Bima Journal of Science and Technology, Vol. 5(3) Jan. 2022. ISSN: 2536-6041

NODE AND LINK FAILURE RECOVERY ALGORITHM FOR A MULTICAST MULTIPROTOCOL LABEL SWITCHING (MPLS) NETWORK

ISHAYA N.[1], and IBRAHIM A. S.[2]

[1,2]Federal College of Education, Zaria Kaduna State, Nigeira

Correspondence email address: fifasaa4u@yahoo.com

ABSTRACT

There is a huge growth in the use of Internet across the globe in the last decade, and novel real-time connection-oriented services like streaming technologies and time critical transaction-oriented services are in use and new ones are currently emerging. Researches on more reliable network becomes inevitable so as to sustainable users' confidence. This paper explores fault recovery based on Multi-Protocol Label Switching (MPLS) on links and nodes connectivity. It discusses the mechanism of using MPLS to enable high scalability, end-to-end connectivity in routed networks. It examines efficiency of Multicast MPLS network transmission of datagrams to a group of zero or more hosts on a single destination group address. The research investigated the failures on nodes and links with and without the proposed new recovery mechanism called Multi-protocol Label Switch Recovery (MPLSR) and employed simulation in Java programming language in a Multicast MPLS network as an effective tool that can improve and guarantee intrusion-free network. MPLSR was compared with Hybrid Link Quality Estimation-Based Reliable Routing (HLQEBRR) and Collection Tree Protocol (CTP) algorithm in terms of end-to-end transmission delay and packet delivery ratio, and MPLSR performed better than them. It concluded by recommending MPLSR algorithm for a Multicast MPLS network to enhance efficiency and reliability.

Keywords: Multi-protocol, Multicast, Network, Intrusion-free, Recovery algorithm

INTRODUCTION

In recent times, the Internet has evolved into a widespread network and is still evolving, this inspired the development of a variety of new applications in e-commerce, remote health monitoring, and other facets of human life. Arunkumar (2014) reported that the increasing demand of high broadband data demanding Internet services has adversely affected the quality of service of data transfers in most networks. Modern networks support real-time services, live steams, and multimedia applications even in the presence of node or link failures. More user friendly applications are being developed which have driven the demand for increased and guaranteed bandwidth requirements in the backbone of the networks. In addition to the conventional data services currently provided over the Internet, new voice and multimedia services are being developed and deployed. Arunkumar (2014) identified two basic techniques for network protection from failures as follows: (i) protection switching where a pre-computed alternative path (usually disjoint from the working path) is set up for every flow, and (ii) rerouting where an alternative path is dynamically recomputed after a fault is detected. For both techniques, the alternative path can be either global or local.

The Internet has emerged as the network of choice for providing these converged services. However, there is high demand on the network by these newly developed applications and services, in terms of speed, reliability, connectivity, bandwidth and accessibility it has strained the resources of

the existing Internet setups. This revolution of the network toward a packet and cell based setup has made uncertainty in the conventional network. There are timely deliveries of data without exploitation of all the available resources is very much essential in vital application scenarios to a group of destinations (multicasting). Efficiency, simplicity, control overhead, resource management, quality of service (QoS) and robustness are the characteristics of good multicast routing protocols.

The motivation for this work is to overcome the shortcomings of the previously proposed schemes for the network restoration mechanism in Multicast MPLS networks during link/node failure. Currently there are many algorithms that can be used to reroute traffic fast when a fault occurs in the MPLS domain, but there is still the problem of packets drop. Therefore, there is need to have an algorithm have will prevent packet drop or data loss.

Gobinath and Tamilarasi (2020) presented a vigorous failure node detection module for detecting link and node failures. A dynamic routing path was determined through the Lyapunoy optimization technique, it used path switching which caused increase in delivery time and energy used during transmission.

Masdari and Özdemir (2020) introduced a distributed fuzzy logic algorithm for fault node detection in Wireless Sensor Network (WSN). It computes a weight factor based on the distance, and sensed values for determining and replacing the faulty nodes. The rate of accuracy of detection of failed node was very small.

The Concept of Multi-Protocol Label Switching Recovery

Multi-Protocol Label Switching (MPLS) is a protocol which is used to strength the Internet Protocol (IP) network. Arunkumar (2014), MPLS is an architecture developed to combine the dynamic nature of IP routing protocols and the efficiency of label switching. MPLS facilitates the use of QoS routing strategies (Ridwan *et al.,* 2019), it is promising solution for the growing number of applications that require different QoS treatments that share the same core network (Dinu, 2020). When a packet enters the MPLS network the router that receives it, and add a label or tag to it. The label is based on certain criteria's like the IP address of the recipient and it is used to route the packet through the next routers. Before the packet leaves the MPLS network, the last router is responsible to remove the label. The MPLS path is determined only when the packet enters the MPLS network. The routers at the length of path do not take any routing decisions they only use the label of the packet as an index to an array which indicates the next router. Also the router must switch the label of the packet, before sending it to the next router. MPLS is one of the most critical high-speed networking technologies and is connection oriented, which implies greater sensitivity to faults, particularly to interruption of services. IXIA report (2014) affirmed that this connection-oriented architecture opens the door to a wealth of new possibilities for managing traffic on an IP network.

MPLS technology gives network operators a great deal of flexibility to divert and route traffic around link failures, congestion and bottlenecks. MPLS does not replace IP routing but works in collaboration with existing and future routing technologies to provide high speed data forwarding between Label Switches Routers (LSRs) together with reservation of bandwidth for traffic flows with different QoS requirements. MPLS will place a vital role in the routing, switching and forward of packets through the next generation network in order to meet the service demands by network users. Multicast

is a mode of communication that involves a sender to group of receivers, unlike broadcast that transmits packet to a group of receiver blindly, multicast then to check for the membership of a node before sending to it a copy of the packet. Hence for a node to receive a packet sent it must be a member of the group. Recovery algorithm is a pseudo code on the steps and actions to take when there is a failure on the network. A recovery algorithm could be reactive or proactive. Proactive is a measure that put in place before a failure occurs. For instance, a back-up path can be created to reroute packet(s) when failure occurs. While reactive is a measure that is taken only after a failure had occurred. Intrusion-free in the context of this research means that there is not cost implication for adding another component to the multicast group.

Related Works

Failure is detected by the end nodes for link failure and by upstream and downstream nodes for node failure. Rohan (2005), considered how the number of the nodes the would not receive a packet in the event of a failure in a network can be reduce and how a segment of the network can be alive by using a bi-directional back up path, rather than having the entire network paralysed. But failed to address the consequence of a node failing to receive packet after a broadcast, the implication is that there will a bridge of communication between the members of the multicast group since all will not have the most recently broadcast packet.

In networks today link and node failure cause disruption in the flow of packet on a network. There are two (2) types of recovery mechanism: protection and restoration. Protection is a proactive approach while restoration is a reactive approach to failure recovery. Me´rindol *et al*. (2011) discusses the basic K-Shortest Path First (K-SPF) algorithm and how to compute multiple paths to the destination. In the bird view model of a wireless sensor network maintaining connectivity between nodes is a big issue, for maintaining connectivity or avoiding congestion, the traditional ad-hoc routing algorithms are used when confronted with mobility. Kumaravel, *et al*. (2014) opined that the limited energy supply for the network devices is not considered by these algorithms i.e Distributed Actor Recovery Algorithm (DARA), Recovery through Inward Motion (RIM). The recovery of the MPLS network is based on the algorithm that is applied in order to detect the faults and route the data flow in an alternative path. Anuradha *et al* (2014), discussed and showed how nodes failure can be resolved by simply replacing a wireless sensor node with another active node. Li, *et al.,* (2021) proposed a Hybrid Link Quality Estimation-Based Reliable Routing (HLQEBRR) algorithm for wireless networks. HLQEBRR provides a recovery mechanism to detects node failure, which improves node recovery time and accuracy. HLQEBRR algorithm significantly performs better than Collection Tree Protocol (CTP) algorithm in terms of end-to-end delay and packet loss ratio, hence it is more reliable than CTP.

Architecture of MPLS Network

The Internet Engineering Task Force (IETF) introduced MPLS in 1997 to originally meticulously address MPLS development. A number of issues with MPLS networks were raised, which are:

a) Increasing scalability of network layer routing using labels to combine forwarding information.
b) Increasing flexibility in routing services using labels to identify and direct traffic with QoS.
c) Applying the label exchanging pattern to enhance network performance in terms of packet delivery.

d) Incorporating Router with cell switching-based knowledge using common addressing, routing and management mechanism.

Advantages of the MPLS Networks

The MPLS mechanism can channel different categories of traffic through the central network. A channel is the path where traffic flows in the network. Channelling is very important in MPLS because only ingress and egress routers that need to know the content of traffic transmitted, other routers in the network are not in the know of the packet contents. Channelling in MPLS makes traffic to be explicitly routed by certain traffic guidelines. It also offers extra protection against data lost, since packet enters only via ingress routers.

MPLS provides the network with cost reduction by allowing network operators to switch a single network to offer different service types (Minei and Lucek, 2011). This feature is crucial due to emerging local network providers' applications which are becoming more condensed in terms of traffic routing and bandwidth depletion. Minei and Lucek (2011), MPLS overhead, which is just 4 bytes per MPLS header, is small and will decrease latency and workload in complex network.

MPLS Protection and Restoration

MPLS network traffic should delivered messages to its destination with zero packet loss and low latency (Cao, Rouskas, Wang, *et al.,* 2013), hence, ensuring that MPLS networks have high packet delivery ratio. This is because of the bandwidth and real-time contents vital applications, with this, data integrity can be guaranteed. There should be no form of data discrepancy from the source to the destination of the network. MPLS networks should have protection and restoration mechanism, which is capable of handling node and link failures (Alouneh, *et al*, 2009).

Timely recovery after a failure is essential, particularly for networks with applications of different priority parameters. Cao *et al*. (2013) introduced MPLS fast reroute (FRR) to offer a guarantee for MPLS pathways when failure occurs. It was the same concept as that obtainable by synchronous optical networking (SONET) automatic protection switching (APS). The major difference between FRR and SONET APS is that FRR can unfailingly provide a lower recovery time because the recovery mechanism is employed locally.

An effective network's recovery mechanism depends on its ability to detect failure in relatively short time and redirect traffic to an alternative path or channel. Timely failure discovery is an important feature of MPLS protection. It can be carried out either through hardware-based methods, such as using packet-over-SONET/synchronous digital hierarchy (SONET/SDH), or non-hardware-based techniques, such as the implementation of an algorithm at a layer in the network (Virk and Boutaba, 2006). For MPLS protection to the effective, it should be able implement both fault detection and fault notification. There are two (2) approaches to protection; end-to-end protection and FRR. End-to-end protection is used mainly in network deployment.

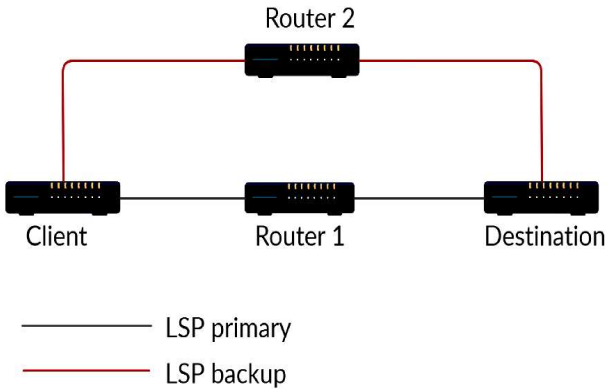

Figure 1: End-to-end protection using the backup LSP
Source: Ridwan, *et al.,* (2019)

Figure 1 demonstrations how label switch path (LSP) protection is realised using a primary and backup LSPs. The backup LSP receives traffic in the event of primary LSP link failure. Upon receiving the resources reservation protocol (RSVP) error at the client's node, the primary LSP redirects traffic to the backup LSP (Calle, Marzo and Urra, 2004). One weakness of this protection mechanism is continuously transmission of traffic over the dead or failed primary LSP until the RSVP error stretches the head end, thus producing delay and data loss. The advantage it has is that there is information about the new pathway for traffic due to the failure. Conversely, the backup LSP path must not be linked to the same main router (Router 1). Protection cannot be provided whenever Router 1 fails and intrusion occurs in both backup and primary LSPs. Hence, there is the need to have multiple path diversion within a network.

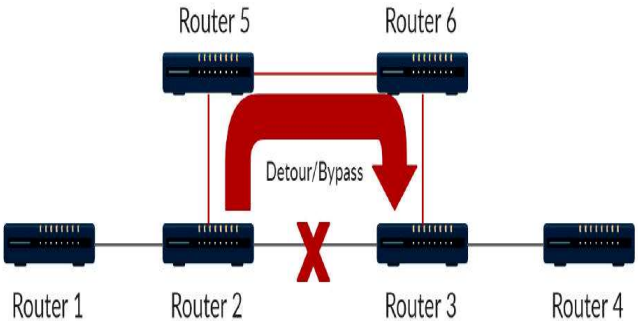

Figure 2: FRR protection by using the detour/bypass LSP
Source: Ridwan, *et al.,* (2019)

FRR protection aims at minimising delay when there is traffic failure. Figure 2 demonstrates how traffic at the failed link is redirected rather than having a protective framework at the end of the entire route. The improvement on FRR is that the network can decide which resources to protect. In the event of failure, protection can be done quickly, as traffic is forwarded to the rerouted path. There are four kinds of local protection namely:

a) Link protection
b) Node protection
c) One-to-one protection
d) Facility protection

The ability to keep traffic from being sent to the LSP in the occurrence of failure along the LSP is referred to as ‘‘link protection’’. For link failure protection, a standby route was established around the link for one-to-one protection. The most common kind of failure in any network is the link failure. A link can fail when the link itself is faulty or the other link-end has node failure, thus cutting off other segment of the network. Local protections have its pros and cons.

A standby path should be set to forward traffic as soon as there is failure detection for guarantee swift protection. For this to be obtainable, all standby paths need be work out and signalled in advance, and the dispatching state must be structure for switching. The dispatching state need be positioned at the head and tail or the merge point (MP) of the standby channel or point of local repair (PLR) to facilitate dispatching of traffic to the standby at PLR, then return to the main LSP at MP (Minei and Lucek,2011).

For MPLS network, LSR transmits packets via label or tag switching, while re-direction resolutions are keep into MPLS tags for safety. Thus, ensuring that the same traffic tags arrive both the standby tunnel and the failed link.

Figure 2 demonstrations how label or tags of data to be transferred to Router 3 through Routers 2 and 6 is the same. If the standby channel tag is pushed on top of the secure LSP tag at PLR (Router 2) and penultimate hoppopping (PHP) must be done to the backup tunnel tag, then traffic will arrive at MP (Router 3) with the accurate tag, before MP.

A network is scalable if it allows for easy expansion and effective data delivery among host nodes. Scalability is a very vital issue which must be addressed for there to be local protection with a network. For enhance protection more outline and computation of manual route must be done. Though, recent computation and establishment of route are carried out with dynamism. The complexity of deploying a network affects the level of resources protection, a network with high deployment complexity with lead to increase data forwarding. Hence, local protection comes at a price, it is therefore important to have the knowledge (Minei and Lucek, 2011).

MATERIALS AND METHODS

Software Requirements

The JDK (Java Development Kit) software was downloaded from the internet and installed first on the system, before Java compiler (net beans version 11.2) was then be installed. For the fact that, setting using a real world scenario for the network will be capital intensive we will use simulation for the research. It will help us to understand how the network performs in a real time situation.

JDK is a program development environment for writing Java applets and applications. It consists of a runtime environment that is ‘‘sit on top’’ of the operating system layer as well as the tools and programming that developers need to compile, debug and run applets and applications written in Java language. So in built classes from JDK were imported into Java and used for this research.

Java programming language was used for the simulation. It is a discrete-event network simulator targeted primarily for research and educational purpose. It presented how packets are transmitted between nodes in a network.

Network Architecture

A Network with tree topology was simulated, with a depth of two (2) and each parent node can only have a fixed number of children (nodes) that receive the packet send via the network from the parent. The number of nodes in our network is twenty one (21), it has a small size, for the scope of the work the

maximum level or depth of the tree is two (2). The packet will be broadcast from the source (root node) to every member of the network to have a copy. While the broadcast is on a daemon (a program that works underneath) will also be launch so as to randomly deactivate a link and a node. thereby making it to fail, this same daemon will also reactivate the link and node (transceiver and power unit) failure. This will ensure that a no point in time the traffic of the network will be brought to a halt.

Algorithm

The algorithm uses a Boolean value 0 or 1 to signify that a link or a node is either alive or dead. For any link or node that returns a 0 when a parameter is passed. The program will have to active it likewise for if it returns a 1 to program may choose to deactivate it. The algorithm was latter implemented using Java programming language. Before then JDK (Java Development Kit) software was first installed on the system. JDK is a program development environment for writing Java applets and applications. It consists of a runtime environment that is ‘‘sit on top’’ of the operating system layer as well as the tools and programming that developers need to compile, debug and run applets and applications written in Java language. When a node did not receive a packet due to link failure, it loops between the children (nodes) for which it is of the same parent with node id from 0 to n (where n is the number of children at a particular level on the tree) in other to get its own copy of the packet. What this implies is that a node will always be available to help other siblings of it when there is a failure in that branch of the tree. Hence, a branch of the network will never be caught off during the broadcast.

RESULT AND DISCUSSION

Algorithm

```
1 # variable declaration
2 leaf_level = 3                    {the level of the tree Network topology}
3 global data =""          {the message to be broadcast}
4 node_index;              {the identification number of the node}
5 link_id;
6 Nodes // an array of all nodes
7 LINK_STATUS_REGISTRY  //an arraylist of Links status
8 NODE_STATUS_REGISTRY  //an arraylist of Nodes status
9 # end of variable declaration
10 BEGIN
11   startDaemon()      {the program that works underneath}
12       for i=0 to leaf_level
13           start_thread
14       num_children = 4^(i+1)
15       node_index=getLiveNode(i)
16       link_id=getLiveLink(i)
17       if node_index >= 0 then
18           //at least one or more node(s) and link at this level is up
19           node=Nodes[i][node_index]
20          storeData(node)
21       else
22          // all nodes at this level are down
```

```
23          dead end for data routing  //reserved for future works
24        endif
25        end_thread
26    endfor
27 END
28 // BEGINING OF SUBROUTINES DECLARATION
29 /* Daemon operation:  */
30 void SUBROUTINE startDaemon()  { activate and deactivate links and nodes }
31  BEGIN
32  while programme is running
33      for i=0 to leaf_level
34              node=Nodes[i]
35              if getLiveNode(i)= 0 then
36             activate node //power unit & transceiver
37           endif
38           if getLiveLink(i)= 0 then
39              activate link //transmission media
40           endif
41           int r=rand(0, 3)
42           disableNode(leaf_level, r)
43           sleep(1000)  //waits for some milliseconds before doing other tasks
44           int k=rand(0, 3)       {random deactivate a link}
45           disableLink(leaf_level, k)
46      endfor
47    endwhile
48 END
```

Table1: Showing the number of broadcast made against the recipients

No of broadcast	Recipients without recovery	No of failed nodes	Nodes expected to receive	Nodes that eventually received
1	16	4	20	20
2	33	7	40	40
3	49	11	60	60
4	66	14	80	80
5	73	27	100	100

Behaviour of the Recovery in different Scenario

The research was evaluated with Li *et al.,* (2021); which came up with HLQEBRR as a better failure recovery mechanism when compared with CTP. The evaluation was carried out with and without failure recovery mechanism in place. From table 2 and table 3, MPLSR outperform HLQEBRR and CTP, however it losses time since there is increase the average end-to-end delay.

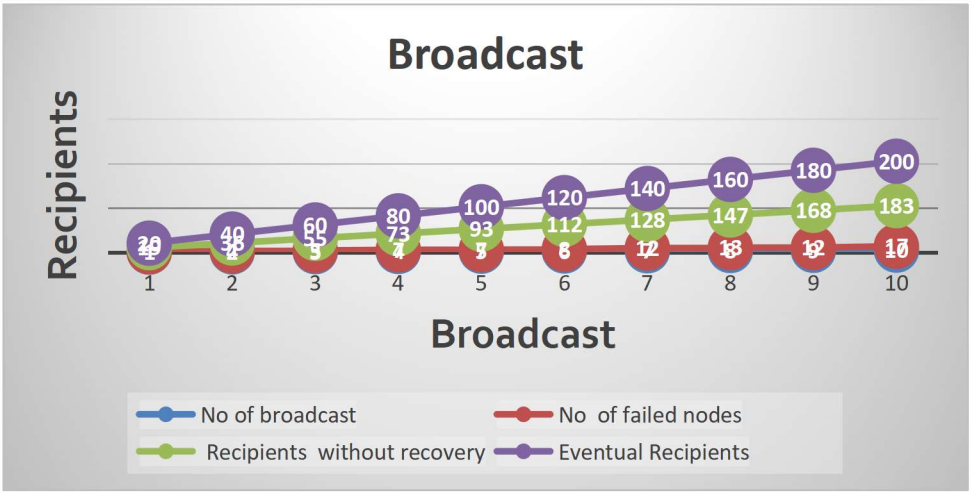

Figure 3: Shows number of Broadcast against Recipients

Table 2: Performance of the entire network with failure without restoration

Routing Mechanism	Average delivery rate	Average end-to-end delay	Total number of packets
HLQEBRR	82.4%	0.0629 s	13039
CTP	83.7%	0.0624 s	12980
MPLSR	79.92%	1.0000s	14500

Table 3: Performance of the entire network

Routing Mechanism	Average delivery rate	Average end-to-end delay	Total number of packets
HLQEBRR	99.5%	0.0965 s	15193
CTP	90.7%	0.0874 s	14690
MPLSR	100%	5.0000s	16256

CONCLUSION

Different approaches and routing protocol have been designed and deployed to tackle must of these challenges, all in a view to make the Multicast MPLS network more efficient and reliable. Yet there is no perfect network, so work still needs to be done in these areas. This prompted the need to have a Multicast MPLS network that reduces the number of failed routers (nodes), reduce end-to-end delay and guarantee packet delivery. Packets should not only arrive at the destination, but it should arrive in good time and in the correct order so as to make a meaning. Node failure is a little more complex than that of link. Link failure can simply be solved by creating a bath up path through which the traffic of the packet could be rerouted i.e., seeking for alternative link. But for the case of a node failure the node has to be given immediate attention. Since it serves as route for which packets are sent. Finally, there is need to further improve this research, by working on the area of its limitation; end-to-end delay. If this can be addressed, MPLSR will be a more efficient recovery mechanism.

REFERENCES

Alouneh, S., Agarwal, A., & En-Nouaary, A.(2009) 'A novel path protection scheme for MPLS networks using multi-path routing', *Comput. Netw.*, 53, (9), pp. 1530–1545.

Arunkumar, C. K. (2014) An Efficient Fault Tolerance Model for Path Recovery in MPLS Networks. *International Journal of Innovative Research in*

Computer and Communication Engineering. 2(6).

Awoyemi, B. S., Alfa, A. S., & Maharaj, B. T. (2018). Network Restoration for Next-Generation Communication and Computing Networks. *Journal of Computer Networks and Communications, 2018, 1–13.*

Barakabitze, A.A., Sun, L., Mkwawa, I., & Ifeachor E. (2019). *Multipath Protections and Dynamic Link Recovery in Softwarized 5G Networks using Segment Routing*, Imperial College London.

Calle, E., Marzo, J.L., & Urra, A. (2004): 'Protection performance components in MPLS networks', *Comput. Commun.*, 27, (12), pp. 1220–1228.

Cao, C., Rouskas, G.N., Wang, J., & Tang, X. (2013): 'Hybrid FRR/p-cycle design for link and node protection in MPLS networks', *AEU - Int. J. Electron. Commun.*,67(6), pp. 470– 478.

Cheng, Z., Zhang, X., Li, Y., Yu, S., Lin, R., & He, L. (2017). Congestion-Aware Local Reroute for Fast Failure Recovery in Software-Defined Networks. *Journal of Optical Communications and Networking, 9(11), 934.*

Cho, C., & Ryoo, J. (2020). Minimizing Protection Switching Time in Transport Networks with Shared Mesh Protection. *International Journal of Network Management*.

Deepa, O., & Suguna, J. (2017). An optimized QoS-based clustering with multipath routing protocol for Wireless Sensor Networks. *Journal of King Saud University - Computer and Information Sciences.*

Dinu, T. (2020). Quality of Service in MPLS Networks, *Journal of Engineering Science, 27 (3), 102 – 110.*

IXIA White paper 2014. Multi-Protocol Label Switching (MPLS) Conformance and Performance Testing.

Jamoussi, B., Andersson, L., Callon, R., Dantu, R., Wu, L., Doolan, P., Worster, T., Feldman, N., Fredette, A., Girish, M., Gobinath, T.,& Tamilarasi, A. (2020). RFDCAR: Robust failure node detection and dynamic congestion aware routing with network coding technique for wireless sensor network, Peer-to-Peer Networking and Applications 13 (6), 2053–2064.

Johan, M.O.P (2005). MPLS Based Recovery Mechanisms. Master thesis, University of Olso, Norway.

Kumaravel, K Sabu, M., & Marimuthu, A. (2014). Optical Routing Algorithm used in Wireless Mesh Networks for Energy Efficiency. *International Journal of Engineering Science & Research Technology*, Vol 3(1).

Lemma, H.G. (2003) ''*Enhanced Fast Rerouting Mechanisms for Protected Traffic in MPLS Networks*'', PhD Thesis, Technical University of Catalonia, Barcelona, Spain.

Li, J., Lee, G., Roh, B., Ryu, D. K., & Park, G. (2020). Software-Defined Networking Approaches for Link Failure Recovery: A Survey. *Sustainability, 12(10), 4255.*

Li, J., Pan, Y., Ni, S. & Wang, F. (2021). A Hybrid Reliable Routing Algorithm Based on LQI and PRR in Industrial Wireless Networks. *Hindawi Wireless Communications and Mobile Computing*.

Masdari, M. & Özdemir, S. (2020) Towards coverage-aware fuzzy logic-based faulty node detection in heterogeneous wireless sensor networks, *Wireless Pers. Commun*. 111 (1), 581–610.

Mérindol, P., Francois, P., Bonaventure, O., Cateloin, S., & Pansiot, J.-J. (2011).

An efficient algorithm to enable path diversity in link state routing networks. *Computer Networks*, 55(5), 1132–1149. Minei, I., & Lucek, J.(2011). '*MPLS-enabled applications: emerging development and new technologies*' John Wiley & Sons Ltd, UK.

Ridwan, M., Radzi, N., Ahmad, W, Abdullah, F., Jamaludin, Z. and Zakaria, M. (2019). Recent trends in MPLS Networks: Technologies, Applications and Challenges *Submission Template for IET Research Journal Papers ,. Disponibil.*

Schüller, T., Aschenbruck, N., Chimani, M. and Horneffer, M. (2021). Failure Resiliency With Only a Few Tunnels – Enabling Segment Routing for Traffic Engineering, IEEE/ACM *Transactions on Networking,* 29(1).

Thomas. K. Multicasting: From Fixed Networks to Ad-hoc Networks. In Handbook of Wireless Networks and Mobile Computing. Ivan Stojmenovic (ed). Pages 495-507,John Wiley & Sons, ISBN 0-471-41902-8, 2002.

Tong, M., Chen, Y., Chen, F., Wu, X., & Shou, G. (2015). An Energy-Efficient Multipath Routing Algorithm Based on Ant Colony Optimization for Wireless Sensor Networks. *International Journal of Distributed Sensor Networks, 11(6), 642189.*

Vanamoorthy, M., & Devendran, V. (2019). Congestion-Free Transient Plane (CFTP) Using Bandwidth Sharing During Link Failures in SDN. *The Computer Journal.*

Virk, A.P.S. & Boutaba, R.(2006). Economical protection in MPLS networks. *Comput. Commun.*, 29(3), pp. 402–408.

Waleed, S. and Faizan, M., and Iqbal, M., and Anis, M. I. (2017). Demonstration of single link failure recovery using Bellman Ford and Dijikstra algorithm in SDN. *International Conference on Innovations in Electrical Engineering and Computational Technologies* (ICIEECT).

Su, Y., Meng, X., Kang, Q., & Han, X. (2018). Dynamic Virtual Network Reconfiguration Method for Hybrid Multiple Failures Based on Weighted Relative Entropy. *Entropy, 20(9), 711.*

Zeng, G. and Wang, B. and Ding, Y. (2010). Efficient multicast algorithms for Multichannel Wireless mesh networks, *IEEE Transactions on Parallel and Distributed Systems 21 (1) 86– 99.*

Zheng, Z.; Zhao, C.; Zhang, J. (2021). Robust and Fast Converging Cross-Layer Failure Correction in Segment-Routed Networks. Electronics 2021, 10, 2874.