Pooja al. International Journal of Recent Research Aspects ISSN: 2349-7688, Vol. 2, Issue 3, September 2015, pp. 50-53

Enhancing Fault Tolerance and Rerouting Strategies in Mpls Networks

Pooja[1], Khushboo Yadav[2]

[1]M.tech student, RPSCET(m/garh), Maharshi Dayanand University, Rohatk, India
[2]Assistant professor, RPSCET (m/garh), Maharshi Dayanand University, Rohtak, India

Abstract: - Multi Protocol Label Switching (MPLS) has been used to provide traffic engineering and high speed networking. MPLS is an evolving network technology. MPLS is a framework which is introduced by IETF. It is a differentiated and scalable framework. MPLS delivers end-to-end IP services with the use of simple configuration and management. Fault tolerance is an important Quality Of Service factor. Fault tolerance needs to be considered to maintain network survivability. Fault tolerance is very important in every network system because it provides the facility to operate the network if any one or more parts of the system are damaged. The network devices are enabled by MPLS to specify path based on quality of service and bandwidth. The main use of MPLS technology is to speed up the network flow with the use of labels.

Keyword:- MPLS, FEC(forward equivalence class), LSP

I. INTRODUCTION

MPLS is a technology which facilitates several problems in internet such as routing performance, speed and fault tolerance. Multi Protocol Label Switching is a set of protocols that is used to manage networks. Networks are of three types-data centric, voice centric and both data and voice centric, in data centric network data is transported while in voice centric network voice is transported. In data and voice networks, both data and voice are transported. Modern networks are examples of voice and data centric networks. These networks are based on a model that uses internet protocol to transport data. MPLS superimposes a connection-oriented framework over the connectionless IP network. Nodes that lie at the edge of the network are also connected with the help of virtual links through the network.

MPLS network combines a label-swapping algorithm, similar to that used in ATM, with network layer routing. A short, fixed-length identifier that is used to forward packets is called label. In MPLS network, the FEC (Forward Equivalence Class) assignment is done just once at the ingress router. The FEC to which the packet is assigned is encoded into a label. The packets are labeled before they are forwarded between Label Switched Routers. MPLS core routers are called Label Switched Router. MPLS network has connection oriented architecture so it is very vulnerable to failures.

The main goal of this paper covers the security issue arises in MPLS networks. The main drawback of MPLS is that there is no guarantee to users that packets do not get read or corrupted. E.g:- A well-established requirement in telephone networks is that the network should display very high levels of reliability and availability. Subscribers should not have their calls dropped, and should always have access to their services.

II. BACKGROUND

Multiprotocol Label Switching (MPLS)

Multi-protocol Label Switching (MPLS) is a reliable broad band technique used to strength the IP networks.

Packets enter the MPLS network through a router called Label Edge Router (LER) or often called Ingress router.

This router is responsible for adding a label on the packet for further transmission. Functionally label is a short fixed

Multi-protocol Label Switching (MPLS) is a framework defined by IETF for fast packet switching and routing. It uses specific labels to forward the packets with in MPLS network. More specifically, MPLS has mechanisms to manage traffic flows of various granularities [1,4]. It is independent of the layer-2 and layer-3 protocols such as ATM and IP.

To provide network survivability in MPLS network, an LSP (Labe1 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.

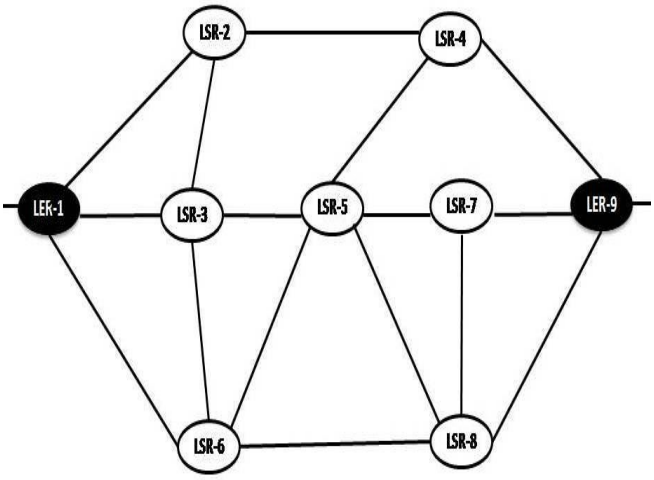


Figure1. **MPLS network**

When fault occurs in LSP, due to failure of link or node in the network, the carried traffic in failed LSP has to be transmitted through the backup LSP and the selection of backup LSP is based on the following criteria:

1) Reducing the request blocking probability
2) Minimizing cost of network
3) Load balancing

1) **Reducing request blocking probability**:-The major task of traffic engineering is to reduce the request blocking probability, to make sure that maximum numbers of requests are accepted in the network, in order to improve operator revenues and increase client satisfaction. Minimum Interference Routing Algorithm (MIRA) [5] is one of the best algorithms for constraint based routing which reduces the request blocking probability. The basic concept of MIRA is based on the relationship between the maximum flow [6] value between two nodes and the bandwidth (that can be routed between nodes). In MIRA critical links are the links, which cause a decrease in maximum flow values between pair of nodes. Therefore, weights are allocated to the links according to their criticality. In the end a shortest path- like algorithm is used to evaluate the path with minimum critical links. But MIRA suffers from computational complexity problem, as this algorithm frequently computes maximum flow.

2) **Minimizing costs of network:-**To accomplish a minimum cost of network, metrics like minimum hop count or link costs, have been conventionally included in routing algorithms. In order to minimize the cost of network many algorithms are proposed, for example Minimum hop algorithm [6]. Moreover, many other algorithms are proposed to make improvement in Minimum hop algorithm. Minimum hop algorithms are easy and computationally proficient. But in case of heavily loaded network, they give worse result [7] in terms of request refusal ratio. Link cost corresponds to the physical link length, so they are used in algorithms mainly for traffic engineering and they have no huge influence in networking architectures.

3) **Load balancing:-** In network, load balancing plays an important role to decrease congestion. The basic concept of load balancing is to distribute load in such a way that improves the overall performance of network. But in lightly loaded network load balancing shows bad performance, for example routing packets on longer paths.

4) **MIRA, Minimizing cost of network and Load Balancing**:- In this approach [7], three criteria (Load Balancing, MIRA and Minimizing cost of network) are used to calculate the path for the affected traffic. But this approach suffers from the problem computational overhead, because this approach computes all the three criteria throughout the process of packet forwarding.

Mpls Fault Tolerance

In fast restoration model the backup LSP is established and configured in advance, therefore bandwidth has to be reserved. In dynamic protection model the backup LSP is established after a failure occurs, and correspondingly bandwidth reservation is not applied until the failure occurs. The dynamic protection model may not be suitable for time sensitive applications because of its large recovery time [2] [3].

III. RELATED WORK

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. Resources required for the establishment of recovery path are reserved. Protection switching pre-establishes a recovery path or path segment based on network routing policies, the restoration requirements of the traffic on the working path and administrative consideration.

Rerouting

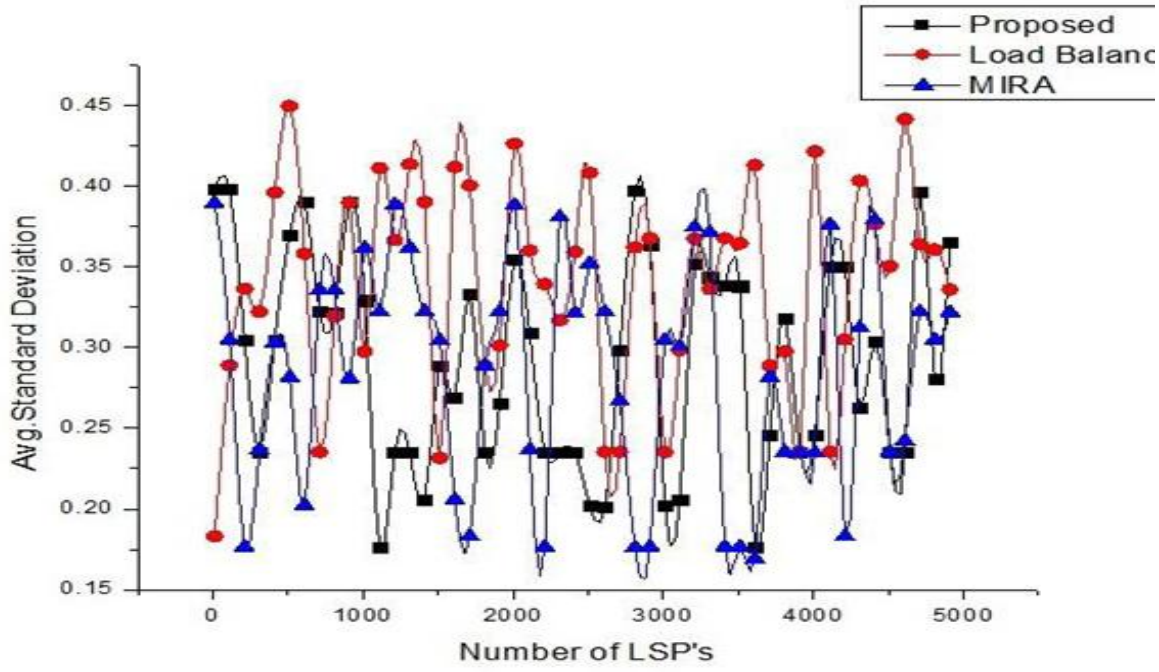
Rerouting, a fault recovery technique where a recovery path is established on demand after a fault occurs. The Recovery path can be based on fault information, network routing policies and network topology information[8,9] The new paths may be based upon fault information, network routing policies, pre-defined configurations and network topology information. Thus, on detecting a fault, paths or path segments to bypass the fault are established using signaling. On the other hand rerouting has the disadvantage that resources may not be available at the time of computing recovery path that may leads to major[9,10]

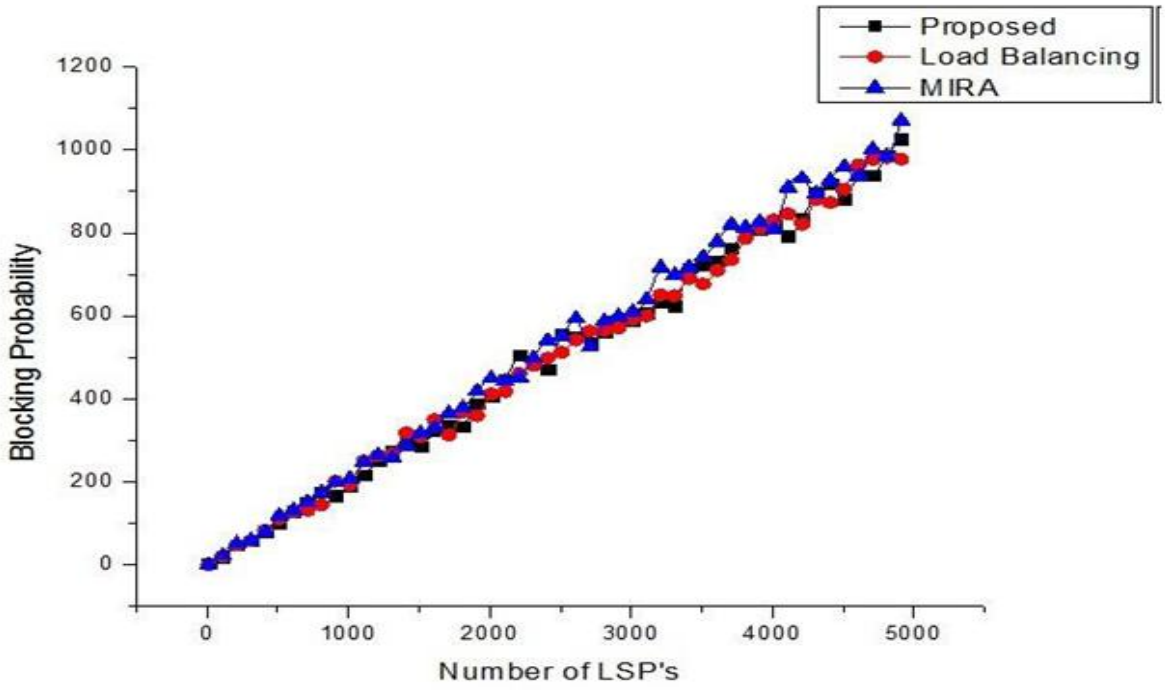
IV. OBJECTIVE OF RESEARCH WORK

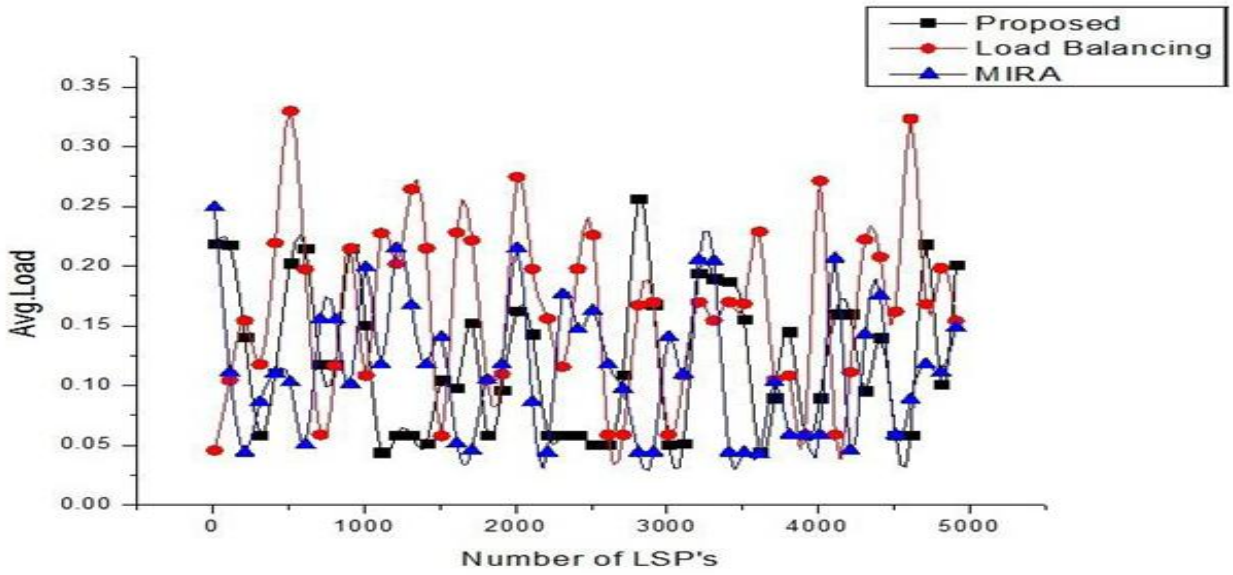
We shall follow these objectives as following:

1. MPLS is a standardized network based technology, which uses labels to make forwarding decision with network layer routing in the control components.
2. The objective is to provide a solution that MPLS provide integrated service model including RSVP and support operation, administration and maintenances facilities.
3. MPLS must run over any link layer technology and support unicast and multicast forwarding.
4. MPLS must be capable of dealing the ever growing demand of traffic onto the network and provide extending routing capabilities more than just destination based forwarding.
5. Along with reduced cost and offers new revenue generating customer's services in addition with providing high quality of base services.

V. RESULTS







VI. 6 .CONCLUSION

In this project, we identify relevant objectives for fault tolerance of MPLS network. We set up clear common criteria for these algorithms, namely: request reducing blocking probability, minimizing cost of network, and load balancing. We categorize and evaluate the appropriate approaches for this problem. The study shows the drawbacks of partial considerations, and the need for a global solution. Finally, we propose a solution that covers the different criteria presented in the project. Our formulation helps in clarifying all the trade-offs involved in CBR, thus enables the design of more complete solutions. Our approach shows that combination of our set of objectives achieves better overall satisfying results. The simulations presented in this project could be extended to encompass a discrete-event approach taking into account limited life-time LSPs. Moreover, the objectives we fixed can be the basis for further studies of CBR with emphasis on techniques for on-line design of survivable networks with multi-priority traffic.

VII. ACKNOWLEDGMENT

Our thanks to IJRRA for allowing us to modify templates they had developed. Also I take this opportunity to express my special gratitude to my supervisor **Miss. khushboo Yadav** generously making herself available for her most valuable guidance, encouragement. It would get not be possible for me to make this paper without her guidance.

REFERENCES

[1]. CISCO. Multiprotocol Label Switching CICSO.

[2]. L. Hundessa and J. D. Pascual, "Optimal and Guaranteed Alternative LSP for Multiple Failures," in Proceeding ICCCN 2004, Chicago, USA, Oct 2004, pp. 59- 64.

[3]. C. Huang, and V. Sharma, "Building Reliable MPLS Networks Using a Path Protection Mechanism," IEEE Communication Magazine, March 2002, pp. 156 – 162.

[4]. G.Kaur, D.Kumar, "MPLS Technology on IP Backbone Network", *International Journal of Computer Applications (0975-8887)*, 2010.

[5]. K. Kar, M. Kodialam, T.V. Lakshman, "Minimum Interference Routing of Bandwidth Guaranteed Tunnels with MPLS Traffic Engineering Applications", IEEE Journal on Selected Areas in Communications, December 2000.

[6]. J. Moy, "OSPF: Anatomy of an Internet Routing Protocol", New York: Addison-Wesley, 1998

[7]. Q. Ma, P. Steenkiste, "On path selection for traffic with bandwidth guarantees", In Proceedings of IEEE International Conference on Network Protocols, Atlanta, GA, October 1997.

[8]. M.Had, C.Geo, M.Pap, V.Vass. "A Haybrid Fault-Tolerant Algorithm for MPLS Networks", *WWIC 2008, LNCS 5031*, pp. 41-52, 2008.

[9]. S.Alo, A.Aga, A.Nou. "A Novel Approach for Fault Tolerance in MPLS Networks", IEEE 2006.

[10]. Johan Martin. Thesis on "MPLS Based Recovery Mechanisms", 2005.

[11]. V.Sharma. "Framework for Multi-Protocol Label Switching (MPLS)-based *Recovery", RFC-3469*, Ferruary 2003.

