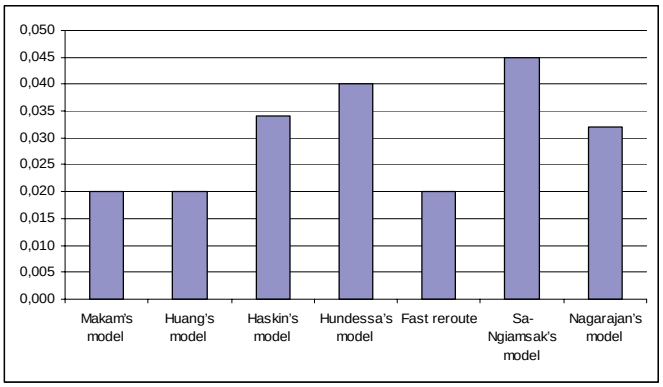

Fig. 2. Service Disruption Time

The service disruption time depends just like the number of dropped packages on the time for failure detection, failure notification, recovery path calculations and recovery path setup. This means that the rerouting mechanism will have higher service disruption time then protection switching, because with rerouting time is used for path calculations and path setup and this is not needed in protection switching.

3. **The number of pre-reserved resources used for the recovery operation –** Observe that the number of resources reserved depends on the topology of the network. Both Makam's and Haskin's model depends on a global recovery path, Haskins model will always use more resources then Makam's because it needs the reverse backup path in addition to this global recovery path. For most topologies fast

reroute will use more resources then Haskin's model, but this example is used to show that when the topology is right, fast reroute will use the same amount of backup resources as Haskins model. Both the best effort and rerouting model setup the backup path on demand after the failure has occurred, and therefore no backup resources are reserved before the failure in those models. The fig.3 presents these results.

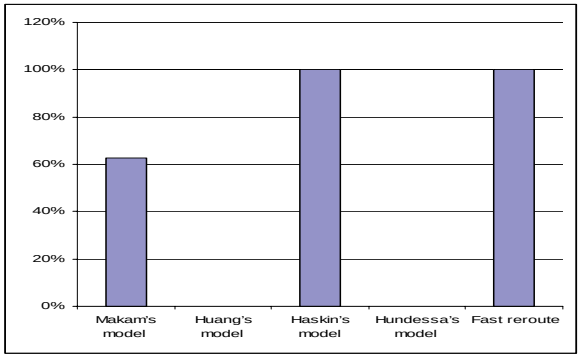

Fig. 3. Pre-reserved resources

When the multiple failure is occurred in wireless network Nagarajan's model and Sa-Ngiamsak's model are used and they recover LSP for different time. It is presented in the fig.4.

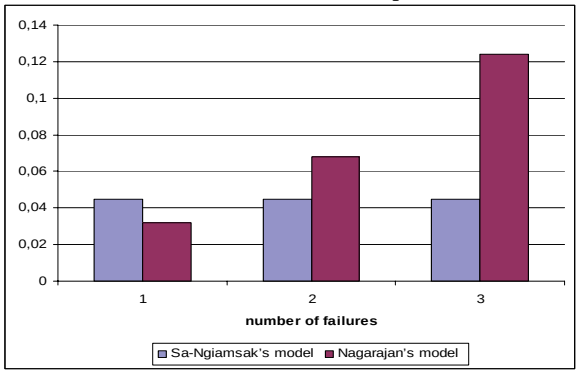

Fig. 4. Rerouting response time /ms/

IV. CONCLUSION

If recovery by re-routing is used the recovery time depends on the time to discover the fault, the time to notify the PSL of the failure, the time to calculate a recovery path (if it is not pre-calculated) and the time for a new recovery path to be set up. This can be slow and can take up to several seconds which is unacceptable for many real time applications.

If recovery by protection switching is used, the recovery time can be decreased because recovery path calculations are not needed. When the recovery path is pre-established, there is no need to signal the recovery path and recovery time, and then only depends on fault detection time and the time for the FIS to travel to the PSL.

Results indicate that the flexible signalling protocol for LSP in mobile wireless networks can effectively and efficiently handle rerouting in dynamic networks with a low protocol signalling overhead as compared to contemporary MPLS rerouting protocols. This would enable the MPLS based IP-QoS support mechanisms to extend to dynamic network topologies.

For further work it is planed to simulate the difference between the shortest paths after failure compared to the paths set up by each rerouting technique, then measure the time between occurrence of failure and instance of traffic resumption and observe the response time for each technique and finally measure and compare the total rerouting overhead for each technique. Based on this research, new model of recovery will be created, which evaluate these existing rerouting schemes via simulations. It is thinking about a low protocol overhead compared to the existing rerouting schemes and with the low response time when traffic travel on recovery LSPs.

ACKNOWLEDGEMENT

The work presented in this paper was supported within the project BG 051PO001-3.3.04/13 of the HR Development OP of the European Social Fund 2007-2013.

REFERENCES

[1] S. Blake, D. Black, etc. "An Architecture for Differentiated Services ", http://www.ietf.org/rfc/rfc2475.txt

[2] J.Martin,O. Petersson "MPLS Based Recovery Mechanisms", http://folk.uio.no/johanmp/MPLS%20Based%20Recovery%20Mechanisms.pdf

[3] V. Sharma, Ed. Metanoia, Inc. ,etc. "Framework for Multi-Protocol Label Switching (MPLS)-based Recovery", http://www.faqs.org/rfcs/rfc3469.html

[4] J. Ash , M. Girish ,etc. "Applicability Statement for CR-LDP", http://www.ietf.org/rfc/rfc3213.txt

[5] D. Awduche , L. Berger , etc. "RSVP-TE: Extensions to RSVP for LSP Tunnels", http://www.rfc-editor.org/rfc/rfc3209.txt

[6] G. Swallow "MPLS Advantages for traffic engineering", IEEE Communications Magazine December 1999

[7] http://nsnam.isi.edu/nsnam/index.php/User_Information

[8] S. Makam, etc. "Protection/ Restoration of MPLS Networks", http://zinfandel.levkowetz.com/html/draft-makam-mpls-protection-00

[9] C.Huang, V.Sharma, K.Owens, S.Makam "Building Reliable MPLS Network Using a Path Protection Mechanism"IEEE Communicaion Magazine March 2002

[10] D. Haskin, R. Krishnan "A method for setting an Alternative Label Switched Path to Handle Fast Reroute" , http://tools.ietf.org/html/draft-haskin-mpls-fast-reroute-01

[11] L.Hundessa, J.Pascual "Fast rerouting mechanism for a protected label switched path" Proceedings of the IEEE International Conference on computer Communication 01, October 2001

[12] P. Pan, G. Swallow, A.Atlas,"Fast Reroute Extensions to RSVP-TE for LSP Tunnels", http://www.rfc-editor.org/rfc/rfc4090.txt

[13] Sa-Ngiamsak, etc. "A Recovery Sheme for Qos Guaranteed Mobile IP Over MPLS Network" Wireless Pervasive Computing, 2006 1st International Symposiumon 16-18 Jan. 2006, http://ieeexplore.ieee.org/iel5/10746/33870/01613583.pdf

[14] Ramprasad Nagarajan, Eylem Ekici1 "An efficient and flexible MPLS signaling framework for mobile networks" Wireless Networks, Volume 14, Number 6 / December, 2008, http://www.springerlink.com/content/772114375010t173/?p=337b181cd2634c2ebccb7c663cc7d40e&pi=8