International Journal of Software Engineering and Computer Systems (IJSECS)
ISSN: 2289-8522, Volume 5 Issue 1, pp. 16-35, February 2019
©Universiti Malaysia Pahang
https://doi.org/10.15282/ijsecs.5.1.2019.2.0052

AN EFFICIENT FAULT TOLERANCE MODEL FOR SINGLE AND MULTI-FAULT IN MPLS NETWORKS

Belal A. Al-Fuhaidi[1*], Hasan A. A. Asaad[2], Sadik Al-Taweel[3]

[1,2,3] Institute of Department of Computer Science, Faculty of Computing and IT,
University of Since & Technology, Sana'a, Yemen.
[1*]Email: belalarh@gmail.com
[2]Email: hasanasaad9@gmail.com
[3]Email: dr.sadiq@ust.edu

ABSTRACT

The ever increasing demands for the performance improvement in Multiprotocol Label Switching (MPLS) network have motivated to develop a resistant MPLS network to the failures at link, node and software of the MPLS network devices. The occurrence fault at link degrades the network performance due to data packets loss. This paper proposes an efficient model for rerouting traffic in MPLS network when a single and multi-fault occur in working link based on the protection switching and rerouting algorithms. In this model three algorithms are developed for fast fault recovery in MPLS network based on ingress LSR, alert LSR and core LSR. The proposed model has been simulated using Network Simulator (NS2) version 2.34, simulation results show that the proposed model significantly improves the network performance such that eliminates packet disorder, reduces the packets loss, get better PDR, decreases end to end delay and enhance throughput. The proposed model has less space complexity compared to other methods that reached to 13.33% in single fault and 33.33% in multi-fault and has a fast recovery time compared to other methods.

Keywords**:** MPLS; Single-fault; Multi-fault; TAP; LSR.

INTRODUCTION

MPLS is a type of data-carrying technique for high-performance telecommunication networks. The MPLS directs data from one network node to the next based on short path labels rather than long network addresses. MPLS belongs to the family of packet switched networks and operates at a layer that is considered to lie between open system international (OSI) layer 2 and layer 3, and thus it is referred to as a layer 2.5 protocol. MPLS can be used to carry many different kinds of traffic, including IP packets, as well as native Asynchronous transfer mode (ATM), synchronous optical network (SONET) and Ethernet Frames (De Ghein et al. 2016, Huawei Technologies Co. 2013, Mishra, K. et al. 2015).

MPLS is an evolving network technology that has been used to provide Traffic Engineering and high speed networking. There has been current demand on Internet Service Providers, which support MPLS technology, to provide Quality of Service (QoS) guarantees and security (Alouneh, S. et al. 2010, Sun, X. 2012, Jamali, A. et al. 2012, Singh, R. K. et al. 2012, Al Mamun, A. et al. 2016). MPLS network is a connection-oriented network and hence it is prone to failure. Failures are of different types: link failure, node failure, software failure hardware failure, faults can affect the network operation and QoS which degrades the network performance. Therefore, fault tolerance is an important QoS factor that needs to be considered to maintain network survivability (Jamali, A. et al. 2012, Hadjiona, M. et al.2008, Kompella, K. et al. 2017). The fault-tolerant issue concerns how to protect traffic in a carried path against node and link failures. Fault tolerance includes many sections in terms of hardware and software, as well as Node and link where most researches work in single and multi-faults at Node and link of the MPLS Networks. Fault tolerance is used to resolve the faults, errors and failure and increase the speed of the system when a failure occurred. Fault tolerance provides higher availability and higher reliability which allows the system to work with faults and errors (Agarwal, A. et al. 2002, Awduche, D. O. 1999).

Most researchers work in single and multi-faults tolerance, the authors in (Haskin, D. 2000) have presented a method for setting up an alternative LSP to handle fast rerouting of traffic upon a detected single failure in the protected working path (PWP) and protected backup path (PBP) for redirected the traffic to the first alternative path (FAP), this method gives minimum packet loss but has maximum packet disordering, average traffic delay, increasing in space complexity and works in Single fault only. In (Makam, S. et al. 1999), the authors have suggested two recovery techniques: pre-established and dynamic recovery. These mechanisms use a fault notification message (FIS) to convey the information about the fault occurrence on the PWP, the alert label switching router (ALSR) signals to the upstream nodes which is the intermediate LSRs on the PWP between the Ingress LSR and the Alert LSR. The Ingress LSR redirects the traffic over the pre-established path which is called the rerouting technique. Makam’s Method does not have packet disordering but causes more packet loss and works in single fault only. Authors in (Hundessa, L. et al. 2001) proposed a mechanism to perform a fast rerouting traffic in the MPLS networks where the researcher follows the principles that described in (Haskin, D. 2000), this method start storing the incoming packet on the primary path in a local buffer and notify the last packet to follow on the backward path. This method avoiding packet disorder and reducing the average traffic delay but suffers from the increasing in space complexity and works in single fault only. For single and multi-faults tolerance, authors in (Chandana B, P. P. 2014) proposed a method based on the combination of protection switching technique and rerouting technique. In the beginning Chandana’s method establish several paths such as original LSP (PWP) for traffic flow, alternative LSP (FAP), second alternative LSP (SAP) and backward LSP (PBP). If any fault found in LSP, immediately FIS message is transferred to Ingress LSR. Then, the Ingress LSR switches the traffic to alternative path. If the faults occur in alternative LSP, then the traffic is switched to the second alternative path. This method reduces the packet loss and provides a good throughput in multi-fault, but there is increasing in space complexity and disordering packet when the fault occurs.

This paper presents an efficient model for rerouting traffic in MPLS network when a fault occurs in the working link. The paper has considered link failure because failures in the link lead to a large amount of data drops. The proposed model has been developed to handle single and multi-faults based on existing protection switching and rerouting algorithms and approaches for fault recovery consists of three algorithms in

MPLS network. The first algorithm uses a pre-established alternative path called FAP in order to restore traffic when a fault occurs in the PWP. In addition, a second alternative path (SAP) is established to restore traffic when the second fault occurs in the FAP. In the second algorithm a Temporary Alternative Path (TAP) is established by the ALSR that detects the fault on the working LSP. This TAP has been established between ALSR and Egress LSR (destination) to carry packets, which are in transit between Ingress LSR and ALSR which leads to transfer LSP traffic to destination and send FIS to ingress LSR. The core LSR algorithm is working after TAP established which leads to transfer packets that incoming on TAP LSP to destination for eliminate disordering packet and reduce packet loss to provide high throughput and reduce recovery time.

The rest of this paper is organized as follows. Second section describes the proposed model for single and multi-fault tolerance. Third Section describes the simulation scenarios of the proposed model and the MPLS network metrics. In fourth section, the comparative studies for space complexity are discussed. Simulation results and analysis are presented in fifth section. Conclusions and feature works are presented in sixth section.

PROPOSED MODEL FOR SINGLE AND MULTI-FAULT TOLERANCE

This section presents the proposed model which contains three developed algorithms which developed to tolerate faults that occurred at PWP, FAP, and SAP. The fault tolerance occurred at Ingress LSR, ALSR and Core LSR. The three algorithms are included in one model because these algorithms are integrated to each other and works for single and multi-fault tolerance, see figure 1. More explanation details about the proposed model operations are demonstrated in three scenarios that depicted in next section.

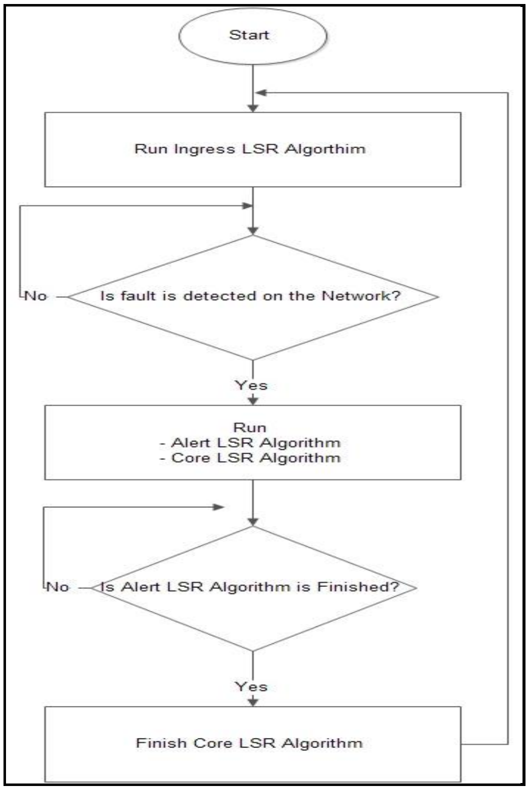

Start
Run Ingress LSR Algorthim
No
Is fault is detected on the Network?
Yes
Run
- Alert LSR Algorithm
- Core LSR Algorithm
No
Is Alert LSR Algorithm is Finished?
Yes
Finish Core LSR Algorithm

Figure 1. Proposed Model for Single and Multi-Fault Tolerance

The Ingress LSR Algorithm

This developed algorithm is based on protection switching and rerouting approaches which are the existing techniques are used for fault recovery in the MPLS network (Yongwook Ra et al. 2019). 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 (De Ghein et al. 2016, Corti, A., Fiorone, R. et al. 2016, trelkovskaya, I. et al. 2015), and rerouting approach is only used to establish the second alternative path (SAP) on demand, that is when a fault occurs on FAP (De Ghein et al. 2016, Corti, A., Fiorone, R. et al. 2016, trelkovskaya, I. et al. 2015). Figure 2 shows the pseudo code for ingress LSR algorithm.

Ingress LSR Algorithm

```
Begin
Establish PWP and Pre-Establish FAP
SEND Traffic to PWP
IF  Receiving of FIS on PWP THEN
 SWITCH Traffic to FAP
     IF PWP Restored THEN
          SWITCH Traffic to it
     ELSE Continue with FAP
     IF Receiving of FIS on FAP THEN
          IF Is there another path THEN
               Calculate the Second Alternative Path (SAP) using SPF,
               SEND Traffic to SAP,
          IF Receiving of FIS on SAP THEN
                    IF [(PWP OR FAP) have been restored THEN
                         Switch Traffic to Restored Path
```

Figure 2. Pseudo Code for Ingress LSR Algorithm

It is clear from the above that the algorithm works with three categories of failures (or faults) as follows:

1) The first fault may occurs on the primary working path (PWP).
   Let us call it FF (PWP).
   FF (PWP): First Fault on PWP.
2) The second fault may occurs on the First Alternative Path (FAP).
   Let us call it SF (FAP).
   SF (FAP): Second Fault on FAP.
3) The third fault may occurs on the Second Alternative Path (SAP).
   Let us call it TF (SAP).
   TF (SAP): Third Fault on SAP.

Based on these three faults, Table 1 illustrates the mechanism of the proposed algorithm as shown below:

a) Fault encoding is as follows:
   “0”: No Fault exists on the path.
   “1”: The path is faulty.
b) Traffic encoding is as follows:
   “0”: No traffic on the path (whether the path is faulty or not).
   “1”: The path carries traffic.
c) “-“ : Normal

Table 1. Algorithm Operation table

Fault Types			**Traffic On**			**Case Of Operation**
TF (SAP)	**SF (FAP)**	**FF (PWP)**	**PWP**	**FAP**	**SAP**	**(Link Status)**
0	0	0	1	0	0	Normal on PWP
0	0	1	0	1	0	Normal on FAP
0	1	0	1	0	0	Normal on PWP
0	1	1	0	0	1	Normal on SAP
1	0	0	-	-	0	Normal on PWP or FAP
1	0	1	0	1	0	Normal on FAP

1	1	0	1	0	0	Normal on PWP
1	1	1	0	0	0	Termination

The Alert LSR (ALSR) Algorithm

On the Alert LSR (ALSR), rerouting approach is only used to establish a temporary alternative path (TAP) on demand, which is when a fault occurs in PWP. Figure 3 illustrates the pseudo code of the algorithms in ALSR and TAP respectively.

```
Alert LSR Algorithm
    1:  Begin
    2:  SEND Received Traffic Downstream
    3:  IF a fault is detected on the original path THEN
                SEND FIS to the Ingress LSR,
                IF (path found against failure) THEN
                        Calculate the Temporary Alternative Path (TAP) using SPF,
                        Store incoming packet in local buffer,
                        SEND “ID Bit=1” to all LSRs on the TAP,
                        SEND Traffic to TAP,
                ELSE
                        TERMINATE ALGORITHM
                IF the Original LSP has been restored THEN
                        SEND “ID Bit =0” to all LSRs on TAP,
                        SWITCH Traffic to original path,
                        TERMINATE ALGORITHM


                IF Last Packet Sent on TAP THEN
                        SEND “ID Bit =0” to all LSRs on TAP,
                                TERMINATE ALGORITHM
                        ELSE Continue on TAP
4:          ELSE
                        Continue on original path
5: END
```

Figure 3. Pseudo code for Alert LSR Algorithm

Note: that the alert LSR (ALSR) that detects the fault becomes the Ingress LSR for the Temporary Alternative Path (TAP).

The Core LSR Algorithm on the Temporary Alternative Path (TAP)

The following pseudo code shows the algorithm that work for the core LSR on the temporary alternative path (TAP). Figure 4 shows the pseudo code of the Core LSR algorithm.

```
Core LSR Algorithm
    1:  Begin
    2:  SEND Traffic Via its original path
    3:  IF “ID Bit =1” is detected THEN
                GIVE Priority to Traffic coming via TAP,
                STORE Traffic coming via the original path in a Buffer
                IF “ID Bit =0” is detected on TAP THEN
                        SWITCH Traffic in the Buffer to the original path,
```

Figure 4. Pseudo code for Core LSR Algorithm

SIMULATION SCENARIOS OF THE PROPOSED MODEL

The proposed routing method given in this paper has been designed to handle single and multi-fault in the MPLS networks. On the other hand, Haskin's, Makam's, and Hundessa methods (Haskin, D. 2000, Hundessa, L. et al. 2001, Makam, S. et al. 1999) each one of them had been designed to handle only a single fault in the MPLS networks. If a second fault occurs in FAP, the two methods fail to handle this second fault in comparison with the proposed model. Therefore, the simulation platform for the proposed model is the same of the Haskin and Makam methods, when the fault occurs in PWP. The first scenario contains eleven nodes and illustrates the single fault occurrence in PWP, where the proposed model compared with Haskin's and Makam's methods. Whenever, the second scenario contains eleven nodes and illustrates the multiple faults occurrence in PWP, FAP, and SAP of the proposed model. Finally the third scenario contains one hundred nodes and illustrates the multi-faults occurrence in PWP, FAP, and SAP, where the proposed model compared with Chandana's method (Chandana B, P. P. 2014).

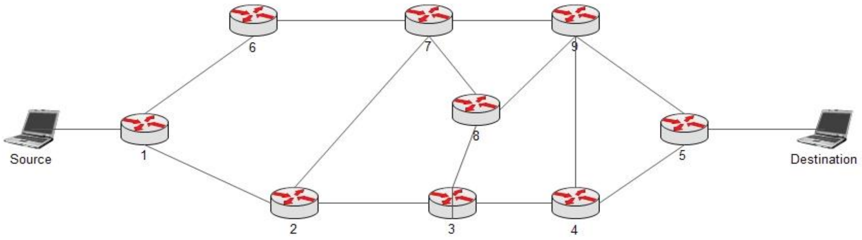


Figure 5. Network topology used in the simulation process

First Scenario for Single-Fault

The first scenario works when a single fault occurrence in PWP on the network topology that shown in figure 5 and uses the parameters in Table 4. The operations of the first scenario for the proposed model are described in the following two cases.
Case (a): The Network is in Normal Operation that shown in figure 6.

Case (b): When the single Fault Occurs on PWP, alert LSR starts creating TAP for switch incoming packet and sends FIS to Ingress LSR for redirect traffic to FAP path. Figure 7 (a, b, and c) show the case sequences.

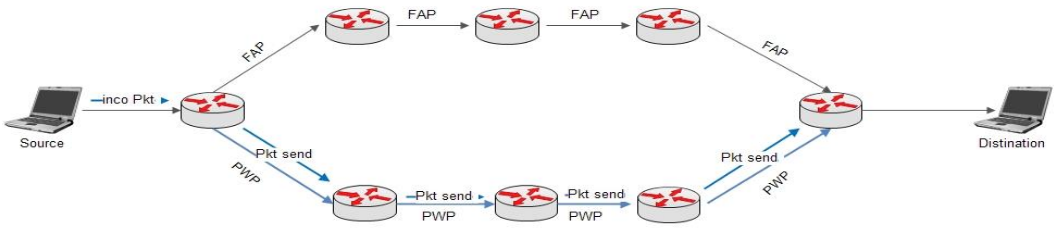


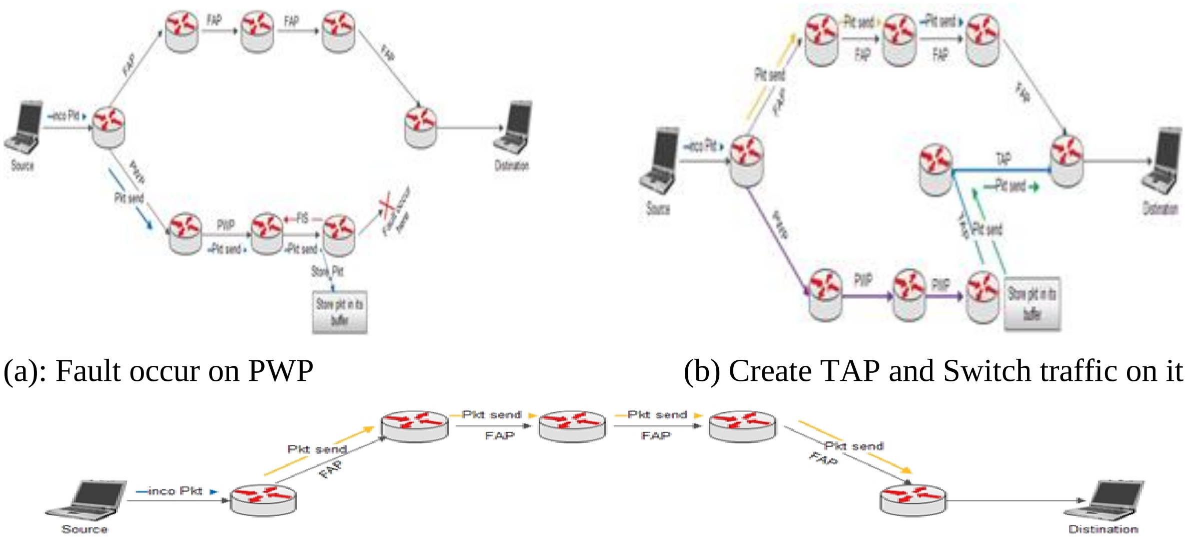
Figure 6. The Network is in the normal condition

Second Scenario for Multi-Fault

The second scenario works when the multi-fault occurrence in PWP, FAP and SAP on the network topology that shown in figure 5 and uses the parameters in Table 4. The operations of the second scenario for the proposed model are described in the following four cases.

Case (a): The Network is in Normal Operation that shown in figure 6.

Case (b): When the First Fault Occurs on PWP, alert LSR starts creating TAP for switch incoming packet and sends FIS to Ingress LSR for redirect traffic to FAP path. Figure 7 (a, b, and c) show the case sequences.

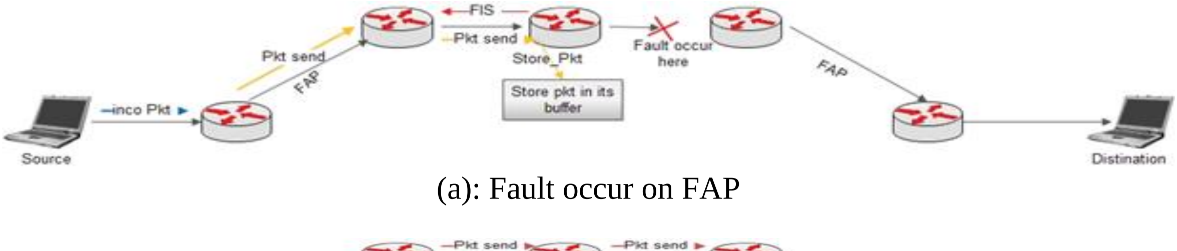


(a): Fault occur on PWP

(b) Create TAP and Switch traffic on it

(c) Switch traffic on FAP

Figure 7. First fault occurs on PWP, (a) Fault occur on PWP, (b) Create TAP and Switch traffic on it, (c) Switch traffic on FAP



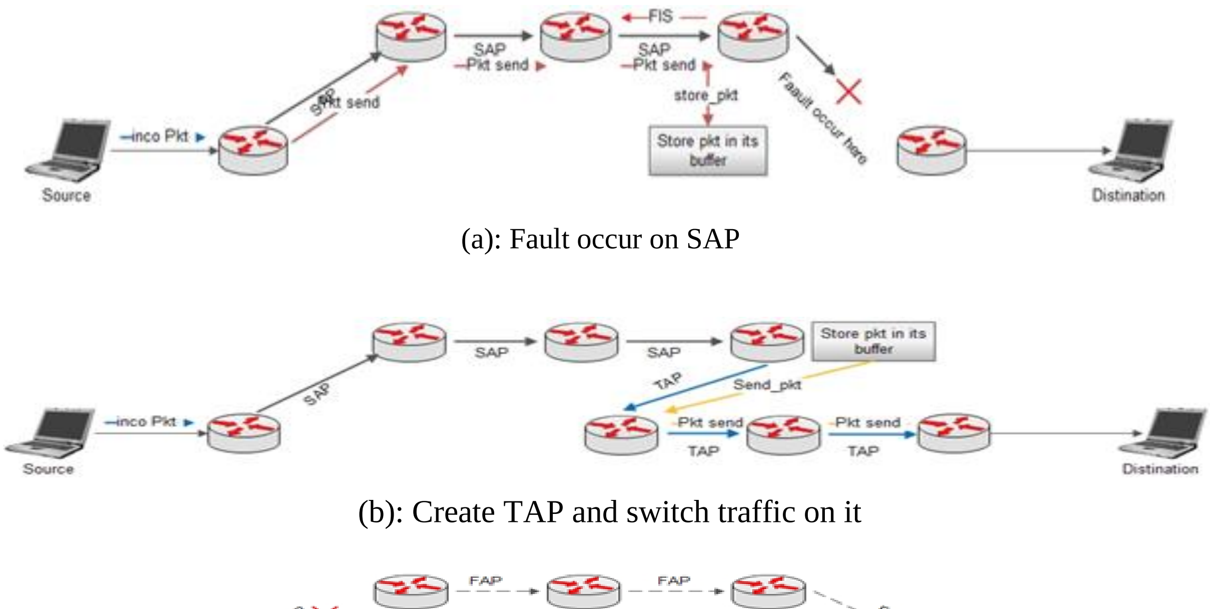
(a): Fault occur on FAP

Figure 8. Second fault occurs on FAP and PWP has not been restored yet, Fault occur on FAP, (b) Switch traffic of TAP and Create SAP, (c) Switch traffic on SAP.

Case (c): When the Second Fault Occurs on FAP and PWP has not been restored yet; the Ingress LSR starts the SAP path calculation to switch packet to this path. Figure 8 (a, b, and c) show the case sequences.

Case (d): When the Third Fault occurs on SAP even PWP and FAP paths have not been restored, the traffic network operation is terminated. Figure 9 (a, b, and c) show the case sequences.

In the proposed model, the intermediate LSRs between the Ingress LSR and Alert LSR, which detects the fault, continues sending packets downstream on the PWP/FAP until last packet. Once the ALSR finishes establishing the Temporary Alternative LSP (TAP), starts sending the packets stored in its buffer via TAP. By this way, packet losses are reduced and packet disorder is avoided in comparison to the already implemented methods that exit in NS2.



(a): Fault occur on SAP

(b): Create TAP and switch traffic on it

Figure 9. Third fault occurs on SAP and no one of the two LSPs (PWP & FAP) has been restored, (a) Fault occur on SAP, (b) Create TAP and switch traffic on it, (c) Faults occur on PWP and FAP at the same time

Third Scenario for Multi-Fault

The third scenario contains one hundred nodes and illustrates the multi-fault occurrence in PWP, FAP, and SAP, where the proposed model compared with Chandana's method (Chandana B, P. P. 2014). The operations of the third scenario for the proposed model are the same as the operations of the second scenario for multi-fault that described in sub-section 3.2, but using big network contains 100 nodes and uses the parameters in Table 5.

The metrics which are used to evaluate the performance of the proposed model and effect on the Quality of Service (QoS) on the MPLS network are:

Packet Loss

This metric is observed in the time interval between the fault detection in the working LSP and data flow switching to the alternative LSP. In addition, this metric influences the throughput and the recovery time proportionally, (Behrouz A. Forouzan 2012, Larry L. Peterson et al. 2010), Eq.(1) shows the computation of the packet loss and can be written as follow:

Packet Loss = Generated Packet – Received Packets *(1)*

Throughput

This metric is a measure of the rate at which data can be sent through the computer network (Behrouz A. Forouzan 2012), Eq.(2) describe the throughput computation as following:

Throughput = (total no. of bytes received /simulation time)(8/1000) kbps* *(2)*

Packet Delivery Ratio (PDR)

The PDR is also called packet loss ratio which is defined as the ratio of the packets number received by the destination to the packets sent by the source (Nandal, K. a. 2015). Eq.(3) shows the computation of PDR and can be written as following:

*Packet Delivery Ratio = Received Packet / Generated Packet * 100%* (3)

End-to-End Delay

The end-to-end delay defines how long an entire message takes to completely arrives at the destination from the first bit time sent for the source. Eq.(4) shows the computation of the average end-to-end delay (Behrouz A. Forouzan 2012).

*Average end-to-end delay = time (last Received Packet) – time (packet sent)/total Packets received * 100%* (4)

COMPARATIVE STUDIES FOR SPACE COMPLEXITY

In this section, the comparative studies for the space complexity will be performed among the following routing methods:

1) Proposed model.
2) Chandana's method
3) Haskin's methd
4) Makam's method
5) Hundessa's method

The purpose of these comparative studies is to describe the space complexity of each method based on the number of pre-established LSPs required by each method and the number of detected faults. The studies will be in two directions. The first direction is with methods that deal with a single fault and the second direction is with the methods that deal with multi-fault.

Space Complexity for Single Fault

Chandana's method (Chandana B, P. P. 2014) and the proposed model can handle both single and multiple faults. On the other hand, Haskin's method (Haskin, D. 2000), Makam's method (Makam, S. et al. 1999), and Hundessa's method (Hundessa, L. et al. 2001) can handle single fault only. The requirements of each one of the five methods are illustrated in Table 2.

Table 2. Methods Requirement

Routing Method	FRT used	PWP	BWP	FAP	SAP	TAP
Haskin	FRR	√	√	√	×	×
Makam 1	FRR	√	×	√	×	×
Makam 2	RR	√	×	×	√	×
Hundessa's	FRR	√	√	√	×	×
Chandana	FRR+RR	√	√	√	√	×

Proposed	FRR+RR	√	×	√	√	√

From the above table, the total Number of pre-established paths = 15

- Number of pre-established paths by Haskin = 3
- Number of pre-established paths by Makam 1 = 2
- Number of pre-established paths by Makam 2 = 1
- Number of pre-established paths by Hundessa = 3
- Number of pre-established paths by Chandana = 4
- Number of pre-established paths by the Proposed model = 2

Calculation of the space complexity (SC) for pre-establish path for all methods are given by the following equations:

$$SC\ Haskin = Number\ (PWP+BWP+FAP) / Total\ paths *100\% \tag{5}$$

$$SC\ Makam\ 1 = Number\ (PWP\ +FAP) / Total\ paths *100\% \tag{6}$$

$$SC\ Makam\ 2 = Number\ (PWP) / Total\ paths *100\% \tag{7}$$

$$SC\ Hundessa = Number\ (PWP+BWP+FAP) / Total\ paths *100\% \tag{8}$$

$$SC\ Chandana's = Number\ (PWP+BWP+FAP+SAP) / Total\ paths *100\% \tag{9}$$

$$SC\ Proposal = Proposal\ (PWP+FAP) / Total\ paths *100\% \tag{10}$$

The percentages of space complexity:

1) Chandana =26.67%
2) Haskin = 20.0%
3) Hundessa = 20.0%
4) Makam 1 = 13.33%
5) Makam 2= 6.67%
6) Proposed = 13.33%

It is clear from the above analysis that the space complexity associated with:

1) For the methods that can handle single fault, Makam 2 has the lowest space complexity and Chandana has the highest space complexity. The proposed model and Makam 1 have the same complexity which is better than the space complexity associated with both Haskin's and Hundessa methods. In other words, excluding Makam 1 and Makam 2, the proposed model has the lowest complexity in comparison to the other three methods.
2) For the methods that can handle multi-fault, the proposed model has the lowest space complexity.

Space Complexity for Multi-faults

The methods that can handle multiple faults are:

1) The proposed model.
2) Chandana's method (Chandana B, P. P. 2014).

Table 3 illustrates the requirements of each method.

Table 3. Chandana’s and proposed model requirements

Routing Method	FRT used	PWP	BWP	FAP	SAP	TAP
Chandana	FRR+RR	√	√	√	√	×
Proposed	FRR+RR	√	×	√	√	√

Where:

- FRT: Fault Recovery Technique.
- FRR: Fast Rerouting (Protection Switching).
- RR: Rerouting (Dynamic).

Total number of pre-computed paths= 6

- Number of pre-computed paths by Chandana’s method=4, (i.e, PWP, BWP, FAP, and SAP)
- Number of pre-computed paths by the proposed model =2, (i.e, PWP and FAP)

The space complexity (SC) for pre-establish path for Chandana’s method and Proposed model given by the Eqs.(11) and (12) respectively:

$$SC_{Chandana's} = Number\ (PWP+BWP+FAP+SAP)\ /\ Total\ paths\ {*}100\% \qquad (11)$$

$$SC_{Proposal} = Proposal\ (PWP+FAP)\ /\ Total\ paths\ {*}100\% \qquad (12)$$

The percentages of space complexity:

1) Chandana =66.67%
2) Proposed=33.33%

The space complexity of these two methods is shown in figure 10.

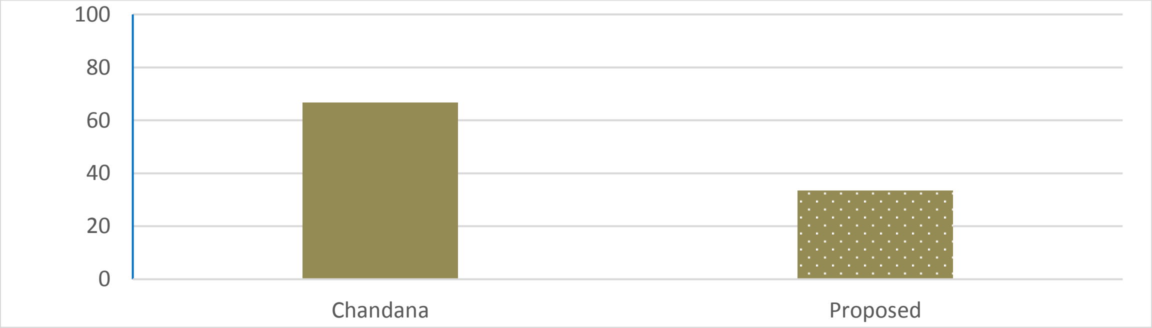


Figure 10. Space complexity of both Chandana’s method and Proposed model, for multi-fault

Chandana’s method detects two faults. The first one occurs in PWP and the second one occurs in FAP. When the two paths are faulty and a new fault is occurred in SAP, the algorithm is terminated and the packets that sent previously via SAP are neglected. Whenever in the proposed model, the packets that sent previously via SAP are not neglected because the ALSR that detects the fault in SAP continues sending the packets to the destination via the TAP. The algorithm is only terminated when no one of the three paths is restored.

SIMULATION RESULTS AND ANALYSIS

This section will present the simulation and discussion results for all scenarios that explained in section 3.

Simulation Results for Single Fault in Small Network Topology

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 is multimedia and CBR is useful for streaming multimedia due to limited capacity of the multimedia networks. The simulation parameters used in three runs with the proposed model, Haskin's method (Haskin, D. 2000) and Makam's method (Makam, S. et al. 1999), are shown in Table 4.

Table 4. Simulation Parameters used in various Runs with Data Rate (DR) = 400kbps and 1Mbps

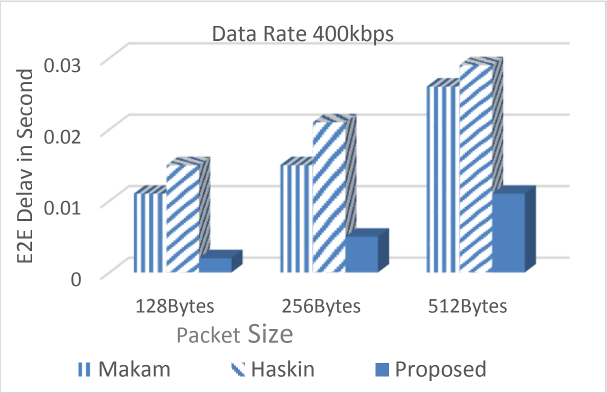
Parameter	**Run 1**	**Run 2**	**Run 3**
Simulator	Ns-2.34	Ns-2.34	Ns-2.34
Simulation Time	60 second	60 second	60 second
Packet Size	128 Bytes	256 Bytes	512 Bytes
Traffic Type	CBR (UDP)	CBR (UDP)	CBR (UDP)
Bandwidth	2Mbbs	2Mbbs	2Mbbs
Propagation Delay	10msec	10msec	10msec
Node Numbers	11	11	11

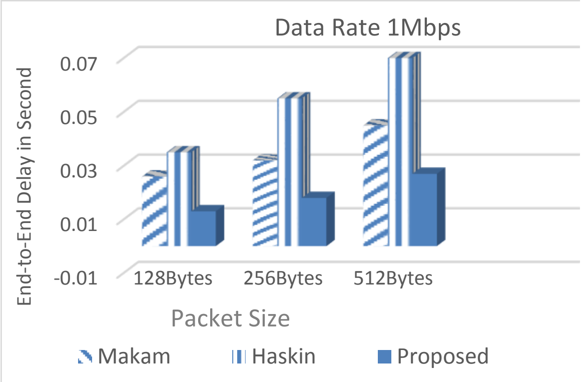
Based on the first scenario that depends on a single fault occurs in PWP (see section 3.1) and assumed that a fault occurs in PWP after 12 second, Figs. 11-20 include the results of the MPLS network metrics which obtained by the simulator (NS-2.34).

Figures 11 and 13 illustrate the results when the data rate (DR) is 400kbps, while figures 12 and 14 illustrate the results when the data rate (DR) is 1Mbps. The results in figures 15 and 16 are representing the throughput when the data rate is 400 kbps and 1Mbps respectively.

End-to-End Delay

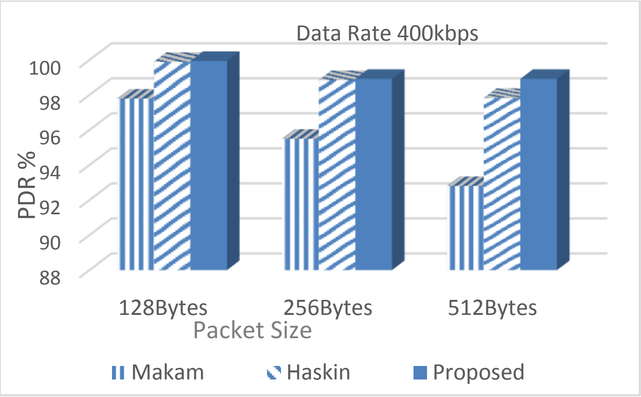
Figures 11 and 12 show that the proposed model has lowest delay compared to the Makam's method and Haskin method. Because in Haskin's method, those packets arriving from the reverse direction are taken more time to arrive to the Ingress LSR for switching the traffic to the FAP LSP while the proposed model find the TAP LSP so that the proposed model has a fast recovery time when a fault occurred.





Packet Delivery Ratio (PDR)

PDR is an important performance metric to ensure the arrival of received packets and depend of packet loss. The results in figures 13 and 14, show that the proposed model outperform Makam's and Haskin's methods in case of PDR, because the proposed model introduce the TAP algorithm in ALSR.



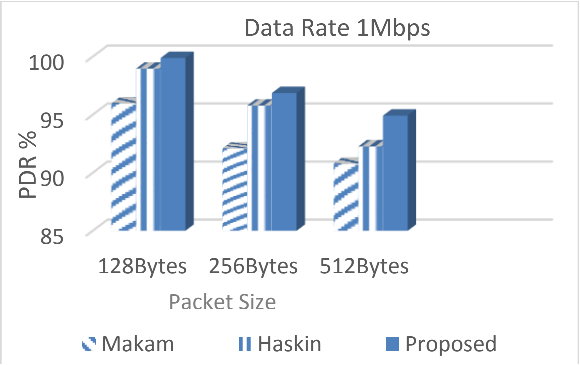
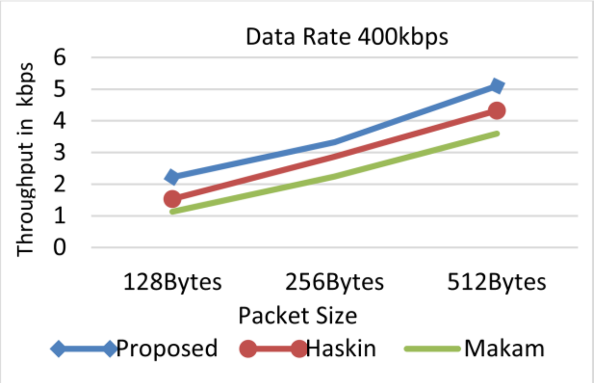


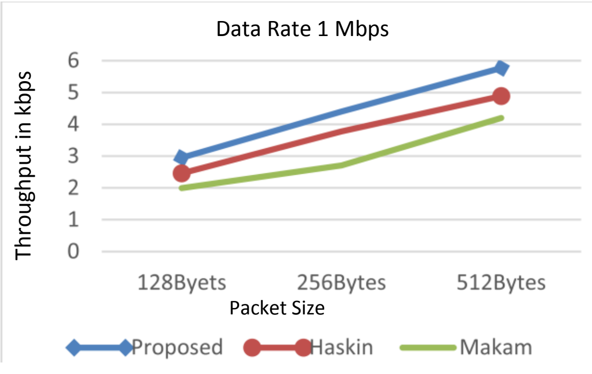
Figure 13. PDR vs. Packet size (DR=400kbps)

Figure 14. PDR vs. Packet size (DR=1 Mbps)

Throughput

The results given in figures 15 and 16, show that the proposed model gives better throughput than Makam's method and Haskin's method. This is because the higher packets loss decreasing in the proposed model compared to other methods.

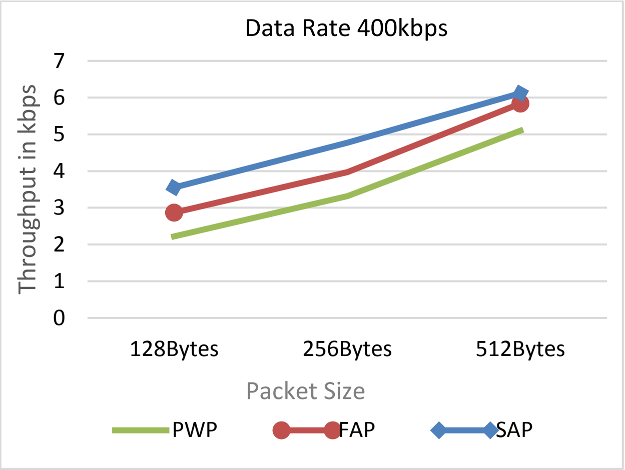




Simulation Results for Multi-Fault in Small Network Topology

The results in this subsection based on the second scenario that contains eleven nodes and illustrates the multiple faults occurrence in PWP, FAP, and SAP of the proposed model. The simulation parameters are shown in Table 4.

The results of the proposed model will be presented in figures 17 and 18. These results are based on the following faults respectively: First fault occurs on PWP after 12 seconds, second fault occurs on FAP after 20 seconds, third fault occurs on SAP after 30 seconds.



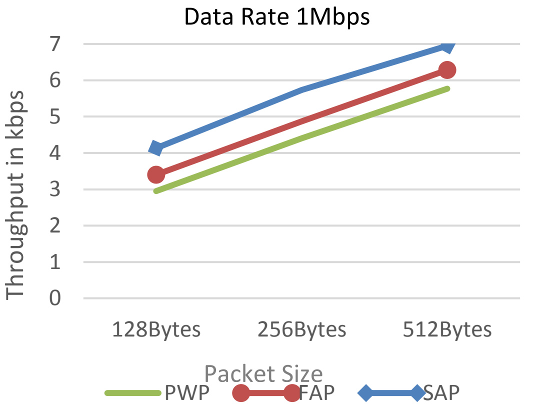


Figure 17. Throughput vs. packet size DR=400kbps

Figure 18. Throughput vs. packet size DR=1 Mbps

It is clear from the obtained results given in figures 17 and 18, that the proposed model gives high throughput even the increasing in the fault numbers. The throughput increases proportionally to the time and the packet size. The higher throughput achievement in the proposed model occurred due to the better PDR with any one of the working LSPs. The better achievement in PDR reduces packets loss and the reduction in packets loss leads to a higher throughput.

Since there is no implemented method in the NS2 for handling multiple faults in the MPLS network to be used as a reference for comparison purposes, the previous results for multiple faults in the MPLS network (which are obtained by the proposed model) are reasonable and hence the proposed model can be used as a reference for comparison purposes to relate works that will come later.

Multiple-Fault Results for Big Network Topology

The results in this subsection based on the third scenario that contains one hundred nodes and illustrates the multiple faults occurrence in PWP, FAP, and SAP, where the proposed model compared with Chandana's method (Chandana B, P. P. 2014). The simulation parameters used in this scenario of the proposed model are shown in Table 5.

Table 5 Simulation Parameters used in multi fault

Parameter	**Run 1**
Simulator	Ns-2.34
Simulation Time	60 second
Packet Size	128 Bytes
Traffic Type	CBR (UDP)
Bandwidth	2Mbps
Node Numbers	50,60,70,80,90,100

Figures 19 and 20 present the results of the proposed model and Chanadana's method in terms of PDR and throughput respectively.

Figure 19 show the results for PDR of the proposed model and Chandana's method. Where the PDR is the number of packets delivered at the egress router to the average value of packets sent.

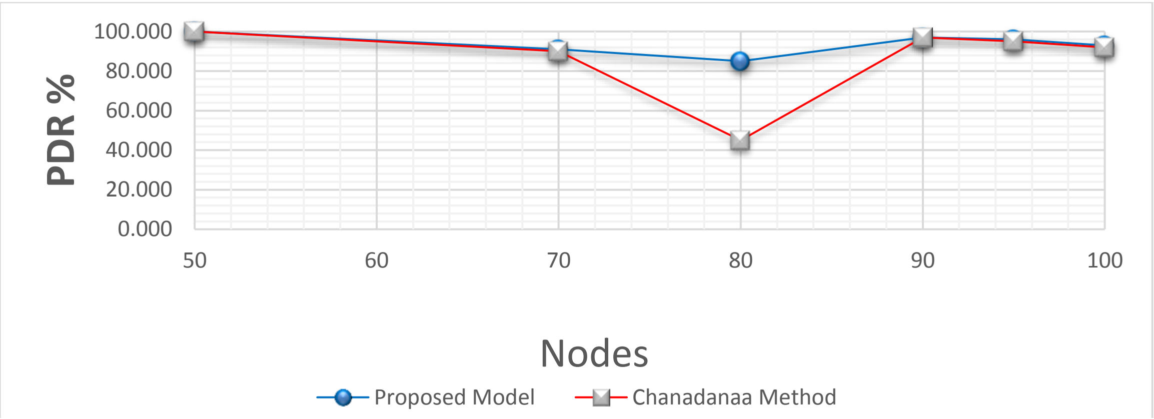


Figure 19. PDR for proposed model and Chanadana's method

From the results in the above figure, the proposed model is able to recovery faults with less packet loss compared to Chandana's method, when the packet loss number in Chandana's method reached to 40% of total packets. Whenever, the packet loss number in the proposed model reached to 20% of the total packets. The result in figure 19 shows that the proposed model outperforms the Chandana's method in term of packet delivery ratio.

Figure 20 show the throughput results of the proposed model and Chandana's method.

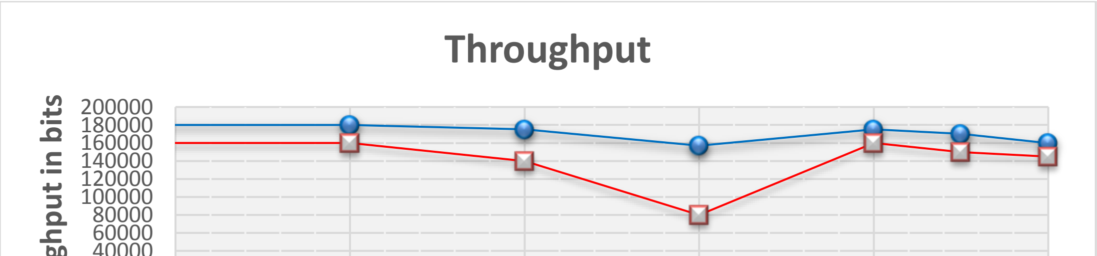


Figure 20. Throughput versus number of nodes for proposed model and Chandana's method

Figure 20 show that the proposed msodel achieved the better PDR which reduces packet loss and higher throughput than Chandana's method. When the faults occurs after 80 nodes that shown in figure 20 and the results that show the throughput in the proposed model decreases from 180000bps to 160000bps, whenever the throughput in Chandana's method decreases from 160000bps to 80000bps. These results show that the proposed model outperforms the Chandana's method in term of throughput.

CONCLUSIONS AND FEATURE WORKS

The paper focused on single and multi-fault tolerance in the MPLS network. This paper proposed a reliable and efficient routing model in the MPLS network to tolerate occurrence failures in the MPLS network specified at links. The proposed model has the ability to detect and correct single and multi-faults in the MPLS network and recover from faults quickly by development three algorithms. These algorithms based on both protection switching and rerouting algorithms.

Based on the simulation results and analysis, one can conclude that the proposed model can be used for QoS provision. Proposed model outperforms other methods in terms of throughput, PDR, E-to-E delay and packet disorder for single and multi-fault tolerance. In addition to the network performance enhancement, the proposed model has less space complexity compared to other methods that reached to 13.33% in single faults and 33.33% in multi faults.

An improvement of the proposed model given in the paper is required to solve the problem when the TAP-LSP cannot be found in network topology. Also an extension of the proposed model to works with failures occurrence in both node and link at the same time.

REFERENCES

Alouneh, S., & Abed, S. e. (2010). "Fault tolerance and security issues in MPLS networks". Paper presented at the Proceedings of the 10th WSEAS international conference on Applied computer science, World Scientific and Engineering Academy and Society (WSEAS),134-138.

Al Mamun, A., Sheltami, T. R., Ali, H., & Anwar, S. (2016). "Performance evaluation of routing protocols for video conference over mpls vpn network", *Journal of Ubiquitous Systems & Pervasive Networks, 7*(1), 01-06.

Agarwal, A., & Deshmukh, R. (2002).”Ingress failure recovery mechanisms in MPLS network”, Paper presented at the MILCOM, Proceedings, IEEE,1150-1153.

Awduche, D. O. (1999). "MPLS and traffic engineering in IP networks", *IEEE Communications magazine, 37*(12), 42-47.

Behrouz A. Forouzan, (2012). "*Data Communications and Networking*", 5th Edition ed, McGraw-Hill, 1264.

Chandana B, P. P. (2014). "An Efficient QOS Routing Algorithm for Protection of Data Flow in MPLS Network". *International Journal of Innovative Research in Computer and Communication Engineering, 7*.

Corti, A., Fiorone, R., & Martinotti, R. (2016). "Re-routing traffic in a communications network".

De Ghein, L. (2016)."MPLS Fundamentals": Cisco Press, 672.

Hadjiona, M., Georgiou, C., Papa, M., & Vassiliou, V. (2008). "A hybrid fault-tolerant algorithm for MPLS networks". Paper presented at the International Conference on Wired/Wireless Internet Communications, Springer, 41-52.

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

Huawei Technologies Co., L. (2013)."Enterprise Data Communication Products Feature Description - MPLS".

Hundessa, L., & Pascual, J. D. (2001). "Fast rerouting mechanism for a protected label switched path".Proceedings Tenth International Conference on Computer Communications and Networks (Cat. No.01EX495), 527-530, doi: 10.1109/ICCCN.2001.956316 , 15-17 Oct.

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).

Kompella, K., Swallow, G., Pignataro, C., Kumar, N., Aldrin, S., & Chen, M. (2017). "Detecting Multiprotocol Label Switched (MPLS) Data-Plane Failures".

Larry L. Peterson and Bruce S. Davie, (2010). "Computer Networks A Systems Approach".

Makam, S., Sharma, V., Owens, K., & Huang, C. (1999). "Protection/restoration of MPLS networks". Work in Progress, draft-makam-mpls-protection-00.txt.

Mishra, K., & Vats, P. (2015). "A Literature Review on Security Aspects for Fault Tolerance in Networks".*International Journal of Computer Science and Information Technologies, Vol. 6* (4), 3836-3843.

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

Singh, R. K., Chaudhari, N., & Saxena, K. (2012). "Enhanced traffic aware LSP selection method in MPLS networks".2012 Ninth International Conference on Wireless and Optical Communications Networks (WOCN), 1-4.

Strelkovskaya, I., Solovskaya, I., & Paskalenko, S. (2015). "Solution to a problem of routing in MPLS-TE network with additional directions of traffic transmission".Problems of Infocommunications Science and Technology (PIC S&T), 2015 Second International Scientific-Practical Conference, 54-57.

Sun, X. (2012). "Research on QoS of next generation network based on MPLS", International Conference on, IEEE, Paper presented at the Information Science and Technology (ICIST),294-296.

Yongwook Ra ; Junseong Bang ; Jeong-dong Ryoo. (2019). “Implementation of FPGA-based MPLS -TP linear protection switching for 4000+ tunnels in packet transport network for optical carrier Ethernet”, *IET Communications, Volume: 13* , Issue: 5, PP: 481 – 488.