Volume: 06 Issue: 06 Pages: 2529-2532 (2015) ISSN: 0975-0290

Performance Evaluation of Source Routing over MPLS Networks for Failure Detection and Recovery

AamaniNemtur, Mohamed El-Sharkawy and Maher Rizkalla
Electrical and Computer Engineering
Purdue School of Engineering and Technology
723 W Michigan St
Indianapolis, IN 46202, USA

---ABSTRACT---

Multi-Protocol Label Switching is an emerging technology which is the initial step for the forthcoming generation of Communication. It uses Labels in order to identify the packets unlike the conventional IP Routing Mechanism which uses the routing table at each router to route the packet. There exits certain methods which are used to recover the failure of any link and/or node failure in the given Network. It uses the techniques of FRR with the help of RSVP/CR-LDP to overcome the link and/or node failures in the network.

On the other hand there are certain limitations/Drawbacks of using the above mechanisms for Failure Detection and Recovery which are multiple protocols such as RSVP/CR-LDP over OSPF/IS-IS and complex algorithms to generate backup path since each router works individually in order to create a backup tunnel. So to overcome the listed limitations, this paper discusses a relatively new technique for MPLS Network which is Source Routing. Source Routing is the technique in which the source plays the role of directing the packet to the destination and no other router plays the role of routing the packet in the network. Using OPNET Modeler 17.5 tool for implementing source routing when there is a network failure is performed and the results are compared by implementing RSVP/CR-LDP over the same failed network.

Keywords: **Multi-Protocol Label Switching, IP Routing, OPNET, FRR and RSVP/CR-LDP.**

Date of Submission: April 29, 2015 Date of Acceptance: May 24, 2015

I. INTRODUCTION

Source Routing is a type of routing where sender of the packet determines the entire path through which the packet should travel to reach the destination. Source Routing is the replacement of the other signaling protocols like RSVP/CR-LDP in the case of failure detection and recovery. Source Routing mainly uses stack of labels and the important difference is to use a Domain Wide Label (DWL) for the communication. A Domain Wide FEC to bind a label is always desired. In Domain wide FEC to label binding, a label is always bound to the same FEC on all the network links. This label is generally called as Domain Wide Label. The difference between Local Label and Domain wide label is in the former one multiple FECs can map to a particular label on different links whereas in later same FECs map to the label on all the links.

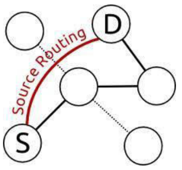


Fig. 1: Source Routing

DWL Allows a way to support Source Routed LSP in an LDP enabled network using stack of labels. The Source contains the entire stack of labels through which the packet should be passed through. Since the labels are constant throughout the network this routing is possible over MPLS Networks [2, 3, 4, 6 and 7] . Label Stack is updated based on the route the packet needs to travel and the path is computed at the source. So other LSRs does not push another label as in the other signaling protocols but just pop the label of its own from the label stack and forwards the packet with the remaining stack of labels.

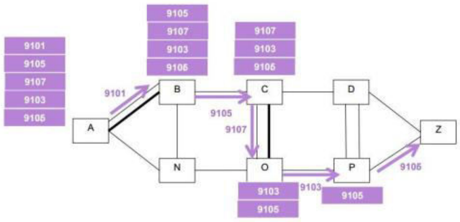


Fig. 2: Label Stack Mechanism in Source Routing.

1. Protection Lists:

It is the list of segments encoding the detour path from the protecting node S to the repair node R avoiding the link which is failed.

2. Protection Techniques for Link Failure using LFA:

If a path to a destination D from a neighbor N of S does not contain S (i.e. N is a loop-free alternate of S for the failure of link S-F), then S can pre-install a repair forwarding information to deviate the packet data to node N uponthe failure of S-E. In the case of LFA applicability, the protection list is empty. A protecting router S needs to send the protected packet as is to its LFA neighbor N.

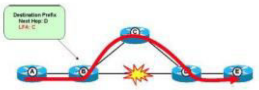


Fig. 3: LFA Mechanism in MPLS Network.

3. Protection Techniques for Link Failure using RLFA:

If there is no LFA neighbor which is not on the path of the failed link, then Source may create a virtual LFA by using a tunnel to carry the packet to a point in the network that is not a direct neighbor of S, and from which the packet will be delivered to the destination without looping back to S. The Remote LFA proposal [4] calls such a tunnel a repair tunnel. The tail-end of this tunnel (R) is called a ”remote LFA”.

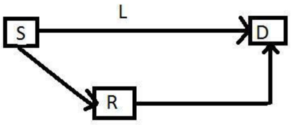


Fig. 4: RLFA Mechanism in MPLS Network.

The difference between LFA and RLFA is there will be some cases where the neighboring node may not be present to form a backup path as mentioned in the concept of LFA.In the below figure source s needs to send data to node d. Suppose there is a link failure between s-a. So the alternate path to reach node d is through node b. But because ECMP,node b tend to send date to node d again through the path b-s-a-d.So there occurs loss of data and results in performance degradation. In this case the importance virtual tunnel is realized where the virtual repair tunnel is created between node S to node e and from node e the data is flown to the destination d. In this case there is very less scope of loss of data in the network.

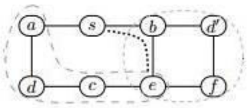


Fig. 5: Repair Tunnel in RLFA

4. Advantages of Source Routing:

Zero Signaling and Maintenance overhead: Since all the routing work is done at the source there is no signaling required and also no maintenance required in the network. Only the start end of the LSP needs to maintain the state. Other LSRs on the LSP are not even aware of the existence of such LSPs.

Zero Signaling Delay: In Source Routing LSPs are immediately used after the stack of labels is determined. It inherits the concept of make before break.

II. Proposed Work:

In this paper, the Implementation of MPLS Network with FRR Techniques with both RSVP and CR-LDP is presented for both node and link protection. In order to evaluate the network performance in the MPLS with node and link failure backup tunnels are to be pre-computed and they are maintained in order to use them during the network failures. Source Routing is implemented over the same network which issued to analyze the performance of RSVP and CR-LDP. Simulations are carried on by failing the link in one case and node in the second case. This performance is compared with the performance of the network with the RSVP and CR-LDP Signaling Protocols. All the Implementation is carried using Network Simulation tool OPNET Modeler 17.5 [5].

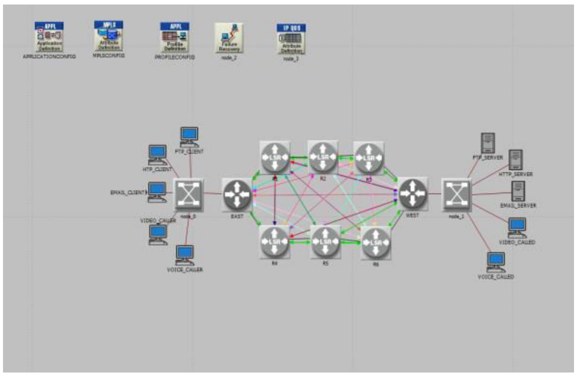


Fig. 6: OPNET Simulation Network.

III. SIMULATIONS:

The Network Simulation tool OPNET 17.5 Modeler is used to generate the results for the MPLS Based Network. OPNET provides several modules for the simulation comprising a vast collection of Network protocols and network elements. The main feature of OPNET is that it provides various real-life network configuration capabilities that make the simulation environment close to reality. The advantages of OPNET compared to other simulators include GUI interface, comprehensive library of network protocols and models, graphical interface to view the results, availability of documentation for the user to develop the network models etc. The Network used for the study has 6 LSRs and one Ingress and one Egress Router are setup and the source signal is obtained from one of the five workstations (voice, video, mail, HTTP, File) as mentioned in Figure 6.

In the above network implementation which is designed using OPNET Modeler there are in total 6 LSRs and 2 Switches and in the source side we have 5 Workstations. In the Receiver side there 2 receiving work stations and other 3 are servers.

In order to implement the MPLS Network first important thing to do is to create Dynamic LSPs across the MPLS Domain and setup the link parameters. The Signaling protocol RSVP-TE and CR-LDP is selected in the list of protocols listed in OPNET Modeler.

Link Failure Protection: In the network a particular link is forcibly made to fail and the option of failing that node for a particular time frame is provided by the tool. The network performance is been studied without deploying any repair mechanism after failing the node.

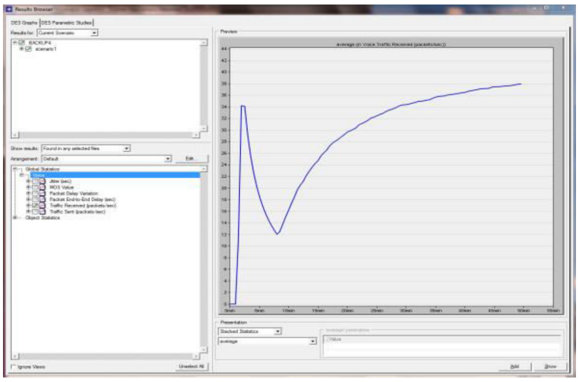

Results Browser
DES Graphs | DES Parametric Studies
Results for: Current Scenario
BACKUP4
scenario1
Show results: Found in any selected files
Arrangement: Default
Edit...
Global Statistics
Voice
Jitter (sec)
MOS Value
Packet Delay Variation
Packet End-to-End Delay (sec)
Traffic Received (packets/sec)
Traffic Sent (packets/sec)
Object Statistics
Preview
average (in Voice Traffic Received (packets/sec))
Presentation
Stacked Statistics
average
Ignore Views
Unselect All
Add
Show

Fig. 7: Traffic Received when no FRR.

The above graphs show the traffic received. If there is no repair technique deployed in the network there is a complete loss of data in the time frame in which link is made to fail.

If there is LFA Mechanism which is deployed in the network which uses the Source Routing then there will be not much disturbance in the traffic received even in the time frame in which the link is in fail state.

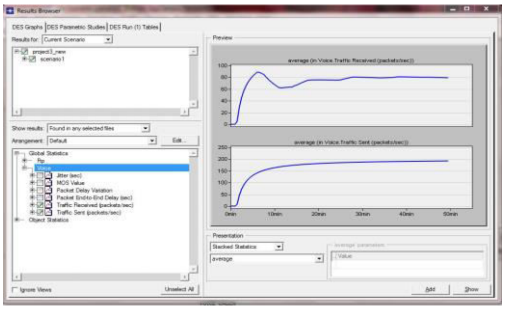

Results Browser
DES Graphs | DES Parametric Studies | DES Run (1) Tables
Results for: Current Scenario
project3_new
scenario1
Show results: Found in any selected files
Arrangement: Default
Edit...
Global Statistics
Ftp
Voice
Jitter (sec)
MOS Value
Packet Delay Variation
Packet End-to-End Delay (sec)
Traffic Received (packets/sec)
Traffic Sent (packets/sec)
Object Statistics
Preview
average (in Voice Traffic Received (packets/sec))
average (in Voice Traffic Sent (packets/sec))
0m
10m
20m
30m
40m
50m
Presentation
Stacked Statistics
average
Ignore Views
Unselect All
Add
Show

Fig. 8: Traffic Received when LFA is Implemented using Source Routing

If RLFA Mechanism is deployed in the network which uses the Source Routing then the traffic received has better performance which means the loss of data is less.

The comparison graph of the traffic received during the link fail in the network with RSVP, CR-LDP, LFA Source Routing, and RLFA Source Routing is as shown in Figure 10.

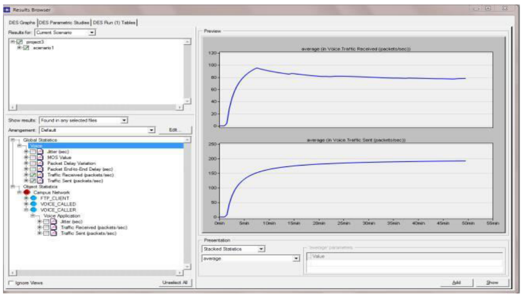

Results Browser
DES Graphs | DES Parametric Studies | DES Run (1) Tables
Results for: Current Scenario
project3
scenario1
Show results: Found in any selected files
Arrangement: Default
Global Statistics
Voice
Jitter (sec)
MOS Value
Packet Delay Variation
Packet End-to-End Delay (sec)
Traffic Received (packets/sec)
Traffic Sent (packets/sec)
Object Statistics
Campus Network
FTP_CLIENT
VOICE_CALLED
VOICE_CALLER
Voice Application
Preview
average (in Voice Traffic Received (packets/sec))
average (in Voice Traffic Sent (packets/sec))
Presentation
Stacked Statistics
average
Ignore Views
Unselect All
Add
Show

Fig. 9: Traffic Received when RLFA is Implemented using Source Routing.

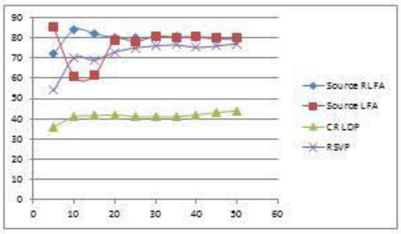


Fig. 10: Comparison of traffic Received in all 3 cases.

The Y-axis is the average packets received. The graph clearly shows that the performance of CR-LDP is very lessas compared to other 3 techniques. The difference in the packets received is mainly concentrated in the time frame of 5 to 10 sec where the link is made to fail. It shows that implementing RLFA Technique over the network which uses Source Routing has much better performance over RSVP and LFA Technique.

Voice Packet Delay Voice packet delay variation is the difference in end to end one way delay between selected packets in a flow with any lost packets being ignored. The Voice packet delay in case of Source Routing in the MPLS Network is shown below.

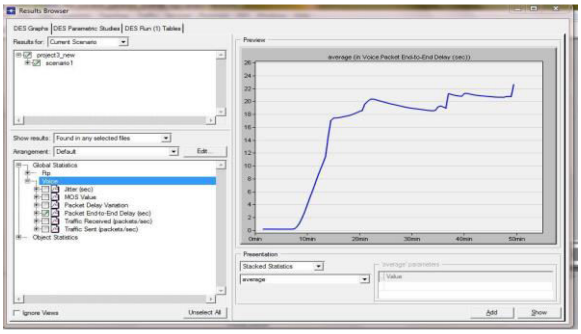

Results Browser
DES Graphs | DES Parametric Studies | DES Run (1) Tables
Results for: Current Scenario
project3_new
scenario1
Show results: Found in any selected files
Arrangement: Default
Edit...
Global Statistics
Ftp
Voice
Jitter (sec)
MOS Value
Packet Delay Variation
Packet End-to-End Delay (sec)
Traffic Received (packets/sec)
Traffic Sent (packets/sec)
Object Statistics
Preview
average (in Voice Packet End-to-End Delay (sec))
0m
10m
20m
30m
40m
50m
Presentation
Stacked Statistics
average
Ignore Views
Unselect All
Add
Show

Fig. 11: Voice Packet Delay in Source Routing.

The comparison graph of the Voice Packet Delay during the link fail in the network with RSVP, CR-LDP and Source Routing is as shown below:

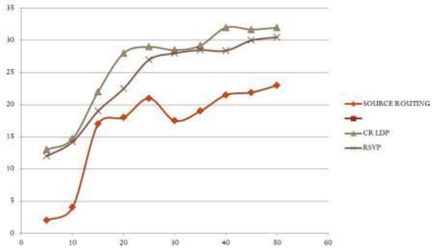
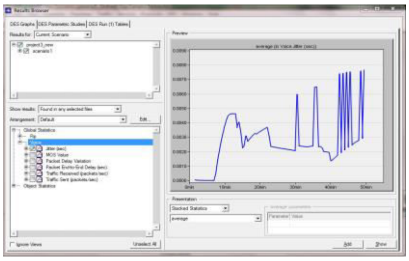


Fig. 12: Comparison of Voice Packet Delay in 3 cases.

The comparison graph clearly shows that the delay is much lower in the case of Source Routing because in the case of source routing the virtual tunnel is automatically created after the study of the network at the source. So the decision of creating the backup path at the point of failure delays the packet to reach the destination which happens in the case of RSVP and CR-LDP.

Voice Jitter: Jitter is the time variation between the packets that are arriving due to Route changes in the network, Congestion in the network and timing drift.



Results for: Current Scenario

Show results: Found in any selected files

Arrangement: Default

Stacked Statistics

average

Fig. 13: Voice Jitter in Source Routing.

The comparison graph of the Voice Jitter during the link fail in the network with RSVP, CR-LDP and Source Routing is as shown below.

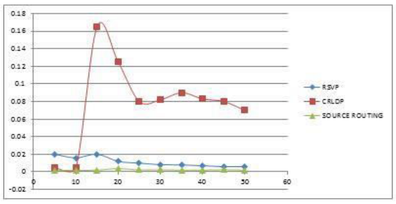


Fig. 14: Comparison of Voice Jitter in all 3 cases.

The above graph shows that the disturbance in the voice signal in the case of Source routing is much lower almost close to 0. The jitter is very high in case of CR-LDP Signaling Protocol. Since there is no congestion in the network during Source routing because of the virtual link created around PLR. This virtual link is pre-computed so the packet which needs to flow though the link which is failed automatically goes through the virtual repair tunnel instead of waiting for the tunnel creation with certain handshake signals like RESV and RESP messages in RSVP Protocol.

IV.CONCLUSION

This Paper explains about the MPLS Network and various repair mechanisms which are been used in order to enhance the network performance in conditions of network Failure in both RSVP and CR-LDP Signaling protocols over MPLS Network. Source Routing is implemented in the MPLS Network with LFA and RLFA Technique. All the performance metrics such as traffic received, Voice Packet Delay, Voice Jitter shows that RLFA Based Source Routing has best performance compared to Conventional RSVP and CR-LDP Signaling mechanisms.

References:

[1] Csikor, L. and Retvari, G.,"IP fast reroute with remote Loop-Free Alternates: The unit link cost case", 663-669, October, 1991.

[2] Yu Tao and Chen Shanzhi and Li Xin and Qin Zhen, "Increasing IP network survivability in harsh scenarios with dynamic source routing", 1-4, September, 2007.

[3] Rasiah, P. and Jong-Moon Chung, "Traffic engineering optimal routing for LSP setup in MPLS", III-272-III-275 vol.3, 2000.

[4] Jong-Moon Chung,"Analysis of MPLS traffic engineering", 550-553 vol.2, August, 2002.

[5] Chang, Xinjie, Network Simulations with OPNET, Phoenix, Arizona, USA.

[6] Y. Xiao, H. Jiang, B. Liu, Y. Li, and X. Li, "A novel failure detection mechanism for fault-tolerant MPLS network," in Advanced Computer Theory and Engineering(ICACTE), 3rd International Conference, vol. 1, pp. V1{168{V1{172, August2010.

[7] A. Bongale, N. Nithin, and L. Jyothi, \Tra_c prioritization in MPLS enabled OSPFnetwork," in World Congress on Information and Communication Technologies (WICT), pp. 132{137, October 2012.