IMPROVEMENT OF LINK FAILURE RESTORATION UTILISING MULTI-PROTOCOL LABEL SWITCHING (MPLS) AS A MEANS TO MAINTAIN QUALITY OF SERVICE (QOS)

M. Asante[1] and R. S. Sherratt[2]
[1]Department of Computer science,
Kwame Nkrumah University of Science and Technology, Kumasi, Ghana
[2]Signal Processing Laboratory, School of Systems Engineering,
The University of Reading, UK

ABSTRACT
This paper proposes a practical approach to the enhancement of Quality of Service (QoS) routing by means of providing alternative or repair paths in the event of a breakage of a working path. The proposed scheme guarantees that every Protected Node (PN) is connected to a multi-repair path such that no further failure or breakage of single or double repair paths can cause any simultaneous loss of connectivity between an ingress node and an egress node. Links to be protected in an MPLS network are predefined and a Label Switched path (LSP) request involves the establishment of a working path. The use of multi-protection paths permits the formation of numerous protection paths allowing greater flexibility. Our analysis examined several methods including single, double and multi-repair routes and the prioritization of signals along the protected paths to improve the Quality of Service (QoS), throughput, reduce the cost of the protection path placement, delay, congestion and collision. Results obtained indicated that creating multi-repair paths and prioritizing packets reduces delay and increases throughput in which case the delays at the ingress/egress LSPs were low compared to when the signals had not been classified. Therefore the proposed scheme provided a means to improve the QoS in path restoration in MPLS using available network resources. Prioritizing the packets in the data plane has revealed that the amount of traffic transmitted using a medium and low priority Label Switch Paths (LSPs) does not have any impact on the explicit rate of the high priority LSP in which case the problem of a knock-on effect is eliminated.

Keywords: *Convergence, QoS, Repair paths, MPLS, Routing*

INTRODUCTION

The design of a network involves the initial consideration of several factors including load, bandwidth and traffic characteristics. However network conditions change with time due to the addition of new requests, amount of data packets traversing along the links and topological changes in which case the QoS of a network must be maintained for reliability. The transmission of voice, video and data has brought about the need for convergence which must be fully exploited. Convergence switching is the merger of packet switching technology with telephony signalling and call-processing intelli-

gence, allowing carriers to consolidate typically separate voice, video, data and overlay networks and provide new and differentiated integrated communication services. Convergence technologies are changing the way carriers transmit traditional voice and data traffic. Businesses today demands reliable and scalable networks that reach anywhere and deliver guaranteed performance at an affordable cost. An architecture involving Multi-Protocol Label Switching (MPLS) allows network service providers to create Virtual Private Networks (VPNs) that offer flexibility of Mobile Internet Protocol (MOIP) and the Quality of Service (QoS) of Asynchronous Transmission Medium (ATM). MOIP enables users to keep the same IP address regardless of its location in which case data packets can be re-routed if the user moves to a different position on the Internet. In the traditional way, IP tunneling is the method used by Home Agents (HAs) to transmit packets that are meant for a Mobile Node (MN). This method appears to be inefficient especially if more that one MN from the same HA but attached to different foreign networks are all transmitting or receiving signals and also if a breakage occurs in the links. MPLS provides the traffic engineering tools that service providers need to deliver quality voice, video and data services to a static node and also to a roaming MN. However short comings such as delay and the breakage of the links connecting the LSP and nodes need to be looked at. The impact of transport path failures is mitigated by using multilayer protection/rerouting schemes such as Synchronous Optical Network (SONET)/ *Synchronous digital hierarchy* (SDH) and emerging MPLS-based methods such as Fast Re-Route (FRR). MPLS-based recovery can provide much finer granularity and presents an efficient, attractive and complementary alternative to SONET/SDH-based protection. The creation of repair paths which will switch over traffic from a broken working path to an alternative path will go a long way to enhance the QoS in data transmissions using MPLS (*Luc De Ghein, 2007, Asante and Sherratt, 2004, Elwalid et al, 2001*)) . Quality of Service (QoS) routing schemes use specific capabilities of MPLS network but then major MPLS QoS routing schemes use ingress-egress node knowledge. If sufficient bandwidth is not available to set up both the working and recovery paths, the request is rejected. In order to increase throughput and to prevent packet loss, delay, congestion and collision due to interference from remote/local signals, a multi-repair path should be provided at all nodes. The prioritization of the signals and the setting up of prioritized routes will also enhance the transfer of signals on a multi-repair path. Setting up protection against only single and double link/ node failures is considered and the corresponding analysis using multi-link node is also considered in this paper. In our case we assume the bandwidth and packet size to be uniform throughout. The effect of delay due to interfering signals on LSPs and Nodes are also analyzed. A simulation framework to verify the effectiveness of this approach is carried out and the results are presented in the last section.

ROUTING INFORMATION

The basic information needed by any routing protocol to make appropriate path selection decisions is the state of the network. Every routing protocol uses this information to forward packets. The information about the state of the network includes the network topology along with resource availability for QoS purposes. Each change in the state of the network should be detected and disseminated to all the routers in the same Autonomous System (AS) and also propagated across AS boundaries until all ASs have been informed of this change. The main cause for state change is resource availability variation in the network since topology variations are less frequent *(Rekhter and Aggarwal, 2007)*. The large amount of information exchange for state update can compromise the scalability of the routing schemes. To reduce this amount, two approaches are possible: reducing either the frequency of updates or the details in the updates. The former is achieved by using various mechanisms such as class-based, threshold-based, and periodic updates.

The latter is achieved by aggregating the network state information. In the case of MPLS networks, a centralized network manager can also be used for network operation, in which case the problem of information dissemination becomes redundant (*Rahman et al 2008 , El-walid et al 2001,* Kalyanaraman et al 2000).

ROUTING ALGORITHMS

Routing algorithms can be categorized into *static* or *dynamic* depending on the type of routing information used for computing LSP routes. Static algorithms only use existing network information; dynamic algorithms use the current state of the network, such as link load, number of local or remote nodes transmitting to the network and blocking probability. Routing algorithms can be executed either *online* (on demand) or *offline* depending on the situation. Path requests are attended to one by one in online transmissions but route computation of a new path is not allowed on offline routing.

The main goal of a routing algorithm is to find a feasible path (a path with enough bandwidth) that achieves efficient resource utilization (*Porwal et al, 2008., Evans and Filsfils, 2007).* In addition, repair paths or routes selected by using QoS routing must have sufficient resources for the requested QoS requirements taking into consideration, delay, congestion and throughput *(Pham and Lavery 2002*). Two situations are considered in this work, the first of which is to select the path with the minimum hop count among all feasible paths; if more than one path is eligible, the one with Maximum Reservable Bandwidth (MRB) which is the minimum of the available bandwidth of all links on the path is selected.

BACK-UP REPAIR SCENARIO

Global Repair Model

In this model, the protection is activated by ingress node irrespective of where the failure path occurs and it is responsible for resolving the restoration as the Fault Indication Signal (FIS) arrives. This method involves an alternate disjoint backup path for each active path. Therefore a failed signal has to be propagated all the way back to the source node before a protection switch is activated. Fault indication can only be activated as a result of failure of a path continuity test if no reverse LSP is created. Figure1 illustrates a network formed by seven Label Switch Routers (LSRs) where a working path (shortest possible path) from LSP1 to LSP3 is R1-R2 and a Global Recovery Path (GRP = R8-R4-R3 and R7-R6-R5-R3 are pre-established. In a normal operation, traffic from ingress router LSR1 to egress router LSR3 is carried through the best possible path. In the event of a link failure (e.g. between LSR2 and LSR3), traffic is switched to the LSP Recovery Path (RP). This means ingress node (LSR1) must be a Protection Switch Label (PSL) which is a transmitter for both the working path (WP) traffic and its corresponding backup path traffic and should be able to switch the traffic between the working path and the recovery path. A PSL is the origin of the backup, but does not necessarily have to be an ingress node which means for effective backup path creation, all nodes needs to be configured as a PSL within an MPLS. A critical node receives both working path traffic and its corresponding backup path traffic, and merges their traffic into a single outgoing path.

The critical node is the destination of the recovery path, but may or may not be the destination of the working path. This method can only set up one backup path per working path which means in the event of a break or a failure in this path, no signals can be retransmitted which is a disadvantage. Signals transmitted through this method are likely to experience greater delay, congestion and collisions due to interference from remote or other internal signals.

Local Repair

Similarly a local repair path serves as an alternative path for the working path against a link or node failure. In the local repair method, the restoration procedure simply starts from the point of failure. The protection is activated by an LSR. When a link failure occurs at R2 in Figure 1, LSR2 switches traffic from broken segment R2 to a R1. From Figure1, if link R2

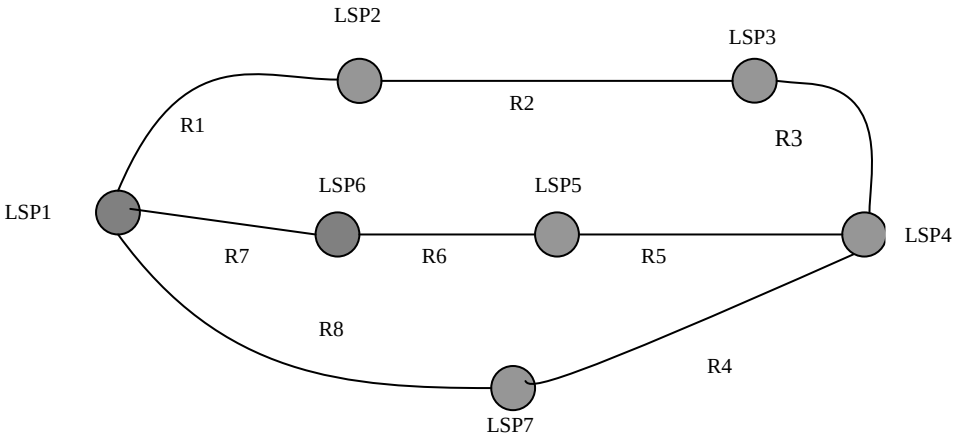

Fig. 1: Repair model and LSP backup utilization (*designed by authors*)

fails, the repair path would be R1-R3, R1-R6-R5, R1-R5-R3 for signals from LSP1 to LSP4. Therefore, traffic can be forwarded through path (R6, R5, and R3). The main advantage is that the distance of traverse by signals is less and therefore offers transparency to the ingress node and faster restoration time than global mechanisms but if the repair path is single then it becomes a disadvantage in case the link breaks up again. On the other hand if the node that links the local LSP happens to be a critical path then packets will experience delay, congestion, collisions and a reduced throughput therefore creating multi repair LSPs based on the shortest possible path approach at a minimal interference will be more advantageous.

Reverse Backup

This method can reverse traffic at the point of failure of the protected LSP back to the source switch (ingress node) via a reverse backup LSP. When a failure along the protected path is detected, the LSR at the head of the failed link reroutes incoming traffic by redirecting this traffic into the alternative LSP traversing the path in the opposite direction to the ingress node of the LSP. As illustrated in Figure 1, LSP working and recovery paths are established as in the global model; and in addition, there is a reverse recovery path (RRP =R1-R2-R1-R7-R6-R5-R3) that routes back to the ingress node. When a link failure is detected in link (R2), the traffic is switched back to LSR1 (ingress node) through the reverse backup LSP, and then carried through the LSP recovery path as in the global model. A disadvantage of the reverse backup could be poor resource utilization as signals travel back to ingress router before onward transmission to the destination. Further failure of this path will also terminate packet transfer and also time is wasted in sending the reverse fault indication back to the ingress router (*Akar et al, 2003; Bartos and Raman,2001).*.

Multi-level backup repair

In the development of path/breakage repair a multilevel protection is proposed. In order to achieve different protection levels, several protections paths are maintained depending on the link resources and type of traffic. The application of multi-level protection link failure methods could improve performance over single and double link failures as it provides flexibility. One advantage of using multilevel protection approach to a link failure repair is when a network involving several thousand nodes experience several link failures, several alternative routes becomes available.

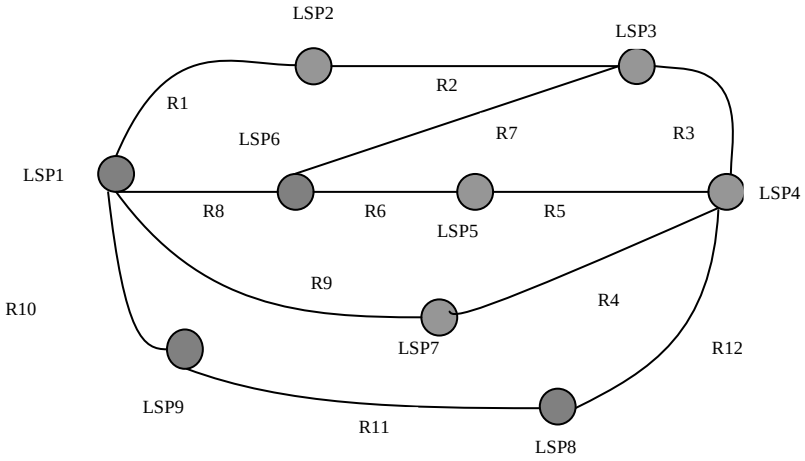

Fig. 2: Multi-repair path (*designed by authors*)

As illustrated in Figure 2, in the Working Path (WP) R8-R6-R5, if the link R6 fails, any of the routes R8-R1-R2 and R1-R9 can be used or a local repair route R8-R9 can be used. If the link R8 also fails, the LRP R1- R2-R3, R9- R4, R10 -R11-R12 can be used thus increasing flexibility and throughput (*Dongmei and Guangzhi 2008., Kodialam and Lakshman 2000; Marzo et al 2003, Nelakuditi et al , 2002).*

METHODOLOGY

In order to investigate the effectiveness of the multi-path LSP at the ingress/egress levels, we have configured a network similar to the one used in Figure 2. The aim was to analyze the effectiveness of the usage of link repair paths. We used an event-driven packet based Network simulator called Prophesy. The simulator allows topology specification and the simulation of movement of traffic. The distances in-between LSPs/nodes were assumed to be equal. The delays along the various links within the network whenever a failure occurs were determined.

RESULTS AND DISCUSSION

Upon execution, the delay generated by packets traversing from the ingress LSR to the egress LSR along several selected routes were recorded and the delay on repair routes due to the diversion of packet movement from all failure repair paths were also measured. Our investigation revealed that an unknown number of remote nodes may interfere with signals towards the ingress/egress LSP or node especially when wireless is the medium of transmission. In this situation the configuration of only a single or double repair path is ineffective. Interference will still pose a threat to the QoS to the transmitted signals therefore as an extension to our simulation; the packets were further classified into grades or in order of priority. The first one being the High priority LSP (H-LSP) for voice, the second being Medium priority LSP (M-LSP) for video and the third being the Low priority LSP (L-LSP) for Data, were established between each IP router pair located at the edge of an MPLS cloud. Once such an assignment for a new flow is made, all packets of the same flow are forwarded using the same LSP (high, medium or low) in case of a failure along a working path. We propose that each switch in MPLS runs a separate instance of an Available Bit Rate (ABR) control algorithm. This algorithm rounds for the high, medium and low classes while also providing explicit rate information back to source for every LSP using that interface. Each IP router at the edge of the MPLS cloud maintains three queues (high, medium and low queues) per destination.

The mean delays due to the movement of prioritized and non prioritized packets along the routes R7-R6-R5 and all other routes with a single/double link failure and without failure were measured and compared with that of multiple link failure in the same manner. Results are illustrated in Figure 3.

Similar comparisons were made for prioritized and non-prioritized packets movement along all the routes with the provision of single/double repair paths and a multiple repair path and the results were illustrated in Figure 4.

It can be inferred from the two figures that creating multi-repair paths and prioritizing packets reduces delay and increases throughput as illustrated in Figure 4. In this case the delays at the ingress/egress LSPs were low compared to when the signals had not been classified.

We also found out from our analysis that there will still be some setbacks when transmitting Voice, Video and Data as the quality of service will be compromised in the case of voice when the delay at the ingress/egress LSPs/Node is high as a result of interference from numerous remote signals.

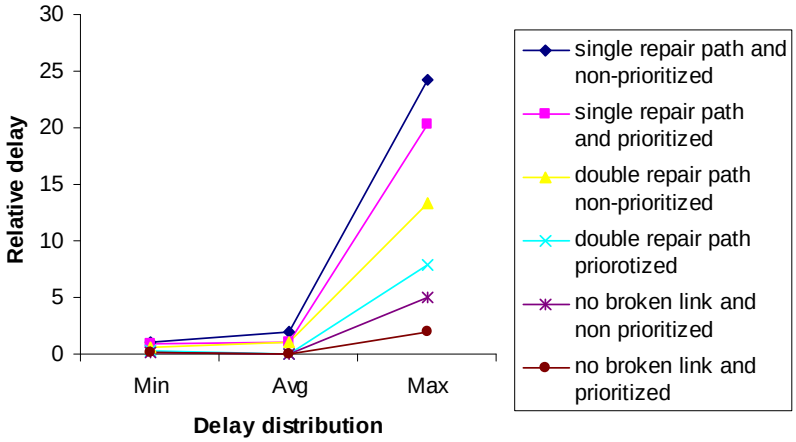

Fig. 3: Delays resulting from single and double link failures on a single and double repair path

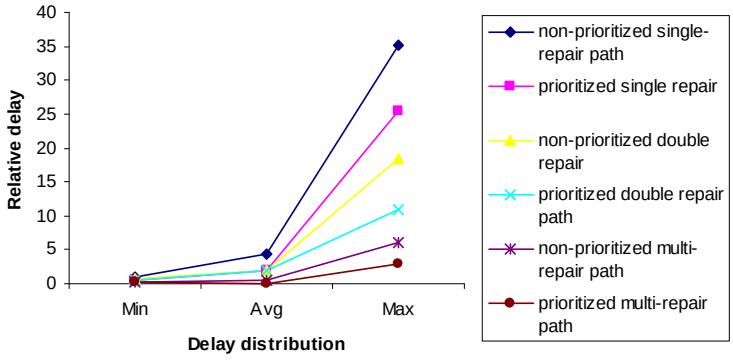

Fig. 4: Delays resulting from Multiple link failures on a multi-link repair path

CONCLUSION

This paper has analyzed a scheme to restore broken links in an MPLS network. The proposed scheme considers provision of multi-paths from an ingress LSP/Router to the egress LSP/Router as a means to increase throughput, reduce interference, delay congestion and collision in case of failure. Protection using multiple paths allows greater flexibility.

Simulation results show that the proposed scheme provides a means to improve the QoS in path restoration in MPLS using available network resources. Prioritization of packets in the data plane as proposed in the paper ensures that the amount of traffic transmitted using a medium and low priority LSPs does not have any impact on the explicit rate of the high priority LSP in which case the problem of a knock -on effect is eliminated.

Mobile Nodes mainly utilizes wireless links to connect to a foreign network when away from home and since wireless is vulnerable to attacks such as eavesdropping, man-in-the middle attacks, manipulation attacks, Address Resolution Protocol poisoning, denial-of-service attacks, reliable authentication and encryption methods should be used by all networks using reliable firewalls as well. Defensive techniques such as data encryption, authentication, packet filtering, intrusion detection and intrusion prevention methods must be included in network designs to avoid unnecessary breakages and disruptions.

REFERENCE

Akar; N., Atik, M. and Karasan, E.,(2003)"A Re-ordering-free Multi-path Traffic Engineering Architecture for Diffserv MPLS Networks", 3rd IEEE Workshop on IP Operations and Management, 1-3 Oct. 2003, pp. 107-113

Asante, M., Sherratt, R.S.,(2004)"Convergent Mobile Internet Protocol in Multi-Protocol Label Switching (MPLS) Architecture", 5th Annual Postgraduate Symposium on The Convergence of Telecommunications Networking & broadcasting. Liverpool John Moores University, U.K, 28-29 June 2004, pp. 188-191

Bartos, R. and Raman, M.,(2001) "A Heuristic Approach to Service Restoration in MPLS Networks" IEEE International Conference on Communications, 2001, 11-14 June 2001, Vol.1, pp. 117-121

Dongmei Wang., Guangzhi Li (2008) **"**Efficient Distributed Bandwidth Management for MPLS Fast Reroute**"** Dongmei Wang; Guangzhi Li; Networking, IEEE/ ACM Transactions ,April 2008 Volume 16, Issue 2, Page(s):486 - 495

Elwalid, A., Jin, C., Low, S. and Widjaja, L., (2001) "MATE: MPLS adaptive traffic engineering", 20th Annual Joint Conference of the IEEE Computer and Communications Societies, 2001, pp. 1300-1309

Evans, J., Filsfils, C (2007) "Deploying IP and MPLS QoS for Multiservice Networks: Theory and Practice" (Morgan Kaufmann, 2007, ISBN 0-12-370549-5)

Kalyanaraman,S., Jain, R., Fahmy, S; Goyal, R., and Vanderlove, B., (2000) "The ERICA switch Algorithm for ABR traffic management in ATM networks", IEEE/ ACM Transactions on Networking, 2000, Vol.8, no.1, pp.87-89

Kodialam, M., Lakshman, T.V., (2002) "Minimum Interference Routing with application to MPLS traffic Engineering,", 19th Annual Joint Conference of the IEEE Computer and Communications Societies, 2002, Tel-Aviv, Israel, March 2002, Vol. 2, pp. 884-893

Luc De Ghein.,(2007) **"**MPLS Fundamentals: Forwarding Labeled Packets" www. *Cisco Press.com*. pp. 249–326. Jan 5, 2007.

Marzo, J.L., Calle, E. and Anjali, T., (2003) "Adding QoS Protection in order to Enhance MPLS QoS Routing" IEEE International Conference on Communications, 2003, 11-15 May 2003, Vol. 3, pp. 1973-1977

Nelakuditi, S., Zhang, Z. L. and Tsang, R. P., (2002) "Adaptive Proportional Routing: A localized QoS routing approach.", IEEE/ ACM Transactions on Networking, Vol.10, Issue 6, Dec. 2002, pp. 790-804

Pham, H. and Lavery, B., (2002) "New Dynamic Link Weight Algorithm for Online Calculation of LSPs in MPLS Networks", 8th IEEE International Conference on Communication Systems, 2002. 25-28 Nov. 2002, Vol.1, pp. 117-121

Porwal, M.K., Yadav, A., Charhate, S.V ., (2008) **"**Traffic Analysis of MPLS and Non MPLS Network including MPLS Signaling Protocols and Traffic Distribution in OSPF and MPLS"Emerging Trends in Engineering and Technology, 2008. ICETET '08. First International Conference 16-18 July 2008 Page(s):187 - 192

Rahman, M.A., Kabir, A.H., Lutfullah, K.A.M., Hassan, M.Z., Amin, M.R., (2008) "Performance analysis and the study of the behavior of MPLS protocols**"** Computer and Communication Engineering, 2008. ICCCE 2008. International Conference, 13 -15 May 2008 Page(s):226 – 229

Rekhter ,Y., Aggarwal, R,(2007) "Graceful Restart Mechanism for Border Gateway Protocol with MPLS" RFC4781, January 2007