IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering

ISO 3297:2007 Certified

Vol. 6, Issue 1, January 2017

Fast Re-Route Mechanism in Multiple Link Failure Environment in MPLS Network

Prof. Dipti Sonawane[1], **Mr. Mangesh T. Chaudhari**[2]

G.H. Raisoni College of Engineering, North Maharashtra University, Jalgaon, India[1, 2]

Abstract: Multiprotocol Label Switching (MPLS) is switching network and provides significant benefits to the network by fast forwarding Internet Protocol (IP) packets. MPLS is scalable network and which provides end-to-end quality of service (QoS), also it enables efficient utilization of existing networks. MPLS is implemented in Mobile Ad-hoc Network (MANET) environment, then there is need to control over this network because the nodes in the network can be move at any point of time in MANET environment. If link failure occur in the network, then there is need to tolerate this failed link packet. For to tolerate this failed link use MPLS Fast Re-route (FRR) mechanism. The MPLS FRR mechanism based two types local and global. The local FRR mechanism which tolerate single link instead of path of network which is in global. The MPLS FRR mechanism is based on preplanned established link in the network. If link failures occur then packet of failed link is switch-over to the backup path that is created initially. In the proposed system, existing link or local based restoration with fast re-routing (FRR) mechanism for MPLS network is used and then analyses the problem such as packet loss, packet reordering, delay and overhead in the network after link failure. This FRR mechanism provides fast traffic recovery when a link failure occurs, MPLS-FRR uses link based local restoration mechanism for each failure. The main focus of the proposed work is to select optimal backup link with FRR mechanism and bellman ford algorithm during link failure. The FRR mechanism with bellman ford algorithm can reduce packet loss ratio and delay in the network and this can be simulated through network simulator version 3(ns3).

Keywords: MPLS, FRR, ns3, MANET, etc.

1. INTRODUCTION

Multiprotocol Label Switching (MPLS) is the backbone network for IP domain and it is the new fastest growing communication network to enhance the speed, scalability of network. MPLS network has feature is that it support traffic engineering tunnels by avoiding congestion and utilizing all the available network bandwidth with an efficient way. The main functionality of Traffic Engineering [13] of MPLS network is resource reservation, fault-tolerance and optimal Resources utilization. Multiprotocol Label Switching technology (MPLS) allows traffic engineering (TE) and enhances the performance of the existing protocols over the traditional IPv4 network. It is foreseen that MPLS will be chosen as the bearer of IP network in future large backbone networks. The main focus of MPLS network is to attach a short fixed-length label to packets at the ingress router of the MPLS domain. The packet forwarding in network depends on the tagged label, not on longest address match, as in traditional IP forwarding. A router or nodes placed on the edge of the MPLS network called Label Edge Router (LER) that is associated to a label on the basis of a Forwarding Equivalence Class (FEC). In the MPLS network, internal routers that perform swapping and label-based packet forwarding are called Label Switching Routers (LSRs).

MPLS Architecture:

The operation of MPLS network such as classification and identification of IP packets at the ingress node or router with having short, fixed-length size, and locally significant identifier called a label, and forwarding the IP packets to a router that are modified to operate with such labels. The modified routers or nodes use only these labels to switch or forward the IP packets through the network and do not use the network layer addresses.

From this MPLS architecture [15], the forwarding of IP packets in MPLS network is done by using the label in the MPLS header. MPLS header has to be inserted into IP packets that are to be routed in the MPLS domain. For data link layer switching technologies like ATM, the MPLS header is inserted in the native label field for that protocol. In the case where the Layer 2 technology does not support a native label field, the MPLS header [14] must be inserted between the Layer 2 and Layer 3 headers of TCP/IP layer.

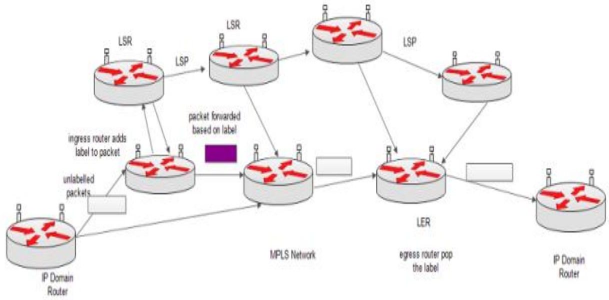

Figure 1: MPLS Architecture

DOI 10.17148/IJARCCE.2017.6115

IJARCCE
ISSN (Online) 2278-1021
ISSN (Print) 2319 5940
International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 6, Issue 1, January 2017

1. MPLS Label:
This MPLS header is 32 bits long and is often called ”shim” header or MPLS label. The MPLS header contains four fields such as. The label is 20 bit, the 3 bits for experimental which defines the class of service used and Explicit Congestion Notification (ECN) bits for alert message when there is congestion in the MPLS network then this bit is set to 1 otherwise the bit is not set. Third field for label stack bit if it set to 1 then there is label in the label stack. The last field is Time to Live (TTL) which indicates the total time taken by an IP packet to travel or valid time for IP packet in the MPLS network.

Label	Exp.	S	TTL

Figure 2: MPLS Label

Where;
32 bit MPLS label
Label: label value, 20
Exp: experimental, 3 bits (was class of service)
S: Bottom of stack, 1 bit (1= last entry in label stack)
TTL: Time to Live, 8 bits

2. Forwarding Equivalence Class (FEC):
In MPLS network, all IP packets that are forwarded over the same path and treated in the same manner belong to the same class or FEC. The traffic flows or set of packets that are aggregated in MPLS are called an FEC. There should be a FEC to assign any unlabeled incoming packet into a group or class that will become MPLS labeled packets. MPLS FEC membership is not strictly based on shortest path first (SPF) destination address calculations as in IP, but can be determined based on other parameters such as packet source, and some QoS parameters found in the network, transport and application headers. The classification is based on the five-tuples (source and destination IP addresses, source and destination Transmission Control Protocol (TCP) or User Datagram Protocol (UDP) ports, and a protocol number). This results in fine-granularity FECs of packets. If the classification of packet is based just on the destination IP address, then the resulting FECs are of medium-granularity. If the FEC classification of packet is based on the egress LSR, this creates coarse-granularity FECs.

3. Label Switched Path (LSP):
When an IP packet traverses through a MPLS domain, it follows a predetermined path or LSP depending on the FEC to which it was assigned by the ingress LER. The path the packet or traffic follows through the MPLS domain is called the Label Switched Path (LSP). LSPs are unidirectional so to build a duplex communication two LSPs are needed for that network. When various Layer 3 packets are entering the Ingress LSR, they are classified based on FEC. Once the packets are classified, they are forward to respective LSP for this FEC. An LSP may carry more than one FEC classes. The packet is forwarded based on the information in the MPLS header available and the interface that the packet arrived on, which is used as an index in table lookups. There are three types of operations that can be applied to incoming IP packet such as Push the label stack, Swap the top label with a new label and Pop the label stack.

4. Label Switch Router (LSR):
A Label Switch Router (LSR) is a device that is capable of forwarding packets at layer 3 and forwarding frames that encapsulate the packet at layer 2. It is both a router and a layer 2 switch that is capable of forwarding packets to and from an MPLS domain. The edge LSRs are also known as Label Edge Routers (LERs). The ingress LSR pushes the label on top of the IP packet and forwards the packet to the next hop.

5. Label Edge Router (LER):
End routers in the MPLS network are called LER; there are types of LER routers such as Ingress router and Egress router. The ingress router is the start node of MPLS network and egress is end router of MPLS network.

6. Label Distribution Protocol (LDP):
In MPLS, two adjacent Label Switching Routers (LSRs) must agree on the meaning of labels used to forward traffic between them and through them. The label distribution protocol (LDP) is a protocol for distributing labels in MPLS network. LDP is a set of procedures and messages by which LSRs establish Label Switched Paths (LSPs) through a network by mapping network layer routing information directly to data link layer switched paths.

2. LITERATURE SURVEY

2.1 Existing Systems:

There are some recovery models are present for link failure environment. If occur in the network while packet transmission then there are some possible models which are either on path or link based or node or router based. Some of the existing solutions for path and link failures as follow. There are various re-routing methods used in MPLS network for tolerate failed link such as dynamic routing, Haskin’s proposal and Makam’s proposal, etc. These methods can be useful during link failure but this method has some advantages and disadvantages which are discussed as follows.

1. Haskin’s Proposal:
This is useful method when there is failure occur in the network. This method establishing the preplanned alternative or backup link or Label Switching Path (LSP) from the ingress Label Switching Router (LSR) [10]. This mechanism work when failure occur is when packet is forwarding to the link and if failure occur in the link then this mechanism returns the packets from faulty point to the ingress LSR and these re-route them to the alternative LSP together with incoming traffic. This resulting that there is

minimum packet loss and maximum packet disordering. In this mechanism there is no optimal path to select and there is only one alternative available for switch-over the packets. This mechanism having more resource requirement due to preplanned edges are used for switch-over the packets.

2. Makam's Proposal:
This mechanism also based on preplanned alternative LSP from the ingress LSR. This mechanism uses notifications messages to the ingress node after a failure to re-route traffic from the ingress LSR to previously established alternative LSP [11]. This mechanism will result in higher packet loss and minimum packet disorder. If packet loss is more than the packet disorder is less and vice-versa. This mechanism having more complexity due to use of more notifications messages at ingress router. This mechanism does not have an optimal path or link for forward or switch-over the packets while failure of link. This also exist only one alternative link for to protect a failed link. This mechanism has low resource requirements. This mechanism generates one only message for each LSP and which makes reduce the number of messages.

3. Dynamic Re-routing:
This mechanism work based on the current situation of the network. The re-routing can be possible when there is failure occur [12]. When failure occurs then node uses messages flooding to locate the backup or alternative link to route that can bypass the failed link or route. This mechanism dynamically searches the backup link, then decides and generates the alternative or backup link or LSP when there is failure occur. This mechanism having more complexity due more messages where generated while failure occur. This mechanism can have more packet loss during searching for backup link in the network. There is no guaranteed that the optimal path or link is found in the network. The resource requirement is very less as this mechanism is based on dynamically searches its backup link when failure occurs.

In paper [1], depicts that for protecting a link failures use a MPLS Fast Re-route (FRR) mechanism. FRR mechanism has two approaches such as link based or local and other one is path based approach. In path based restoration approach, if single link failure occur then there need to re-route entire flow in the network. While in link based or local approach, backup path created for each link and if link failed then this link based restoration only replace this failed link with backup path without changing the rest of the route. This paper depicts that the main objective is to maintain the connectivity after multiple failures without causing congestion. For distributing state information or routing use some routing protocol such as open shortest path first (OSPF) and also reconfiguring backup paths use some distributed algorithm.

In paper [2], depicts that integrating the layer-II label-switching technique with the layer-III ad-hoc routing and analyze the effect of Multiprotocol Label Switch (MPLS) mechanism on the performance of Mobile Ad-Hoc Network (MANET). This integration of MPLS in MANET shows some effects on the QoS parameters such as throughput, delay, packet loss ratio and these number of effects can be analyzed be using some simulation tools. Some of the routing protocols to be consider for in MANET environment such as Ad-hoc On-demand Distance Vector (AODV), Dynamic Source routing protocol (DSR) for distributing state information to a destination. These routing protocols reactive that is on demand.

In paper [3], that fast re route mechanism is beneficial over a link based or local based restoration. This paper addresses the hybrid combination of p-cycles and FRR mechanism. While using only FRR backup paths are planned for each network link, the hybrid scheme selects backup paths embedded within a set of p-cycles; this is based on holistic view of network performance that is selecting the LSP which is less congested or less traffic available on that LSP. This FRR protection is special case of p-cycle scheme because p-cycle scheme is a set of cycles are defined over the whole network such that each link is either on-cycle link or a straddling link (i.e., a link that connects two nodes on the same cycle but is not itself part of the cycle). Hamiltonian p-cycle created for whole network for used to protect all links.
This scheme uses backup paths along a set of pre-configured p-cycles that can be selected using design methodologies that consider the overall network performance. The benefits of the hybrid scheme increase with the density of the network; hence adopting a p-cycle design is an attractive alternative for MPLS network operators.

In paper [6], depicts that Fast-reroute mechanism especially for establishing backup path while link failures, but it is not effective for multiple failures frequently occurring in backbone networks. Here consider a protocol to reconfigure impacted backup paths after a link failure, improving survivability from a subsequent failure. Backbone network, router-to-router links carry the traffic of multiple end-to-end connections. If link failure occurs then all the connections traversing it that failure link also fails. The main focus is on recovering end-to- end connections using path protection techniques. Although path protection is efficient in resource utilization, it has the disadvantages of higher complexity, poor scalability and large recovery times requires. In link protection using MPLS fast reroute is to pre-compute alternate paths to handle dual-link failures, they are more complex. Because a first link failure may affect the backup path of a other link, the precomputed backup paths for each link would have to consider all possible combinations of failures of other links.
This paper also addresses, cross-layer reconfiguration technique is used to improve survivability from a subsequent link failure occur in the MPLS network. Here

DOI 10.17148/IJARCCE.2017.6115

IJARCCE
ISSN (Online) 2278-1021
ISSN (Print) 2319 5940
International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 6, Issue 1, January 2017

uses OSPFTE and RSVP and is a natural extension to the MPLS fast-reroute. The main focus is that each node running a simple reconfiguration algorithm independently. Further we can deal with multiple concurrent failures in a scalable and adaptive manner by exploiting the capability of Layer 3 protocols (OSPF) to disseminate (spread information) the backup path information for a failed link, so as to reconfigure other backup paths.

In paper [7] depicts that in Multiprotocol Label Switching (MPLS) network if any link failed then there is need of re-routing the Internet Protocol (IP) packets of failed link to different link. For that MPLS Fast Re-route (FRR) mechanism is used to forward the failed link packets to alternate link or path. There are various methods of FRR that find an alternate path after a link failure from a source node to a destination node before the OSPF used to re-converge in response to the failure. Some of the methods of FRR as conjunction with label-based forwarding (LDP) which creates an RSVP primary tunnel between each pair of nodes, Loop Free Alternative (LFA) method and extension of the basic LFA methodology is the u-turn method, Recursive Loop-Free Alternative (RLFA) method, Centralized alternate routing methods, Multiple Routing Configurations (MRC) method computes a set of backup configurations.
The time for an IGP to reconverge after a link failure can be hundreds of milliseconds; the method not requiring tunnels is much simpler. The alternative of storing precomputed paths requires preprocessing and storage requirement for these alternate paths.

2.2 Comparative Analysis:

Re-routing methods/Parameters	Delay	Packet loss Ratio	Packet re-ordering	Optimal path option	Resource Require-ment	Complexity	Protection for protected LSP
Fast Re-Route (FRR)	Less	Minimum	More	Yes	More, if not shared	If failure is not occur then there is much more complexity	More alternatives or backup links
Dynamic Re-routing	Less	Much more	Less	Depends on path selected	Minimum due to dynamic in nature	More complexity because it uses notification messages at ingress router in run time.	Need to search dynamically and generate
Makams proposal	Less	High	Minimum	No	Minimum	High (it uses notification messages at ingress router if failure occur)	One alternative
Haskins method	Medium	Minimum	High	No	Same as FRR plus backward LSP during recovery time	It is similar to FRR but it select backward path also so it slightly more complex than FRR.	One alternative

Figure 3: Comparative Analysis of various re-routing mechanisms

In this literature we study the existing re-routing methods for Multiprotocol Label Switching (MPLS) network for tolerating link failures. In MPLS network, routing methods used to avoid some amount of IP packet loss due to link failure. The re-routing for failed link can be possible with the help of simulation tool called network simulator version 3 (ns3). Different re-routing methods compared in this survey are Fast Re-Route (FRR), dynamic re-routing, Makam's proposal and Haskins method. These different re-routing methods compared based on Quality of Service (QoS) parameters such as delay, packet loss ratio, packet reordering, optimal path option, resource requirement, complexity etc.

3. PROPOSED SYSTEM

3.1 Problem Statement:
To design network in MANET environment for selection of optimal link based on MPLS Fast Re-route mechanism and bellman ford algorithm for to tolerate packet loss ratio of a failed link.

3.2 Proposed Hypothesis:
Implement a MPLS Fast Re-route (FRR) mechanism in MANET for link failure environment. This can be done by configuring backup paths to each node in the network. The main objective of this proposed work is to select a optimal link after a link failure occur. The optimal link selection can be possible with the help of bellman ford algorithm which select shortest path based on the cost of link. Finally the network will have less packet loss ratio and delay. This is done through a network simulator version 3 tools (ns3).

3.3 Overview:
Fast Re-Route (FRR) is a mechanism for protecting MPLS Traffic Engineering (TE) label switched paths (LSPs) from link failures by locally repairing the LSPs at the point of failure, allowing data to continue to flow on them while their head-end routers attempt to establish new end-to-end LSPs to replace them. FRR locally repairs the protected LSPs by rerouting them over backup tunnels that bypass failed links. Backup tunnels that bypass only a single link of the LSPs path provide Link Protection. They protect LSPs if a link along their path fails by rerouting the LSPs traffic to the next hop (bypassing the failed link). These are referred to as next-hop (NHOP) backup tunnels because they terminate at the LSPs next hop beyond the point of failure.

3.4 Methodology:
When the primary or main label switched path (LSP) encounters a problem due to link failure, the packet that travels it needs to be re-routed over an alternative or backup path (LSP). This is equivalent to using a new LSP to carry the packet or traffic. The backup LSP can be established after a protected LSP failure is detected, or it can be established beforehand in order to reduce the LSP switch-over time. The former option has a slow response in the re-routing function. The latter has a much better

IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 6, Issue 1, January 2017

response time. In our proposal we use the fast re-routing technique with pre-established backup LSPs to protect the packets travelling in the protected LSP.

In MPLS network contain Label Switching Routers (LSR) and aach LSR maintain Label Forwarding Information Base (LIB) for packet forwarding based on content of LIB entries. The LIB table mainly consists of various content such as incoming and outgoing interfaces and its labels. The field is that failure status of link which is either is ’Yes’ or ’No’. This failure status field indicates that there is failure or not if there is failure then the status field contains ’Yes’. After the status contain ’Yes’, then this point to the explicit routing information routing base (ERB) for checking which backup path is available. The ERB contains the Label Switching Path (LSP) ID, Forward Equivalence Class (FEC), Lib entry number and its available backup path or link is shown in Figure 6.1.

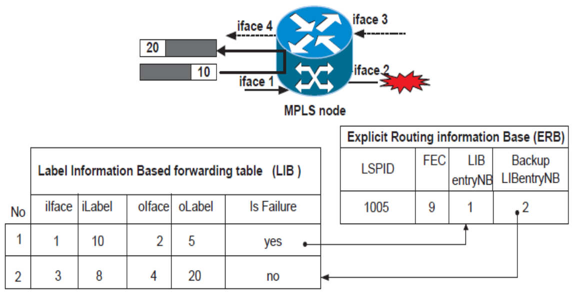

Figure 4: LIB entry with Backup paths

3.4.1 Fast Re-route (FRR) mechanism:

State Machine Diagram for Proposed Mechanism

It is important to take into account the modification we made in the label information base-forwarding table (LIB). We introduce a new field called STATUS in the LIB, and manage five states in this field. They are: NORMAL, FAULT DETECT, ALTERNATIVE DETECT, STORE BUFFER and SEND BUFFER.

NORMAL: This state corresponds to the normal operation condition. It means no fault is detected on the protected LSP: the LSR continues working in the normal condition.

FAULTS DETECT: As the name implies, this is the state to indicate the condition of a faulty link. The node becomes an alert LSR. When a tagged packet is forwarded through the backward LSP, or after a certain time depending on the implementation, the LSR removes the LIB entry.

ALTERNATE DETECT: This state is in charge of notifying the incoming protected LSP packets of the failure after receiving a packet from the backward LSP. It waits for the first packet coming through the protected LSP, which will be tagged and transmitted.

STORE BUFFER: This state is in charge of indicating the need to store packets travelling in the protected LSP after detecting the presence of packets through the backward LSP and sending the tagged packet to downstream LSRs. This avoids the unnecessary trip of packets downstream and back again.

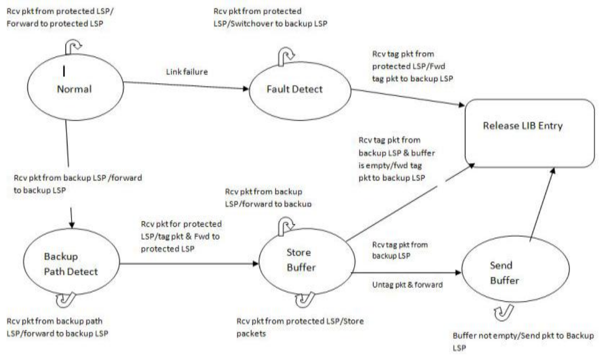

Figure 5: State Machine Diagram for MPLS FRR mechanism

SEND BUFFER: The state in which the stored packets (i.e., packets stored during the STORE BUFFER time) will be drained from the buffer to the alternative or backward LSP (if it is the ingress LSR or an intermediate LSR, respectively). This state is activated when the tagged packet is received at the ingress or at each intermediate LSR through the backward LSP. Figure presents the state machine diagram of the proposed algorithm. The ingress LSR forwards packets to the alternative LSP while the intermediate LSR forwards packets through the backward LSP.

3.4.2 Fast Re-route (FRR) mechanism in wireless environment

Step 1. Establish the link before failure occurs. As the Fast Re-route mechanism based on pre-computation of links n the network.

$$E=n(n-1)/2$$

Where:- E is the number of edges in the network, n is number of nodes in the network.

Step 2. The link failure detection can be done with the help of AODV (Ad-hoc On-demand Distance Vector Routing) protocol. The AODV protocol uses messages such as Route Request (RREQ) and Route Reply (RREP). The link failure detection can be done with RREP and RREP messages by broadcasting in the network.

Step 3. The MPLS LSR router maintains all the neighboring nodes information. This LSR also maintain a LIB table for all the connected interfaces with its label value. This LIB table pointed to the explicit routing information base (ERB) for storing backup links. This is done in network simulator version 3 (ns3) and trace metric tool. The bellman ford algorithm is used for shortest path or link selection in this mechanism. The bellman ford algorithm calculates the cost of link in wireless environment with the help of co-ordinate values of nodes. This bellman ford algorithm is explained in detail in section 6.3.3.

IJARCCE
ISSN (Online) 2278-1021
ISSN (Print) 2319 5940
International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 6, Issue 1, January 2017

MPLS FRR mechanism is best for when there is failure in MPLS Fast Re-Route mechanism considered performance parameters such as resource requirement, fault recovery time, packet loss ratio, packet re-ordering, complexity, distance between two routers, packet switchover time. This proposed work design with simulation tool such as Network Simulator version 3 (ns3). The Round Trip Time (RTT) for MPLS FRR mechanism is calculated based on transmission delay queuing delay and. propagation delay in the network. The transmission delay (TD) is calculated as

$$TD= P/B$$

Where:-P= packet size
B= LSP Bandwidth (peak rate)
The queuing delay is negligible so it does not consider.

The propagation delay (PD) calculated as

$$PD= d/v$$

Where:-d= distance between two LSRs
v= velocity or speed of packet travel through a LSP
The round trip time (RTT) or link delay can be calculated as

$$RTT= QD+ 2PD+ TD$$

The full restoration time need to calculate and also buffer size is maintained at ingress LSR. After detection of failure, the total times required by LSR detecting the failure and switch-over all packets including buffered packets and time for tagged packet to return to the immediate upstream node must be calculate. This is equal to link delay for first packet switched over to reach the upstream LSR along the backward LSP in addition to RTT or link delay for tagged packet to return to its LSR and switchover time (Ts) is calculated as

$$Ts= 3*RTT$$

Where:-RTT= 2PD+ TD+ QD
This is done by assuming queuing delay and processing delay are negligible

3.4.2 Bellman ford Algorithm:

The bellman ford is used for shortest path or link finding based on the cost of link. In wireless environment it is calculated with the help of co-ordinates of node in the network. The bellman ford algorithm also capable of negative edge calculation.
1. Let V be the number of nodes or routers in the MPLS network.
2. Let W be the weight of link or LSP of MPLS network.
3. Let u be the source node in the network This is shortest path finder based on link cost with negative edge weight cycle detection for v in V.

STEP 1
Distance [v] = 0 ————————-initially
else distance [v] = infinity
Predecessor [v] =null

STEP 2
Relax edges repeatedly
for i from 1 to size (vertices)-1:
for each edge (u,v) in graph with weight W in edges
if distance [u]+W = distance [v]
distance [v] = distance [u] +W
predecessor [v] = u ————————this is first node in the shortest path by bellman ford algo

STEP 3
check for negative weight cycles
for each (u,v) in graph with weight W in edges
if distance [u] +W < distance [v]
error graph contains a negative weight cycle
return distance [], predecessor []

The bellman ford algorithm work in wireless environment then there is need to find cost of each link. In wireless environment cost of link can be calculated with assigning co-ordinate values to the nodes in the network. After assigning co-ordinate to the nodes, the cost calculation of link as follows.

$$m1=\sqrt{(x1-x2)^2+(y1-y2)^2}$$

where:
m1 is co-ordinates of the neighboring node from the ingress LSR. The m1 is co-ordinates of node in the network and if the node m1 is in the radius of ingress router i.e. the m1 satisfy the following condition then only it treated as next node for forwarding packet with the help of bellman ford algorithm.
if(m1<=3.14)

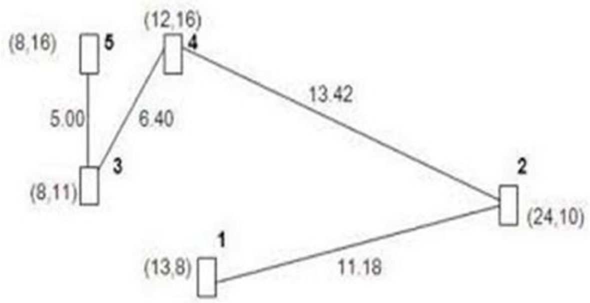

Figure 6: Distance calculation for bellman ford algorithm

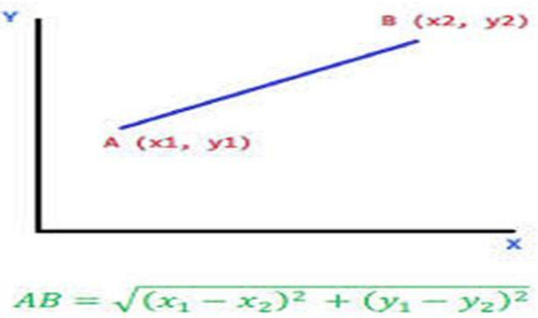

Figure 7: Co-ordinates assignment for node in wireless environment

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 6, Issue 1, January 2017

Then the node is in the path of bellman ford algorithm. This satisfies that the node m1 is in the radius of communication of the ingress router with minimum cost.

4. RESULTS AND DISCUSSIONS

In this section we present the evaluation of proposed system. After describing our experimental setup, we quantitatively evaluate the detection rate and the true positives for experiment. We have also measured the packet loss ratio, overhead of backup paths and delay in the MPLS network.

4.1 Experimental setup:

We run our experiments in network simulator version 3 (ns3) that has shown to produce realistic results. ns3 simulator runs deployable C++ or python code, but here use C++ code. In our simulations, we use MPLS label switching router for communication. For detection of failed link use protocol called AODV(Ad-hoc On Demand Distance Vector) routing protocol. Here we install ns3.19 version for compatibility with MPLS on Ubuntu. MPLS act as connection oriented so it works like TCP protocol which is as transport layer protocol. For packet capturing of each node can be analyzed with wires-hark. There is another tool for ns3 simulation analysis called Trace Metric. This trace metric can be used for analysis of number of packet sent, received, dropped, etc. This Trace Metric can also be calculating the throughput of the network. The trace file is generated when the net-animation run and pcap i.e. packet captured files also generated with NetAnim.

4.2 Topologies for Experimentation:

We have considered there topologies of nodes as shown in Figure 8.1, 8.2, respectively. The placement of node are random in wireless network, but here we consider the set of node into clusters of nodes and then number of cluster make a sector of cluster. The group of five node called a cluster, each cluster maintain a cluster head for cluster level communication.

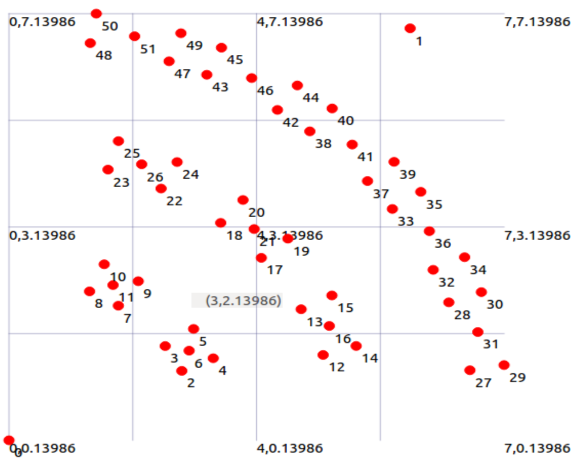

Figure 8: Network design for LSR nodes in MANET environment

Topology is adjusted such that each node should be in the range of at least one other node, such that tree structure formed and network partition should not be there.

The network design of proposed work is shown in Figure 8 and it defines the how the nodes are arranged in MANET environment with clustered form and also clusters are

The Figure 9 defines that how the packet is switching from source node to destination node and also the co-ordinates are assigned to the nodes (LSR) in the MANET environment. The packets are routed from source to destination with MPLS Fast re-route mechanism and bellman ford algorithm. This routing of packets is done with minimum link cost of network is selected

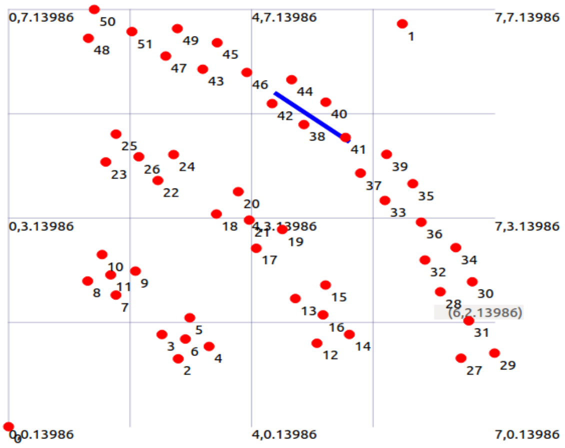

Figure 9: Network design while packet switching between LSR

The Figure 10 define the network design with co-ordinates assignment to the nodes (LSR) in the MANET environment. In each LSR is assigned with IP addresses and MAC addresses. This co-ordinate assignment is for shortest link calculation with the help of bellman ford algorithm. The packets are also routed based on the link cost which is calculated through co-ordinates

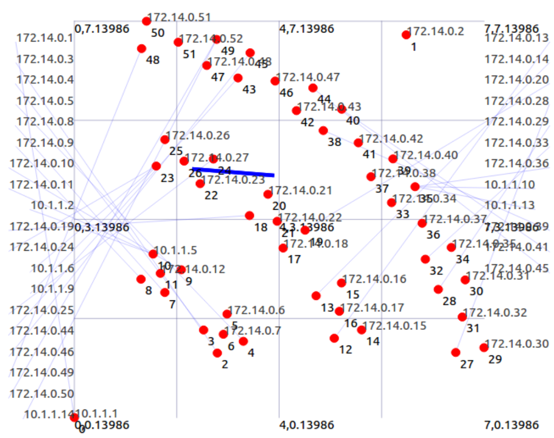

Figure 10: Network design with IP address assignment to LSR with packet switching

IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 6, Issue 1, January 2017

4.3 Calculation of Quality of Service (QoS) parameters:
MPLS Fast Re-Route mechanism considered performance parameters such as resource requirement, fault recovery time, packet loss ratio, packet re-ordering, complexity, distance between two routers, packet switchover time. This proposed work design with simulation tool such as Network Simulator version 3 (ns3).

4.3.1 Delay:
The delay is main parameter which will affect on quality of service of network. There are four types of delays to be considered such as:

1. Propagation delay:
The time taken by a packet to reach it its destination is called propagation delay and propagation delay (PD) calculated as

PD= d/v

Where:-d= distance between two LSRs
v= velocity or speed of packet travel through a LSP

2. Transmission Delay:
The time taken a packet to load from queue to link to forward with available bandwidth is called as transmission delay. The transmission delay (TD) is calculated as
TD= P/B
Where:-P= packet size
B= LSP Bandwidth (peak rate)

3. Queuing Delay: The queuing delay is the time taken by packet to move into a router or node queue and it is negligible so that not consider this delay.

4. Processing Delay:
The time taken by packet to move from queue to next router address finding. The Round Trip Time (RTT) is total time taken by a packet to reach its original source.
The Round Trip Time (RTT) for MPLS FRR mechanism is calculated based on transmission delay queuing delay and propagation delay in the network. The queuing delay is negligible so it does not consider. The round trip time (RTT) or link delay can be calculated as

RTT= QD+ 2PD+ TD

Where: - QD=Queuing Delay
PD=Propagation Delay
TD=transmission Delay

The full restoration time need to calculate and also buffer size is maintained at ingress LSR. After detection of failure, the total time required by LSR detecting the failure and switch-over all packets including buffered packets and time for tagged packet to return to the immediate upstream node must be calculate. This is equal to link delay for first packet switched over to reach the upstream LSR along the backward LSP in addition to RTT or link delay for tagged packet to return to its LSR and switchover time (Ts) is calculated as

Ts= 3*RTT

Where:-RTT= 2PD+ TD+ QD

This is done by assuming queuing delay and processing delay are negligible.

4.3.2 Packet Loss Ratio:
The another Quality of Service(QoS) parameter is packet loss ratio. This QoS parameter calculated based on number of packets sent and received.

Packet Loss Ratio (PLR)=Tr /Ts

Where Tr= Number of packet received,
Ts= Number of packet sent.

The fig 11 showing that traces metric used for analysis of packets flow from one LSR to another LSR. When failure occur in the network then there is much more packet loss, this can be reduced here with the help of FRR mechanism and bellman ford algorithm. The tracing of number of packet captured, number of packets received at destination, number of packets dropped done at trace metric. This trace file is generated when the net-animation run the code.

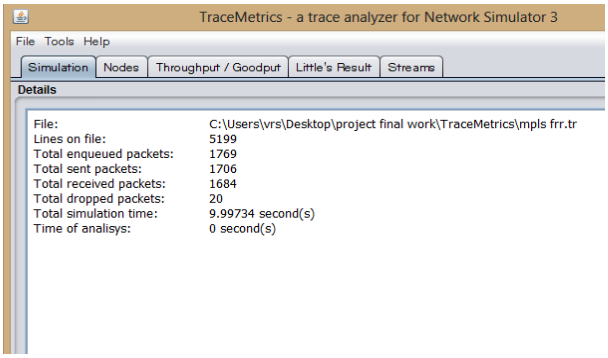

Figure 11: Trace Metric showing the packet loss during link failure in the network

The Figure 12 and 13 defines the each node capture how many packets, dropped packets and also sent packets from that node (LSR), this is shown in the trace metric tool. This if for captured packet analysis at each LSR in the MPLS network with Fast Re-route mechanism and bellman ford algorithm. The trace metric is ns3 analyzer for each nodes in the network.

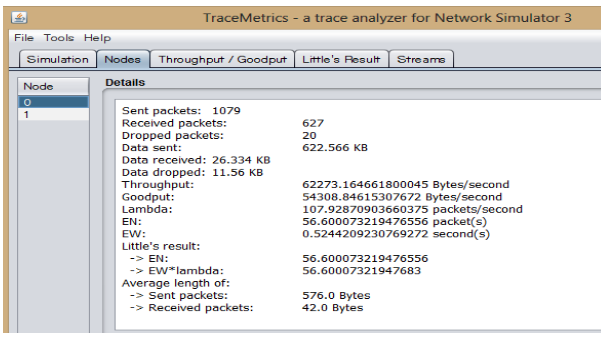

Figure 12: Number of packets sent, received and dropped at each LSR

IJARCCE
ISSN (Online) 2278-1021
ISSN (Print) 2319 5940
International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 6, Issue 1, January 2017

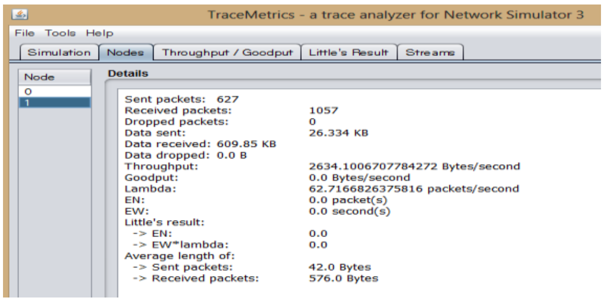

Figure 13: Number of packets sent, received and dropped at each LSR.

The packet loss ratio for different re-routing mechanism of PLS network are compared with graph. These methods such as Fast Re-route (FRR), Haskin's Method, Makam's proposal and Dynamic Re-routing. This is based on number of packet sent, received and dropped when there is link failure occur.

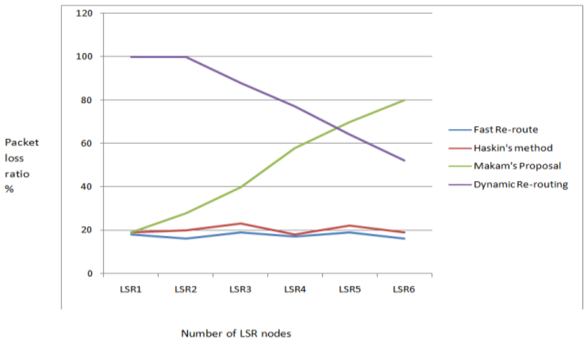

Figure 14: Packet Loss Ratio (PDR) of various re-routing methods

4.3.3 Throughput:

The throughput of the network depends upon various parameters. It varies with different Quality of Service (QoS) parameters. If the network contain more delay, packet loss ratio, jitter, overhead then the throughput of the network is degrades with this.

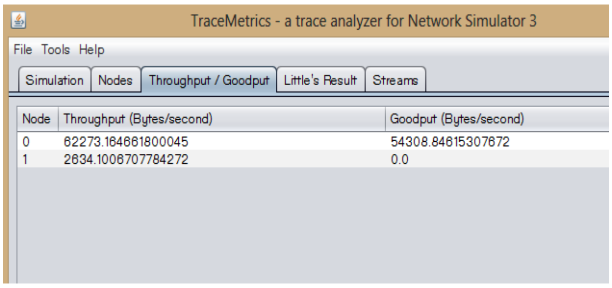

Figure 15: Throughput of network for each LSR

4.3.4 Overhead:

The overhead of the network need to consider as the numbers of edges are increased with this mechanism then there is much over-utilization of network. If there are k failures occur, then if there is no failure occur and use this mechanism then the edge utilization is 2 to the power of k times.

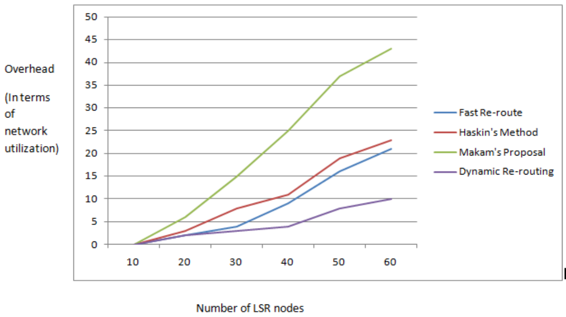

Figure 16: Overhead after failure not occur

5. CONCLUSION AND FUTURE WORK

CONCLUSIONS:-

Multi-protocol Label Switching (MPLS) is scalable network and act as backbone network for IP network. MPLS is implemented in Mobile Ad-hoc Network (MANET) so there is possibility of multiple link failure due to nodes can move at any point of time. These link failures are a common cause of network which degrades the performance of network. This link failure can cause more packet loss.

To avoid more packet loss due to link failure here proposes MPLS Fast Re-routing mechanism adopted as a solution for more packet loss due to link failure. Fast Re-routing depends on pre-planning and requires that a backup link or Label Switching Path to be establish. The MPLS FRR mechanism establishes backup link for failed link initially. This is for to reduce packet loss during finding alternative or backup link.

The FRR with bellman ford algorithm is useful for selecting a optimal backup link for packet switching of failed link. The bellman ford algorithm is used for finding a shortest path in network for packet forwarding to destination. This FRR with bellman ford algorithm used in wireless environment. This mechanism can be analyzed with the help of network simulator version 3 (ns3). The ns3 useful for analysis of various Quality of Service parameters such as delay, packet loss ratio, throughput, etc. The packet loss can be analyzed with the help of trace metric. The trace metric used for packet capturing analysis. The analysis of packet capturing can also be done with wire-shark. This analysis resulting less packet loss ratio and minimum delay in the network after link failure occur..

FUTURE WORK:-

This approach may further improved for other quality of service parameter such as packet disorder, jitter, bandwidth, etc. The Fast Re-Route mechanism can useful in future for improve the performance specially for load balancing of the network with the help of threshold method. The Reliable Fast Re-route(RFRR) mechanism is possible to used for to improve the performance of network.

IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 6, Issue 1, January 2017

REFERENCES

[1] Rakesh K. Sinha, Funda Ergun, Kostas N. Oikonomou, K. K. Ramakrishnan. "Network Design for Tolerating Multiple Link Failures Using Fast Re-Route (FRR)", In IEEE, 2014.

[2] Sasan Adibi. "MPLS IMPLEMENTATIONIN MOBILE AD-HOC NETWORKS (MANETs)." Ubiquitous Computing and Communication Journal, 2011.

[3] Chang Cao, George N. Rouskas, "Hybrid FRR/p-Cycle MPLS Link Protection Design", In IEEE Communications Society subject matter experts for publication in the IEEE Globecom , 2011.

[4] Suksant Sae Lor, Redouane Ali, Raul Landa, and Miguel Rio, "Recursive Loop- Free Alternates for Full Protection against Transient Link Failures", In, IEEE, 2010.

[5] Micha Piro, Artur Tomaszewski, Cezary Zukowski, David Hock, Matthias Hartman, Michael Menth, "Optimized IP-Based vs. Explicit Paths for One-to-One Backup in MPLS Fast Reroute.", In, IEEE, 14th International Telecommunications Network Strategy and Planning Symposium(NETWORKS 2010),Warsaw, Poland, sept 2010.

[6] Ajay Todimala, K. K. Ramakrishnan and Rakesh K. Sinha,"Crosslayer Reconfiguration for Surviving Multiple-link Failures in Backbone Networks ",In,IEEE,2009.

[7] Lemma Hundessa and Jordi Domingo-Pascual, "Reliable and Fast Rerouting Mechanism for a Protected Label Switched Path.", In Departament dArquitectura de Computadors Universitat Polit'ecnica de Catalunya (UPC) C/ Jordi Girona 1-3, 08034. Barcelona, Spain.

[8] Maria Hadjiona, Chryssis Georgiou and Vasos Vassiliou,"A Hybrid Fault- Tolerant Algorithm for MPLS Networks", In Department of Computer Science University of Cyprus.

[9] Cezary Zukowski, Artur Tomaszewski, Micha Piro, David Hock, Matthias Hartmann and Michael Menth, "Compact node-link formulations for the optimal single path MPLS Fast Reroute layout,", ADVANCES IN ELECTRONICS AND TELE COMMUNICATIONS, VOL. 2, NO. 3, SEPTEMBER 2011.

[10] D. Haskin and R. Krishnan, "A Method for Setting an Alternative Label Switched Paths to Handle Fast Reroute Work in progress, Internet draft ¡draft-haskin-mpls-fast-reroute-05.txt¿, November 2000.

[11] S. Makam, V. Sharma, K. Owens, and C. Huang, "Protection/Restoration of MPLS Networks", Work in progress, Internet draft ¡draft-makam-Mpls protection- 00.txt¿, October 1999.

[12] [Lemma Hundessa Gonfa, "ENHANCED FAST REROUTING MECHANISMS FOR PROTECTED TRAFFIC IN MPLS NETWORKS", UPC. Universitat Politecnica de Catalunya, 2011.

[13] Md. Arifur Rahman, Ahmedul Haque Kabir, K. A. M. Lutfullah, M. Zahedul Hassan, M. R. Amin, "Performance Analysis and the Study of the behavior of MPLS Protocols ",In Proceedings of the International Conference on Computer and Communication Engineering 2008.