ISSN:0975-9646

Multi-Protocol Label Switching Traffic Engineering-Link Protection

[1]Balaji Tedla, [2]Dr.K.Suresh Babu

[1] *Assistant Professor, Dept. of CSE, Vasavi College of Engineering, Hyderabad.*
[2] *Assistant Professor of CSE, SIT, JNT University, Hyderabad.*

Abstract- One of the attractive highlights of any network is its capacity to keep services running notwithstanding a connection disappointment Flexible systems recoup from a disappointment via repairing themselves consequently by occupying activity from the fizzled piece of the network to another segment of the network.. The new way taken by a redirected movement can be processed at the time a disappointment happens through a methodology called rerouting. Then again the way can be processed before a disappointment happens through a strategy called quick reroute. In this paper, we dissect the diverse methodologies of activity rerouting in MPLS domain that are versatile to the disappointment. We propose another model Guaranteed Reduced Hoard (GRH) an enhanced system such that activity interest can be rerouted in the system as quick as would be prudent. Our methodology serves to attain to a quick reroute of movement on way disappointment, when contrasted with existing recuperation models. Further, our methodology obliges less number of hubs on the reinforcement way when contrasted with recuperation models proposed by Makam's or Haskin.

Index Terms- Multi-Protocol Label Switching, Makam's Model, Haskin Model.

1.INTRODUCTION

MPLS is todays generally utilized for Traffic Engineering and I will subsequently begin by portraying what traffic engineering is and why traffic engineering is essential. The interior gateway protocols used today like OSPF and ISIS compute the shortest way to the destination and routers forward traffic according to the routing tables build from those calculations. The main issue with conventional routing protocols is that they do not take capacity constraints and traffic characteristics into account when routing decisions are made. The outcome is that some segments of a network can become congested while other segments along alternative routes become under-utilized.

Traffic engineering is the process of controlling how traffic flows through a network to optimize resource utilization and network performance, Traffic engineering is basically concerned with two problems that occur from routing protocols that only use the shortest path as constraint when they construct a routing table. The shortest paths from different sources overlap at some links, causing congestion on those links. The traffic from a source to a destination exceeds the capacity of the shortest path, while a longer path between these two routers is under-utilized.

MPLS can be used as a traffic engineering tool to direct traffic in a network in a more efficient way then original IP shortest path routing. MPLS can be used to control which paths traffic travels through the network and therefore a more efficient use of the network resources can be achieved. Paths in the network can be reserved for traffic that is sensitive, and links and router that is more secure and not known to fail can be used for this kind of traffic. MPLS is short for Multi-Protocol Label Switching. The Multi-Protocol indicates that MPLS is developed to work independent of what layer 2 and layer 3 protocols that are used in the network. The MPLS domain can be divided into MPLS core and MPLS edge[5]. The core consists of nodes neighboring only to MPLS capable nodes, while the edge consists of nodes neighboring both MPLS capable and incapable nodes. The nodes in the MPLS domain are often called LSRs (Label Switch Routers). The nodes in the core are called transit LSRs and the nodes in the MPLS edge are called LERs (Label Edge Routers).

In MPLS numerous methodologies or models have been proposed to move traffic from faulty active path to recovery path like Makam's Model[2], Haskin Model[3] and Fast Reroute one-to-one back model[4] etc.,. Makam's model provides end to-end protection for a LSP by setting up a global recovery path between the ingress and egress LSR. This recovery path is totally link and node disjoint with the working path. When a failure is detected anywhere along the working path, a fault indication signal (FIS) is used to convey information about the occurrence of the failure to the ingress node. The ingress is then responsible for switching traffic over to the recovery path.

The idea of Haskin's Model 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, a different concern for Haskin's model is there is a high probability that reverse traffic will change the order of packets and the less efficient use of resources, as the total length of the recovery path gets longer than the original working path. The positive side of this model is that the number of packages dropped when a failure occurs, can be decreased as no FIS is needed when traffic from the reverse backup path acts as FIS for the PSL. Traffic can be switched onto an alternative path by protection switching directly when a failure is detected.

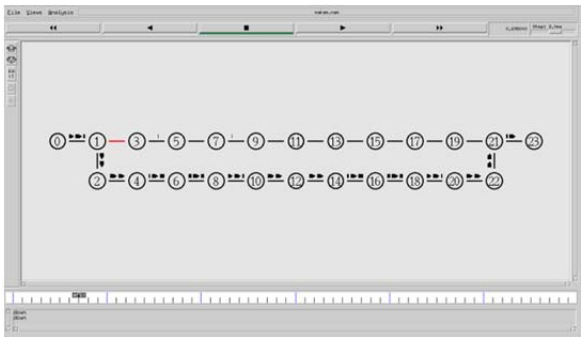

Figure 1: Makam's Model

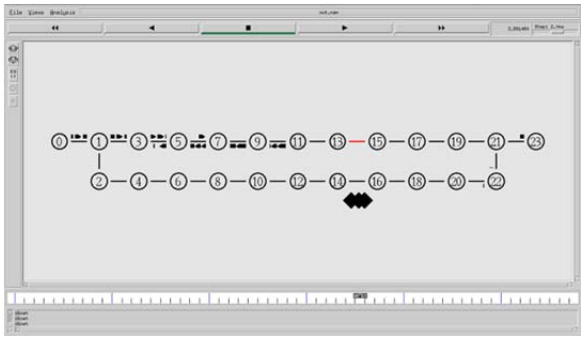

Figure 2: Haskin Model shows reverse data flow when link fails between nodes 13-15.

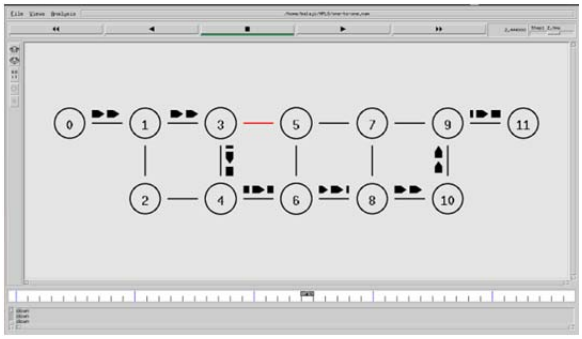

Figure 3: Fast Reroute one-to-one backup model.

The Fast route one-to-one back-up Model expends extensive measure of assets like transmission capacity and routers. We watch that there are numerous difficulties in existing recuperation models like either long delay in recovery(Makam's model) or require large number of resources (Fast Reroute Model) or cause packet reordering(Haskin's Model), Utilizing our methodology, we can beat these difficulties.

II. GUARANTEED REDUCED HOARD (GRH) MODEL

We propose the GRH model in which, a set of nodes LSRs/links can be protected by a backup router.

General GRH model: In general in the GRH model, a backup path is setup for the entire working path. The backup path is disjoint from the working path. This backup path is connected with the working paths after every alternative hop. On working path failure the nearest LSR which is connected to a backup path, takes the switchover decision, the FIS is not sent to the ingress LSR. The connection with backup path after every alternative hop ensures redundancy and at the same time lesser resources are needed. Further, since the nearest LSR takes the switchover decision, the switchover is faster as compared to other models.

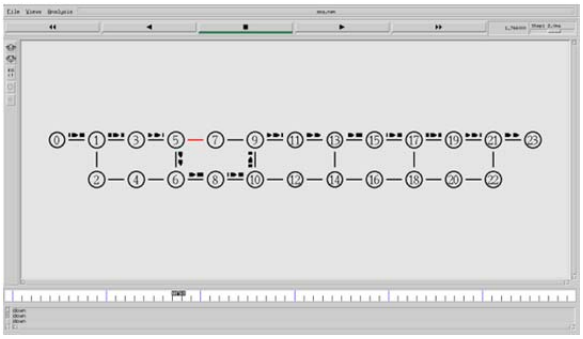

Figure 4: Guaranteed Reduced Hoard (GRH) Model

In figure 4 GRH Model is shown with 1 -22 MPLS nodes and 0 and 23 non MPLS nodes, the backup path is setup using the LSRs 2,6,10,14,18 and 22. Every alternate LSR on the working path is connected with recovery path. LSR 1 is the path switch LSR, responsible for switching the traffic from active path to pre-established backup path is connected with LSR 2.

A. Simulation and Validation of GRH Model

We use NS2 for our simulations. We test our model through 24 node chain in a working path. Figure 4 is a nam file visualization in ns2, Nam is a tcl based animation tool that is used to visualize the ns simulation. The nam file contains the topology information like nodes, links, queues and node connectivity etc.

The working of simulation setup is shown in figure 4. Each MPLS Node will exchange LDP (Label Distribution Protocol) mapping request sent by the neighboring nodes. Each LSR will receive the LDP mapping request. At the point when Node 0 sends an IP packet to Node 23 in the MPLS system, it sends an un-labeled packet (i.e. an IP packet in an Ethernet frame without MPLS label). Node 1 is the ingress LSR, after checking the destination IP address furthermore, other related data in the packet header; it pushes a label into the packet and forwards the labeled packet to the output port. Node 3 LSR, receives the labeled packet from the Node 1 LSR. It inspects the label and executes a table look-up at forwarding table to discover a new label and the output port. Node 3 then switches the old label with new label and routes the new labeled packet to the output port. Other LSRs will perform similar tasks. The labeled packet will reach the Node 21, the egress LSR. It then inspects the label and executes a table look-up at the forwarding table to find that the packet is to be sent to non-MPLS Node 23. It then removes the label and sends the unlabelled packet to destination Node. At the point when any link fails on the working path (or backup path), the downstream node sends a fault indication signal (FIS) to the nearest LSR connected to the backup path (or working path). In the GRH Model, in the simulations, the center node of backup path is connected to the working path using a link. This will decrease the time required for the fault indication to reach the ingress LSR to notify about the failure in the current working path.

We do a comparison of both Makam's Model and GRH Model utilizing diverse situations with 12-hub, 24-hub, While correlation considers two diverse methods of name dispersion - one is control-driven mode and another is Data driven mode. The Control-driven mode means Label bindings created when control information arrives, assigned in response to processing of protocol traffic, control traffic etc., here LDP(Label Distribution Protocol) distributes messages between all MPLS nodes. In data-driven mode Label bindings created by LDP when data packets arrives.
Control Driven Mode:- Link failure between LSR 9 and 11

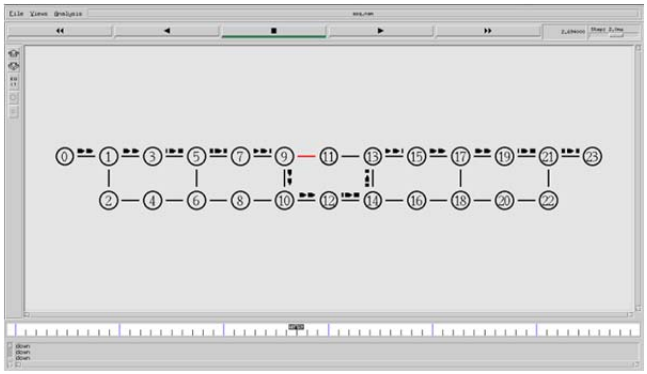

Figure 5: Link failure between LSR 9 and LSR 11.

In Figure 5 there is a link failure between LSR 9 and LSR 11, LSR 9 is directly connected to backup path, so FIS will reach to LSR 10 immediately. On receiving the FIS, LSR 10 will send the mapping message to its respective neighbors and packets will switch over from working path to recovery path. So the new path will be 1-3-5-7-9-10-12-14-13-15-17-19-21-23.

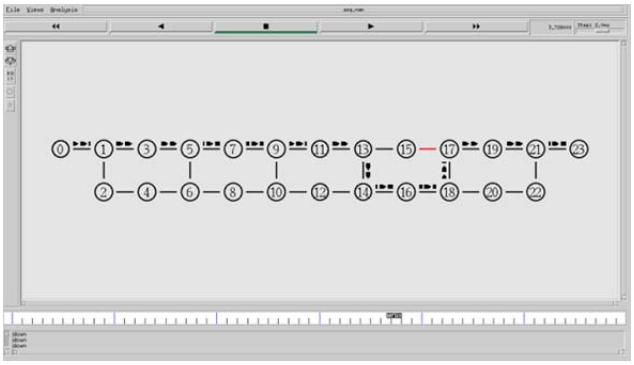

Figure 6: Link failure between LSR 15 and LSR 17.

In Figure 6, the there is a link failure occurs between LSR 15 and LSR 17. LSR 15 will send FIS to neighboring LSR. Once LSR 13 will receive the FIS, it will immediately transfer the control from the current failed working path to backup path.

III RESULTS

The outcomes demonstrated the examination between Makam Model and GRH Model for two distinctive chain modes 12 nodes & 24 nodes in control driven mode. The simulation analysis is done for different stages after a link down in the working path. The stages are as per the following:

i. Reception of first FIS at ingress router
ii. First label packet on backup path
iii. Labels are removed from the packet
iv. Receive data packet at destination

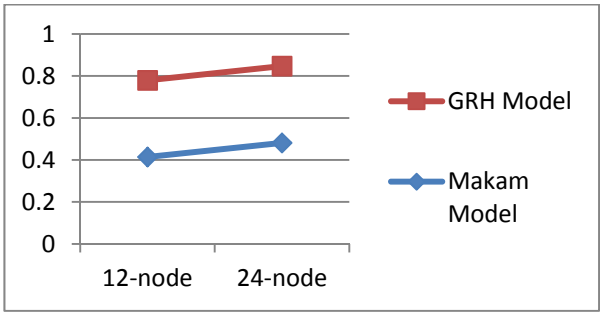

Figure 6: Reception of first FIS at ingress router

S.NO		12-node	24-node
1	**Reception of first FIS at ingress router**		
	Makam Model	0.414	0.481
	GRH Model	0.365	0.366
2	**First label packet on backup path**		
	Makam Model	0.437	0.483
	GRH Model	0.367	0.409
3	**Labels are removed from the packet**		
	Makam Model	0.587	0.727
	GRH Model	0.451	0.541
4	**Receive data packet at destination**		
	Makam Model	0.6	0.842
	GRH Model	0.464	0.552

Table 1: Four different stages in Control driven mode.

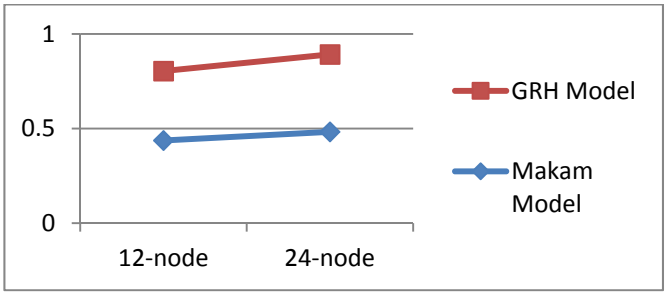

Figure 7: First label packet on backup path

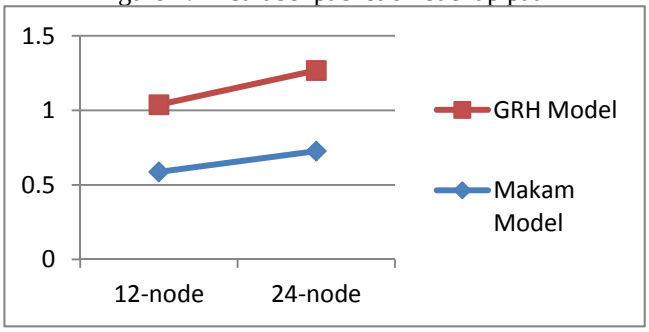

Figure 8: Labels are removed from the packet

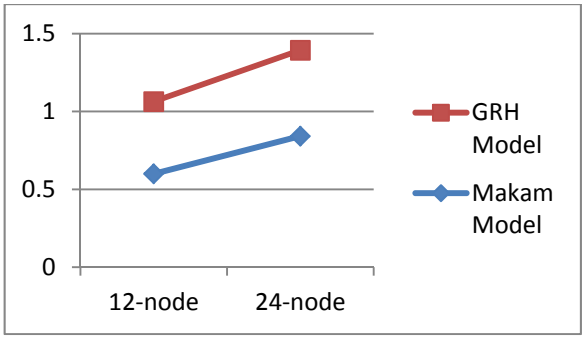

Figure 9: Receive data packet at destination
Note: for graphs Y-axis time in Milliseconds

IV Analysis

The GRH Model performs better in both control driven and data driven mode when contrasted with Makam's Model as given underneath.

sno	Metric for calculation	GRH Model in Milliseconds	Makam Model in Milliseconds
1	Early notice to entrance node	0.371	0.48
2	Switching time	0.412	0.482
3	Reception of data at destination	0.553	0.842

Table 2: Comparison summary for 24 node control driven mode-GRH VS MAKAM Model.

The reason that GRH Model executes well that GRH offers link to backup path from the working path at intermediate nodes. This helps in fast switchover to the backup path on any link failure. Table 2 and Table 3 gives comparison between GRH and Makam model

sno	Metric for calculation	GRH Model in Milliseconds	Makam Model in Milliseconds
1	Early notice to entrance node	0.371	0.476
2	Switching time	0.410	0.48
3	Reception of data at destination	0.551	0.753

Table 3: Comparison summary for 24 node data driven mode-GRH VS MAKAM Model.

V. Conclusions And Future Work

The Makam model is less expensive as compared to other recovery models in MPLS domain, but when system is used to send real-time data like voice and video, other modes like one-to-one backup model is best but it need more resources where as our model is intermediate model which improves speed in terms of delivery of data packets and consumes less no.of resources. The GRH Model is corresponding to Assured QoS Model[11] but the difference is in ASQ working path is connected to backup path after every n hops where as in GRH working path is connected to every alternative hop, both models are best suitable for if Quality of Service is of high priority. But still these are simulation results worked for only 12, 24 node networks further more evaluations ae needed to compare GRH model to other models for different topologies and various traffic circumstances.

References

[1] Changcheng Huang, "Building Reliable MPLS Networks using a path protection Mechanism", Carlton University: IEEE Communications Magazine, pp.156-162,2002.
[2] S.Makam's, V. Sharma, K.Ownes, C Huang "ProtectionlRestoration Of MPLS Networks" draft-Makam's-MPLS-protection-OO.txt, 1999.
[3] D.Haskin, RKrishnan, "A Method of setting an alternative Label switched path to handle Fast Reroute", draft-haskin-MPLS-fastreroute-OS. txt, 2000.
[4] K. Kompella, G.Swallow, "Detecting MPLS Data Plane Failures", Draftietf-mpls-lsp-ping-06.txt, July.2004.
[5] Petersson,J.M, "based Recovery Mechanism", University of Oslo Master Thesis, 2005.
[6] S.Yoon, H. Lee, D. Choi ,Y. Kim "An Efficient Recovery Mechanism for MPLS-based Protection LSP" IEEE ICA TM-200 I September 2001.
[7] V. Sharma, F. Hellstrand "Framework for Multi-Protocol Label (MPLS)based Recovery" IETF, RFC 3469 February 2003.
[8] S. Veni and Dr. G. M Kadhar Nawaz,"Protection Switching and Rerouting in MPLS", India : [EEE Conference ,pp.216-220,201 O.
[9] VINT project at LBL, Xerox PARC,USB and USC/IS The Network Simulator NS2 htm://www.isi. edulnsnam/ns/ (accessed on 2013)
[10] Chuck Semeria. (1999, Sep 27). Juniper Networks [Online]. A vai lable: http://mirror. unpad. ac. id/ orarillibrary/library-ref-eng/ref-eng- /network/mpls/20000 I. pdf
[11] "Multi-Protocol Label Switching Recovery Mechanism" Sulalah Qais Mirkar, Dr.Vijay Thakurdas Raisinghani (MPSTME), International Conference on Signal Propagation and Computer Technology(ICSPCT)2014.