Available online at www.sciencedirect.com

SCIENCE DIRECT®

Computer Communications 29 (2006) 402–408

computer communications

www.elsevier.com/locate/comcom

Economical protection in MPLS networks

Ajay Pal Singh Virk*, Raouf Boutaba

School of Computer Science, University of Waterloo, Waterloo, ON, Canada N2L 3G1

Received 1 September 2004; revised 27 September 2004; accepted 29 September 2004
Available online 2 November 2004

Abstract

The growth of Multi-Protocol Label Switching (MPLS) as the emerging choice for provisioning and managing core networks has placed significant emphasis on MPLS based recovery mechanisms. The present global protection frameworks require extensive involvement of Label Switching Routers (LSRs) in the protection framework. The LSRs are involved in failure propagation and maintenance of information regarding upstream neighbors. This extensive involvement of the LSRs in the protection frameworks may become a scalability issue particularly in case of complex MPLS networks as a single failure may affect many Label Switched Paths (LSPs) and Path Switch LSRs (PSLs). The restoration time in the present frameworks is dependant on the length of the working path. This dependence leads to an increase in the number of PSLs required for effective protection, which thereby increases resource usage. The present frameworks also do not monitor the PSL or the backup path for fault notification—a feature that is important to ensure reliable protection frameworks.

We propose an economical global protection framework that is designed to provide minimal involvement of intermediate LSRs, reduction in the number of PSLs, fast and cost-effective fault notification, and cost-effective fault monitoring of even the PSLs and recovery paths.

Keywords: MPLS; Network survivability; Directory-enabled networks; LDAP; Network reliability

1. Introduction

Multi-Protocol Label Switching (MPLS) [10] is growing in popularity as the approach to provision and manage core networks. MPLS effectively superimposes a connection-oriented framework over the connection-less IP network to provide effective resource reservation and pre-determination of routes. It provides the integration of label switching forwarding paradigm and network layer routing. This integration provides virtual links or tunnels through the core network. MPLS promotes implementation of advanced features such as Quality-of-Service (QoS) and traffic engineering in an effective manner [18].

MPLS involves assignment of labels to packets. A label is an identifier that is used to identify the stream or the Forwarding Equivalence Class that the packet has been assigned. The label is assigned upon entry to the MPLS network. The label is used at each hop to determine the next hop and also the new label which replaces the old label. The routers that support MPLS are known as Label Switching Routers (LSR). The path traversed by a packet by virtue of series of label switching operations is known as Label Switched Path (LSP). The LSRs use the Label Distribution Protocol [19] to establish the LSPs.

The rapid increase in network traffic coupled with the emergence of MPLS as a popular choice for provisioning and managing core networks has motivated the idea of MPLS based recovery mechanisms. The increase in high priority and mission critical traffic has made network reliability and survivability very important issues. Network reliability can be supported at different protocol layers. However, MPLS has emerged as the optimum layer to provide survivability for the core networks. This choice is motivated by the fact that MPLS based recovery mechanisms can provide effective protection for the entire network compared to the link and physical restoration schemes such as those in SONET/SDH.

The importance of MPLS based recovery is also emphasized by the fact that there are inherent limitations associated with current routing algorithms regarding

* Corresponding author.
E-mail addresses: apsvirk@bbcr.uwaterloo.ca (A.P.S. Virk), rboutaba@bbcr.uwaterloo.ca (R. Boutaba).

0140-3664/$ - see front matter © 2004 Published by Elsevier B.V.
doi:10.1016/j.comcom.2004.09.014

recovery time. The current routing algorithms have the advantage of being robust and survivable. However, they can involve significant amount of recovery time to recover from a failure. The improved protection can be provided by augmenting current routing algorithms with MPLS based recovery mechanisms. MPLS involves usage of pre-established label-switched paths (LSPs) to transport data traffic. The pre-establishment of working LSPs potentially allows MPLS networks to pre-establish protection or backup LSPs for the working LSPs. This approach allows significant improvement in the protection switching time compared to legacy IP networks.

This article proposes a framework that aims to provide economical protection in MPLS networks. The proposed framework utilizes a directory service [7,15] and programmable network mechanism to provide MPLS protection. This is the first global protection framework in which the restoration time is independent of the length of the working path. The proposed framework allows the protected working path to be significantly larger than that allowed by the present global protection frameworks. This positive feature in turn reduces the number of PSLs (Path Switch LSRs) required to provide global protection (PSLs are the LSRs that switch the traffic from the working path to the backup path in the case of a failure). The PSLs need to maintain information about the working and backup LSPs and also need to perform the switchover of traffic. The decrease in the number of PSLs required for protection improves resource utilization and provides an economical approach for path protection.

Present global protection mechanisms are also based on the extensive involvement of LSRs in maintenance of information regarding upstream neighbors and failure propagation. The failure notification is propagated along the intermediate LSRs to the PSL. The message processing at each hop adds delay to the failure notification. The involvement of intermediate LSRs may be even more significant in case of complex and large-scale networks. This extensive involvement of LSRs in the protection framework may become a scalability issue in complex MPLS networks as a failure may affect multiple LSPs and multiple PSLs may have to be notified about the failure. This is the first framework that aims to reduce the extensive involvement of LSRs in MPLS based recovery. This feature thus promotes improved utilization of network resources and contributes to the proposed economical framework for MPLS protection.

The proposed framework also has the major advantage of scaling effectively to all LSPs affected by a failure, even in the case of complex and large-scale MPLS networks. The proposed framework is also the first approach to propose effective fault detection and fault notification on the backup path, which is very important to provide reliable MPLS path protection. The present global protection frameworks also lack the feature to monitor the PSLs for any failure. Our approach allows effective monitoring of even the PSLs. In case a PSL is affected by a failure, an alert could be generated and sent to the network administrator. The usage of a directory server in the proposed protection framework allows effective protection across multiple domains, which is a major advantage over other global protection mechanisms. This paper is organized as follows: Section 2 provides an overview of MPLS based recovery. Section 3 provides a survey of MPLS global protection frameworks. The proposed framework for global protection is described in Section 4. Finally, the implementation and simulation results are described in Section 5.

2. MPLS based recovery

Survivability mechanisms are available at different layers such as Synchronous Digital Hierarchy (SDH)/Synchronous Optical Network (SONET), ATM, Optical Transport Network, and MPLS. The recovery mechanisms at the lower layers have fast recovery operations. However, MPLS based recovery mechanisms promote QoS granularity by providing survivability at the network level. MPLS based protection allows the flexibility to choose the granularity at which the traffic is to be protected and also to choose the type of traffic that require protection. MPLS based protection is able to increase network reliability by enabling faster response to failures than is possible with the IP layer alone.

The MPLS based recovery mechanisms can be classified as local protection or global protection [20]. The local protection is performed in a distributed manner and the aim is to protect against a neighboring link or node failure. The local protection mechanisms involve significant backup path computations and management tasks in order to protect the entire MPLS path. This drawback may be more severe in case of complex MPLS networks.

The global protection is performed in a centralized manner and the aim is to protect against any link or node failure on the entire path or on a segment of the path. In case of global protection, the Path Switch LSR (PSL) switches the traffic from the failed working path to the backup path. However, the PSL is not usually adjacent to the point of failure. The global protection mechanisms require the fault notification to be propagated to the PSL in order for the PSL to perform the switch over to the backup path.

The traffic on the working path is switched over to the backup path upon a failure on the working path. However, when the failure on the working path is repaired, the traffic may be switched over back to the working path. This switchover is known as restoration. The restoration may be automatic or manual or may not be performed.

MPLS protection may be pre-negotiated or dynamic. The pre-negotiated approach involves pre-established backup paths and is fast and costly. The dynamic protection does not reserve resources. The dynamic protection improves resource utilization at the cost of recovery time.

3. Survey on MPLS global protection frameworks

The MPLS global protection frameworks have been proposed in various research works [1–4]. The protection framework in Ref. [1] involves setting up a protection domain. The protection domain consists of the Path Switch LSR (PSL), Path Merge LSR (PML), and the nodes between the PSL and PML on the working and recovery path. The PSL is the LSR that performs the switchover to the recovery path when the failure occurs. The PML is the LSR where the working path traffic and recovery path traffic converge. When a link or node fails, the LSR that is immediately upstream of the point of failure detects the failure. The LSR that detects the failure transmits a Fault Indication Signal (FIS) to its upstream neighbor. The upstream LSR upon receiving the FIS extracts information from the FIS to check whether it is the PSL for that fault notification. In case the LSR is not the PSL, then the LSR consults its cross connect table to determine the identity of the upstream LSRs that are effected by the failure. The LSR then transmits the FIS to the upstream LSRs. This process continues till the FIS reaches all the PSLs that are effected by the failure. The PSL upon receiving the FIS terminates the FIS and performs the switch over of the data traffic from the working path to the recovery path.

The framework proposed in Ref. [1] is depicted in Fig. 1. The working path in this case is PSL–LSR1–LSR2–LSR3–PML. The recovery path or backup path is PSL–LSR11–LSR12–LSR13–PML. Let us suppose that LSR3 fails. In such a scenario this failure would be detected by LSR2, which would send a FIS to LSR1. LSR1 would send the FIS to the PSL. The PSL upon receiving the FIS would switch over the traffic from the working path to the recovery path. When the failed link or node has been repaired, the upstream LSR, i.e. LSR2 may initiate a Fault Recovery Signal (FRS) to the PSL through the intermediate LSRs. The PSL upon receiving the FRS may switch the traffic back to the working path.

The global protection framework proposed in Ref. [2] involves transmission of the Fault Indication Signal from the PML to the PSL. The LSR that is downstream of the point of failure sends a FIS to the PML. The PML then sends the FIS along with a reroute request to the PSL along the backup path. The PSL upon receiving the FIS performs the switch over of the data traffic from the failed working path to the recovery path. At the same time the LSR that is upstream of the point of failure sets up a temporary LSP to the PML with the intention of reducing packet loss.

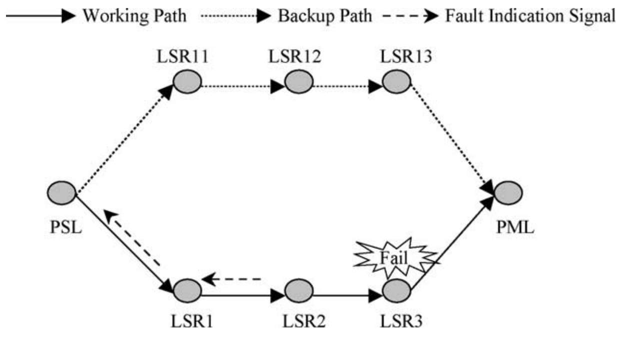

Fig. 1. MPLS global protection framework.

The MPLS global protection proposed in Ref. [3] tries to optimize the protection framework by considering the link usage during backup path selection. Normally the backup LSP is selected once during the backup LSP setup period. This approach [3] on the contrary exchanges network status information among the LSRs so that the backup path selection can be done using up-to-date network information. The aim is to select the optimal backup path considering the present network state. Whenever a LSR receives routing update information, the node updates its recovery path (if one exists) in order to maintain the most recent optimal recovery path. The intermediate LSRs calculate recovery paths between each LSR and its adjacent downstream LSR. When a failure occurs the LSR that detects the failure checks whether there is a recovery path across the point of failure. In case there is no such recovery path across the point of failure then the LSR propagates the Fault Indication Signal upstream towards the PSL.

The global protection framework proposed in Ref. [4] aims to reduce the switch over time required to switch the traffic to the backup path. This framework uses a LSP for fault notification. This LSP is known as Notify Reverse LSP. The Notify Reverse LSP is set up in a direction opposite to that of the working LSP. The use of a Notification LSP specifically for fault notification promotes fast fault notification, which facilitates a faster switch over to the recovery path in case of a failure.

The protection framework proposed in Ref. [5] is not exactly a global protection framework. The nodes on the working path have protection paths that connect the nodes to the egress router of the protected working path. This approach follows a two step protection mechanism. First, a local decision is made by the nodes that are adjacent to the failed link, to switch all the traffic from the failed link over to the protection paths. Simultaneously, the Fault Indication Signal (FIS) is transmitted to inform upstream nodes of the failure. When the upstream nodes receive the FIS, they stop transmitting on the working path and switch the transmission to the protection path that connects these nodes with the egress node. Though this framework is not a global protection framework, it has a feature that is similar to the global protection frameworks—the transmission of the Fault Indication Signal to the upstream nodes.

The restoration time in the global protection frameworks [1–4] described in this section depends upon the length of the working path. This dependence requires the working paths to be smaller in length thereby increasing the number of PSLs required to provide effective protection. These frameworks also require extensive involvement of the intermediate LSRs between the PSL and PML in the protection process. These frameworks also do not monitor the PSL or the backup path for failure. The framework proposed in Ref. [5] also depends upon extensive involvement of intermediate LSRs in the fault notification process. The architecture proposed in Ref. [4] requires a notification LSP for each protected working LSP. This requirement may lead to scalability problems, particularly in cases involving complex and large-scale networks.

We propose a MPLS global protection framework that aims to provide an economical protection model with reduced number of PSLs and cost-effective fault notification with minimal involvement of intermediate LSRS in the protection process. This framework is also ideal to monitor the PSLs and backup paths for failure and also to provide effective protection across different domains.

4. Proposed MPLS global protection framework

This article proposes a framework that uses a directory service to provide a MPLS based recovery framework. The directory service is a service that provides access to the directory. The directory is a logically centralized and physically distributed database that is designed to provide fast lookup of information. The information is maintained in the directory in a hierarchical manner involving parent–child relationships. The Lightweight Directory Access Protocol (LDAP) is the present standard protocol to provide access to the directory [7].

The fundamental purpose of the directory is to provide a common, unifying repository that can be employed to effectively store and share data among multiple applications [15,16]. The MPLS routers (LSRs) also function as LDAP clients, which is required in order for the LSRs to access the directory. Fig. 2 depicts the proposed global protection framework.

The directory is used to maintain information about the operational state of the LSRs on the working and the recovery path. The operational state information refers to information regarding whether the LSRs have been effected by a link or node failure. In case there is any change in the operational information, then the related PSLs that have registered for change notification at the directory server are notified about the latest operational information. The PSLs upon receiving the change notification are able to initiate recovery or restoration procedures.

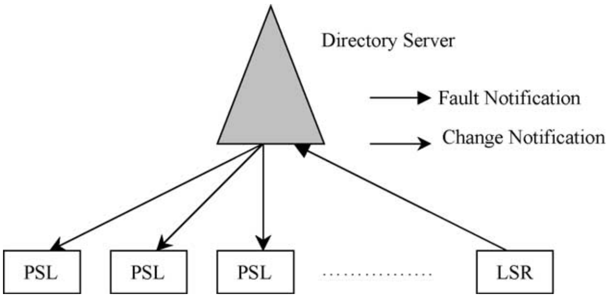

Fig. 2. Proposed MPLS global protection framework.

Our approach provides dynamic notification of changes in the directory to the LSRs. The Lightweight Directory Access Protocol (LDAP) has the important feature of providing mechanisms for enhancing the base set of services offered by LDAP. An LDAP extended operation is a mechanism that allows for new LDAP operations to be defined to enhance the base set of LDAP operations. We have developed LDAP extensions that are able to implement change registration and change notification mechanisms in order to provide dynamic notification related to changes at the directory server.

The PSLs use the change registration mechanism to register for change notification at the directory server. The PSLs as part of the change registration request specify the directory entries that need to be monitored. The directory server maintains a list of all valid registration requests and monitors the Directory Information Tree (DIT) for any change related to the registration requests. If any change made to the DIT matches the criteria specified by a change registration request, then the PSL associated with that change request is notified about that change using the change notification operation. The changes made to the DIT in this case are pertaining to the operational state of the LSRs on the working and recovery path. The directory is ideally suited for information exchange across multiple domains. This information exchange is done through data replication across multiple directory servers. The usage of the directory in the proposed framework allows effective protection across several domains.

The directory entries associated with the proposed framework can be implemented in a very simple manner. Each LSR is associated with a directory entry that has a related boolean attribute. The boolean attribute specifies the operational state of the LSRs—a negative value signifies that the LSR has been effected by a link or node failure. The PSLs register for change notification related to all the LSRs on their working and recovery path. If the value of the boolean attribute changes, the directory server notifies the PSL(s) which can then initiate appropriate actions such as switch over to the backup path in case of failure or switch over to the working path in case of restoration.

Let us consider the protection scenario described in Fig. 1. The directory entries are depicted in Fig. 3. The PSL will register for change notification related to LSR1, LSR2, and LSR3. When the working path is active, the values associated with LSR1, LSR2, and LSR3 will be true. Let us assume that LSR3 fails. LSR2 will update the DIT and set the value associated with LSR3 to false (the value of 0 refers to false and the value of 1 refers to true). The directory server will immediately send a notification to the PSL in order for the PSL to initiate switchover to the backup path. When the fault is repaired, LSR2 will again set the value associated with LSR3 to true. The directory server will again send a notification to the PSL which then initiates

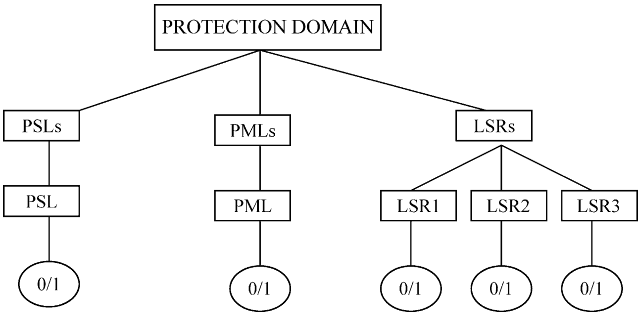

Fig. 3. Directory hierarchy for protection framework.

switchover to the original working path. In a similar manner, the LSRs on the backup path, i.e. LSR11, LSR12, and LSR13 may be monitored for fault notification so that in case of any failure, the PSL may select a new backup path. The network administrator may register for change notification related to the PSLs and PMLs as these special cases may require monitoring.

This framework promotes fast and cost-effective (in terms of resource usage) fault notification. The involvement of intermediate LSRs is significantly reduced, as the LSRs only need to notify the directory server, which further notifies the concerned PSLs. This framework is also able to effectively monitor the PSLs, PMLs, and the backup path in a resource effective manner.

The functional architecture for the proposed global protection framework is depicted in Fig. 4. The directory server includes the functionality to implement the change registration and change notification mechanisms. The following units are implemented in the LSR—the LDAP client, notification unit, and the Local Decision Point (LDP). The LDAP client allows the PSL to register for change notification and receive the change notifications. The LDAP client allows the LSRs to update the directory server with regards to any failure. When a LSR detects a failure, it updates the DIT regarding that failure. The directory server checks whether the update to the DIT matches the criteria specified by any change registration request. If the match is successful, then the directory server notifies the related PSL(s) about the update using the change notification mechanism.

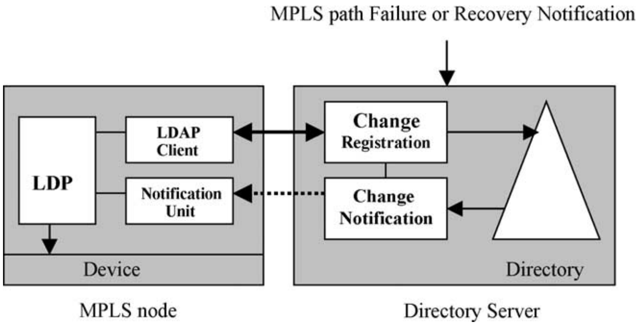

Fig. 4. Functional architecture of proposed MPLS global protection framework.

The change notification extended operation may be implemented using two different models—push model or pull model. In case of the pull model, the directory server notifies the notification unit of the PSL(s) about the related changes. The notification unit informs the LDAP client, which in turn establishes an LDAP session with the directory server and retrieves the changed MPLS path information. The LDAP client transfers the changed configuration information to the LDP. In case of the push model of change notification, the directory server provides the notification unit with the changed MPLS path information, which in turn passes the information to the LDP. The push model has the advantage of reducing the response time to changes in the operational state of the MPLS path, as it does not involve the LDAP connection setup and data request associated with the pull model.

The LDP acts as the interface to the PSL. The LDP uses network programming [11] to initiate the path protection and restoration procedures. The standard network programming interfaces such as IEEE P1520 APIs can be used for this purpose [12,13]. The notification messages may be transmitted using any suitable data communications protocol. The LDAPv3 protocol provides means to implement secure transfer of information between the LDAP server and the LDAP client [14]. In order to make the proposed framework effective, the notification messages should be transmitted as high priority messages.

The restoration process may be followed in case the failed link or failed node has been restored. The MPLS node that detects the link or node restoration notifies the directory server, which in turn notifies the related PSL(s). The PSL(s) may initiate the restoration process (i.e. switchover from the backup path to the working path) upon receiving the recovery notification. The process of self-protection and self-restoration is repeated by the PSL(s) whenever there is a related change on the working or recovery path. Our framework can also be used in case of local protection mechanisms that involve a pre-negotiated recovery path. The LSR that performs the switchover of MPLS traffic across the failed link or node can use the proposed architecture to monitor any failures on the pre-negotiated recovery path.

The usage of directory for storage of routing data and dynamically changing information might raise concerns. However, the proposed framework does not involve storing routing data or dynamically changing information. The proposed framework involves directory entries that are boolean attributes associated with the LSRs. These attributes specify whether a LSR has been effected by a node or link failure. It is not expected that the core MPLS routers and links will be failing on a frequent basis. This fact should allay any concerns related to the usage of directory in our framework. Besides the directory is based on the principle of logical centralization and physical distribution. This effective information replication across multiple directory servers ensures that there is no central point of failure. It is also important to note that the directory operations are typically performed in the range of 8 ms [17]. This operational information regarding the directory server allows our framework to provide fast protection switching and should also allay any processing concerns related to the directory operations.

5. Implementation and performance comparison

The prototype of the proposed framework was built using a runtime environment that supports the implementation of customized software services on network devices. The runtime environment provides the substrate to support secure downloading, installation, and safe execution of services [8] The services which run locally on the network devices, include monitoring, routing, diagnostic, or other user specified functions.

The LSRs download a self-contained downloadable unit to configure the services required as part of the protection framework. The unit installs the following services on the LSR—LDAP client, notification unit, and LDP. The authors have developed change registration and change notification mechanisms, which are LDAP extensions, in a cost-effective manner. These LDAP extensions along with the prototype details have been described in detail in Ref. [9]. We have extended the functionality of the directory server with two server plug-ins, providing the pre-operation and post-operation functions. The directory server, at start-up, loads the server plug-ins and appropriately accesses the plug-in functions during the processing of LDAP operations. The pre-operation function allows the PSL to register for a change notification. The post-operation function allows the directory server to notify or send the configuration data to the notification unit of the PSL(s).

The proposed framework has been compared with the Makam approach [1,6] using a simulation environment. We have used the MPLS Network Simulator [6], which is an extension of the Network Simulator (NS) to perform the simulation. The following environment was used to compare our framework with the Makam approach. The working path consists of 20 LSRs. The links between the LSRs have a capacity of 1 Mb. The LSRs have a failure alarm that is executed at an interval of 0.01 s. The purpose of this alarm is to test the downstream LSR for link or node failures. The packet size used was 200 bytes and the packets were transmitted at a constant bit rate of 1 Mb/s. The directory server was simulated by creating a link between each node on the working path and a node that represented the directory server. The propagation delay for all links in the simulation was assumed to be 10 ms. The directory operations can be typically performed in the range of 8 ms [17].

We performed the simulation assuming a link failure at each link on the working path. The packets received at the PML were monitored to determine the packet loss in both frameworks. Whenever a link failure took place, it was detected by the upstream LSR with the help of the failure alarm. The LSR upon detecting the failure connects to the directory server, which sends a notification to the PSL. When the PSL receives the notification, it switches the traffic to the backup path.

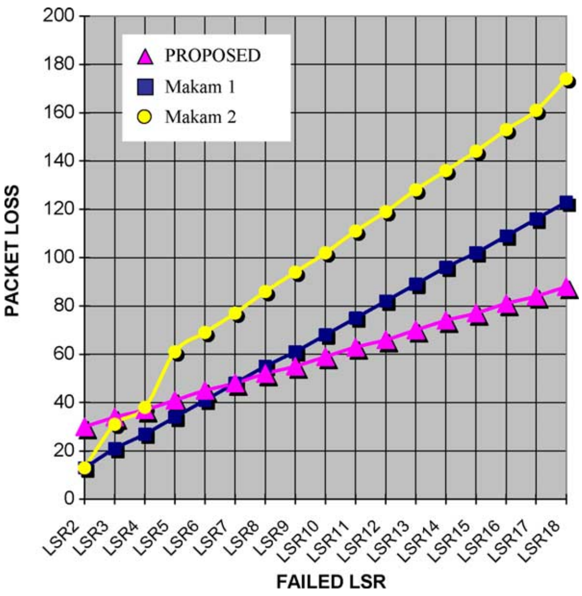

Fig. 5. Performance comparison.

The simulation results comparing the packet loss between our framework and the Makam framework are shown in Fig. 5. Makam 1 and Makam 2 both refer to the Makam framework (Makam 2 refers to the Makam framework with increased traffic between the intermediate LSRs). The advantage of our proposed framework is that it has a reduced packet loss as the size of the LSP increases. This allows us to have larger LSPs, which reduces the number of required PSLs thereby improving resource usage. Besides, our framework is very economical as the intermediate LSRs have minimal involvement in the protection framework compared to other frameworks. The proposed framework promotes cost-effective fault notification and does not propagate fault notification across the entire network. In case of increased traffic between the intermediate LSRs, our approach outperformed the Makam framework. The frameworks were also compared for packet reordering. However, the packet reordering was found to be negligible and constant in case of both the frameworks.

Our framework can be improved significantly by implementing LSPs between the LSRs and the directory server. The implementation of LSPs between the LSRs and the directory server would promote very fast fault notification and thereby would lead to reduced packet loss and larger protected LSPs. This step would at the same time not raise any scalability concerns as only one LSP would be required per LSR as compared to [4] which requires a reverse LSP for every protected working LSP. We plan to implement this feature as part of our future work.

It is important to note that the fault notification in the proposed framework may not essentially be faster than the other approaches in all scenarios. In fact as shown in Fig. 5, the fault notification of the proposed framework is slower than the Makam approach when the failed LSRs are relatively closer to the PSL.

In general, there may be scenarios in which the fault notification of the proposed framework is slower than the other approaches. However, it is also important to consider the numerous advantages associated with the proposed framework. The proposed framework has several advantages such as minimal involvement of intermediate LSRs, cost-effective fault notification and cost-effective fault monitoring of even the PSLs and the recovery paths and these features are absent in the other global protection frameworks. In brief, the several advantages associated with the proposed framework outweigh any probable minor delays in the fault notification.

6. Conclusion

In this article we have proposed an economical MPLS global protection framework. This framework is the first framework that reduces the extensive involvement of intermediate LSRs in the global MPLS protection process. The proposed framework promotes improved utilization of network resources, as it greatly reduces the involvement of LSRs in MPLS protection. The substantial reduction in the involvement of intermediate LSRs provides an economical approach for protection in MPLS networks.

The proposed framework also has the major advantage of scaling effectively to all LSPs affected by a failure, even in cases of complex and large-scale MPLS networks as there is minimal involvement of the intermediate LSRs in the protection process. In summary, the proposed framework promotes effective global MPLS protection by introducing several features that are absent in contemporary global protection frameworks such as minimal involvement of intermediate LSRs, cost-effective fault notification and cost-effective fault monitoring of even the PSLs and the recovery paths.

References

[1] H. Changcheng, V. Sharma, K. Owens, S. Makam, Building reliable MPLS networks using a path protection mechanism, IEEE Communications Magazine 40 (3) (2002).

[2] S.K. Das, P. Venkataram, A method of designing a path restoration scheme for MPLS based network, Fifth IEEE International Conference on High Speed Networks and Multimedia Communications, 2002.

[3] Y. Sangsik, L. Hyunseok, C. Deokjai, K. Youngcheol, L. Gueesang, M. Lee, An efficient recovery mechanism for MPLS-based protection LSP, Joint Fourth IEEE International Conference on ATM (ICATM 2001) and High Speed Intelligent Internet Symposium, 2001.

[4] V. Suraev, Global path recovery enhancement using Notify Reverse LSP, IETF Internet Draft, work in progress, April 2001.

[5] R. Bartos, M. Raman, A. Gandhi, New approaches to service restoration in MPLS-based networks, EUROCON'2001 (International Conference on Trends in Communications), 2001.

[6] G. Ahn, W. Chun, Simulator for MPLS path restoration and performance evaluation, Joint Fourth IEEE International Conference on ATM and High Speed Intelligent Internet Symposium, 2001.

[7] J. Hodges, R. Morgan, Lightweight directory access protocol (v3): technical specification, IETF RFC 3377 September (2002).

[8] R. Jaeger, R. Duncan, F. Travostino, T. Lavian, J. Hollingsworth, Dynamic Classification in Silicon-Based Forwarding Engine Environments, IEEE LAN/MAN Workshop, Australia, 1999.

[9] R. Boutaba, S. Omari, A.P. Virk, SELFCON-an architecture for self-configuration of networks, Journal of Communications and Networks 3 (4) (2001).

[10] E. Rosen, A. Viswanathan, R. Callon, Multiprotocol label switching architecture, IETF RFC 3031 January (2001).

[11] D. Tennenhouse, J. Smith, W. Sincoskie, D. Wheatherall, G. Minden, A survey of active network research, IEEE Communications Magazine 35 (1) (1997).

[12] Programming Interfaces for IP Networks, White Paper IEEE P1520/TS/IP001.

[13] Programming Interfaces for IP Routers and Switches, an Architectural Framework Document, IEEE P1520/TS/IP003.

[14] M. Wahl, H. Alvestrand, J. Hodges, R. Morgan, Authentication methods for LDAP, IETF RFC 2829 May (2000).

[15] J. Strassner, Directory Enabled Networks, Macmillan, 1999.

[16] DMTF Directory Enabled Networks (DEN) Initiative, http://www.dmtf.org/.

[17] X. Wang, H. Schulzrinne, D. Kandlur, D. Verma, Measurement and analysis of LDAP performance, ACM SIGMETRICS International Conference on Measurement and Modeling of Computer Systems, 2000.

[18] D. Awduche, J. Malcolm, J. Agogbua, M. O'Dell, J. McManus, Requirements for traffic engineering over MPLS, IETF RFC 2702 September (1999).

[19] L. Andersson, P. Doolan, N. Feldman, A. Fredette, B. Thomas, LDP specification, IETF RFC 3036 January (2001).

[20] V. Sharma, F. Hellstrand, Framework for multi-protocol label switching (MPLS)-based recovery, IETF RFC 3469 February (2003).