An Efficient Routing Method for Protection Data Flow in the MPLS Network

Hasan Abdul Raqib Abdo Asaad (1,*)
Belal Al-Fuhaidi [1]

[1]Department of Computer Science, Faculty of Computing and Information Technology, University of Since and Technology, Sana'a, Yemen
* Corresponding author: hasanasaad9@gmail.com

https://doi.org/10.20428/JST.22.2.5

An Efficient Routing Method for Protection Data Flow in the MPLS Network

Abstract:

This paper presents an efficient method for rerouting traffic in the Multiprotocol Label Switching (MPLS) network, when a fault occurs in the working link. The method has been designed to handle both single and multiple faults based on the protection switching and rerouting techniques. The proposed method leads to less packets loss, has better Packet Delivery Ratio (PDR), good throughput and eliminates packet disorder.

The proposed method has been simulated using the Network Simulator (NS2) version 2.34 and the simulation results have shown that the proposed method significantly improves the network performance in comparison to similar existing methods.

Keywords: MPLS network, Working link, Protection switching, Rerouting, Network simulator.

https://doi.org/10.20428/JST.22.2.5

1. Introduction:

MPLS stands for Multiprotocol Label Switching. It is a famous networking technology belongs to the family of packet switching networks. MPLS had been designed to overcome the limitations of IP based forwarding. It uses labels which are attached to packets to forward them through the network. The MPLS technology improves QoS by defining Label Switching Paths (LSPs) that can meet Specific Service Level Agreements (SLAS) on traffic latency, jitter and packet loss[1, 2].

Several works related to routing traffic problem in MPLS network when a fault occurs in the working link have been reported [3- 6]. Some of these works handle single fault [4 -6] and others handle single or multiple fault [3]. The proposed method given in this paper can hand both single and multiple faults that occur in the MPLS network. However, only the results for the single fault are presented. The paper is organized as follows: Section 2, is about the MPLS Terminology, a brief reference to related works is given in Section 3, the proposed method is given in Section 4, Section 5, is for the simulation and results, and Section 6 includes the conclusions of the paper.

2. MPLS Terminology:

The terminology of the MPLS network is based on the concepts, architecture and operation involved in the MPLS network [7 -9]. This terminology is given below:

a) MPLS Label:

MPLS works by prefixing packets with an MPLS header. The header contains one or more labels. The MPLS label identifies the path a packet should traverse in the MPLS domain. The MPLS label is similar to the ATM VPI/VCI and the Frame Relay DLCI.

b) FEC:

FEC stands for Forwarding Equivalence Class. It is a group of packets with same attributes. These group of packets are processed in the same way by LSRs during transmission.

c) Label switched path (LSP):

The path that an FEC passes through in the MPLS network is called Label Switched Path (LSP). This path is set up prior to data transmission. It functions similarly to Virtual Circuits of ATM and Frame Relay.

d) Label Distributing Protocols (LDP):

The MPLS control Protocols (namely, signaling protocols) are called Label Distributing Protocols. These protocols are used to classify FECs, distribute labels, and establish and maintain LSPs through an MPLS network.

e) Label Edge Routers (LERs):

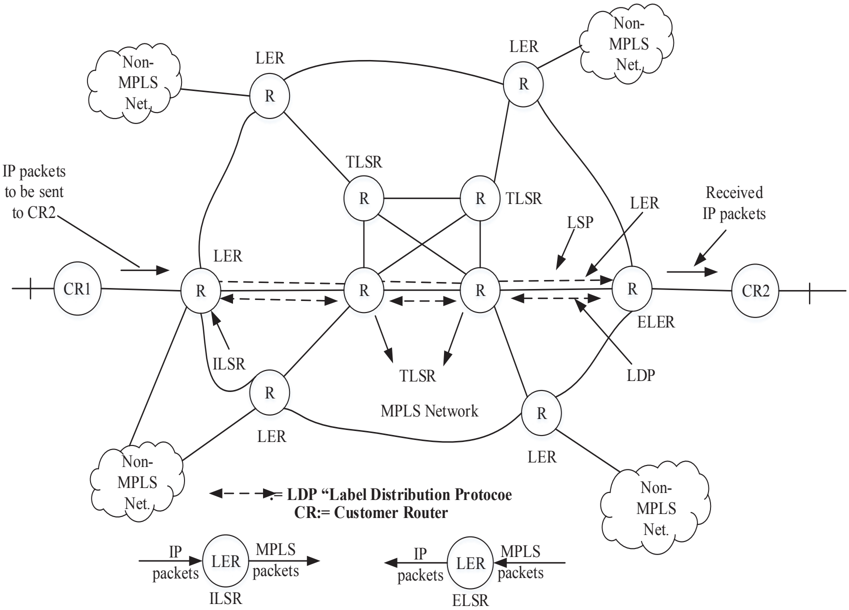
These routers operate at the edge of an MPLS network and act as entry and exit points for the network as follows:

1. Ingress LERs: Ingress LER indicates the beginning node of an LSP. An Ingress LER (ILSR) receives a packet that is not labeled yet, inserts (pushes) a new label to the packet and encapsulates the IP packet as an MPLS packet and forwards the labeled packet into the MPLS domain.
2. Egress LERs: Egress LERs indicates the end node of an LSP. An Egress LER (ELSR) receives the labeled packets (MPLS packets), removes labels (POPS) and forwards the packets towards the customer router.

f) Transit Routers (TLSRs):

The transit LSR indicates the middle node of an LSP. More than one transit router may exist on an LSP. The transit LSR strips out the incoming label and assigns a new label (Swaps) to complete the forwarding of MPLS packets. Figure (1) shows the positions of the MPLS network components, that is, MPLS routers, LSP and LDP.

https://doi.org/10.20428/JST.22.2.5



Figure(1): MPLS Network Components

3. Related Works:

In this section several works related to the subject of this paper will briefly be introduced as follows:

Haskin's Method [6] provides a fast rerouting protection mechanism by pre-establishing the alternative LSP (FAP, First Alternative LSP) prior to the occurrence of a failure in the PWP (Primary Working Path). When the ingress LSR receives the first packet from the PBP (Primary Backward LSP) it switches traffic to the alternative LSP. The method results in a minimum packet loss and a maximum packet disordering.

Makam's Method [5], the authors have proposed a method uses a fault indication signal (FIS) to convey the information about the occurrence of a fault on the original LSP. This method results in a maxmim packet loss and no packet disordering.

Hundessa's method [4], follows the principle given in [6] and the main objective of the paper is to avoid packet disorder and reduce the average traffic delay.

Chandana's method [3], the authors have proposed a method based on the combination of the protection switching technique and rerouting technique. The method can handle single or multiple faults in MPLS network. The authors have claimed that their approach achieves less recovery time, reduces packet loss and has high throughput.

4. Proposed Method:

The proposed method is based on protection switching and rerouting approaches which are the existing techniques used for fault recovery in the MPLS network. On the Ingress LSR, protection switching is used to pre-establish the first alternative path (FAP) in advanced to carry the traffic when a fault occurs in PWP, and rerouting approach is only used to establish the second alternative path (SAP) on demand, that is when a fault occurs on FAP. On the Alert LSR (ALSR), rerouting approach is only used to establish a temporary alternative path (TAP) on demand that is when a fault occurs in PWP. Figures 2, 3 and 4 show the proposed algorithms on the Ingress LSR, Alert LSR and core LSR respectively.

https://doi.org/10.20428/JST.22.2.5

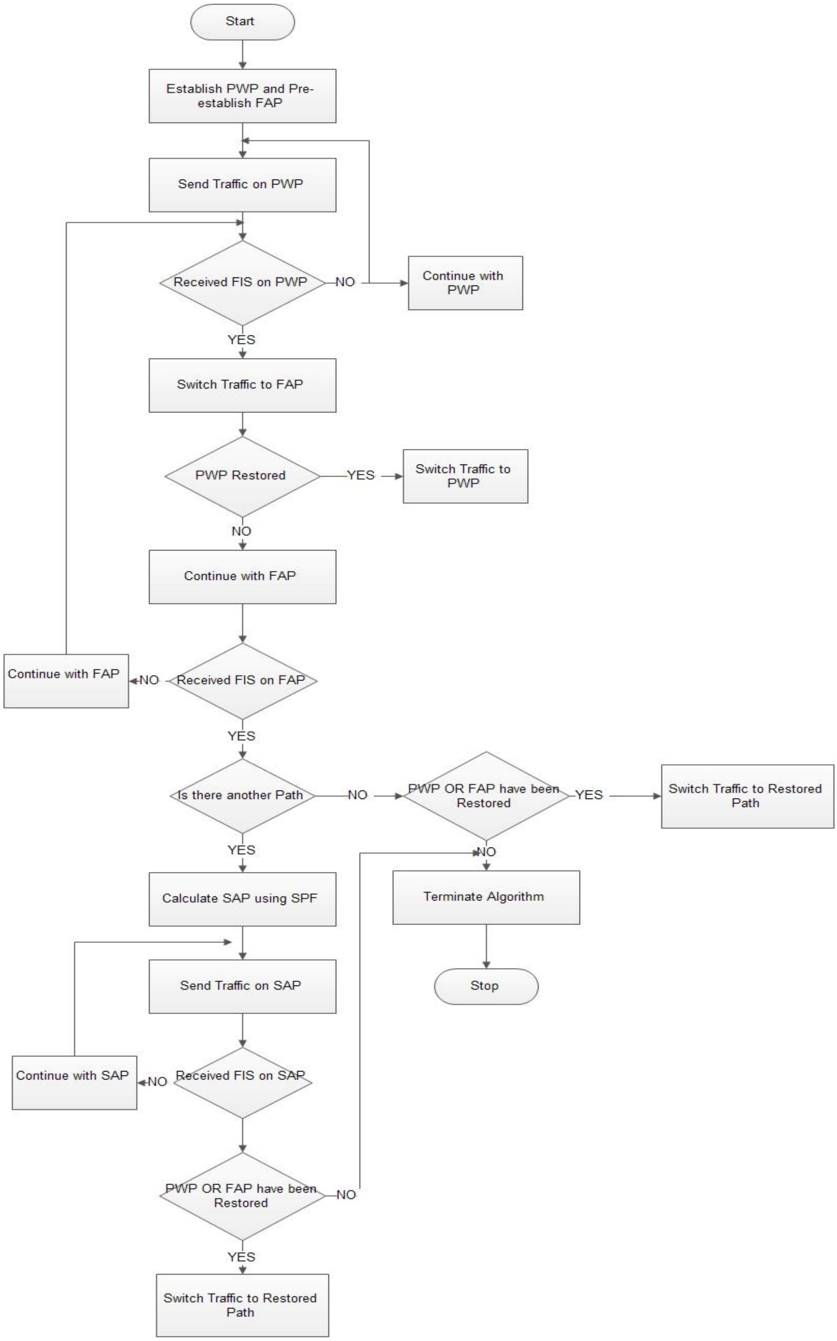


Figure (2): Flow Chart for proposed algorithm on the Ingress LSR

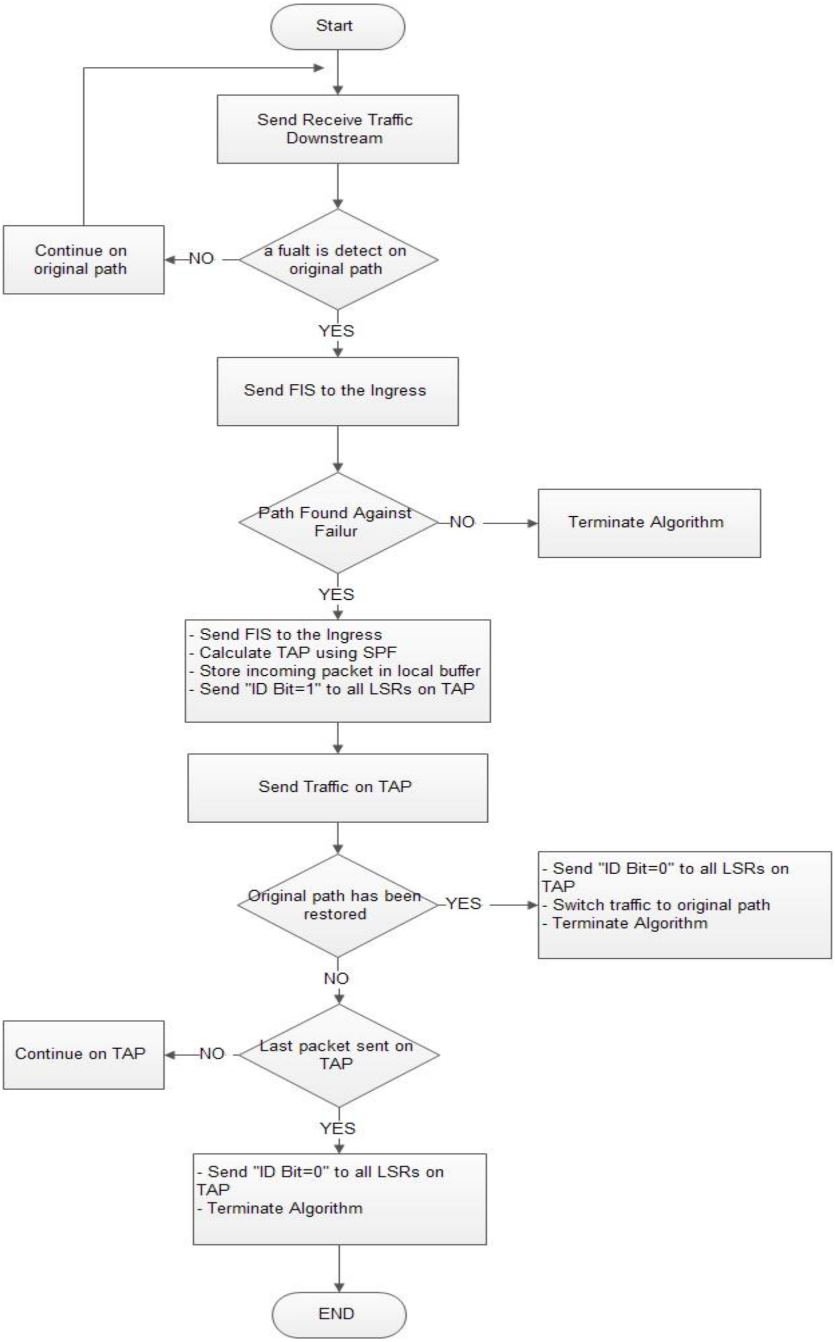


Figure (3): Flow Chart for proposed algorithm on the ALSR

https://doi.org/10.20428/JST.22.2.5

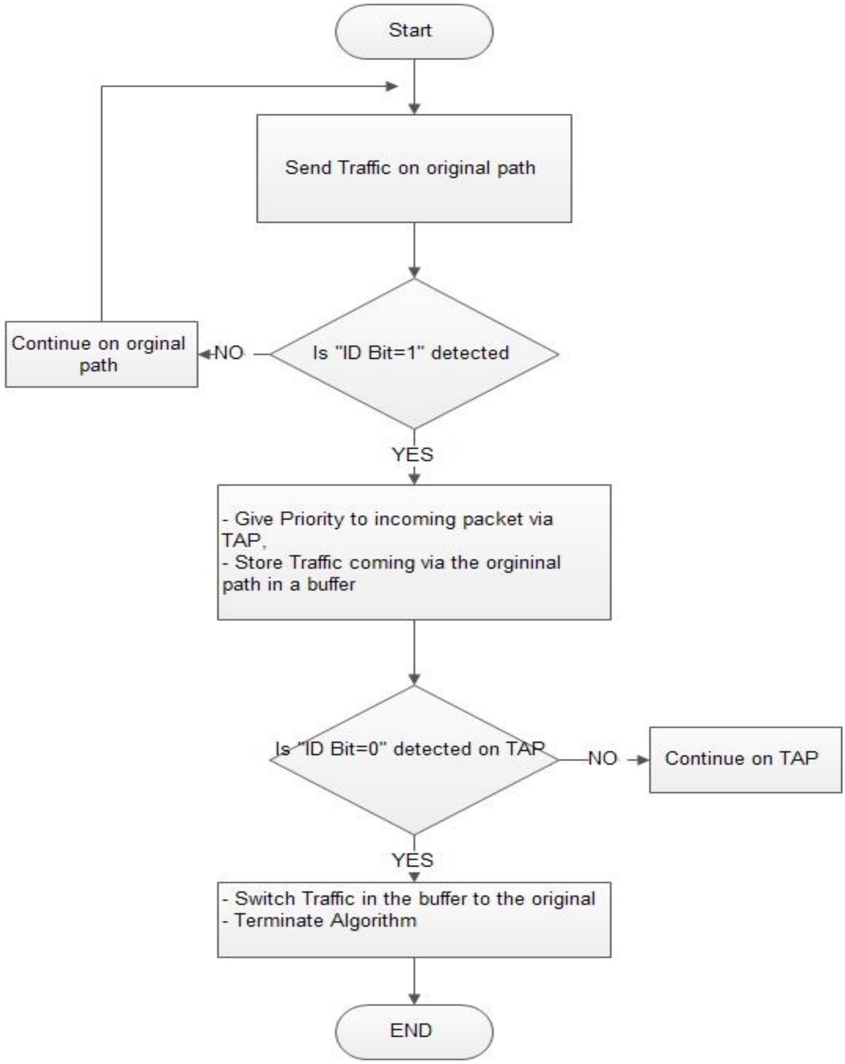


Figure (4): Flow Chart for proposed algorithm on the core LSR

5. Simulation and Results:

In this section we will evaluate the results of the implementation of our proposed method for protection of data flow in MPLS network. The simulations are performed on Network Simulator (NS2) [10- 12]. All links were set up as duplex with 10ms delay and using DropTail Queuing, which serves packets on First Come First Service (FCFS) basis. Also, the link have a bandwidth of 2Mbps and the types of the transmitted data in the network are multimedia.

The simulation parameters used in three runs as shown in Table (1), and the simulated scenario is as shown in Figure (5).

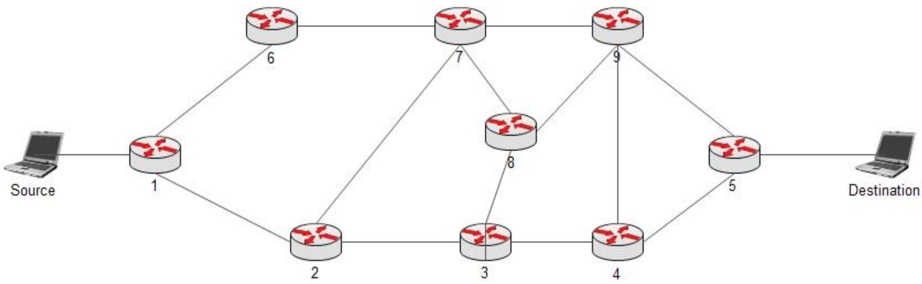


Figure (5): The network topology used in the simulation process

Table (1): Simulation Parameters used in various Runs with Data Rate=400kbps and 1 Mbps

Parameter	Run 1	Run 2	Run 3
Simulator	Ns-2.34	Ns-2.34	Ns-2.34
Simulation Time	60 second	60 second	60 second
Packet Size	128 Bytes	256 Bytes	512 Bytes
Traffic Type	CBR (UDP)	CBR (UDP)	CBR (UDP)

It is assumed that a fault occurs in PWP after 12 second. Figures 6, 8, 10 and 12 illustrate the results based on 400kbps data rate while figures 7,9,11 and 13 illustrate the results based on 1Mbps data rate.

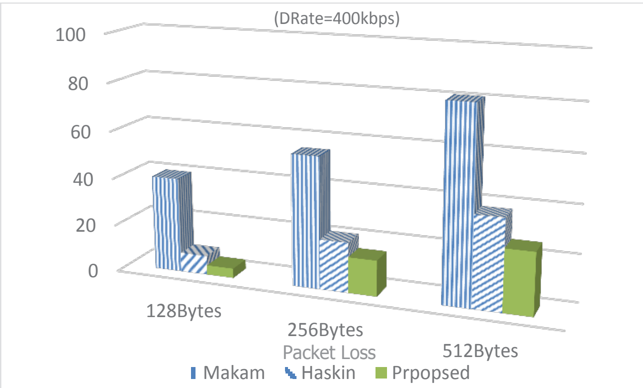


Figure (6): Packet loss versus packet size

https://doi.org/10.20428/JST.22.2.5

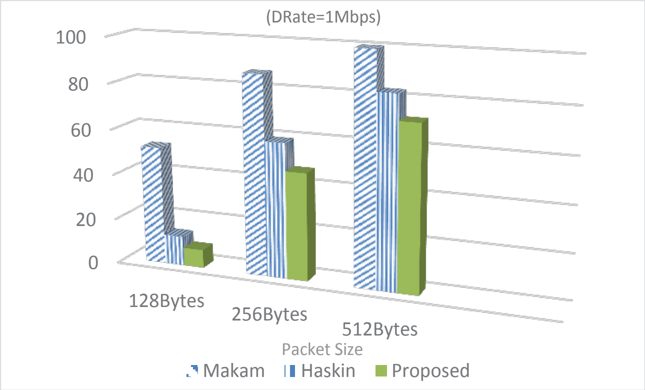


Figure (7): Packet loss versus packet size

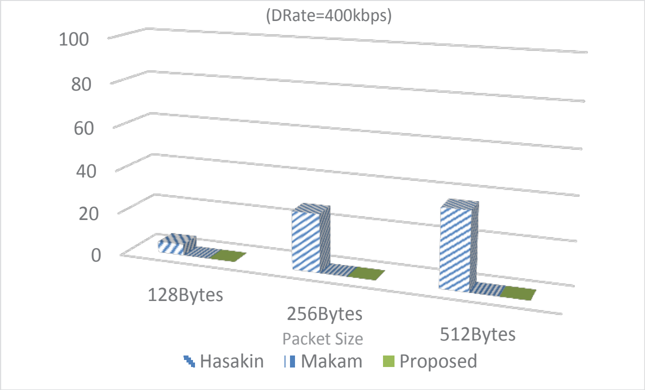


Figure (8): Packet disorder versus packet size

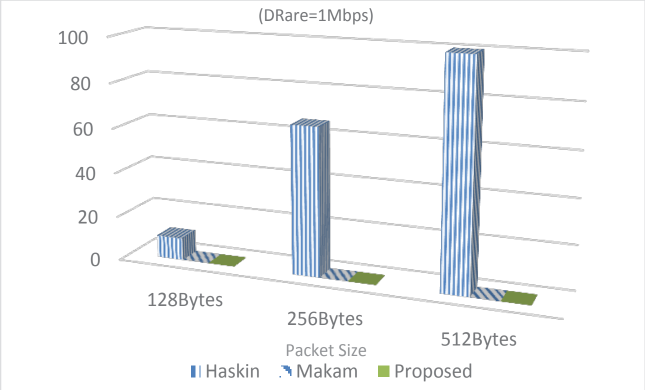


Figure (9): Packet disorder versus packet size

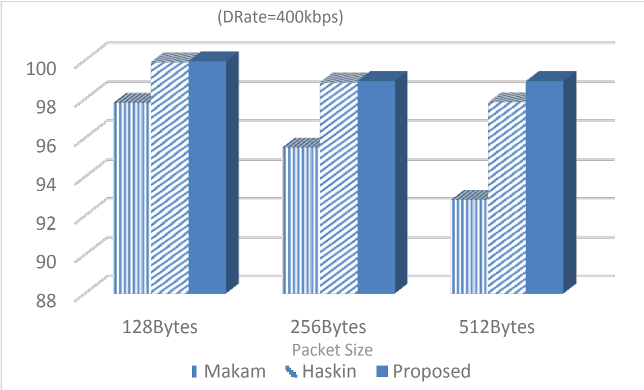


Figure (10): Packet delivery ratio versus packet size

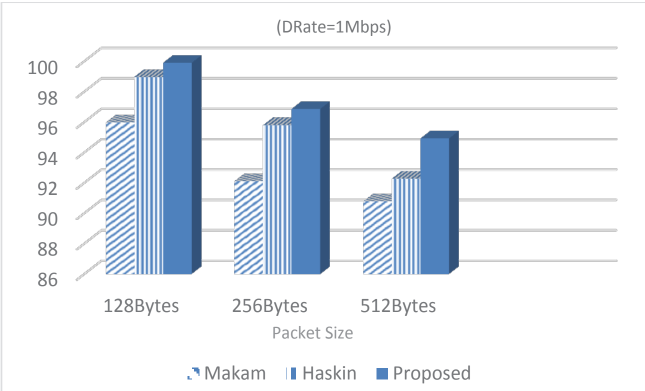


Figure (11): Packet delivery ratio versus packet size

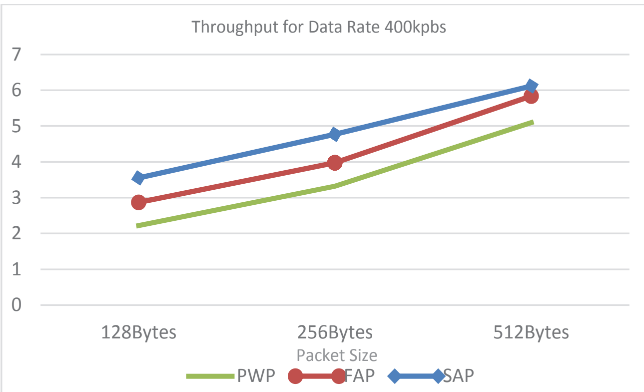


Figure (12): Throughput versus packet size

https://doi.org/10.20428/JST.22.2.5

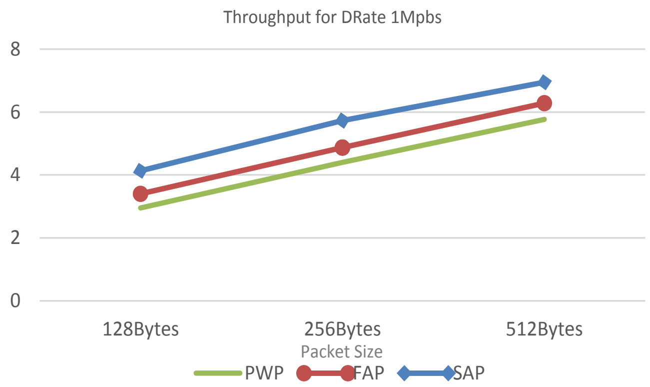


Figure (13): Throughput versus packet size

5.1 Comparative Analysis:

A comparative analysis of the performance metrics will be given in this section based on the results shown in the previous figures:

a) Packet Loss: It is very clear from the results shown in figures 6 and 7 that the proposed method has less packets loss than Haskin's method and Makam's method under all packet sizes. Makam's method introduces more packets loss than Haskin's method.

b) Packet Disorder: It is clear from the results shown in figures 8 and 9 that the proposed method avoids packets disordering as the case with Makam's method. While in Haskin's method, packets arriving from the reverse direction are mixed with the entering packets (incoming packets to the Ingress LSR) which results in packet disordering through the alternative LSP (FAP) during the restoration period. Also, in Haskin's method, packet disorder increases in proportion to the distance between the Ingress LSR and the alert LSR.

c) Packet Delivery Ratio: the packet delivery ratio is an important performance metric to ensure the arrival of received packets. Figure 10 and 11 show that the PDR of the proposed method is better than the PDR of Makam's method and the PDR of Haskin's method. In other words, the proposed method gives more PDR than Makam's method and Haskin's method.

d) Throughput: Based on the results given in figure 12 and 13 one can see that the proposed method gives better throughput than Makam's method and Haskin's method. This is because increase in packets loss gives reduced throughput, but the proposed method has achieved better PDR and hence gives good throughput.

6. Conclusions:

The paper has presented a method to detect single and multiple faults in the MPLS network. The method is based on both protection switching and rerouting algorithms that used to reroute traffic in the MPLS network. The main motivation behind the work given in this paper is to obtain a reliable and efficient QoS routing method for data in the MPLS network when failures occur in the network.

Once an intermediate LSR on the working path detects a fault on the link, it sends the FIS to the Ingress LSR, stores the incoming packets (the packets which are in transit on the working path between the Ingress LSR and the LSR which detects the fault), computes a temporary alternative path (TAP), sends a logic "id bit" to all LSRs on the TAP and finally switches the packets stored in its buffer to the TAP.

The proposed method avoids packet disorder, reduces packets loss, improves PDR and achieves good throughput.

In summary, the proposed method has the following advantages:

1) Avoids packet disorder.
2) Reduces packets loss.
3) Improves packet delivery ratio, which is an important performance metric to ensure the arrival of received packets for multimedia applications.
4) Handles single and multiple faults in the MPLS network.
5) Gives good throughput.

7. References:

[1] Er. Abinaiya N, M.J.J., A Survey On Multi Protocol Label Switching. ijteee, 2015(02): p. 4.

[2] Shruti Thukral1, B.C., A Survey on QoS Behavior in MPLS Networks. International Journal of Advanced Research in Computer and Communication Engineering, 2015. 4(3, March 2015): p. 5.

[3] Chandana B, P.P., An Efficient QOS Routing Algorithm for Protection of Data Flow in MPLS Network. International Journal of Innovative Research in Computer and Communication Engineering, 2014: p. 7.

[4] Hundessa, L. and J.D. Pascual. Fast rerouting mechanism for a protected label switched path. in Proceedings Tenth International Conference on Computer Communications and Networks (Cat. No.01EX495). 2001.

https://doi.org/10.20428/JST.22.2.5

[5] Makam, S., et al., Protection/restoration of MPLS networks. Work in Progress,< draft-makam-mpls-protection-00. txt, 1999.

[6] Haskin, D., A method for setting an alternative label switched paths to handle fast reroute. Internet Draft, draft-haskin-mpls-fast-reroute-05. txt, 2000.

[7] Asaad, A.R.A., Fundamentals of Wide Area Computer Network Engineering. 2017. 98.

[8] Ghein, L.D., MPLS Fundamentals: A Comprehensive Introduction to MPLS Theory and Practice. 2007, Cisco Press, Indianapolis.

[9] Huawei Technologies Co., L., Enterprise Data Communication Products Feature Description - MPLS, in Huawei Technologies. 2013. p. 139.

[10] Issariyakul, T. and E. Hossain, Introduction to network simulator NS2. 2011: Springer Science & Business Media.

[11] Hossain, T.I.E., Introduction to Network Simulator NS2. Springer, 2009: p. 438.

[12] Ahn, G. and W. Chun. Design and implementation of MPLS network simulator (MNS) supporting QoS. in Information Networking, 2001. Proceedings. 15th International Conference on. 2001. IEEE.

[13] Nandal, K. a. (2015). “MMPLS: Modified Multi-Protocol Label Switching.” Network. International Journal of Innovative Research in Computer and Communication Engineering (01), 5.

[14] Jamali, A., Naja, N., & El Ouadghiri, D. (2012).” An Enhanced MPLS-TE for Transferring Multimedia packets.” International Journal of Advanced Computer Science and Applications, (IJACSA), 3(8).

[15] Singh, R. K., Chaudhari, N., & Saxena, K. (2012). “Enhanced traffic aware LSP selection method in MPLS networks. Paper presented at the 2012” Ninth International Conference on Wireless and Optical Communications Networks (WOCN).

[16] https://www.isi.edu/nsnam/vint/.

[17] http://www.gns3.net.

[18] http://www.isi.edu/nsnam/ns/.

[19] http://www.ee.surrey.ac.uk/Personal/L.Wood/ns/.

[20] http://www.slogix.in/ns2-wired-sample-programs.

[21] https://www.riverbed.com/gb/products/steelcentral/opnet. html?redirect =opnet.

[22] http://www.omnetpp.org.